Stockholms läns sjukvårdsområde
Sjukvårdsdirektören

BESLUTSUNDERLAG
2021-09-28

SLSO 2021-2620
RS 2021-0750

Yttrande över Remiss – Sveriges säkerhet - behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)

Nämnden för Stockholms läns sjukvårdsområde (SLSO) har av Rotel I Finans-, fastighets- och serviceroteln getts möjlighet att avge yttrande över Remiss – Sveriges säkerhet - behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63).

Ärendet

Utredningen överlämnade sitt delbetänkande *Kompletterande bestämmelser till EU:s cybersäkerhetsakt* (SOU 2020:25) i september 2020. Regeringen har efter remissbehandling av utredningens delbetänkande överlämnat proposition 2020/21:186 *Kompletterande bestämmelser till EU:s cybersäkerhetsakt* till riksdagen och i den lämnat förslag på en ny lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt. I den föreslagna lagen finns kompletterande nationella bestämmelser om bl.a. nationell myndighet för cybersäkerhetscertifiering, tillsyn, sanktioner och förfarandet vid cybersäkerhetscertifiering.

Riksdagen har den 9 juni 2021 beslutat i enlighet med vad som föreslås i angivna proposition och fattat beslut om att lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt ska träda i kraft den 28 juni 2021.

Regeringen tillsatte aktuell utredning eftersom man bedömde att det fanns anledning att överväga om ytterligare nationella krav bör införas för att säkerställa att nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet uppfyller de krav som behövs för att upprätthålla skyddet av sådana verksamheter. Utredningen visar sammantaget att det finns allvarliga brister i informations- och cybersäkerheten hos myndigheter vars verksamhet har betydelse för Sveriges säkerhet. Utredningen kommer därför med ett antal förslag för att åtgärda dessa brister.

Utredningen föreslår att Försvarets materielverk (FMV) får i uppdrag att, i samråd och samverkan med bl.a. de myndigheter som ingår i det nationella cybersäkerhetscentret, utveckla formerna för hur gemensamt framtagna hot-, sårbarhets- och riskbedömningar samt skyddsprofiler kan tas fram till stöd för kravställning på produkter, tjänster och processer avseende informations- och kommunikationsteknik (IKT) som ska användas i nätverks- och informationssystem i säkerhetskänslig verksamhet.

Utredningen föreslår också att Myndigheten för samhällsskydd och beredskap (MSB) inom ramen för sitt befintliga bemyndigande i föreskrifter

ska ange krav på att statliga myndigheter använder certifierade IKT-produkter, -tjänster och -processer i nätverks- och informationssystem.

Mot bakgrund av de allvarliga brister i informations- och cybersäkerheten som framkommer av offentliga utredningar och myndighetsrapporter föreslår utredningen ett antal åtgärder som berör driftsättning och väsentlig förändring av informationssystem i säkerhetskänslig verksamhet.

Åtgärderna som föreslås är i huvudsak följande.

- Säkerhetsskyddsförordningens bestämmelser om förberedande åtgärder inför driftsättning av informationssystem ska överföras till säkerhetsskyddslagen.
- Befintligt krav på verksamhetsutövare att göra en särskild säkerhetsskyddsbedömning utvidgas till att även omfatta planerade väsentliga förändringar av informationssystem som kan ha betydelse för säkerhetskänslig verksamhet.
- Verksamhetsutövare ska pröva lämpligheten av en planerad driftsättning eller väsentlig förändring av informationssystem som har betydelse för säkerhetskänslig verksamhet. Om lämplighetsprövningen leder till bedömningen att det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt ska det inte inledas.
- Lämplighetsprövningen ska, liksom den särskilda säkerhetsskyddsbedömningen, dokumenteras.
- I fall verksamhetsutövarens lämplighetsprövning leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt ska verksamhetsutövaren – om övriga rekvisit för samråd är uppfyllda – samråda med samrådsmyndigheten (Säkerhetspolisen eller Försvarsmakten).
- Verksamhetsutövares skyldighet att, inför driftsättning eller väsentlig förändring av vissa informationssystem, samråda med Säkerhetspolisen eller Försvarsmakten ska inte begränsas till att ske i form av en skriftlig process.
- Säkerhetspolisen och Försvarsmakten ska, i egenskap av samrådsmyndigheter enligt säkerhetsskyddslagen, få inleda samråd och inom ramen för ett samråd besluta åtgärdsföreläggande mot verksamhetsutövaren att vidta en säkerhetsskyddsåtgärd i berört informationssystem.
- Samrådsmyndigheterna ska även få möjlighet att förbjuda en ur säkerhetsskyddssynpunkt olämplig driftsättning eller förändring av informationssystem och besluta sanktionsavgift mot den som åsidosätter samrådsskyldigheten eller agerar i strid med meddelat förbud.
- Tillsynsmyndigheterna får en ny undersökningsbefogenhet genom möjligheten att, vid äventyr av vite, få tillgång till verksamhetsutövares informationssystem.

Förvaltningens motivering och yttrande
Förvaltningens bedömning är att utredningen och de föreslagna åtgärderna innebär att staten tar ett större samlat ansvar för att säkerställa hög säkerhet och enhetlighet avseende system som har betydelse för Sveriges säkerhet. Förslagen har goda förutsättningar att motverka de brister som har identifierats avseende informations- och cybersäkerhet och skapa en högre säkerhet i system som har betydelse för Sveriges säkerhet. Vidare innebär kravet på samråd med Säkerhetspolisen eller Försvarsmakten ett bra stöd för de myndigheter som är i färd med att driftsätta eller förändra ett system som träffas av bestämmelserna.

För SLSO:s del bedöms förslagen vara av begränsad betydelse. Anledningen till detta är att de system SLSO använder i allmänhet inte kan anses ha betydelse för Sveriges säkerhet. Bedömningen är dock att de förslag som utredningen presenterar är mycket bra och skulle innebära en trygghet och säkerhet i arbetet med att driftsätta ett system som är av betydelse för Sveriges säkerhet.

För Region Stockholms del kan det framförallt vara SL som berörs av regleringen eftersom verksamhet som avser kommunikationer nämns som exempel på verksamhet som kan ha betydelse för rikets säkerhet. Möjligtvis om SLSO i framtiden får ansvaret för alla IT-system inom Region Stockholms hälso- och sjukvård kan det komma att ha relevans.

Stockholms läns sjukvårdsområde följer de av regionfullmäktige beslutade styrande dokumenten: Riktlinjer för informationssäkerhet (LS 2018-0652), Informationssäkerhetspolicy (LS 1112-1733) samt Strategi för IT och digitalisering (RS 2019-0669).

Centralt inom Region Stockholm finns CERT (Computer Emergency Response Team) som är en funktion inom enheten Informationssäkerhet, Regionledningskontoret. Funktionen har i uppdrag att minska omfattning och skadeverkan av it-säkerhetsrelaterade hot och incidenter genom att stödja regionens förvaltningar och bolag att upptäcka och hantera dessa. Stödet ska omfatta såväl händelser som har skett och som pågår i realtid. Funktionen är bemannad med it-säkerhetsspecialister som ska stötta med expertkunskap, metoder och verktyg, samt att ge vägledning och rekommendationer kring aktuella hot och händelser så att förvaltningar och bolag kan förebygga och hantera oönskade it-säkerhetsincidenter. CERT har även i uppgift att analysera hot och bedöma omvärldsutvecklingen inom området.

SLSO samverkar med CERT för att förebygga, upptäcka och hantera it-angrepp och genom att följa de inom Region Stockholm beslutade styrande dokumenten arbetar förvaltningen strukturerat och metodiskt med IT-säkerhets- och informationssäkerhetsfrågor.

Stockholms läns sjukvårdsområde har för övrigt inga synpunkter på utredningens förslag.

Förslag till beslut
Nämnden för Stockholms läns sjukvårdsområde föreslås besluta

att avge Yttrande över Remiss – Sveriges säkerhet - behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63) enligt ovanstående, samt

att förklara paragrafen omedelbart justerad.

Mikael Ohrling
Sjukvårdsdirektör

Annika Jerhamre
Kanslichef

Region Stockholm

REMISS

2021-09-27 RS 2021-0750

Rotel I – Finans-, fastighets- och serviceroteln

Fastighets- och servicenämnden
Karolinska Universitetssjukhuset
Stockholms läns sjukvårdsområde

Ärende:

Remiss – Sveriges säkerhet - behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)

Yttrande från berörd nämnd/styrelse senast: **2021-10-22**

Handläggare: **Tobias Sjö**

Yttranden skickas till regionledningskontorets registrator:

E-post: registrator.rlk@regionstockholm.se

Adress:
Regionledningskontoret
Registraturen
Box 22550
104 22 Stockholm

Internadress:
Regionledningskontoret, Registraturen, Lindhagensgatan 98 plan 6

Regeringskansliet

Remiss

2021-09-22
Fö2021/00796

Försvarsdepartementet

Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)

Remissinstanser

Adda

Affärsverket svenska kraftnät

Bolagsverket

Borås kommun

Botkyrka kommun

Domstolsverket

Ekonomistyrningsverket

Energimyndigheten

Falkenbergs kommun

Finansinspektionen

Fortifikationsverket

Försvarets materielverk

Försvarets radioanstalt

Telefonväxel: 08-405 10 00
Fax: 08-723 11 89
Webb: www.regeringen.se

Postadress: 103 33 Stockholm
Besöksadress: Jakobsgatan 9
E-post: fo.registrator@regeringskansliet.se

Försvarsmakten

Försäkringskassan

Förvaltningsrätten i Stockholm

Gotlands kommun

Haninge kommun

Huddinge kommun

Härnösands kommun

Innovationsföretagen

Inspektionen för strategiska produkter

Institutet för rymdfysik

Integritetsskyddsmyndigheten

Internetstiftelsen

It- och telekomföretagen

Jönköpings kommun

Justitiekanslern

Kalmar kommun

Kammarkollegiet

Kammarrätten i Stockholm

Karlstad kommun

Kiruna kommun

Kommerskollegium

Konkurrensverket

Konsumentverket

Kramfors kommun

Kronofogdemyndigheten

Kungl. Tekniska högskolan

Kustbevakningen

Lantmäteriet

Linköpings kommun

Luftfartsverket

Lunds universitet (Juridiska fakulteten)

Länsstyrelsen i Norrbottens län

Länsstyrelsen i Skåne län

Länsstyrelsen i Stockholms län

Länsstyrelsen i Västmanlands län

Länsstyrelsen i Västra Götalands län

Malmö kommun

Myndigheten för digital förvaltning

Myndigheten för samhällsskydd och beredskap

Nacka kommun

Norrköpings kommun

Näringslivets regelnämnd

Pensionsmyndigheten

Piteå kommun

Polismyndigheten

Post- och telestyrelsen

Regelrådet

Region Jämtland Härjedalen

Region Norrbotten

Region Skåne

Region Stockholm

Region Östergötland

Riksarkivet

Riksdagens ombudsmän

Riksgäldskontoret

Riksrevisionen

RISE Research Institutes of Sweden AB

Rymdstyrelsen

Skatteverket

Skellefteå kommun

Småföretagarnas Riksförbund

Spelinspektionen

Statens servicecenter

Statistiska centralbyrån

Statskontoret

Stockholms kommun

Stockholms universitet (Juridiska fakulteten)

Strålsäkerhetsmyndigheten

Styrelsen för ackreditering och teknisk kontroll

Svenljunga kommun

Svenska Journalistförbundet

Svensk Handel

Svenskt Näringsliv

Sveriges advokatsamfund

Sveriges Kommuner och Regioner

Sveriges Konsumenter

Sveriges Standardiseringsförbund

Säkerhets- och försvarsföretagen

Säkerhetspolisen

Söderhamns kommun

Södertälje kommun

Teknikföretagen

Tierps kommun

Totalförsvarets forskningsinstitut

Trafikverket

Transportstyrelsen

Trollhättans kommun

Trosa kommun

Tullverket

Uddevalla kommun

Upphandlingsmyndigheten

Uppsala kommun

Verket för innovationssystem

Vetenskapsrådet

Åklagarmyndigheten

Örebro kommun

Östersunds kommun

Östhammars kommun

Remissvaren ska ha kommit in till Försvarsdepartementet **senast den 10 januari 2022**. Svaren bör lämnas per e-post till fo.remissvar@regeringskansliet.se. Ange diarienummer Fö2021/00796 och remissinstansens namn i ämnesraden på e-postmeddelandet.

Svaret bör lämnas i två versioner: den ena i ett bearbetningsbart format (t.ex. Word), den andra i ett format (t.ex. pdf) som följer tillgänglighetskraven enligt lagen (2018:1937) om tillgänglighet till digital offentlig service. Remissinstansens namn ska anges i namnet på respektive dokument.

Remissvaren kommer att publiceras på regeringens webbplats.

I remissen ligger att regeringen vill ha synpunkter på förslagen eller materialet i betänkandet. Om remissen är begränsad till en viss del av betänkandet, anges detta inom parentes efter remissinstansens namn i remisslistan. En sådan begränsning hindrar givetvis inte att remissinstansen lämnar synpunkter också på övriga delar.

Myndigheter under regeringen är skyldiga att svara på remissen. En myndighet avgör dock på eget ansvar om den har några synpunkter att redovisa i ett svar. Om myndigheten inte har några synpunkter, räcker det att svaret ger besked om detta.

För **andra remissinstanser** innebär remissen en inbjudan att lämna synpunkter.

Betänkandet kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Remissinstanserna kan utan kostnad beställa tryckta exemplar av betänkandet via ett beställningsformulär hos Elanders Sverige AB.

Råd om hur remissyttranden utformas finns i Statsrådsberedningens promemoria Svara på remiss – hur och varför (SB PM 2003:2, reviderad 2009-05-02). Den kan laddas ner från Regeringskansliets webbplats www.regeringen.se.

Michael Cherinet
Departementsråd

Kopia till

Elanders Sverige AB, e-postadress: betankande@elanders.com

Sveriges säkerhet

– behov av starkare skydd för nätverks- och informationssystem



BETÄNKANDE AV
CYBERSÄKERHETSUTREDNINGEN

STATENS OFFENTLIGA UTREDNINGAR

SOU 2021:63

Sveriges säkerhet

– behov av starkare skydd för nätverks- och informationssystem

Slutbetänkande av Cybersäkerhetsutredningen

Stockholm 2021

STATENS OFFENTLIGA UTREDNINGAR

SOU 2021:63

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck och remisshantering: Elanders Sverige AB, Stockholm 2021

ISBN 978-91-525-0177-1 (tryck)
ISBN 978-91-525-0178-8 (pdf)
ISSN 0375-250X

Till statsrådet Peter Hultqvist

Regeringen beslutade den 31 oktober 2019 att tillkalla en särskild utredare (dir. 2019:73) med uppdrag att lämna förslag till anpassningar och kompletterande författningsbestämmelser som EU:s cybersäkerhetsakt ger anledning till och att överväga behovet av vissa ytterligare krav på nätverks- och informationssystem till skydd för Sveriges säkerhet.

Den 3 februari 2020 förordnades lagmannen Nils Cederstierna som särskild utredare. Som sakkunniga förordnades den 2 mars 2020 rättssakkunniga Karin Byström, Försvarsdepartementet, ämnesrådet Catharina Hallström, Försvarsdepartementet, ämnesrådet Richard Henriksson, Utrikesdepartementet, departementssekreteraren Linnéa Jannes, Utrikesdepartementet, numera kanslirådet Staffan Lindmark, Infrastrukturdepartementet, numera kanslirådet Emelie Smiding, Justitiedepartementet, och militärsakkunniga Anna Weibull, Försvarsdepartementet. Samma dag förordnades bedömningsledaren Curt-Peter Askolin, Styrelsen för ackreditering och teknisk kontroll (Swedac), verksjuristen Charlotte Hakelius, Säkerhetspolisen, verksamhetschefen Ronny Harpe, Myndigheten för samhällsskydd och beredskap (MSB), kommendör Per-Ola Johansson, Försvarsmakten, juristen Britt-Marie Jönson, Post- och telestyrelsen, director Mats F. Nilsson, Teknikföretagen, ordföranden för Cyberförsvarsgruppen Richard Oehme, Säkerhets- och försvarsföretagen (SOFF), handläggaren Tommy Schönberg, Vinnova, och chefen för FMV/CSEC Dag Ströman, Försvarets materielverk, som experter i utredningen. Den 13 mars 2020 förordnades även kanslirådet Anneli Hagdahl, Försvarsdepartementet, som sakkunnig i utredningen och biträdande säkerhetsskyddschefen Ylva Söderlund, Trafikverket, som expert. Den 8 oktober 2020 entledigades Anna Weibull som sakkunnig. Ämnessakkunnige Christer Hellsten, Försvarsdepartementet, förordnades som sakkunnig den 25 november 2020. Catharina Hallström och

Curt-Peter Askolin entledigades den 12 december 2020. Samma dag förordnades som expert utredaren Magnus Pedersen, Styrelsen för ackreditering och teknisk kontroll (Swedac). Ylva Söderlund entledigades den 24 februari 2021.

Som sekreterare i utredningen anställdes den 3 februari 2020 hovrättsassessorn Patrik Roos. Seniora rådgivaren Thomas Wallander anställdes som huvudsekreterare den 10 februari 2020.

Utredningen har tagit namnet Cybersäkerhetsutredningen (Fö 2019:1).

Genom tilläggsdirektiv den 14 maj 2020 förlängdes utredningstiden för den del av uppdraget som avser anpassningar med anledning av EU:s cybersäkerhetsakt (dir. 2020:57). Den 18 februari 2021 beslutade regeringen i tilläggsdirektiv till utredningen (dir. 2021:10) att förlänga utredningstiden för den del som avser ytterligare krav på verksamheter av betydelse för Sveriges säkerhet.

Utredningen överlämnade delbetänkandet *EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering* (SOU 2020:58) i september 2020. Härmed överlämnar utredningen slutbetänkandet *Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem* (SOU 2021:63).

Utredningens uppdrag är därmed slutfört.

Stockholm i juli 2021

Nils Cederstierna

/Thomas Wallander
Patrik Roos

Innehåll

Förkortningar **17**

Sammanfattning **19**

Summary **33**

1 Författningsförslag **47**

1.1 Förslag till lag om ändring i säkerhetsskyddslagen (2018:585) 47

1.2 Förslag till förordning om ändring i säkerhetsskyddsförordningen (2018:658) 51

2 Uppdraget **53**

2.1 Inledning 53

2.2 Bakgrund 53

2.3 Uppdragets andra del 56

2.4 Definitioner 58

2.5 Uppdragets omfattning 59

2.6 Utredningsarbetet 62

2.7 Betänkandets disposition 64

3 Utgångspunkter **67**

3.1 Inledning 67

3.2 Informations- och cybersäkerhet i olika styrdokument 68
3.2.1 Försvarsbeslutet för perioden 2021–2025 68
3.2.2 Den nationella säkerhetsstrategin 72
3.2.3 Nationell strategi för samhällets informations- och cybersäkerhet 75
3.2.4 Nationell digitaliseringsstrategi 76
3.3 Det nationella cybersäkerhetscentret 78
3.4 Samlad informations- och cybersäkerhetshandlingsplan 2020–2023 80
3.5 Författningsbestämmelser om informations- och cybersäkerhet 83
3.5.1 Säkerhetsskydd 84
3.5.2 Samhällsviktiga och digitala tjänster 85
3.5.3 Det europeiska ramverket för cybersäkerhetscertifiering 87
3.5.4 Regleringen avseende statliga myndigheter 88
3.5.5 Regioner och kommuner 89
3.6 Offentliga utredningar och rapporter 89
3.7 Digitaliseringen och kraven på informations- och cybersäkerhet 90

4 Digitalisering och informations- och cybersäkerhet 91

4.1 Inledning 91
4.2 Bakgrund 92
4.3 Politikens mål för digitalisering 94
4.3.1 Digitaliseringsstrategier 94
4.3.2 Utvecklingen 95
4.4 Internationella jämförelser (index) 97
4.5 Digitala sårbarheter 99
4.6 Digitalisering och informations- och cybersäkerhet i otakt 105

5 Utvecklingen av hot, sårbarheter och risker 111

5.1 Inledning 111

5.2 Hot, sårbarheter och risker 111

5.3 Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden 2020 115

5.4 Cyberangrepp mot myndigheter 119

5.5 Cyberangrepp mot företag 120
5.5.1 CYBERHOTEN – Så ser hotbilden och attackerna ut mot svenska teknikföretag (2019) 122
5.5.2 Cybersäkerhet – En kartläggning av Sveriges nuläge 2020 och framtidsutsikter för branschen 124

6 Säkerhetskänslig verksamhet 127

6.1 Inledning 127

6.2 Säkerhetsskyddslagen 128
6.2.1 Sveriges säkerhet 128
6.2.2 Internationellt åtagande om säkerhetsskydd 129

6.3 Vad som avses med säkerhetsskydd 129

6.4 Konsekvenskategorier 133
6.4.1 Konsekvensnivåer 134
6.4.2 Särskilt säkerhetskänslig verksamhet 134

6.5 Grundläggande bestämmelser om säkerhetsskydd 135
6.5.1 Informationssäkerhet 137
6.5.2 Fysisk säkerhet 138
6.5.3 Personalsäkerhet 139
6.5.4 Behörighet att delta i säkerhetskänslig verksamhet 139

6.6 Särskild säkerhetsskyddsbedömning 139
6.6.1 Statliga myndigheter vid upphandling 140
6.6.2 Inför driftsättning av informationssystem 140
6.6.3 Vid förändringar av hotbild eller verksamhet 140

6.7 Samråd ... 141
6.7.1 Upphandling av myndigheter ... 141
6.7.2 Samråd avseende informationssystem ... 141
6.7.3 Samråd och information vid registerkontroll ... 141
6.7.4 Samråd avseende ytterligare föreskrifter och undantag ... 142
6.7.5 Samråd vid sänkning av säkerhetsskyddsklass ... 142

6.8 Säkerhetsskyddsavtal ... 142

6.9 Roller och ansvar ... 143
6.9.1 Säkerhetspolisens roll och uppgifter ... 144
6.9.2 Försvarsmaktens roll och uppgifter ... 144
6.9.3 Tillsynsmyndigheternas roll ... 144
6.9.4 Närmare om verksamhetsutövarens ansvar ... 146

6.10 Säkerhetsskyddsregleringen och NIS-direktivet ... 147

7 Informationssäkerhet ... 149

7.1 Inledning ... 149

7.2 Informationssäkerhet ... 149
7.2.1 Informationssäkerhetens beståndsdelar ... 150
7.2.2 Säkerhetsskyddsklassificerade uppgifter ... 154
7.2.3 Indelning i säkerhetsskyddsklasser ... 154
7.2.4 Uppgifter som omfattas av ett internationellt åtagande om säkerhetsskydd ... 155
7.2.5 Aggregerade och ackumulerade uppgifter ... 156

7.3 Hantering av säkerhetsskyddsklassificerade uppgifter ... 157
7.3.1 Anteckning om säkerhetsskyddsklass ... 157
7.3.2 Förvaring ... 158
7.3.3 Märkning av lagringsmedium ... 158
7.3.4 Distribution ... 158
7.3.5 Förstöring ... 159

7.4 Säkerhetsskyddsanalys ... 159

7.5 Särskild säkerhetsskyddsbedömning ... 160
7.5.1 Allmänt om särskild säkerhetsskyddsbedömning ... 160
7.5.2 Hur ska informationssystemet användas? ... 161

7.5.3 På vilket sätt är informationssystemet av betydelse för säkerhetskänslig verksamhet? 161
7.5.4 Hur exponeras informationssystemet mot andra informationssystem? 162
7.5.5 Vilka säkerhetskrav gäller för informationssystemet? 162
7.5.6 Vilka säkerhetsskyddsåtgärder behöver införas i och kring informationssystemet? 163

7.6 Omvärldsbevakning 163
7.6.1 Allmänt om omvärldsbevakning 163
7.6.2 Kompetens och resursplanering 164

7.7 Utveckling av informationssystem 166
7.7.1 Allmänt om utveckling av informationssystem 166
7.7.2 Behovet av process för utveckling av informationssystem 166
7.7.3 Systemdesign och systemutveckling 167
7.7.4 Allmänt om arkitektur 169
7.7.5 Separation 169
7.7.6 Import och export av data 171
7.7.7 Säkerhetszoner och kontrollerad kommunikation 172
7.7.8 Säkerhetszoner 173
7.7.9 Nödvändig kommunikation 173
7.7.10 Kryptering 175
7.7.11 Identitets- och behörighetshantering 178
7.7.12 Intrångsskydd och intrångsdetektering 180
7.7.13 Granskning vid anskaffning och utveckling 182
7.7.14 Drift- och testmiljö 182

7.8 Säkerhetskonfiguration av informationssystem 183
7.8.1 Allmänt om säkerhetskonfiguration 183
7.8.2 Skydd mot skadlig kod 184

7.9 Funktionstester och säkerhetsgranskning 185
7.9.1 Allmänt om funktionstester och säkerhetsgranskning 185
7.9.2 Funktionstester 186
7.9.3 Säkerhetsgranskning 187

7.9.4 Sårbarhetsskanning ... 188
7.9.5 Penetrationstest ... 188

7.10 Inför driftsättning ... 189
7.10.1 Allmänt om åtgärder inför driftsättning ... 189
7.10.2 Dokumentation ... 191
7.10.3 Verifiering av funktions- och säkerhetskrav ... 191
7.10.4 Driftgodkännande ... 192

7.11 Drift och underhåll ... 192
7.11.1 Allmänt om drift och underhåll ... 192
7.11.2 Styrning av drift och underhåll ... 192
7.11.3 Beslut om undantag av säkerhetsuppdateringar ... 195
7.11.4 Säkerhetskopiering ... 196

7.12 Allmänt om operativ säkerhet ... 196
7.12.1 Säkerhetsloggning ... 197

7.13 Säkerhetsövervakning ... 199
7.13.1 Allmänt om säkerhetsövervakning ... 199
7.13.2 Åtgärder vid upptäckta händelser ... 200
7.13.3 Tekniska hjälpmedel ... 201
7.13.4 Övning och utvärdering ... 202

7.14 Uppföljning och kontroll ... 202
7.14.1 Allmänt om uppföljning och kontroll ... 202
7.14.2 Efterlevnad av kravställning ... 204
7.14.3 Kontroll av åtkomst och behörigheter ... 204
7.14.4 Uppdatering av dokumentation ... 204

7.15 Allmänt om incidenthantering ... 205
7.15.1 Grundläggande förutsättningar ... 206
7.15.2 Genomförande ... 206

7.16 Avveckling ... 207
7.16.1 Allmänt om avveckling ... 207
7.16.2 Avveckling av komponenter ... 208
7.16.3 Avveckling och återanvändning av lagringsmedia ... 208

7.17 Samråd om informationssystem ... 209
7.17.1 Allmänt om samråd ... 209

7.17.2 Samråd inför driftsättning av ett informationssystem ... 209
7.17.3 Samråd vid väsentlig förändring av ett informationssystem ... 210

8 Offentliga utredningar och myndighetsrapporter ... 213

8.1 Inledning ... 215
8.2 Offentliga utredningar och rapporter ... 216

9 Internationell utblick ... 261

9.1 Inledning ... 261
9.2 Finland ... 262
9.3 Norge ... 267
9.4 Danmark ... 275
9.5 Nederländerna ... 279
9.6 Tyskland ... 286
9.7 Frankrike ... 293
9.8 Storbritannien ... 299
9.9 USA ... 307
9.10 Kanada ... 322
9.11 Nya Zeeland ... 329
9.12 Australien ... 336
9.13 Gränsöverskridande system ... 342
9.14 Sammanfattande slutsatser ... 347

10 Allmänna överväganden ... 351

10.1 Inledning ... 351
10.2 Digitaliseringen av samhällsverksamheter ... 351
10.3 Hot, sårbarheter och risker ... 354

10.4 Brister i informations- och cybersäkerhet 356
10.5 Behovet av ökad informations- och cybersäkerhet 358
10.6 Ökat behov av styrning och samordning av informations- och cybersäkerhet 360
10.7 Tillgången på personal med kompetens inom informations- och cybersäkerhet måste öka 362
10.8 Sammanfattning 364

11 Åtgärder för stärkt säkerhet i nätverks- och informationssystem 367

11.1 Inledning 367
11.2 Begreppet informationssystem 368
11.3 Nuvarande brister i säkerheten i informationssystem 369
11.4 Flera olika åtgärder krävs för att öka säkerheten i informationssystem i säkerhetskänslig verksamhet 371

12 Certifiering av nätverks- och informationssystem 375

12.1 Inledning 377
12.2 Utgångspunkter 378
12.3 Finns krav på evaluering/testning av IKT-produkter, -tjänster och -processer i olika verksamheter? 382
12.4 Finns krav på certifiering i andra länder? 390
12.5 Överväganden 394
12.5.1 Behov av att stärka säkerheten i nätverks- och informationssystem 394
12.5.2 Förutsättningar för en nationell certifieringsordning för säkerhetskänslig verksamhet 395
12.5.3 Inhämtade synpunkter från Säkerhetspolisen och Försvarsmakten 403
12.5.4 Behovet av gemensam och fastställd kravbild 404

12.5.5 Behov av nationell sammanställning över certifierade och rekommenderade IKT-produkter, -tjänster och -processer 409
12.5.6 Det föreligger f.n. inte behov av en nationell särskild ordning för certifiering i säkerhetskänslig verksamhet 412

12.6 Uppdrag till berörda myndigheter 422

13 Krav på godkännande och utvidgat samrådsförfarande för informationssystem 427

13.1 Inledning och utgångspunkter 428

13.2 Allvarliga brister i informationssäkerheten 429
13.2.1 Utredningar och kartläggningar 429
13.2.2 Slutsatser om säkerhetsbrister och -behov 433

13.3 Nuvarande system 434
13.3.1 Granskning och godkännande 434
13.3.2 Allmänna krav på informationssäkerhet i statliga myndigheters verksamhet 437
13.3.3 Krav på informationssäkerhet i säkerhetsskyddsregleringen 440
13.3.4 Cybersäkerhetscertifiering i enlighet med EU:s cybersäkerhetsakt 442
13.3.5 Slutsatser om samrådsförfarandet och skyldigheter i säkerhetskänslig verksamhet 443

13.4 Pågående åtgärder för ökad informationssäkerhet 444
13.4.1 Anmälningsplikt 445
13.4.2 Utvidgad samrådsskyldighet och befogenheter vid överlåtelse och utkontraktering av säkerhetskänslig verksamhet 445
13.4.3 Närmare om tillsynsbefogenheter och ingripande möjligheter 447
13.4.4 Slutsatser om föreslagna ändringar i säkerhetsskyddslagen 448
13.4.5 Åtgärder enligt den samlade informations- och cybersäkerhetshandlingsplanen 449

13.5 Krav i andra länder ... 449
13.6 Behov av samordnat samråd och nationellt godkännande för säkerhetskänslig verksamhet ... 451
13.7 Kompletteringarna till säkerhetsskyddslagen kontra godkännandeförfarande ... 452
13.8 Ytterligare stärkt samrådsroll ... 458
13.8.1 Certifiering som komplement ... 469
13.8.2 Bestämmelserna ska tas in i säkerhetsskyddslagen ... 470

14 Tillgång till informationssystem vid tillsyn ... 471
14.1 Inledning ... 471
14.2 Det finns skäl att införa ytterligare en undersökningsbefogenhet ... 472
14.3 Bestämmelserna ska tas in i säkerhetsskyddslagen ... 474

15 Handläggning och överklagande ... 475
15.1 Förvaltningslagen bör gälla vid handläggningen ... 475
15.2 Beslut som bör få överklagas ... 476
15.3 Överklagandeinstans ... 477

16 Offentlighet och sekretess ... 479
16.1 Sekretesskyddet hos samrådsmyndigheten ... 479
16.2 Utlämnande av uppgifter i samband med samråd ... 480
16.3 Sekretess vid tillsyn ... 481
16.4 Partsinsyn och kommunikation ... 481

17 Konsekvensbeskrivning ... 483
17.1 Inledning ... 484
17.2 Utgångspunkter ... 484

17.3 De som berörs av förslagen 484
17.4 Frågan om krav på certifiering 485
17.5 Förslaget om en stärkt samrådsroll 486
17.6 Konsekvenser för samhället 493
17.7 Brottsförebyggande effekter 493
17.8 Övriga konsekvenser 493

18 Författningskommentar 495

18.1 Förslaget till lag om ändring i säkerhetsskyddslagen (2018:585) 495

Referenser 505

Bilagor

Bilaga 1 Kommittédirektiv 2019:73 511
Bilaga 2 Kommittédirektiv 2020:57 525
Bilaga 3 Kommittédirektiv 2021:10 527
Bilaga 4 Formell skrivelse 529

Förkortningar

AI	Artificiell intelligens
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CSEC	Sveriges certifieringsorgan för IT-säkerhet
CERT	Computer Emergency Response Team
cPP	collaborative Protection Profile
COTS	Commercial off-the-shelf
CSIRT	Computer Security Incident Response Team
DIGG	Myndigheten för digital förvaltning
Ds	Departementsserien
ENISA	European Union Agency for Cybersecurity
EU	Europeiska Unionen
EAL	Evaluation Assurance Level
FMV	Försvarets materielverk
FN	Förenta nationerna
FOI	Totalförsvarets forskningsinstitut
FRA	Försvarets radioanstalt
Fö	Försvarsdepartementet
IKT	Informations- och kommunikationsteknik
IT	Informationsteknik
IVA	Kungl. Ingenjörsvetenskapsakademien

LAN	Local Area Network
MSB	Myndigheten för samhällsskydd och beredskap
MUST	Militära underrättelse- och säkerhetstjänsten
NATO	North Atlantic Treaty Organisation
NCSA	National Communications Security Authority
NDA	National Distribution Authority
NSA	National Security Authority
OECD	Organisation on Economic Cooperation and Development
PP	Protection Profile
Prop.	Proposition
PTS	Post- och telestyrelsen
RK	Regeringskansliet
SAMFI	Samverkansgruppen för informationssäkerhet
SIS	Svenska Institutet för Standarder
SOG-IS	MRA Senior Officials Group Information Systems Security – Mutual Recognition Agreement
SOU	Statens offentliga utredningar
Swedac	Styrelsen för ackreditering och teknisk kontroll
ST	Security target
Vinnova	Verket för innovationssystem

Sammanfattning

Uppdraget

Europeiska unionen (EU) har antagit ett antal strategier, policys och förordningar för att stärka cybersäkerheten i unionen och medlemsstaterna. Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) trädde i kraft den 27 juni 2019. Det huvudsakliga syftet med förordningen är att uppnå en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen och säkerställa en väl fungerande inre marknad. Det europeiska ramverket för cybersäkerhetscertifiering, dvs. EU:s cybersäkerhetsakt och de genomförandeakter som utfärdas med stöd av cybersäkerhetsakten, kommer att reglera den cybersäkerhetscertifiering som följer av en europeisk certifieringsordning för cybersäkerhetscertifiering som fastställts av kommissionen.

Utredningens uppdrag i den första delen var att föreslå de anpassningar och kompletterande nationella författningsbestämmelser som EU:s cybersäkerhetsakt ger anledning till och som behöver finnas på plats när förordningen i sin helhet börjar tillämpas den 28 juni 2021. Vidare ingick att även överväga och föreslå vilken befintlig nationell myndighet som ska utses att fullgöra de uppgifter och tilldelas de ansvarsområden som följer av EU:s cybersäkerhetsakt, bl.a. uppdraget att utöva tillsyn över efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering.

Utredningen överlämnade sitt delbetänkande *Kompletterande bestämmelser till EU:s cybersäkerhetsakt* (SOU 2020:25) i september 2020. Regeringen har efter remissbehandling av utredningens delbetänkande överlämnat proposition 2020/21:186 *Kompletterande bestäm-*

melser till EU:s cybersäkerhetsakt till riksdagen och i den lämnat förslag på en ny lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt. I den föreslagna lagen finns kompletterande nationella bestämmelser om bl.a. nationell myndighet för cybersäkerhetscertifiering, tillsyn, sanktioner och förfarandet vid cybersäkerhetscertifiering. Riksdagen har den 9 juni 2021 beslutat i enlighet med vad som föreslås i angivna proposition och fattat beslut om att lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt ska träda i kraft den 28 juni 2021. Regeringen har i anslutning till att lagen ska börja tillämpas utsett Försvarets materielverk till nationell myndighet för cybersäkerhetscertifiering med de uppgifter som följer av det europeiska ramverket för cybersäkerhethetscertifiering, dvs. EU:s cybersäkerhetsakt och de genomförandeförordningar som ska utfördas med stöd av cybersäkerhetsakten.

Samtidigt kan noteras att åtgärder som bl.a. rör försvar och nationell säkerhet faller utanför EU:s kompetens (art. 4.2 EU-fördraget). I artikel 1.2 EU:s cybersäkerhetsakt anges därför att förordningen inte ska påverka medlemsstaternas befogenheter i fråga om nät- och informationssäkerhet, särskilt inte verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på strafflagstiftningens område.

Regeringen framhåller i direktiven till utredningen att det måste kunna ställas särskilda krav på säkerhet på nätverks- och informationssystem för att skydda nationell säkerhet och att det finns anledning att nu överväga om ytterligare nationella krav bör införas för att säkerställa att nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet uppfyller de krav som behövs för att upprätthålla skyddet av sådana verksamheter.

Utredningens uppdrag innefattar därför att bedöma om det finns anledning att införa nationella särskilda krav på att IKT-produkter, -tjänster och -processer, som ingår i ett nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet, ska vara certifierade enligt en nationell särskilt anpassad certifieringsordning utformad för säkerhetskänslig verksamhet.

I uppdraget ingår även att överväga om det finns anledning att införa krav på godkännande från en myndighet för att sådana IKT-produkter, -tjänster och -processer ska få tas i drift i viss eller all säkerhetskänslig verksamhet.

I uppdraget ingår att göra en internationell jämförelse av lagstiftning som innebär särskilda krav med anledning av nationell säkerhet för IKT-produkter, -tjänster och -processer som ingår i ett nätverks- eller informationssystem i de länder som bedöms vara av intresse.

För nätverks- och informationssystem som används i eller har betydelse för säkerhetskänslig verksamhet finns i dag särskilda krav i säkerhetsskyddsförordningen (2018:658). Det rör sig bl.a. om förberedande åtgärder inför driftsättning av informationssystem och om säkerhetskrav som kontinuerligt ställs på informationssystemen. Bestämmelserna innehåller även krav på samråd med Säkerhetspolisen eller Försvarsmakten i de fall informationssystemen kan komma att behandla säkerhetsskyddsklassificerade uppgifter av visst slag och informationssystem där obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är obetydlig. Bestämmelserna föreskriver att det är verksamhetsutövaren som ansvarar för att se till att informationssystemen upprätthåller kraven på informationssäkerhet.

Digitaliseringsutvecklingen och kravet på informations- och cybersäkerhet

Digitaliseringen beskrivs som vår tids starkaste förändringsfaktor och innebär att en allt större andel av aktiviteterna i samhället är beroende av nätverks- och informationssystem som används av myndigheter, organisationer, företag och privatpersoner. Digitaliseringen har skapat nya former av kommunikation, datahantering och datalagring, och som medför stora möjligheter att förbättra och effektivisera olika verksamheter.

Digitaliseringen påverkar hela samhället och området kan beskrivas som horisontellt, bl.a. för att det omfattar alla samhällssektorer. Den pågående globala digitala utvecklingen och i Sverige går på många plan mycket fort och statliga myndigheter, regioner och kommuner och aktörer i näringslivet bedriver sedan många år olika digitaliseringsarbeten. I dag bygger många system för att hantera information huvudsakligen på digital informations- och kommunikationsteknik (IKT).

Med den tilltagande globaliseringen och digitaliseringen, som ökar beroenden över nations-, sektors- och ansvarsgränser, har även följt

en ökad betoning på cyberfrågor i samhället. Beroende av digital infrastruktur och tjänster genom utbredd uppkoppling till internet och anslutna enheter medför ökade sårbarheter vilket ställer högre krav på informations- och cybersäkerhet. Samtidigt som digitala utvecklingen går snabbt ökar inte informations- och cybersäkerheten i samma takt. Detta gap, och om det ökar ytterligare, medför att riskerna för att drabbas av cyberangrepp eller andra it-incidenter också ökar. Gapet kan dock minska genom olika åtgärder som bidrar till att stärka informations- och cybersäkerheten.

Nya hot, sårbarheter och risker

På samma sätt som digitaliseringen av samhällets olika verksamheter kontinuerligt medför fördelar kan den också föra med sig nya eller förändrade hot, sårbarheter och risker som påverkar informations- och cybersäkerheten i bl.a. nätverks- och informationssystem hos olika verksamhetsutövare. Det innebär att risken för cyberangrepp ökar mot olika samhällsverksamheter, särskilt vad gäller säkerhetskänsliga och andra samhällsviktiga verksamheter, som många har höga skyddsvärden. Hoten kommer främst från statliga aktörer som genomför cyberangrepp i olika syften, bl.a. som förberedelser för cyberangrepp och som industrispionage. Hoten kommer även från kriminella aktörer och ideellt motiverade aktörer, som har förmåga till cyberangrepp för olika syften.

Olika förändringsfaktorer, som utvecklingen av t.ex. 5G-system, molntjänster, artificiell intelligens och kvantdatorer, medför nya möjligheter men även ökade sårbarheter och risker som kan utnyttjas och orsaka skada på olika säkerhetskänsliga och samhällsviktiga funktioner och verksamhet men också i näringslivet, t.ex. försvarsindustrin.

Vidare skapar beroendeförhållanden mellan olika samhällsviktiga verksamheter, t.ex. elektronisk kommunikation och energisektorn, sårbarheter och risker, och cyberangrepp mot en samhällsviktig verksamhet kan få allvarliga och omfattande följder för en eller flera andra sådana verksamheter och även för totalförsvarets verksamhet.

Allvarliga brister i informations- och cybersäkerheten

En tillräcklig informations- och cybersäkerhet kan endast uppnås när alla de olika förutsättningar som krävs för en sådan säkerhet är uppfyllda, dvs. enhetlig styrning och organisering av arbetet med informations- och cybersäkerhet, ett systematiskt informationssäkerhetsarbete i verksamheten och tekniska åtgärder samt tillsyn av efterlevnaden av regelsystem och ställda krav.

Av offentliga utredningar och myndighetsrapporter framkommer att det finns allvarliga brister i informations- och cybersäkerheten på många olika områden inom en rad olika samhällsverksamheter. Detta gäller såväl statliga myndigheters verksamhet som regioner och kommuner men även organisationer och näringslivet. Av utredningarna och rapporterna framkommer att allvarliga brister finns hos många verksamhetsutövare, både vad avser det systematiska informationssäkerhetsarbetet och vad avser säkerhet i olika nätverks- och informationssystem. Vidare framkommer att det finns allvarliga brister i styrning och organisering, kunskap och kompetens samt resurstilldelning inom området för informations- och cybersäkerhet.

Utredningen gör ingen annan bedömning av redovisade brister i och nivån på informations- och cybersäkerheten än den som redovisas i de offentliga utredningar och rapporter som offentliggjorts under den senaste femårsperioden och lägger dessa till grund för slutsatsen att det måste anses behövas kraftfulla och omfattande åtgärder på många olika områden för att stärka informations- och cybersäkerheten, dels mer allmänt i samhällets olika verksamheter men särskilt vad avser säkerhetskänsliga och andra samhällsviktiga verksamheter. De allvarliga bristerna innebär uppenbara risker för cyberangrepp mot nätverveks- och informationssystem som kan medföra allvarliga konsekvenser för såväl hela samhället som aktörer inom olika verksamhetsområden, och som därigenom även kan få allvarliga konsekvenser för verksamheten i totalförsvaret.

Uppdraget är avgränsat till att överväga om det finns anledning att införa en nationell särskilt anpassad certifieringsordning för IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet och/eller krav på godkännande av en myndighet innan sådana IKT-produkter, -tjänster och -processer i nätverks- och informationssystem får driftsättas. Utredningen kan samtidigt konstatera att enskilda åtgärder av detta slag inte ensamt

utgör varken tillräckliga åtgärder för att möta generella krav på informations- och cybersäkerhet eller ens möta kraven på säkerhet i nätverks- och informationssystem i säkerhetskänslig verksamhet, då även övriga förutsättningar för en fullgod informations- och cybersäkerhet måste föreligga. Eftersom utredningens uppdrag är inriktat på att överväga de åtgärder som tas upp i utredningsdirektiven har utredningen därför inte närmare övervägt de övriga åtgärder som bör vidtas för att stärka informations- och cybersäkerheten mer allmänt eller i den säkerhetskänsliga verksamheten, utom när det gäller behovet av styrning och samordning då dessa behov även utgör grundläggande förutsättningar för de överväganden som utredningen gör i betänkandet.

Behov av ökad styrning och samordning

Flera offentliga utredningar och rapporter har pekat på behovet av att stärka styrningen och samordningen av digitaliseringen, särskilt när det gäller utbyggnad av infrastruktur och samordning av arbete med informations- och cybersäkerhet. Den nationella marknaden utgör en avreglerad marknad med olika skikt av infrastrukturproducenter, operatörer och tjänsteutvecklare. Sverige är nationellt i en situation där nästan alla grundläggande samhällsfunktioner förutsätter och bygger på en fungerande digital infrastruktur. Det saknas dock regler och systematik för och samordning av den digitala utvecklingen och utbyggnaden.

Mot bakgrund av mängden offentliga aktörer är detta en uppgift av betydande omfattning då frågan berör bl.a. fler än 200 statliga förvaltningsmyndigheter, 21 länsstyrelser, 20 regioner, 290 kommuner, 80 domstolar, 37 lärosäten, och 40 helägda statliga bolag. Det är en omfattande förvaltning som kompliceras av stora skillnader mellan verksamheterna vad gäller uppdrag, storlek, finansiella resurser och kompetens. Till detta kommer näringslivets verksamheter och alla företag som på något sätt utvecklar, driver och förvaltar samhällets digitala infrastruktur.

Motsvarande gäller det övergripande arbetet med att stärka informations- och cybersäkerheten i samhället i stort men även inom säkerhetskänslig och annan samhällsviktig verksamhet. Varje verksamhetsutövare har ansvar för sin egen informations- och cybersäkerhet, bl.a.

vad avser säkerhet i nätverks- och informationssystem. Det saknas emellertid i dag tillsyn över såväl statliga myndigheters verksamhet som regioners och kommuners verksamhet avseende nätverks- och informationssystem, utom såvitt avser säkerhetskänslig verksamhet och verksamhet som avser vissa samhällsviktiga och digitala tjänster. Ansvaret för tillsynsverksamhet av informations- och cybersäkerhet på dessa reglerade områden utövas dock av flera olika samråds- och tillsynsmyndigheter med i vissa fall tillämpning av olika regelsystem. Ansvaret för informations- och cybersäkerhet finns således hos många olika aktörer och styrningen och samordningen brister på både statlig, regional och kommunal nivå. Bristen på styrning och samordning medför ökade sårbarheter och risker i nätverks- och informationssystem i säkerhetskänsliga och andra samhällsviktiga verksamheter. Utredningen bedömer att det bl.a. finns behov av nationell styrning och samordning vid framtagande av en gemensam hot-, sårbarhets- och riskbedömning till stöd i arbetet med informations- och cybersäkerhet. Berörda myndigheter och övriga aktörer behöver därför i större utsträckning än vad som nu sker samverka och samråda i frågor som avser informations- och cybersäkerhet.

Bristande förutsättningar för en nationell certifieringsordning för nätverks- och informationssystem i säkerhetskänslig verksamhet

En nationell särskilt anpassad certifieringsordning för IKT-produkter, -tjänster och -processer som används i nätverks- och informationssystem i säkerhetskänslig verksamhet *kan* – när vissa förutsättningar är uppfyllda – vara en åtgärd som kan stärka säkerheten i dessa system.

Utredningen bedömer att bestämmelserna i säkerhetsskyddslagen och säkerhetsskyddsförordningen redan ger berörda myndigheter möjlighet att föreskriva att certifierade IKT-produkter, -tjänster och -processer, som uppfyller vissa säkerhetskrav, ska användas i nätverks- och informationssystem i säkerhetskänslig och även medge undantag från en sådan skyldighet.

En nationell särskilt anpassad ordning för säkerhetskänslig verksamhet ställer krav på att det finns en nationellt framtagen gemensam hot-, sårbarhets- och riskbedömning som kan ligga till grund

för säkerhetskrav och framtagande av s.k. skyddsprofiler för olika IKT-produkter, -tjänster och -processer i dessa system. En sådan bedömning är också en förutsättning för inriktning av det nationella arbetet med det europeiska ramverket för cybersäkerhetscertifiering. I dag saknas emellertid nationellt organisation och verksamhet som ansvarar för och tar fram en sådan nationell hot-, sårbarhets- och riskbedömning.

Vidare är det europeiska ramverket för cybersäkerhetscertifiering under framtagande och utveckling. Det råder dock i dag oklarhet om i vilken omfattning som certifierade IKT-produkter, -tjänster och -processer kommer att vara tillgängliga med stöd av detta ramverk, bl.a. vad gäller IKT-produkter, -tjänster och -processer på den högsta assuransnivån och som även kan användas – vid behov efter anpassning – i säkerhetskänslig verksamhet.

Det råder även osäkerhet om det finns marknadsmässiga förutsättningar att införa en nationell särskilt anpassad certifieringsordning för säkerhetskänslig verksamhet då den svenska marknaden bedöms vara allt för liten för att företag ska få ekonomiska incitament för att låta certifiera IKT-produkter, -tjänster och -processer för användning i nätverk- och informationssystem i sådan verksamhet. Även om det skulle införas krav på obligatorisk certifiering innebär det inte någon skyldighet att tillhandhålla sådana produkter på den svenska marknaden.

Härtill kommer att det nationella certifieringsorganet CSEC vid Försvarets materielverk redan i dag ansvarar för en nationell ordning för certifiering av it-säkerhet i produkter och system, även om den nationella *Common Criteria*-baserade certifieringsordningen kan komma att ersättas av en europeisk ordning för cybersäkerhetscertifiering (EUCC). Den nationella certifieringsordningen kan på sikt utvecklas till att omfatta certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet.

Sammantaget gör utredningen bedömningen att det för närvarande inte föreligger tillräckliga skäl att föreslå att det införs en nationell särskilt anpassad certifieringsordning för IKT-produkter, -tjänster och -processer som används i nätverks- och informationssystem i säkerhetskänslig verksamhet.

Det finns dock behov av att berörda myndigheter gemensamt tar fram hot-, sårbarhets- och riskbedömningar samt skyddsprofiler för

olika IKT-produkter, -tjänster och -processer som ska användas i nätverks- och informationssystem i säkerhetskänslig verksamhet.

Utredningen föreslår därför att regeringen ger Försvarets materielverk (FMV) i uppdrag att, i samråd och samverkan med främst de myndigheter som ingår i det nationella cybersäkerhetscentret, utveckla formerna för hur gemensamt framtagna hot-, sårbarhets- och riskbedömningar samt skyddsprofiler kan tas fram till stöd för kravställning på IKT-produkter, -tjänster och -processer som ska användas i nätverks- och informationssystem i säkerhetskänslig verksamhet. En sådan nationellt framtagen bedömning med åtföljande kravställning kan även till del utgöra underlag i det nationella arbetet inom ramen för det europeiska ramverket för cybersäkerhetscertifiering.

Utredningen bedömer vidare att informations- och cybersäkerheten i statliga myndigheters verksamhet i övrigt behöver stärkas. Åtgärder bör därför vidtas som bidrar till att myndigheterna använder certifierade IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i verksamheten om inte detta framstår som olämpligt eller omöjligt att genomföra. Myndigheten för samhällsskydd och beredskap (MSB) bedöms redan i dag ha bemyndigande att i föreskrifter ange sådant krav på statliga myndigheter. En sådan ordning kan även bidra med kunskap och erfarenheter om behov och användning av certifierade IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i statlig verksamhet och även ligga till grund för det nationella arbetet med hot-, sårbarhets- och riskbedömningar, som utredningen föreslår ska genomföras.

Utvidgad samrådsskyldighet och möjligheter att besluta åtgärdsföreläggande och förbud mot driftsättning av informationssystem i säkerhetskänslig verksamhet

Med utgångspunkt i utredningsdirektiven och mot bakgrund av de allvarliga brister i informations- och cybersäkerheten som framkommer av offentliga utredningar och myndighetsrapporter, finner utredningen skäl att överväga ett antal åtgärder som berör driftsättning och väsentlig förändring av informationssystem i säkerhetskänslig verksamhet. Det rör sig bl.a. om kontrollstationer såsom krav på godkännande, särskild säkerhetsskyddsbedömning, lämplighetsprövning, samråd, förelägganden och förbud.

Utredningen kan konstatera att ett eventuellt införande av krav på att informationssystem som behandlar hemliga och/eller kvalificerat hemliga uppgifter ska godkännas av en utpekad central myndighet innan driftsättning, kan bidra till att stärka skyddet av informationssystem som har betydelse för säkerhetskänslig verksamhet. Denna typ av godkännandeförfarande är vanligt förekommande i andra länder och kan i sig anses utgöra en rimlig åtgärd för att stärka skyddet för nationell säkerhet.

Utredningen bedömer att nu pågående lagstiftningsåtgärder, däribland de av regeringen föreslagna ändringarna i säkerhetsskyddslagen (prop. 2020/21:194), inte kan likställas med ett formellt myndighetsgodkännande och inte heller kan anses utgöra tillräckliga åtgärder för att skydda informationssystemen i säkerhetskänslig verksamhet. Ett krav på formellt förhandsgodkännande från en central myndighet torde i och för sig medföra en oberoende tredjepartsbedömning som bidrar till skapandet av en minimistandard för kontroll av säkerhet och mer enhetliga säkerhetskrav hos verksamhetsutövarna.

Utredningen gör samtidigt bedömningen att ett nationellt införande av ett generellt krav på myndighetgodkännande av informationssystem i säkerhetskänslig verksamhet medför ett betydande behov av omorganisering och ökade resurser hos samråds- och tillsynsmyndigheter. Vidare skulle ett sådant krav på godkännande behöva utformas i linje med övriga krav på säkerhetsskydd för informationssystem, vilket alltjämt medför att en stor mängd säkerhetskänslig information, om än på lägre nivå, faller utanför regleringen. Innan införandet av ett krav på godkännande övervägs ytterligare bör därför utvärderas om redan föreslagna författningsändringar på säkerhetsskyddsområdet i förening med en stärkt samrådsroll för Säkerhetspolisen och Försvarsmakten utgör tillräckliga åtgärder när det gäller informationssystem i säkerhetskänslig verksamhet (se nedan). Till detta kommer att vissa centrala myndigheter redan inom befintliga mandat kan föreskriva om bl.a. krav på certifierade IKT-produkter, -tjänster och -processer i informationssystem i säkerhetskänslig verksamhet (se ovan) och även som en säkerhetsskyddsåtgärd förelägga en verksamhetsutövare att använda sådana produkter, tjänster och processer.

Ett utvidgat samrådsförfarande och utökade befogenheter

För att göra användningen av ett informationssystem i säkerhetskänslig verksamhet säkrare, och därmed stärka skyddet för Sveriges säkerhet, föreslår utredningen ändringar i säkerhetsskyddslagen. Föreslagna ändringar innebär bl.a. följande åtgärder.

– Säkerhetsskyddsförordningens bestämmelser om förberedande åtgärder inför driftsättning av informationssystem ska överföras till säkerhetsskyddslagen.

– Befintligt krav på verksamhetsutövare att göra en särskild säkerhetsskyddsbedömning utvidgas till att även omfatta planerade väsentliga förändringar av informationssystem som kan ha betydelse för säkerhetskänslig verksamhet.

– Verksamhetsutövare ska pröva lämpligheten av en planerad driftsättning eller väsentlig förändring av informationssystem som har betydelse för säkerhetskänslig verksamhet. Om lämplighetsprövningen leder till bedömningen att det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt ska det inte inledas.

– Lämplighetsprövningen ska, liksom den särskilda säkerhetsskyddsbedömningen, dokumenteras.

– I fall verksamhetsutövarens lämplighetsprövning leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt ska verksamhetsutövaren – om övriga rekvisit för samråd är uppfyllda – samråda med samrådsmyndigheten (Säkerhetspolisen eller Försvarsmakten).

– Verksamhetsutövares skyldighet att, inför driftsättning eller väsentlig förändring av vissa informationssystem, samråda med Säkerhetspolisen eller Försvarsmakten ska inte begränsas till att ske i form av en skriftlig process.

– Säkerhetspolisen och Försvarsmakten ska, i egenskap av samrådsmyndigheter enligt säkerhetsskyddslagen, få inleda samråd och inom ramen för ett samråd besluta åtgärdsföreläggande mot verksamhetsutövaren att vidta en säkerhetsskyddsåtgärd i berört informationssystem.

– Samrådsmyndigheterna ska även få möjlighet att förbjuda en ur säkerhetsskyddssynpunkt olämplig driftsättning eller förändring

av informationssystem och besluta sanktionsavgift mot den som åsidosätter samrådsskyldigheten eller agerar i strid med meddelat förbud.[1]

– Tillsynsmyndigheterna får en ny undersökningsbefogenhet genom möjligheten att, vid äventyr av vite, få tillgång till verksamhetsutövares informationssystem.

Konsekvenser

Utredningen bedömer att skyddet för Sveriges säkerhet stärks genom förslagen.

Utredningens förslag att Försvarets materielverk (FMV) ska ges i uppdrag att i samråd och samverkan med andra myndigheter och aktörer ta fram formerna för arbetet med en nationell gemensam hot-, sårbarhets- och riskbedömning kan antas medföra vissa kostnader. Med anledning av dessa kostnader bör FMV:s anslag ökas. Eventuella kostnader för övriga berörda myndigheter bedöms rymmas inom befintliga anslagsramar.

För de verksamhetsutövare som kommer att träffas av övriga förslag kan de medföra vissa administrativa bördor och ökade kostnader som bedöms vara begränsade, främst när det gäller det utvidgade samrådsförfarandet.

Förslagen innebär även vissa ökade förvaltningskostnader för de myndigheter som kommer att vara samrådsmyndigheter (Säkerhetspolisen och Försvarsmakten). Dessa kostnader är främst beroende av i vilken omfattning som samråd kommer att ske och är i dag svåra att uppskatta. Eventuella kostnader bedöms emellertid vara begränsade och kunna rymmas inom befintlig anslagsram och förväntat utökat anslag (se prop. 2020/21:30). Förslagen bedöms också medföra ökat behov av samverkan mellan samråds- och tillsynsmyndigheter som kan generera vissa begränsade kostnader, vilka bedöms kunna rymmas inom myndigheternas anslag.

[1] De utökade befogenheterna motsvarar i allt väsentligt vad som föreslås gälla (prop. 2021/21:194) för tillsynsmyndigheter vid verksamhetsutövares anskaffning och överlåtelse av säkerhetskänslig verksamhet. När det gäller verksamhetsutövarens skyldigheter är dock särskilt långtgående krav på säkerhet motiverade vid just driftsättning och väsentlig förändring av informationssystem som kan komma att behandla säkerhetsklassificerade uppgifter.

Förslaget om en ny undersökningsbefogenhet för tillsynsmyndigheterna ökar möjligheten till effektiv tillsyn och bedöms inte påverka kostnaderna för tillsynsmyndigheterna i nämnvärd utsträckning.

Förslaget om att tillsynsmyndigheterna ska ha rätt att få tillgång till verksamhetsutövares informationssystem kan leda till att Kronofogdemyndighetens hjälp behövs vid ett antal tillfällen, men ökningen bedöms inte bli särskilt stor och förväntas inte påverka myndighetens verksamhet mer än att konsekvenserna kan hanteras inom befintliga anslag för myndigheten.

Också den nya bestämmelsen om sanktionsavgift kan komma att bidra till en ökad efterlevnad av regelsystemet och effektivare tillsyn samt i begränsad omfattning öka antalet indrivningsärenden hos Kronofogdemyndigheten.

Vidare medför förslagen i fråga om överklagande av samrådsmyndighetens beslut att de allmänna förvaltningsdomstolarna får något ökad måltillströmning och därmed fler arbetsuppgifter. Utredningen bedömer emellertid att ökningen av antalet mål kommer att bli begränsad och att kostnadsökningarna för domstolarna bör rymmas inom befintliga anslagsramar.

Förslagen påverkar i viss mån den kommunala självstyrelsen. Den föreslagna regleringen går dock inte utöver vad som är nödvändigt för att skydda de mest skyddsvärda verksamheterna i samhället.

Även om någon ny kriminalisering inte föreslås kan förslagen antas ha vissa brottsförebyggande effekter. Eftersom de utökade befogenheterna torde underlätta för Säkerhetspolisens brottsbekämpande verksamhet på säkerhetsskyddsområdet, och då skärpta krav ställs för driftsättning respektive förändring av informationssystem i säkerhetskänslig verksamhet, bedöms förslagen bl.a. motverka dataintrång.

Utredningen bedömer att nu nämnda förslag, utöver vad som anförts ovan, inte berör andra områden som anges i 15 § kommittéförordningen. Förslagen och bedömningarna i övrigt, bl.a. att certifierade IKT-produkter, -tjänster och -processer i ökad utsträckning bör användas av statliga myndigheter, bedöms inte medföra några konsekvenser som behöver redovisas närmare i konsekvensanalysen.

Summary

Remit

The European Union (EU) has adopted a number of strategies, policies and regulations to strengthen cybersecurity in the EU and its Member States. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)* entered into force on 27 June 2019. The main purpose of this Regulation is to achieve a high level of cybersecurity, cyber resilience and trust within the Union, and to support the proper functioning of the internal market. The European cybersecurity certification framework, i.e. the EU Cybersecurity Act and implementing acts issued pursuant to the Cybersecurity Act, will regulate cybersecurity certification ensuing from a European cybersecurity certification scheme laid down by the Commission.

The Inquiry's remit for this first part consisted of proposing the adaptations and supplementary national statutory provisions necessitated by the EU Cybersecurity Act and which must be in place when the entire Regulation begins to apply on 28 June 2021. The remit also included considering and proposing which existing national authority should be designated to perform the tasks and be assigned the areas of responsibility ensuing from the Cybersecurity Act, including the task of supervising compliance with the European cybersecurity certification framework.

The Inquiry submitted its interim report, *Supplementary provisions to the EU Cybersecurity Act* (SOU 2020:25) in September 2020. Subsequent to the Interim Report of the Inquiry being circulated for comment, the Government has submitted a Bill 2020/21:186 *Kompletterande bestämmelser till EU:s cybersäkerhetsakt* [Supplementary

provisions to the EU Cybersecurity Act] to the Riksdag proposing a new act containing supplementary provisions to the EU Cybersecurity Act. The proposed act includes supplementary national provisions on a national authority for cybersecurity certification, supervision, fines, and the procedure for cybersecurity certification. On 9 June 2021, the Riksdag passed the government bill and decided that the Act with supplementary provisions to the EU Cybersecurity Act will enter into force on 28 June 2021. In connection with the act entering into force, the Government has designated the Swedish Defence Materiel Administration (FMV) as the national authority for cybersecurity certification with the tasks ensuing from the European cybersecurity certification framework, i.e. the EU Cybersecurity Act and the implementing regulations to be issued with the support of the Cybersecurity Act.

At the same time, it should be noted that measures relating to areas such as defence and national security fall outside the competences of the EU (Article 4(2) of the EU Treaty). Article 1(2) of the EU Cybersecurity Act therefore states that the Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the State in areas of criminal law.

In the terms of reference of the Inquiry, the Government stresses that it must be possible to impose special security requirements on network and information systems in order to protect national security and that there is now reason to consider whether additional national requirements should be introduced to ensure that network and information systems that will be used in security-sensitive activities meet the requirements necessary to maintain the protection of such activities.

The Inquiry's remit therefore includes assessing whether there is reason to introduce national special requirements that ICT products, services and processes which are part of a network and information system that will be used in security-sensitive activities must be certified under a specially adapted national certification scheme designed for such operations.

The remit also includes considering whether there is reason to introduce administrative approval requirements for such ICT products, services and processes before they may be deployed in certain or all security-sensitive activities.

The remit includes an international comparison of legislation that entails special national security requirements on ICT products, services and processes that are part of a network or information system in countries deemed to be of interest.

For network and information systems used in or of importance to security-sensitive activities, there are currently special requirements in the Protective Security Ordinance (2018:658). These include preparatory measures prior to the deployment of information systems and ongoing security requirements imposed on these information systems. The provisions also contain requirements for consultation with the Swedish Security Service or the Swedish Armed Forces in cases where the information systems may process classified information of a certain type and information systems where unauthorised access to these systems could cause harm to Sweden's security that is not insignificant. The provisions prescribe that the operator is responsible for ensuring that information systems comply with the information security requirements.

The growth of digitalisation and the requirement on information security and cybersecurity

Digitalisation is described as the most powerful force for change in our time and has resulted in a growing proportion of societal activities becoming dependent on networks and information systems, which are used by government agencies, organisations, companies and private individuals. Digitalisation has created new forms of communication, data processing and data storage that offer major opportunities to improve and streamline different activities.

Digitalisation affects the whole of society and this area can be described as horizontal in that it covers all sectors of society. Digital transformation is progressing very rapidly on many levels, globally as well as in Sweden, and central government authorities, regions, municipalities and actors in the business community have been pursuing various digitalisation projects for many years. Today, many information processing systems are based primarily on digital information and communications technology (ICT).

Following in the wake of increasing globalisation and digitalisation, which increase dependencies over national and sectoral borders

and across areas of responsibility, is also an increased focus on cyber issues in society. Dependency on digital infrastructure and services through widespread Internet connectivity and connected devices results in increased vulnerability, which places higher demands on information security and cybersecurity. Even though digital transformation is progressing rapidly, information security and cybersecurity are not keeping pace. This gap, and if it increases further, also increases the risk of being subjected to cyber-attacks or other IT incidents. However, this gap can be reduced by means of various measures that help to strengthen information security and cybersecurity.

New threats, vulnerabilities and risks

Just as the digitalisation of society's various activities continues to bring benefits, it can also bring with it new or changed threats, vulnerabilities and risks which can have an impact on information security and cybersecurity in the network and information systems of various operators. This means that the risk of cyber-attacks against various critical infrastructures is increasing, in particular against security-sensitive activities and other essential services, many of which have critical assets. The threats come primarily from state actors who carry out cyber-attacks for various purposes, including preparations for cyber-attack and as industrial espionage. The threats also come from criminal actors and ideologically motivated actors who have the capacity to carry out cyber-attacks for various purposes.

Various factors that can cause significant change, such as the development of 5G systems, cloud services, artificial intelligence and quantum computers, bring with them new opportunities, but also increased vulnerabilities and risks that can be exploited and cause harm to various security-sensitive and essential services and activities, but also to business and industry, such as the defence industry.

Furthermore, dependencies between various essential services and activities, such as electronic communications and the energy sector, create vulnerabilities and risks, and cyber-attacks on an essential service can have serious and extensive consequences for one or more of these services and also for the activities of Sweden's total defence.

Serious shortcomings in information security and cybersecurity

Adequate information security and cybersecurity can only be achieved when all the different conditions required for such security are met: uniform governance of information security and cybersecurity measures and how they are organised; systematic information security work in activities and technical measures; and supervision of compliance with the regulations and set requirements.

It has emerged from Swedish Government Official Reports and government agency reports that there are serious shortcomings in information security and cybersecurity in many different areas in a range of societal activities. This includes the activities of central government authorities as well as the regions and municipalities, but also the activities of organisations and the business community. It has emerged from Swedish Government Official Reports and government agency reports that there are serious shortcomings within the activities of many operators, both in terms of systematic information security work and the security of various network and information systems. Furthermore, there are serious shortcomings in governance and how information security is organised, as well as knowledge and skills and resource allocation in the area of information security and cybersecurity.

The Inquiry makes no other assessment of the identified shortcomings in and level of information security and cybersecurity than that which is described in the Swedish Government Official Reports and government agency reports published over the last five years, and these have been the foundation for the conclusion that a need for powerful and comprehensive measures in many different areas to strengthen information security and cybersecurity must be deemed to exist; on the one hand, more generally in various societal activities, but in particular with regard to security-sensitive activities and other essential services. The serious shortcomings entail manifest risks of cyber-attacks against network and information systems that can have serious consequences for society as a whole as well as for actors in different spheres of activity, which thus can also have serious consequences for activities in Sweden's total defence.

The remit is limited to considering whether there is reason to introduce a specially adapted national certification scheme for ICT

products, services and processes in network and information systems in security-sensitive operations and/or to introduce requirements for administrative approval before such ICT products, services and processes in network and information systems can be deployed. At the same time, the Inquiry can conclude that individual measures of this kind do not alone constitute sufficient measures to meet general requirements on information security and cybersecurity, or even to meet the security requirements of network and information systems in security-sensitive operations, since other conditions for adequate information security and cybersecurity must also exist. Because the Inquiry's remit is focused on considering the measures set out in the terms of reference of the Inquiry, the Inquiry has therefore not considered in detail the other measures that ought to be taken to strengthen information security and cybersecurity more generally or in security-sensitive activities, apart from the need for governance and coordination, since these needs also constitute fundamental conditions for the Inquiry's considerations in its report.

Need for increased governance and coordination

Swedish Government Official Reports and government agency reports have highlighted the need to strengthen the governance and coordination of digitalisation, in particular with regard to the expansion of infrastructure and the coordination of work with information security and cybersecurity. The national market is a deregulated market with different layers of infrastructure producers, operators and service developers. Nationally, Sweden is in a situation where almost all basic social functions presuppose and are based on a functioning digital infrastructure. However, rules and a systematic approach to and coordination of the digital transformation and its expansion are lacking.

In view of the large number of public actors, this is a considerable task, since the matter concerns, among others, more than 200 central government administrative authorities, 21 county administrative boards, 20 regions, 290 municipalities, 80 courts, 37 higher education institutions, and 40 wholly state-owned companies. This is an extensive administration which is complicated by large differences between these activities in terms of remit, size, financial resources and powers. In addition, there are the activities of the business community and

all companies that develop, operate and manage society's digital infrastructure in some way.

The same applies to the overall work to strengthen information security and cybersecurity in society at large, but also in security-sensitive activities and other essential services. Each operator is responsible for their own information security and cybersecurity, including the security of their network and information systems. However, there is currently no supervision of either the activities of central government authorities or those of the regions and municipalities in the area of network and information systems, except in the area of national security and activities relating to certain essential and digital services. However, supervision of information security and cybersecurity in these regulated areas is exercised by a number of responsible consultation and supervisory authorities with, in some cases, the application of different regulations. Responsibility for information security and cybersecurity thus lies with many different actors, and governance and coordination are lacking at the central, regional and municipal levels. The lack of governance and coordination increases the vulnerability of and risks in network and information systems in security-sensitive activities and other essential services. The Inquiry considers that there is a need for national governance and coordination in the development of a common threat, vulnerability and risk assessment to support work with information security and cybersecurity. The relevant authorities and other actors therefore need to cooperate and consult more extensively than is currently the case on questions relating to information security and cybersecurity.

Insufficient conditions for a national certification scheme for network and information systems of importance to national security

A specially adapted national certification scheme for ICT products, services and processes used in network and information systems in security-sensitive activities *may* – when certain conditions are met – be a measure that can strengthen the security of these systems.

The Inquiry considers that the provisions in the Protective Security Act and the Protective Security Ordinance already give the relevant authorities the powers to prescribe the use of certified ICT

products, services and processes that meet certain security requirements in network and information systems in security-sensitive activities, and additionally admit the possibility of derogation from such a requirement.

A specially adapted scheme for security-sensitive activities is predicated on the existence of a nationally developed and common threat, vulnerability and risk assessment that can serve as the basis for security requirements and the development of protection profiles for different ICT products, services and processes in these systems. Such an assessment is also essential to the focus of national efforts with the European cybersecurity certification framework. Today, however, there is no organisation or activity that is responsible for and produces such a national threat, vulnerability and risk assessment.

Furthermore, the European cybersecurity certification framework is still in the process of being produced and developed. However, there is currently a lack of clarity on the extent to which certified ICT products, services and processes will be available under this framework, including ICT products, services and processes at the highest assurance level, that can also be used – if necessary after adaptation – in security-sensitive activities.

There is also uncertainty as to whether the market conditions exist for introducing a specially adapted national certification scheme for security-sensitive activities, as the Swedish market is judged to be too small for companies to have any financial incentives for having their ICT products, services and processes certified for use in networks and information systems in such activities. Even if mandatory certification were to be introduced, it would not imply any requirement to sell such products on the Swedish market.

In addition, the national certification body CSEC of the Swedish Defence Materiel Administration is already responsible for a national scheme for the certification of IT security in products and systems, although the national *Common Criteria*-based certification scheme may come to be replaced by a European cybersecurity certification scheme (EUCC). Ultimately, the national certification scheme can be developed to cover the certification of ICT products, services and processes in network and information systems in security-sensitive activities.

All in all, the Inquiry considers that there are currently insufficient grounds for proposing the introduction of a specially adapted

national certification scheme for ICT products, services and processes used in network and information systems in security-sensitive activities.

However, there is a need for affected government agencies to produce joint threat, vulnerability and risk assessments and protection profiles for the ICT products, services and processes to be used in network and information systems in security-sensitive activities.

The Inquiry therefore proposes that, in consultation and cooperation with the government agencies that are part of the *nationellt cybersäkerhetscenter* [national cybersecurity centre] in particular, the Government tasks the Swedish Defence Materiel Administration (FMV) with developing the forms for how common threat, vulnerability and risk assessments and protection profiles can be produced to support prescribing requirements on ICT products, services and processes to be used in network and information systems in security-sensitive activities. Such a nationally developed assessment with attendant prescribing of requirements can also be used as the basis for national efforts in the context of the European cybersecurity certification framework.

Furthermore the Inquiry considers that information security and cybersecurity in the activities of central government authorities in general need to be strengthened. Measures should therefore be taken that contribute to the use of certified ICT products, services and processes in network and information systems by government agencies in their activities unless this seems inappropriate or impossible to implement. The Swedish Civil Contingencies Agency (MSB) is already judged to have the authority to specify such requirements for central government authorities in regulations. Such a system could also contribute knowledge and experience about the needs and uses of certified ICT products, services and processes in network and information systems in public sector activities and also serve as the basis for work with threat, vulnerability and risk assessments at the national level, which the Inquiry proposes should be implemented.

Expanding the consultation requirement and powers to issue remedial orders and prohibitions in relation to the deployment of information systems in security-sensitive operations

Based on the terms of reference of the Inquiry and in light of the serious shortcomings in information security and cybersecurity that have emerged from Swedish Government Official Reports and government agency reports, the Inquiry finds that there is reason to consider a number of measures relating to the deployment of and substantial changes in information systems in security-sensitive activities. These include checkpoints such as requiring administrative approval, special protective security assessment, suitability assessment, consultation, orders and prohibitions.

The Inquiry can conclude that introducing requirements on information systems that process secret and/or top secret information to be approved by a designated central government agency prior to deployment could help to strengthen the protection of information systems of importance to national security. This type of approval procedure is common in other countries and can in itself be regarded as a reasonable measure for strengthening the protection of national security.

The Inquiry considers that the ongoing legislative measures, including the amendments proposed by the Government to the Protective Security Act (Govt Bill 2020/21:194), cannot be equated with a formal administrative approval, nor can they be considered to constitute sufficient measures to protect information systems in security-sensitive activities. A requirement for formal prior approval by a central authority ought in itself to entail an independent third-party assessment which would contribute to the creation of a minimum standard for checking security and more uniform security requirements among operators.

At the same time, the Inquiry assesses that the introduction nationally of a general requirement for administrative approval of information systems in security-sensitive activities would entail a significant need for reorganisation and increased resources for the consultation and supervisory authorities. In addition, such an administrative approval requirement would need to be designed in line with other protective security requirements for information systems,

which would still mean that a large amount of security-sensitive information, albeit at a lower level, would fall outside the scope of the regulation. Therefore, before further consideration is given to the introduction of an administrative approval requirement, there ought to be an evaluation of whether already proposed legislative amendments in the area of protective security, combined with a strengthened consultative role for the Swedish Security Service and the Swedish Armed Forces, constitute sufficient measures when it comes to information systems in security-sensitive activities (see below). In addition, within their existing mandates certain central authorities can already make provision for requiring certified ICT products, services and processes in information systems in security-sensitive activities (see above) and also, as a protective security measure, order an operator to use such products, services and processes.

An expanded consultation procedure and greater powers

In order to make the use of an information system in security-sensitive activities more secure, and thereby strengthen the protection of Sweden's security, the Inquiry proposes amendments to the Protective Security Act. The proposed amendments include the following measures.

- The provisions of the Protective Security Ordinance on preparatory measures prior to the deployment of information systems should be transferred to the Protective Security Act.
- Existing requirements on operators to perform a special security assessment are extended to also cover planned substantial changes in information systems that may be of importance to security-sensitive activities.
- Operators are to examine the suitability of a planned deployment of or substantial change in an information system that is of importance to security-sensitive activities. If the suitability assessment leads to the conclusion that the planned procedure is unsuitable from a protective security point of view, the procedure is not to be commenced.
- The suitability assessment, as well as the special security assessment, must be documented.

- If the operator's suitability assessment leads to an assessment that the intended procedure is not unsuitable from a protective security point of view, the operator – provided that other necessary prerequisites for consultation are met – is to consult with the consultation authority (the Swedish Security Service or the Swedish Armed Forces).
- The operator's requirement to consult with the Swedish Security Service or the Swedish Armed Forces prior to the deployment of, or a substantial change in, certain information systems, should not be limited to a written process.
- In their capacity as consultation authorities under the Protective Security Act, the Swedish Security Service and the Swedish Armed Forces are to be permitted to initiate consultation and within the context of a consultation to issue remedial orders to the operator to take a protective security measure in the information system.
- The consultation authorities are to also be given the power to prohibit a deployment of, or change in, an information system that is unsuitable from a protective security point of view, and to impose an administrative fine on a person who fails to comply with the consultation requirement, or acts in contravention of a prohibition that has been issued.[1]
- The supervisory authorities are given a new power of investigation through the possibility, under penalty of a fine, of gaining access to operators' information systems.

Consequences

The Inquiry assesses that its proposals strengthen the protection of Sweden's security.

The Inquiry's proposal that the Swedish Defence Materiel Administration (FMV), in consultation and collaboration with other authorities, should be given the task of developing the forms for a common threat, vulnerability and risk assessment at national level entails

[1] The expanded powers correspond in substance to what is proposed to apply (Govt Bill 2021/21:194) for supervisory authorities when operators acquire and transfer ownership of security-sensitive activities. However, with regard to requirements on the operator, especially far-reaching security requirements are justified in particular in connection with the deployment of, and substantial changes in, information systems which may process classified information.

certain costs. Due to these costs, FMV's appropriations should be increased. Any costs for other authorities are assessed to be within the existing appropriations.

For the operators who will be affected by the proposals, they may entail certain administrative burdens and increased costs, particularly in respect of the expanded consultation procedure, which are assessed as being limited.

The proposals also entail certain increased administrative costs for the authorities that will be the consultation authorities (the Swedish Security Service and the Swedish Armed Forces). These costs will depend primarily on the extent to which consultations will take place and are currently difficult to estimate. However, any costs are assessed as being limited and able to be accommodated within the existing appropriation framework and the anticipated increased appropriation (see Govt Bill 2020/21:30). Furthermore, the proposals are expected to lead to an increased need for collaboration between the consultation and supervisory authorities, which may generate limited costs. These costs are assessed as being accommodated within the authorities' appropriations.

The proposal for a new power of investigation for the supervisory authorities increases the chances of effective supervision and is not considered to have any significant impact on the costs for the supervisory authorities.

The proposal that the supervisory authorities should have the right to gain access to operators' information systems may lead to the need for assistance from the Swedish Enforcement Authority on a number of occasions, but the increase is not assessed as being particularly great and is not anticipated to affect the Authority's activities more than that the consequences can be accommodated within the existing appropriation for the Authority.

The new provision on an administrative fine may also contribute to increased compliance with the regulations and more effective supervision, and to a limited extent increase the number of enforcement cases at the Swedish Enforcement Authority.

Furthermore, the proposals concerning appeals against the decisions of the consultation authority mean that the administrative courts may have a slightly higher influx of cases and thus more tasks. However, the Inquiry assesses that the increase in the number of cases will be limited and that the increase in costs for the courts

ought to be accommodated within the existing appropriation frameworks.

The proposals affect municipal self-government to some extent. However, the proposed regulation does not go beyond what is necessary to protect the society's most critical assets.

Even if no new criminalisation is proposed, the proposals can be assumed to have some crime prevention effects. Since the increased powers ought to facilitate the Swedish Security Service's law enforcement activities in the area of protective security, and since more stringent requirements are imposed on the deployment of, and changes in, information systems in security-sensitive activities, it is assessed that the proposals will counteract computer fraud, among other things.

Beyond what has been stated above, the Inquiry assesses that the aforementioned proposals do not concern other areas specified in section 15 of the Committees Ordinance. The proposals and assessments otherwise, including that certified ICT products, services and processes should be used by government agencies to a greater extent, are assessed to have no consequences that need to be reflected in more detail in the impact assessment.

1 Författningsförslag

1.1 Förslag till lag om ändring i säkerhetsskyddslagen (2018:585)

Härigenom föreskrivs i fråga om säkerhetsskyddslagen (2018:585)

dels att 6 kap. 3 och 4 §§, 7 kap. 9 § samt 8 kap. 4 § ska ha följande lydelse,

dels att det ska införas ett nytt kapitel, 3 a kap., och en ny paragraf, 7 kap. 2 a §, av följande lydelse.

3 a kap. Skyldigheter inför driftsättning av informationssystem

1 § Innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift, eller i väsentliga avseenden förändras, ska verksamhetsutövaren genom en särskild säkerhetsskyddsbedömning ta ställning till vilka säkerhetskrav i informationssystemet som är motiverade och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses.

Med utgångspunkt i den särskilda säkerhetsskyddsbedömningen och övriga omständigheter ska verksamhetsutövaren pröva om driftsättningen eller förändringen av informationssystemet är lämplig från säkerhetsskyddssynpunkt. Verksamhetsutövaren ska också samråda enligt 2 §.

Den särskilda säkerhetsskyddsbedömningen och lämplighetsprövningen ska dokumenteras.

Om lämplighetsprövningen leder till bedömningen att det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt, får det inte inledas.

2 § Om lämplighetsprövningen enligt 1 § leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt, ska verksamhetsutövaren samråda med den myndighet som regeringen bestämmer (samrådsmyndigheten), innan ett informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre tas i drift, eller i väsentliga avseenden förändras.

Samrådsskyldigheten gäller även i fråga om andra informationssystem än sådana som anges i första stycket, om obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är obetydlig.

Samrådsmyndigheten får besluta att förelägga verksamhetsutövaren att vidta åtgärder enligt denna lag och föreskrifter som har meddelats i anslutning till lagen.

3 § Om verksamhetsutövaren inte samråder med samrådsmyndigheten trots att det finns en skyldighet att göra det, får samrådsmyndigheten inleda samrådet.

4 § Ett informationssystem som ska användas i säkerhetskänslig verksamhet får inte tas i drift förrän det har godkänts från säkerhetsskyddssynpunkt av verksamhetsutövaren. Godkännandet ska dokumenteras.

5 § Om ett beslut om föreläggande enligt 2 § inte följs eller om det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt även om ytterligare åtgärder vidtas, får samrådsmyndigheten besluta att driftsättningen eller förändringen av informationssystemet inte får genomföras (förbud).

Lydelse enligt proposition 2020/21:194	*Föreslagen lydelse*
6 kap.	
3 §	
Tillsynsmyndigheten har i den omfattning som det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra ut-	Tillsynsmyndigheten har i den omfattning som det behövs för tillsynen rätt att få *tillgång till informationssystem och* tillträde

rymmen, dock inte bostäder, som används i verksamhet som omfattas av tillsyn.	till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamhet som omfattas av tillsyn.
4 §	
Tillsynsmyndigheten får besluta att förelägga den som står under tillsyn att tillhandahålla information och ge tillträde enligt 2 och 3 §§. Ett sådant beslut om föreläggande får förenas med vite.	Tillsynsmyndigheten får besluta att förelägga den som står under tillsyn att tillhandahålla information och ge *tillgång eller* tillträde enligt 2 och 3 §§. Ett sådant beslut om föreläggande får förenas med vite.

7 kap.

2 a §

Samrådsmyndigheten får besluta att ta ut en sanktionsavgift av en verksamhetsutövare som

1. har åsidosatt sin skyldighet enligt 3 a kap. 2 § första och andra stycket,

2. har driftsatt eller förändrat ett informationssystem i strid med ett förbud som har meddelats med stöd av 3 a kap. 5 §, eller

3. har lämnat oriktiga uppgifter i samband med samråd enligt 3 a kap. 2 §.

9 §	
En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.	En sanktionsavgift ska betalas till *samråds- eller* tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

En sanktionsavgift tillfaller staten.

8 kap.

4 §

Beslut om föreläggande enligt 4 kap. 9 och 15 §§ och 6 kap. 4 och 6 §§ eller sanktionsavgift enligt 7 kap. 1 och 2 §§ får överklagas till Förvaltningsrätten i Stockholm. När ett sådant beslut överklagas är tillsynsmyndigheten motpart. Prövningstillstånd krävs vid överklagande till kammarrätten.	Beslut om föreläggande enligt *3 a* kap. *2 §*, 4 kap. 9 och 15 §§ och 6 kap. 4 och 6 §§ eller sanktionsavgift enligt 7 kap. 1, 2 *och 2 a* §§ *eller beslut om förbud enligt 3 a kap. 5 §* får överklagas till Förvaltningsrätten i Stockholm. När ett sådant beslut överklagas är *samråds- eller* tillsynsmyndigheten motpart. Prövningstillstånd krävs vid överklagande till kammarrätten.

Beslut om förbud enligt 4 kap. 11, 17 och 18 §§ och föreläggande enligt 4 kap. 12 och 19 §§ får överklagas till regeringen.

Andra beslut enligt denna lag får inte överklagas.

---

1. Denna lag träder i kraft den 1 juli 2022.

2. Äldre föreskrifter gäller fortfarande för ärenden om samråd som har inletts före ikraftträdandet.

3. En sanktionsavgift enligt 7 kap. 2 a § får beslutas endast för överträdelser som skett efter ikraftträdandet.

1.2 Förslag till förordning om ändring i säkerhetsskyddsförordningen (2018:658)

Härigenom föreskrivs i fråga om säkerhetsskyddsförordningen (2018:658)

dels att 3 kap. 1 § ska ha följande lydelse,

dels att 3 kap. 2 och 3 §§ ska upphöra att gälla.

Nuvarande lydelse	*Föreslagen lydelse*
3 kap.	
1 §	
Innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift ska verksamhetsutövaren genom en särskild säkerhetsskyddsbedömning ta ställning till vilka säkerhetskrav i systemet som är motiverade och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses. Säkerhetsskyddsbedömningen ska dokumenteras.	*Säkerhetspolisen och Försvarsmakten är samrådsmyndigheter enligt säkerhetsskyddslagen (2018:585) inom sina respektive tillsynsområden.*

Denna förordning träder i kraft den 1 juli 2022.

2 Uppdraget

2.1 Inledning

Cybersäkerhetsutredningens uppdrag består av två delar, dels att analysera och lämna förslag på kompletterande nationella bestämmelser till EU: cybersäkerhetsakt, dels överväga om det finns behov av att stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet.

Uppdragets första del har fullgjorts i och med att delbetänkandet *EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering* (SOU 2020:58) överlämnades till statsrådet Peter Hultqvist, Försvarsdepartementet, i september 2020.

I detta slutbetänkande behandlas uppdragets andra del, dvs. överväganden och förslag när det gäller frågan om det finns behov av att stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet.

2.2 Bakgrund

Digitaliseringen beskrivs som vår tids starkaste förändringsfaktor och innebär att en allt större andel av aktiviteterna i samhället är beroende av nätverks- och informationssystem som används av myndigheter, organisationer, företag och privatpersoner. Den digitala utvecklingen ger stora möjligheter att förbättra och effektivisera människors vardag och olika verksamheter. Digitaliseringen har skapat nya former av kommunikation, datahantering och datalagring. I dag bygger många system för att hantera information huvudsakligen på digital informations- och kommunikationsteknologi (IKT).

Med den tilltagande digitaliseringen och globaliseringen, som ökar beroenden över nations-, sektors- och ansvarsgränser, har följt en ökad betoning på cyberfrågor i samhället. Informations- och cyber-

säkerhetsarbete, av såväl offentliga som privata aktörer, ses som nödvändigt vid digitaliseringsprocesser för att samhället ska kunna fungera och utvecklas i linje med de mål som finns inom olika politikområden.

Samtidigt som allt fler länder utvecklar strategier, doktriner och förmågor inom cyberområdet ökar förekomsten av cyberattacker mot olika intressen och verksamheter. Hoten kan utgöras av politiskt, ekonomiskt och brottsligt motiverade angrepp, men även oavsiktliga incidenter som påverkar cybersäkerheten ökar. Den kraftiga tillväxten av bl.a. sakernas internet (IoT), molnet (cloud) och stordata (Big Data) medför större utsatthet för säkerhetsbrister.

Cyberangrepp och -incidenter kan störa tillhandahållandet av nödvändiga tjänster som elektricitet, vatten, hälso- och sjukvård, mobila tjänster, m.m. Möjligheterna till påverkan i nätverks- och informationssystem i demokratiska valprocesser och desinformationskampanjer är också en utmaning. Genom att samhället och människorna blir alltmer beroende av digital infrastruktur och tjänster genom anslutna enheter och utbredd uppkoppling till internet ökar sårbarheten mot cyberattacker till alltmer oroande nivåer. Vidare finns en ökad hotbild avseende antagonistiska aktörer med hög förmåga till cyberattacker. Vikten av fullgod informations- och cybersäkerhet ökar därför i motsvarande grad.

Det europeiska ramverket för cybersäkerhetscertifiering

EU har antagit ett antal strategier, policys och förordningar för att stärka cybersäkerheten i unionen och medlemsstaterna.[1] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) trädde i kraft den 27 juni 2019. Förordningen började tillämpas direkt med undantag för vissa artiklar som kräver kompletterande bestämmelser på nationell nivå och som därför ska börja tillämpas den 28 juni 2021. Det huvudsakliga syftet med förordningen är att

[1] En närmare redogörelse för EU:s strategier och policy finns i utredningens delbetänkande *EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering* (SOU 2020:58).

uppnå en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen och säkerställa en väl fungerande inre marknad.

EU:s ramverk för cybersäkerhetscertifiering, dvs. EU:s cybersäkerhetsakt och de genomförandeakter som utfärdas med stöd av cybersäkerhetsakten, kommer att reglera den cybersäkerhetscertifiering som följer av en europeisk certifieringsordning för cybersäkerhetscertifiering som fastställts av kommissionen. Cybersäkerhetsakten är en EU-förordning vars bestämmelser har direkt effekt och tillämpning i medlemsstaten samt ger utrymme för medlemsstaten att besluta om kompletterande nationell lagstiftning och annan författningsreglering.

Utgångspunkten kommer att vara att certifieringen även i framtiden ska vara frivillig, oavsett om en europeisk ordning för cybersäkerhetscertifiering finns på plats eller inte. Detta är dock upp till varje medlemsstat att bestämma. Den största skillnaden är att när en sådan europeisk ordning för cybersäkerhetscertifiering finns på plats, får inte längre nationella cybersäkerhetscertifieringar utföras inom det område som täcks av den europeiska ordningen för cybersäkerhetscertifiering. Förordningen innebär också att när en europeisk ordning för cybersäkerhetscertifiering ska användas reglerar förordningen vilka krav som ställs på certifieringen, certifieringsorganen och de leverantörer och producenter som innehar ett sådant certifikat.

Utredningens uppdrag i den första delen har varit att föreslå de anpassningar och kompletterande nationella författningsbestämmelser som EU:s cybersäkerhetsakt ger anledning till och som behöver finnas på plats när hela förordningen i sin helhet börjar tillämpas den 28 juni 2021. I uppdraget har ingått att överväga och föreslå vilken befintlig nationell myndighet som ska utses att fullgöra de uppgifter och tilldelas de ansvarsområden som följer av EU:s cybersäkerhetsakt, bl.a. uppdraget att utöva tillsyn över efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering. Det har även ingått att undersöka vilka kompletterande nationella bestämmelser, bl.a. processuella bestämmelser och bestämmelser om sanktioner, som förordningen kräver eller som det annars finns anledning att införa.

Regeringen har efter remissbehandling av utredningens delbetänkande i proposition 2020/21:186 *Kompletterande bestämmelser till EU:s cybersäkerhetsakt* lämnat förslag på en ny lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt. I den föreslagna lagen finns kompletterande bestämmelser till EU:s cybersäkerhetsakt, bl.a.

om nationell myndighet för cybersäkerhetscertifiering, vissa handläggningsregler vid cybersäkerhetscertifiering, tillsyn och sanktioner. Den nya lagen föreslås träda i kraft den 28 juni 2021. Riksdagen har den 9 juni 2021 beslutat i enlighet med vad som föreslås i propositionen.

2.3 Uppdragets andra del

I utredningsdirektivet konstateras att åtgärder för att skydda nationell säkerhet faller utanför EU:s kompetens (art. 4.2 EU-fördraget). I artikel 1.2 i EU:s cybersäkerhetsakt anges också att förordningen inte ska påverka medlemsstaternas befogenheter i fråga om nät- och informationssäkerhet, särskilt inte verksamhet som bl.a. berör allmän säkerhet och försvar. Samtidigt framhålls i direktivet att särskilda krav på säkerhet måste kunna ställas på nät- och informationssystem för att skydda *nationell säkerhet*. Säkerhetsskyddslagen (2018:585) gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet).

För nätverks- och informationssystem som används i eller har betydelse för säkerhetskänslig verksamhet finns särskilda krav i säkerhetsskyddsförordningen (2018:658). Det rör sig bl.a. om förberedande åtgärder inför driftsättning av nätverks- och informationssystem och om säkerhetskrav som kontinuerligt ställs på dessa system. Bestämmelserna innehåller även krav på samråd med Säkerhetspolisen eller Försvarsmakten i vissa fall. Detta gäller för nätverks- och informationssystem som kan komma att behandla säkerhetsskyddsklassificerade uppgifter av visst slag och informationssystem där obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är obetydlig. Bestämmelserna innebär att det är verksamhetsutövaren som ansvarar för att se till att nätverks- och informationssystemen upprätthåller kraven på informationssäkerhet.

Enligt direktivet finns det anledning att nu överväga om ytterligare krav bör införas för att säkerställa att nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet uppfyller de krav som behövs för att upprätthålla skyddet av sådana verksamheter. En möjlighet kan vara – enligt direktivet – att införa krav på att IKT-produkter, -tjänster och -processer i nätverks- och informations-

system som ska användas i säkerhetskänslig verksamhet ska vara certifierade enligt särskilda certifieringsordningar som ställer krav anpassade för användning i säkerhetskänslig verksamhet. En kompletterande eller alternativ möjlighet är att införa krav på godkännande från en utpekad myndighet innan en sådan produkt, tjänst eller process tas i drift i säkerhetskänslig verksamhet.

Utredningen ska enligt direktivet därför:

- bedöma om det finns anledning att införa särskilda krav på att IKT-produkter, -tjänster och -processer som ingår i ett nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet, ska vara certifierade enligt särskilda certifieringsordningar utformade för säkerhetskänslig verksamhet,
- överväga om det finns anledning att införa krav på godkännande från en myndighet för att sådana produkter, tjänster och processer ska få tas i drift i viss eller all säkerhetskänslig verksamhet,
- göra en internationell jämförelse av andra länders lagstiftning som ställer särskilda krav med anledning av nationell säkerhet på IKT-produkter, -tjänster och -processer som ingår i ett nätverks- och informationssystem,
- lämna förslag, förenliga med EU-rätten, på hur ett sådant regelverk skulle kunna se ut, inklusive vilken eller vilka myndigheter som skulle ansvara för uppgiften och vilka sanktioner en sådan reglering bör förenas med,
- lämna nödvändiga författningsförslag som behövs och är lämpliga.

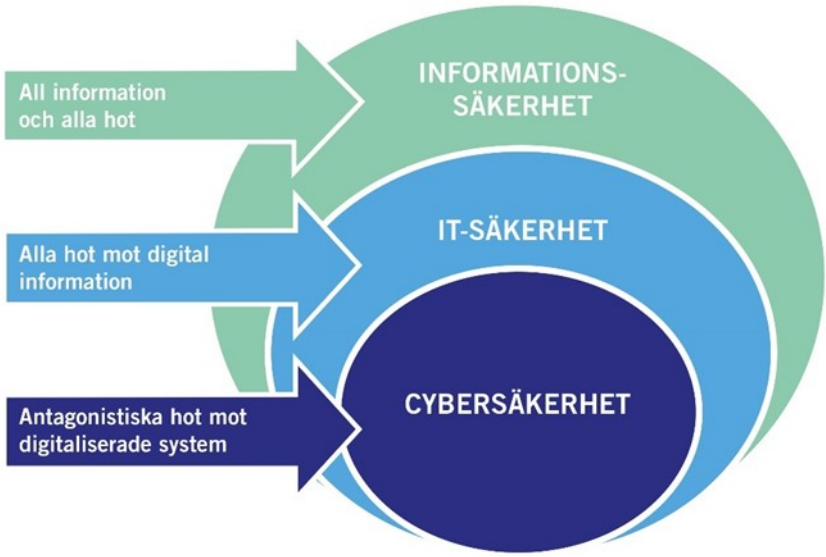
Utredningen ska enligt direktiven i denna del att förhålla sig till betänkandet *Kompletteringar till den nya säkerhetsskyddslagen* (SOU 2018:82) som förberetts i Regeringskansliet. Regeringen har efter remissbehandling av betänkandet i proposition 2020/21:194 *Ett starkare skydd för Sveriges säkerhet* föreslagit ett flertal ändringar i säkerhetsskyddslagen (2018:585).[2]

[2] Se vidare kapitel 8 och 13.

2.4 Definitioner

Utredningen behandlar frågor och verksamheter som rör begrepp som digitalisering, cyber, informations- och cybersäkerhet, m.m. Begrepp som informationssäkerhet, it-säkerhet och cybersäkerhet förekommer i många olika sammanhang, såväl nationellt som internationellt.

Figur 2.1 Av figuren framgår hur begreppen cybersäkerhet, it-säkerhet och informationssäkerhet förhåller sig till varandra



Som framgår av delbetänkandet förekommer begreppen i såväl olika författningar som i nationella styrdokument, handlingsplaner och allmänna råd. Att begreppen används med delvis olika betydelse i olika sammanhang kan ge upphov till begreppsförvirring om vad som egentligen avses med begreppet i det sammanhang det används. Det finns skäl för att begreppen – som utredningen tidigare framhållit i delbetänkandet – i största möjliga utsträckning bör ges samma betydelse när det tillämpas nationellt och internationellt, särskilt när det gäller det europeiska samarbetet. Det kan i detta sammanhang noteras att EU:s cybersäkerhetsakt, som är en unionsrättslig författning som är direkt tillämplig i medlemsstaterna, innehåller definitioner av de

olika begrepp som förekommer i akten, bl.a. cybersäkerhet[3] och nätverks- och informationssystem[4]. Eftersom cybersäkerhetsakten är direkt tillämplig på nationell nivå bör i akten förekommande begrepp och deras innebörd i största möjliga utsträckning användas även i frågor och på områden som formellt inte omfattas av aktens tillämpningsområde, om det inte finns skäl att använda ett annat begrepp eller ge det ett annat innehåll. Det kan då finnas skäl att begrepp kan behöva anpassas till nationella förhållanden. Ett exempel på begrepp som används i nationell reglering är begreppet *informationssystem* i säkerhetsskyddsförordningen, med vilket avses ett system av sammansatt mjuk- och hårdvara som behandlar information[5]. I det europeiska ramverket för cybersäkerhetscertifiering respektive i NIS-direktivet används begreppet *nätverks- och informationssystem*.

I betänkandet används ett antal begrepp som är centrala för utredningens arbete. Några av begreppen har definierats i författning eller andra styrdokument medan andra saknar legaldefinition. Begrepp som *certifiering*, *informationssystem*, *nätverks- och informationssystem* samt *säkerhetskänslig verksamhet* förekommer i olika författningar med angivande av kriterier för begreppen. Andra begrepp, bl.a. *godkännande*, *driftsättas*, *nät- och informationssäkerhet* samt *nationell säkerhet*, saknar i många fall dock tydliga och fastlagda definitioner varför de används med den betydelse som framgår av det sammanhang som de används i betänkandet.

2.5 Uppdragets omfattning

Enligt direktivet ska utredningen analysera behovet av *stärkt säkerhet* i *nätverks- och informationssystem* i *säkerhetskänslig verksamhet*, t.ex. överväga om ytterligare krav bör införas för att säkerställa att nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet uppfyller de krav som behövs för att upprätthålla skyddet av sådana verksamheter. Som ovan framgår kan en åtgärd vara att införa krav på att *IKT-produkter*, *tjänster* och *processer* i *nätverks- och informationssystem* som ska användas i *säkerhetskänslig verksamhet* ska vara *certifierade* enligt särskilda certifieringsordningar som ställer

[3] All verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.
[4] Ett nätverks- och informationssystem enligt definitionen i artikel 4.1 i direktiv (EU) 2016/1148.
[5] 5 § säkerhetsskyddsförordningen (2018:658).

krav anpassade för användning i säkerhetskänslig verksamhet. En annan möjlighet är att införa *krav på godkännande* från en utpekad myndighet innan en sådan *produkt, tjänst* eller *process* tas *i drift* i säkerhetskänslig verksamhet.

Säkerhet i nätverks- och informationssystem

Utredningen kan konstatera att *säkerhet* i nätverks- och informationssystem, oavsett om dessa finns i verksamheter som är säkerhetskänsliga eller i annan typ av samhällsviktig verksamhet, inte endast berör säkerhet i tekniska funktioner utan graden av säkerhet definieras även av bl.a. om och hur ett systematiskt informationssystemsäkerhetsarbete bedrivs av verksamhetsutövaren och graden och omfattningen av it-säkerhetsåtgärder som verksamhetsutövaren vidtagit eller vidtar för att skydda nätverks- och informationssystemen i sin verksamhet.

Det *systematiska informationssäkerhetsarbetet* omfattar organisation, styrning, administration, tekniska åtgärder, resurstilldelning, uppföljning, m.m. Av stor betydelse för säkerhet i nätverks- och informationssystem är – utöver att alla de åtgärder vidtagits som omfattas av ett systematiskt informationssäkerhetsarbete – att dessa även är skyddade genom olika *tekniska åtgärder* som säkerställer konfidentialitet, riktighet och tillgänglighet i systemen. Därtill kommer att nätverks- och informationssystem i olika former av samhällsverksamheter uppställer varierande krav på organisatoriska, administrativa, och tekniska säkerhetsåtgärder för att uppnå fullgod säkerhet i den aktuella verksamheten. Säkerhet i nätverks- och informationssystem är därför beroende av både organisation, styrning, administration, resurser, mänskligt handlade och teknisk funktionalitet. Graden av säkerhet i nätverks- och informationssystem grundas således på ett antal olika förutsättningar och kriterier och för att man ska kunna anse att det föreligger en tillräcklig säkerhet i nätverks- och informationssystem i en verksamhet måste därför många olika åtgärder ha vidtagits. En analys av brister och behov av ytterligare åtgärder för att stärka säkerheten i nätverks- och informationssystem är därför såväl komplicerad som omfattande och förutsätter tillgång till ett antal olika expertresurser.

Vad som utgör säkerhetskänslig verksamhet

Som ovan framgår ska utredningen analysera behovet av att *stärka* säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet. När det gäller nätverks- och informationssystem i säkerhetskänslig verksamhet utgör skyddsföremålet inte endast sådan *information* (uppgifter) som omfattas av säkerhetsskyddsregleringen utan regleringen syftar även till att skydda *nätverks- och informationssystem i övrigt* som är av betydelse för Sveriges säkerhet, dvs. oavsett om systemen i sig innehåller säkerhetskänsliga uppgifter eller inte.

Enligt direktiven är uppdraget avgränsat till nätverks- och informationssystem i den säkerhetskänsliga verksamheten. Säkerhetskänslig verksamhet utgörs enligt säkerhetskyddsregleringen av sådan verksamhet som är av betydelse för Sveriges säkerhet. Varken säkerhetsskyddslagen eller den till lagen anslutande säkerhetsskyddsförordningen innehåller någon legaldefinition av vad som avses med verksamhet av betydelse för Sveriges säkerhet. I lagmotiven till säkerhetsskyddslagen, och i den utredning som låg till grund för propositionen med förslag om ny säkerhetsskyddslag kan viss vägledning fås i frågan om vilken samhällsverksamhet som kan anses ha betydelse för Sveriges säkerhet och därför utgör säkerhetskänslig verksamhet enligt den angivna regleringen. I lagmotiven framhålls att utöver verksamhet inom det militära försvaret är även civil samhällsverksamhet av betydelse för Sveriges säkerhet, t.ex. verksamhet som berör statsledningen, energiområdet, kommunikationer, rättsväsendet, m.m. Även viss verksamhet inom näringslivet kan vara av betydelse för Sveriges säkerhet och bedöms som säkerhetskänslig verksamhet. Samtidigt framhålls att det endast är sådan verksamhet som är särskild skyddsvärd som ska omfattas av regleringen, även om samhällsutvecklingen över tiden kan komma att påverka omfattningen av vilken verksamhet som ska bedömas var av betydelse för Sveriges säkerhet.

Utredningen kan konstatera att i begreppet säkerhetskänslig verksamhet ligger utöver verksamhet på det militära området även en omfattande civil samhällsverksamhet och då särskilt många verksamheter inom det civila försvaret som, i vart fall i dagsläget, inte är helt enkel att avgränsa från annan verksamhet som inte utgör säkerhetskänslig verksamhet. Som framgår nedan pågår en uppbyggnad och utveckling av bl.a. det civila försvaret inom ramen för totalförsvaret

och det fortsatta arbetet på området kan i framtiden komma att tydliggöra den närmare avgränsningen.

2.6 Utredningsarbetet

Arbetet i denna del av uppdraget inleddes i oktober 2020. Utredningen har inledningsvis inhämtat underlag i form av offentliga utredningar, propositioner, faktapromemorior, nationella strategier, olika studier m.m.

Utredningen har haft tre utredningssammanträden med sakkunniga och experter. Möjligheten till sedvanliga sammanträden med sakkunniga och experter närvarande har begränsats av rådande omständigheter och begränsningar i förutsättningarna att hålla digitala möten för att behandla frågor som rör säkerhetskänslig verksamhet. Utredningen har dock varit angelägen om att – där det varit möjligt – ha en öppen dialog och samverka med myndigheter och andra aktörer/intressenter som på olika sätt har bedömts beröras av och ha intresse av utredningens arbete. Utredningen har därför när så förutsättningar förelegat fortlöpande haft möten (digitala) och kontakter med olika företrädare för myndigheter och olika aktörer. Syftet har varit att både informera om utredningens arbete och att inhämta synpunkter.

Utredningen har som stöd i arbetet haft flera kontakter med företrädare för vissa närmare berörda myndigheter, bl.a. Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap, Post- och telestyrelsen och Säkerhetspolisen. Sekretariatet har haft enskilda möten med experter i utredningen i syfte att inhämta fördjupad kunskap inom vissa av de sakområden som behandlas i uppdraget samt haft möten (digitala) med privata aktörer med en nära koppling till området.

Utredningen har också inhämtat underlag om informations- och cybersäkerhetsverksamhet i andra länder som bedömts vara av intresse för utredningen.

Utredningen har i enlighet med direktiven hållit sig informerad om arbetet i Regeringskansliet med betänkandet *Kompletteringar till den nya säkerhetsskyddslagen* (SOU 2018:82).

Utredningen har samverkat med *It-driftsutredningen* (SOU 2021:1) i frågor som har beröringspunkter med bl.a. säkerhet i nätverks- och informationssystem.

Utredningen har även hållit sig uppdaterad om *Utredningen om civilt försvar* (Ju 2018:05) som under våren 2021 lämnat slutbetänkandet *Struktur för ökad motståndskraft* (SOU 2021:25).

Utredningen har också hållit sig underrättad om utvecklingen av cybersäkerhet i EU, bl.a. vad gäller arbetet med att ta fram genomförandeakter med stöd av EU:s cybersäkerhetsakt och arbetet med NIS2-direktivet.

Utredningen har löpande hållit företrädare för Försvarsdepartementet respektive Justitiedepartementet informerade om utredningsarbetet.

Det har funnits begränsningar, bl.a. av sekretesskäl, att kunna ta in ett tillräckligt detaljerat underlag från berörda verksamhetsutövare av säkerhetskänslig verksamhet. Det har påverkat förutsättningarna för att i grunden kunna analysera behovet av att kunna stärka säkerheten i nätverks- och informationssystem på området som är betydelse för utredningsfrågorna. Härtill kommer att verksamhet som bedöms vara säkerhetskänslig och därför omfattas av regleringen om säkerhetsskydd naturligen även omfattas av sekretess i stora delar, vilket också påverkar uppdraget med att analysera behovet av att stärka säkerheten i nätverks- och informationssystem i sådan verksamhet.

Utredningen har initialt i utredningsarbetet noterat förekomsten av ett relativt stort antal offentliga utredningar och rapporter som antingen haft som uppdrag att analysera frågor som berör nätverks- och informationssäkerheten hos framför allt offentliga aktörer i form av myndigheter, regioner och kommuner eller som annars inom ramen för sitt uppdrag berört dessa frågor. Det föreligger även rapporter som behandlar nätverks- och informationssäkerheten i näringslivet (kapitel 8 Det kan noteras att utöver de brister som kan observeras i mer allmänna termer och som till stor del grundas på öppna källor, bl.a. offentliga utredningar och myndigheters rapporter, omfattas uppgifter om förekommande brister i nätverks- och informationssystem i säkerhetskänslig verksamhet av sekretess, i vissa fall av kvalificerad sekretess.

Utredningen gör bedömningen att en sammanställning av offentliga utredningar och rapporter som behandlar nätverks- och informationssäkerheten i samhället ger förutsättningar att kunna få en

översiktlig och samlad bild av nivån på och omfattningen av säkerheten i nätverks- och informationssystem allmänt hos berörda aktörer, men även i begränsad utsträckning vad gäller säkerheten i nätverks- och informationssystem hos verksamhetsutövare som bedriver säkerhetskänslig verksamhet.

Utredningens analys av brister och behovet av att stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet grundas därför till stor del på offentliga utredningar och rapporter på området samt under utredningstiden inhämtade uppgifter från ett begränsat antal berörda verksamhetsutövare i förening med synpunkter som lämnats av utredningens sakkunniga och experter.

2.7 Betänkandets disposition

I kapitel 1 lämnas författningsförslag.

I detta kapitel (2) presenteras uppdraget, definitioner, uppdragets omfattning och avgränsningar, utredningsarbetets genomförande samt betänkandets utformning.

I kapitel 3 redogörs för mer centrala utgångspunkter som ligger till grund för utredningsarbetet.

I kapitel 4 behandlas mer allmänna frågor om digitalisering och informations- och cybersäkerhet.

I kapitel 5 redogörs för utvecklingen av hot, sårbarhet och risker inom informations- och cybersäkerhet.

I kapitel 6 behandlas vissa frågor om regleringen av säkerhetsskydd i säkerhetskänslig verksamhet.

I kapitel 7 lämnas en närmare beskrivning av begreppet informationssäkerhet i säkerhetskänslig verksamhet.

I kapitel 8 lämnas en översiktlig redogörelse för offentliga utredningar och rapporter som berör informations- och cybersäkerhet.

I kapitel 9 redogörs översiktligt för regelsystem om informations- och cybersäkerhet i några andra länder.

Del två av betänkandet innehåller utredningens överväganden och förslag (se nedan).

I kapitel 10 lämnas en redogörelse för utredningens allmänna överväganden om digitaliseringen och behoven av ökad säkerhet i nätverks- och informationssystem.

I kapitel 11 redogörs närmare för utredningens överväganden om behovet av att stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet.

I kapitel 12 behandlas frågan om behov av en nationell särskilt anpassad certifieringsordning för certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet.

I kapitel 13 analyseras behovet av krav på myndighetsgodkännande inför driftsättning av IKT-produkter, -tjänster och -processer inom nätverks- och informationssystem i säkerhetskänslig verksamhet, dvs. system som hanterar säkerhetsskyddsklassificerade uppgifter av visst slag eller som i övrigt är av betydelse för Sveriges säkerhet.

I kapitel 14 behandlas frågan om tillgång till nätverks- och informationssystem i samband med tillsyn.

I kapitel 15 behandlas vissa processuella frågor om handläggningsregler och överklagande av beslut.

I kapitel 16 behandlas frågor om sekretess.

I kapitel 17 lämnas en konsekvensbeskrivning.

I kapitel 18 finns författningskommentarer.

Bilagorna 1–3 innehåller kommittédirektiven. I bilaga 4 återfinns utredningens formella skrivelse med frågor till myndigheter i andra länder.

3 Utgångspunkter

3.1 Inledning

I detta kapitel tar utredningen upp några av de utgångspunkter som bör beaktas i den fortsatta analysen av behovet av att stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet. Frågan om ökad informations- och cybersäkerhet behandlas i många olika sammanhang, bl.a. i frågor som rör den mer generella utvecklingen av digitaliseringen inom olika samhällsområden. Flera av dessa samhällsområden innefattar verksamheter som bedöms vara säkerhetskänsliga eller som rör samhällsviktiga och digitala tjänster och som är beroende av säkerhet i nätverk och informationssystem i verksamheten.

Riksdagen och regeringen har också i olika styrdokument och beslut understrukit vikten av informations- och cybersäkerhet i samhället allmänt och särskilt i totalförsvarets verksamhet, bl.a. i den säkerhetskänsliga verksamheten, men även i andra viktiga samhällsverksamheter.

En utgångspunkt är regeringens beslut om att inrätta ett nationellt cybersäkerhetscenter och de olika myndighetsuppgifter som följer av beslutet. Berörda myndigheter har även tagit fram samlad informations- och cybersäkerhetsplan med beskrivning av olika åtgärder som ska genomföras för att bl.a. stärka informations- och cybersäkerheten i samhället.

Ytterligare en utgångspunkt är de olika författningar som berör informations- och cybersäkerhetsområdet samt offentliga utredningar och myndighetsrapporter som behandlar frågor om informations- och cybersäkerhet på olika områden.

En annan utgångspunkt är utvecklingen av EU:s ramverk för cybersäkerhetscertifiering och regleringen av samhällsviktiga och digitala

tjänster (NIS-direktivet) samt förslaget till reviderat NIS-direktiv, s.k. NIS2-direktivet.

3.2 Informations- och cybersäkerhet i olika styrdokument

Frågor som rör behovet av stärkt informations- och cybersäkerhet i olika samhällsverksamheter behandlas bl.a. i 2020 års försvarsbeslut för perioden 2021–2025[1], den nationella säkerhetsstrategin,[2] den nationella strategin för samhällets informations- och cybersäkerhet[3] samt den nationella digitaliseringsstrategin[4].

3.2.1 Försvarsbeslutet för perioden 2021–2025

Regeringens försvarspolitiska proposition (prop. 2020/21:30) *Totalförsvar 2021–2025* behandlar, inom ramen för förslag om övergripande mål för totalförsvaret och nya mål för det militära respektive civila försvaret, behovet av stärkt informations- och cybersäkerhet. Verksamhetsområdet totalförsvar omfattar den verksamhet som är nödvändig för att förbereda Sverige för krig. I propositionen anges att det civila försvaret ska ha förmåga att bl.a. säkerställa de viktigaste samhällsfunktionerna, upprätthålla en nödvändig försörjning, bidra till det militära försvarets förmåga vid väpnat angrepp eller krig i vår omvärld, upprätthålla samhällets motståndskraft mot externa påtryckningar och bidra till att stärka försvarsviljan. Det ska även bidra till att stärka samhällets förmåga att förebygga och hantera svåra påfrestningar på samhället i fred. Vidare anges att genomförandet av den försvarspolitiska inriktningen är ett ansvar för hela samhället, och en fråga som berör samtliga politikområden. Utvecklingen av det civila försvaret kommer att förutsätta åtgärder från många aktörer, bl.a. statliga myndigheter, regioner och kommuner, näringsliv, frivilligorganisationer och enskilda individer. Vidare förutsätter den föreslagna utvecklingen mot en ökad militär förmåga att det civila försvaret har förmåga att ge stöd till Försvarsmakten i händelse av

[1] Prop. 2020/21:30, bet. 2020/21:FöU4, rskr. 2020/21:136.
[2] *Nationell säkerhetsstrategi*, Statsrådsberedningen, januari 2017.
[3] *Nationell strategi för samhällets informations- och cybersäkerhet,* Skr. 2016/17:213.
[4] Regeringens skrivelse 2017/18:47 *Hur Sverige blir bäst i världen på att använda digitaliseringens möjligheter – en skrivelse om politikens inriktning.*

höjd beredskap. I propositionen betonas bl.a. att Sveriges cyberförsvarsförmåga ska stärkas ytterligare och att det systematiska arbetet med informations- och cybersäkerhet behöver stärkas ytterligare hos alla aktörer inom totalförsvaret. Investeringar för att stärka arbetet med säkerhetsskydd och cybersäkerhet ingår i satsningen.

Hotbilden inom cyberområdet

I propositionen konstaterar regeringen att den teknologiska utvecklingen, utbredningen av digitala lösningar och ökade datavolymer skapar stora möjligheter men samtidigt risker och sårbarheter för samhället i stort och för myndigheter och andra aktörer. Sårbarheter finns i alltifrån elektroniska kommunikationer, sjö- och luftfart till elnät, industriella styrsystem och i det finansiella systemet. Även den data som genereras medför i sig såväl sårbarheter som möjligheter. Många av de system som är kritiska för att upprätthålla samhällets funktionalitet är redan i fredstid sårbara för störningar. Det pågår ständigt intrångsförsök mot internetanslutna system.

I propositionen framhåller regeringen vidare att den delar Försvarsberedningens bedömning att en högre grad av nationell samordning behövs på cyberområdet. En viktig komponent i detta arbete är inrättandet av ett cybersäkerhetscenter, som ska ge konkret effekt på Sveriges förmåga att förebygga och hantera antagonistiska hot. Centret ska, i enlighet med vad regeringen redovisar i budgetpropositionen för 2021, stärka Sveriges förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige och minska sårbarheter (se nedan).

Cyberförsvar

I propositionen anges vidare att ett cyberangrepp kan inför eller under hela eller delar av en konflikt komplettera politiska, diplomatiska, ekonomiska eller militära medel. Sådana angrepp kan hota en stats handlingsfrihet och ytterst dess suveränitet. Effekterna av ett antagonistiskt cyberangrepp kan få lika stora konsekvenser för samhällsviktiga funktioner och kritiska it-system som ett konventionellt väpnat angrepp. Regeringen konstaterar att antalet statsunderstödda

cyberangrepp ökar fortlöpande och angriparnas metoder utvecklas.[5] Många stater har byggt upp avsevärda resurser i syfte att kunna verka offensivt genom cyberattacker. Förutom att dessa stater utvecklar avancerade metoder och offensiva verktyg har de skapat förmåga att slå brett mot många mål och att upprätthålla uthållighet över tid.

I propositionen framhålls att förmågan att i fredstid hantera antagonistiska hot behöver förbättras, bl.a. vad avser cyberattacker. Sårbarheter behöver minskas och verksamheter av betydelse för Sveriges säkerhet ska stärka sitt säkerhetsskydd. I detta sammanhang betonas vikten av förmågan att kunna agera samlat för att möta utmaningar och hot såväl i fred som vid höjd beredskap, bl.a. vad avser arbetet med att stärka informations- och cybersäkerheten och minska sårbarheten för att säkerställa de viktigaste samhällsfunktionerna.[6] Många av de system som är kritiska för att upprätthålla samhällets funktionalitet är redan i fredstid sårbara för störningar. Verksamheter av betydelse för Sveriges säkerhet behöver därför stärka sitt säkerhetsskydd. Det framhålls att bl.a. Svenska kraftnät, Energimyndigheten och Strålsäkerhetsmyndigheten har identifierat behov av åtgärder för att stärka cybersäkerheten.

Regeringen framhåller vidare att Sveriges cyberförsvar bidrar till att försvåra och höja tröskeln för en aktör som överväger att angripa eller utöva påtryckningar mot Sverige eller svenska intressen. Mot bakgrund av hotbilden anser regeringen,[7] att Sveriges cyberförsvarsförmåga[8] bör stärkas ytterligare inklusive förmågan att genomföra offensiva[9] och defensiva[10] operationer i cyberdomänen. Utvecklingen av offensiv och defensiv cyberförsvarsförmåga bygger på tre samverkande delar:

[5] Se även 5 kap. om hotbilder, sårbarheter och risker.
[6] I propositionen noteras att även Försvarsberedningen anser att stärkt informations- och cybersäkerhet, ökad redundans och förbättrat säkerhetsskydd är viktigt i den fortsatta utvecklingen (s. 148).
[7] Detta i likhet med Försvarsberedningens bedömning och i enlighet med vad regeringen framhåller i budgetpropositionen för 2021.
[8] *Cyberförsvar* kan definieras som en nations samlade förmågor och åtgärder, såväl defensiva som offensiva, till skydd för dess kritiska samhällsfunktioner samt förmågan att kunna försvara sig mot cyberangrepp från kvalificerade motståndare.
[9] *Offensiva* operationer syftar till att förhindra motståndaren att använda sina system eller att tvinga motståndaren att avbryta angrepp mot svenska system.
[10] *Defensiva* operationer syftar till att försvara informationssystem inklusive elektroniska kommunikationsnät för att på så sätt förhindra motståndare att påverka information, informationssystem, datorer eller nätverk.

– kunskap om hoten,
– skyddsåtgärder, och
– motåtgärder.

I propositionen framhålls att Försvarsmakten ansvarar för Sveriges offensiva cyberförsvarsförmåga. Cyberdomänen är en av flera domäner där myndigheten ska kunna möta ett antagonistiskt hot med stöd av andra myndigheter, t.ex. Försvarets radioanstalt (FRA) och övriga försvarsunderrättelsemyndigheter, Säkerhetspolisen och Myndigheten för samhällsskydd och beredskap (MSB). Det systematiska arbetet med informations- och cybersäkerhet behöver dock stärkas ytterligare hos aktörer inom totalförsvaret.[11] Det finns ett betydande värde av samarbetet mellan FRA, Försvarsmakten och Säkerhetspolisen om utvecklat skydd för de mest skyddsvärda verksamheterna i Sverige mot de allvarligaste hoten. Det finns även skäl att överväga om kvalificerat stöd bör kunna lämnas även till enskilda verksamheter som är att anse som särskilt skyddsvärda.

Regeringen konstaterar vidare att kvalificerad personal krävs för att långsiktigt kompetensförsörja och stärka både den offensiva och defensiva cyberförsvarsförmågan. Vidare krävs till följd av den snabba teknikutvecklingen kontinuerlig forskning och utveckling för att bidra till vidmakthållande och utveckling av cyberförsvarsförmågan.

I propositionen betonar regeringen att en förutsättning för ett starkt cyberförsvar är, i enlighet med vad regeringen även framhåller i budgetpropositionen för 2021, att samtliga aktörer inom totalförsvaret har en god informations- och cybersäkerhet. Det systematiska arbetet med informations- och cybersäkerhet behöver stärkas ytterligare hos dessa aktörer.[12] För att säkerställa en hög informations- och cybersäkerhet i totalförsvaret är det nödvändigt att informations- och cybersäkerhetsperspektivet beaktas redan i anskaffningsfasen av exempelvis nätverk och it-system.

Regeringen, liksom Försvarsberedningen, understryker vikten av det förebyggande arbetet och av att öka medvetenheten såväl som

[11] Den cyberrelaterade hotbilden beskrivs utförligt i bl.a. Försvarsberedningens rapporter, den nationella strategin för samhällets informations- och cybersäkerhet (skr. 2016/17:213) och i flera myndigheters årsrapporter.
[12] Regeringen framhåller att en del i detta är en ökad rapportering av it-incidenter till MSB enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, liksom anmälan vid säkerhetshotande händelser och verksamhet till Säkerhetspolisen och Försvarsmakten enligt säkerhetsskyddsförordningen (2018:658).

förmågan hos alla användare av it-system för att skapa förutsättningar för utvecklingen av en säkerhetskultur i hela samhället.

Regeringen framhåller även att den delar Försvarsberedningens bedömning att en god ledningsförmåga ställer krav på att metoder och infrastruktur för säkra samband fungerar även under störda förhållanden och med beaktande av krav på sekretess. Myndigheter och organisationer med ansvar inom totalförsvaret behöver, i enlighet med vad regeringen anger i budgetpropositionen för 2021, ha tillgång till säkra och robusta kommunikationstjänster samt nätlösningar med höga säkerhetskrav som är ändamålsenliga för hantering och kommunikation av säkerhetsskyddsklassificerad information. Av särskild vikt är den it-infrastruktur som stöder verksamheten så att information kan utbytas på ett säkert och robust sätt.

3.2.2 Den nationella säkerhetsstrategin

Under 2017 antogs en nationell säkerhetsstrategi som innehåller en samlad redovisning av regeringens syn på säkerhet ur ett brett perspektiv.[13] Strategin syftar till att stärka förmågan att samordnat och effektivt förebygga och möta omedelbara och långsiktiga hot och utmaningar. I strategin anges inriktningen och den utgör ett övergripande ramverk för det arbete som krävs för att gemensamt värna Sveriges säkerhet, inom och mellan olika politikområden. I strategin noteras att förutsättningarna för säkerhetsarbetet i Sverige förändras snabbt. I ökad utsträckning påverkas Sverige av vad som sker både nationellt som internationellt. De interna och externa hot som samhället i dag möter bedöms vara mer komplexa än tidigare samt uppstår och förändras snabbare än förr. Det handlar om nya sorters hot från nya konstellationer av aktörer. Det går dock inte att förutse exakt vilka nya hot som mest sannolikt kommer att tränga sig på eller vilka strategiska vägval som Sverige kan behöva göra för att avvärja dessa. Men genom att tydligt rikta in det samlade säkerhetsarbetet mot de prioriterade områden och nationella intressen som strategin stakar ut kommer Sverige att kunna stå bättre rustat att förebygga och förhindra samt möta både dagens och morgondagens säkerhetsutmaningar.[14]

[13] *Nationell säkerhetsstrategi*, Statsrådsberedningen, januari 2017.
[14] S. 5.

Strategin tar sin utgångspunkt i ett antal brett definierade mål för säkerhet och de värden som ligger till grund för dessa mål. I strategin identifieras ett antal områden där Sverige har särskilda intressen att försvara och där det behövs ett förstärkt säkerhetsarbete. Sammantaget utgör detta kärnan i den nationella säkerhetsstrategin.

Digitala risker och informations- och cybersäkerhet

I den nationella säkerhetsstrategin framhålls att digitaliseringen påverkar alla delar av samhället. I stort sett hela samhället är i dag beroende av fungerande it-system. Det sker en ständigt växande hantering av information i elektroniska kommunikationsnät och it-system och även i industriella och andra styrsystem. It-tjänster i moderna verksamheter är ofta komplexa och utspridda. Det gäller såväl fysiskt och organisatoriskt som nationellt och globalt. Information blir i allt högre grad allmänt tillgängliga. Samtidigt som digitaliseringens fördelar välkomnas står det klart att de risker och hot som den är förknippad med är några av våra mest komplexa säkerhetsutmaningar. Detta medför att hot blir svårare att upptäcka, att riskerna blir mer svårbedömda och att beroenden blir svårare att överskåda. Exempel på sådana utmaningar är antagonistiska hot såsom informationsoperationer och elektroniska angrepp mot skyddsvärda informations- och kommunikationssystem, t.ex. i form av dataintrång, sabotage eller spionage mot bl.a. totalförsvarets verksamhet. It-angrepp för att bedöma, påverka eller störa samhällsviktiga funktioner som ett förstadium till en väpnad konflikt hör också hit. It-angrepp riskerar också att otillbörligt påverka utgången av demokratiska val. När det uppstår brister i hanteringen av information, och i synnerhet i dess säkerhet, riskerar detta att få omfattande konsekvenser både för samhället i stort och för enskilda invånares integritet. Tilliten till digitaliseringen kan äventyras.

I strategin noteras att målet för it-politiken är att Sverige ska vara bäst i världen på att utnyttja digitaliseringens möjligheter. I strategin för den samlade digitaliseringspolitiken ska ingå att hantera den sårbarhet som ofrånkomligen följer av digitaliseringen. It-system med hög driftsäkerhet och starkt skydd mot externa attacker är av mycket stor vikt för säkerheten i samhället och för möjligheterna att hantera olika krisförlopp. En god informations- och cybersäkerhet utmärks

av att samtliga aktörer känner tillit till information och dess hantering på alla nivåer i samhället. Bästa möjliga förutsättningar ska skapas för alla att ta del av, ha ansvar för och känna tillit till det digitala samhället.

I strategin anges vidare att för att bemästra utmaningarna inom informations- och cybersäkerhetsområdet är det viktigt att fortlöpande arbeta för att minska sårbarheter. Detta är en uppgift för alla aktörer i samhället. Förmågan att förebygga, identifiera och hantera it-incidenter och antagonistiska attacker behöver därtill förbättras inom alla samhällsviktiga funktioner. De mest skyddsvärda verksamheterna ska dessutom svara upp mot de krav som ställs i säkerhetsskyddslagstiftningen. Arbetet med att minska sårbarheter tar sin grund i verksamhetens risk-och sårbarhetsanalys och/eller säkerhetsanalys. En förutsättning för arbetet är en utvecklad samordning och samverkan mellan myndigheter och andra aktörer, för att identifiera vad som ska skyddas och vilka ytterligare säkerhetsåtgärder som behöver sättas in. Enligt strategin kommer genomförandet av EU-direktivet om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet) att spela stor roll. Därtill är en robust cyberförsvarsförmåga en viktig del av den samlade ansatsen att stå emot riktade angrepp och försök till påverkan.

I strategin betonas vidare att syftet med den nationella strategin för informations-och cybersäkerhet, som bl.a. bygger på NIS-direktivet, är att skapa nödvändiga förutsättningar för kapacitetsutveckling, effektiv samverkan och arbete mot en gemensam målbild för att skydda det öppna samhället mot de sårbarheter som följer i digitaliseringens spår. De utmaningar som Sverige står inför delas med flertalet andra länder. Internationellt samarbete på cyberområdet, inte minst inom EU-kretsen, är en viktig del av den svenska förmågan att främja säkerheten. Därtill bör arbetet med de globala dimensionerna av informations- och cybersäkerhetsfrågorna intensifieras.

3.2.3 Nationell strategi för samhällets informations- och cybersäkerhet

År 2017 antogs även den nationella strategin för samhällets informations- och cybersäkerhet.[15] De huvudsakliga syftena med den nationella strategin för samhällets informations- och cybersäkerhet är dels att höja medvetenheten och kunskapen i hela samhället dels att bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet.

I strategin pekar regeringen ut ett antal strategiska prioriteringar varav en är att säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet. Målsättningen i denna del är bl.a. att offentlig förvaltning ska ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet och bedriva ett systematiskt informationssäkerhetsarbete. För att förbättra förutsättningarna för, i första hand, statsförvaltningen att bedriva ett systematiskt informationssäkerhetsarbete på ett mer samordnat sätt uttalar regeringen att det ska finnas en nationell modell till stöd för detta arbete. Vidare ska det finnas en ändamålsenlig tillsyn som skapar förutsättningar för ökad informations- och cybersäkerhet i samhället. Regeringen framhåller att en förutsättning för att reglerna på informationssäkerhetsområdet ska få det genomslag som är avsett är att det finns en tillsyn som kan utföras på ett ändamålsenligt och effektivt sätt.

Huvudsyftet med strategin är att bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet samt att höja medvetenheten och kunskapen i hela samhället. Det övergripande ansvaret för den nationella strategin för samhällets informations- och cybersäkerhet är regeringens. Justitie- och inrikesministern är det statsråd som ansvarar för att samordna genomförande och uppföljning av strategin. Alla politikområden är i olika utsträckning berörda av informations- och cybersäkerhetsfrågorna.

Den nationella strategin för samhällets informations- och cybersäkerhet innehåller sex strategiska prioriteringar:

– säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet,
– öka säkerheten i nätverk, produkter och system,

[15] *Nationell strategi för samhällets informations- och cybersäkerhet*, Skr. 2016/17:213. Med begreppet cybersäkerhet avses i skrivelsen informationssäkerhet för digital information.

– stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter,
– öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet,
– öka kunskapen och främja kompetensutvecklingen,
– stärka det internationella samarbetet.

Under respektive prioriterat område finns ett antal målsättningar för hur regeringen ska verka inom området. I juni 2018 kompletterades strategin men en bilaga som innehåller en uppdatering om genomförandet. I bilagan beskrivs en styrningsram som definierar olika aktörers ansvar och roll vid genomförandet av strategin.

I samband med att strategin kompletterades gav regeringen Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Försvarets materielverk, Försvarsmakten, Post- och telestyrelsen, Polismyndigheten och Säkerhetspolisen ett uppdrag att för deras arbete utifrån målen i strategin ta fram en samlad handlingsplan för åren 2019–2022 (se nedan).

Inom Regeringskansliet sker viss uppföljning av arbetet med handlingsplanen och koordinering mellan departementen och arbetet leds av Justitiedepartementet.

3.2.4 Nationell digitaliseringsstrategi

Regeringen fattade 2017 även beslut om en nationell digitaliseringsstrategi.[16] Det övergripande målet i digitaliseringsstrategin är det av riksdagen beslutade målet att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter[17]. Strategin anger inriktningen för regeringens digitaliseringspolitik. Visionen är ett hållbart digitaliserat Sverige. Det övergripande målet är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. Digitalt kompetenta och trygga människor har möjlighet att driva innovation där målmedveten ledning och infrastruktur är viktiga förutsättningar. För att nå det övergripande målet innehåller strategin fem delmål om

[16] Regeringens skrivelse 2017/18:47 *Hur Sverige blir bäst i världen på att använda digitaliseringens möjligheter – en skrivelse om politikens inriktning.*
[17] Prop. 2011/12:1, utg. omr. 22, bet. 2011/12: TU1, rskr. 2011/12:87.

digital kompetens, digital trygghet, digital innovation, digital ledning och digital infrastruktur. Delmålen förklarar hur digitalisering ska kunna bidra till en positiv samhällsutveckling. Delmålen i digitaliseringsstrategin formuleras enligt följande:

- i Sverige ska alla kunna utveckla och använda sin digitala kompetens (D-kompetens),
- i Sverige ska det finnas de bästa förutsättningarna för alla att på ett säkert sätt ta del av, ta ansvar för samt ha tillit till det digitala samhället (D-trygghet),
- i Sverige ska det finnas de bästa förutsättningarna för att digitalt drivna innovationer ska utvecklas, spridas och användas (D-innovation),
- i Sverige ska relevant, målmedveten och rättssäker effektivisering och kvalitetsutveckling ske genom digitalisering (D-ledning),
- hela Sverige bör ha tillgång till infrastruktur som medger snabbt bredband och stabila mobila tjänster och som stöder digitalisering (D-infrastruktur).

Regeringen har uttalat att ett mål för digitaliseringen av den offentliga förvaltningen är en enklare vardag för medborgare, en öppnare förvaltning som stödjer innovation och delaktighet samt högre kvalitet och effektivitet i verksamheten.[18] I Sverige ska det finnas de bästa förutsättningarna för alla att på ett säkert sätt ta del av, ta ansvar för samt ha tillit till det digitala samhället. Förutom bl.a. digital kompetens är trygghet och tillgänglighet viktiga faktorer för digital delaktighet.[19]

Delmålet digital trygghet innebär att människor, företag och organisationer ska känna tillit till och förtroende i användningen av digitala tjänster och att det är enkelt att använda dem. Eftersom digitalisering förändrar samhället i grunden på fler sätt än de som tidigare kopplats ihop med teknikutveckling, ser regeringen ett behov av ett vidare trygghetsperspektiv. Utöver informationssäkerhet och personlig integritet behöver även frågor om människors och företags syn på hur samhället klarar av att hantera de risker som digitaliser-

[18] Budgetpropositionen för 2018, prop. 2017/18:1, utg.omr. 2 s. 93.
[19] www.regeringen.se/regeringens-politik/digitaliseringsstrategin/digital-trygghet/ (publicerad 2018-06-14, hämtad 2020-05-09).

ingen innebär inkluderas. Förutom bl.a. digital kompetens är trygghet och tillgänglighet viktiga faktorer för digital delaktighet. Privata och offentliga aktörer behöver agera på ett ansvarsfullt sätt. Det är angeläget att det digitala samhället genomsyras av ett demokratiskt synsätt och att alla ska känna en grundtrygghet i den digitala samhällsutvecklingen. Alla ska våga lita på digitala tjänster och både vilja och kunna bidra till användningen av dessa. Det krävs dessutom säkra digitala system, som värnar den personliga integriteten och att identifierade sårbarheter hanteras när människor och samhället i allt högre grad blir beroende av att teknik är uppkopplad och kommunicerbar via internet. Digitaliseringskommissionen har identifierat förstärkt säkerhet och integritet liksom tillit till tekniken och till samhället som viktiga frågor att hantera inom ramen för en framåtriktad digitaliseringspolitik.[20]

3.3 Det nationella cybersäkerhetscentret

Cyberhoten mot Sverige och svenska intressen är omfattande. Genom digitalisering och teknikutveckling blir hoten och sårbarheterna fler vilket gör att säkerheten behöver stärkas. I regeringsförklaringen i september 2019 aviserade regeringen att ett nationellt cybersäkerhetscenter ska inrättas 2020. Regeringen uppdrog den 26 september 2019 åt Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap och Säkerhetspolisen att tillsammans vidta förberedande åtgärder och lämna förslag för att ett nationellt cybersäkerhetscenter ska kunna inrättas under 2020. Uppdraget redovisades den 16 december 2019.

Regeringens beslutade i december 2020[21] att uppdra åt Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap och Säkerhetspolisen (myndigheterna) att fördjupa samverkan inom cybersäkerhetsområdet genom att utvecklas samarbetet inom ramen för det nationella cybersäkerhetscentret. Myndigheterna ska fortsatt ha en nära samverkan med Försvarets materielverk, Polismyndigheten och Post- och telestyrelsen som ska ges möjlighet att medverka i cybersäkerhetscentrets verksamhet. Myndigheterna ska även fortlöpande informera Regeringskansliet (Försvarsdeparte-

[20] Digitaliseringsstrategin, s. 11.
[21] Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter, Regeringsbeslut 2020-12-10, Fö2019/01330.

mentet och Justitiedepartementet) om den verksamhet som bedrivs inom cybersäkerhetscentret.[22]

Enligt regeringsbeslutet ska samverkan inom ramen för cybersäkerhetscentret inledas 2020 och utvecklas stegvis 2021–2023. Samarbetets innehåll och former ska fastställas genom skriftliga överenskommelser mellan myndigheterna. Regeringen avser att under 2023 ta ställning till hur cybersäkerhetscentrets verksamhet fortsatt bör inriktas och bedrivas efter 2023.

Närmare om uppdraget

Det övergripande målet med den fördjupade samverkan inom ramen för det nationella cybersäkerhetscentret är att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot. Samverkan med privata och offentliga aktörer ska utgöra en central del av uppdraget i syfte att stärka cybersäkerheten i samhället. Inom ramen för cybersäkerhetscentret ska myndigheterna:

– koordinera arbetet för att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter,
– förmedla råd och stöd avseende hot, sårbarheter och risker,
– utgöra en nationell plattform för samverkan och informationsutbyte med privata och offentliga aktörer inom cybersäkerhetsområdet.

Samverkan inom ramen för cybersäkerhetscentret ska utvecklas stegvis 2021–2023 inom följande områden:

– samlokalisering av relevanta förmågor från myndigheterna,
– stöd vid hanteringen av cyberangrepp och andra it-incidenter,
– upprättande av en plan för samlad hantering på nationell nivå vid allvarliga cyberangrepp,
– tillhandahållande av anpassade och aggregerade lägesbilder och analyser avseende hot, sårbarheter och risker,

[22] En gemensam redovisning av arbetet ska lämnas årligen till Regeringskansliet (Försvarsdepartementet och Justitiedepartementet) i samband med att myndigheternas årsredovisning lämnas till regeringen. Redovisningen ska innehålla såväl en verksamhetsuppföljning som en ekonomisk redovisning.

– riktade och samordnade varningar avseende hot och cyberangrepp,
– samordning av stödet till förebyggande skyddsåtgärder, exempelvis tekniska säkerhetsanalyser och kartläggning av verksamheters beredskap vid it-incidenter,
– samordning av, och utgöra kontaktpunkt för, internationella samarbeten på myndighetsnivå inom cybersäkerhetscentrets verksamhet,
– kunskaps-, kompetens- och informationsutbyte och samverkan med offentliga och privata aktörer, exempelvis avseende detektion, sårbarheter, hot, risker, analys, verktyg och metoder samt internationellt samarbete,
– dialog med aktörer inom forsknings-, kunskaps- och kompetensuppbyggnad, och
– erbjudande av kompetenshöjande insatser, exempelvis övningar och utbildningar för identifierade målgrupper.

Cybersäkerhetscentrets verksamhet ska komma till bred nationell nytta inom såväl offentlig som privat verksamhet. Vad gäller målgruppsanpassade insatser ska dessa under 2021–2023 fokusera på ett urval av prioriterade målgrupper utifrån myndigheternas respektive uppdrag. Myndigheterna som samverkar genom cybersäkerhetscentret ska bidra till verksamheten inom ramen för sina befintliga uppgifter. Den fördjupade samverkan inom cybersäkerhetscentret ska inte ta över det ansvar som ligger på de ingående myndigheterna och andra aktörer.

3.4 Samlad informations- och cybersäkerhetshandlingsplan 2020–2023

Regeringen beslutade 2018 att uppdra åt Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Försvarets materielverk, Försvarsmakten, Post- och telestyrelsen, Polismyndigheten och Säkerhetspolisen att ta fram en samlad handlingsplan för dessa myndigheters arbete utifrån målen i den nationella strategin för samhällets

informations- och cybersäkerhet (skr. 2016/17:213). Handlingsplanen ska omfatta åren 2019–2022.[23]

Av handlingsplanen ska framgå planerade åtgärder som myndigheterna enskilt eller i samverkan med andra aktörer avser att vidta för att höja informations- och cybersäkerheten i samhället. Den samlade handlingsplanen bör – enligt regeringen – syfta till att bidra till att det sker en samordning avseende myndigheternas åtgärder och aktiviteter. I framtagandet av handlingsplanen ska myndigheterna särskilt samverka bl.a. med den eller de myndigheter som utövar tillsyn med stöd av lagen om informationssäkerhet för samhällsviktiga och digitala tjänster samt Myndigheten för digital förvaltning. Myndigheterna bör även på ett systematiskt sätt inhämta idéer och råd och i övrigt samverka med andra relevanta statliga myndigheter, regioner, kommuner, Sveriges Kommuner och Regioner, företag och andra organisationer som kan bidra i arbetet. Handlingsplanen kan även omfatta planerade åtgärder inom ramen för internationella samarbeten. Enligt regeringen finns i det fortsatta arbetet ett behov av en samlad redovisning av vilka åtgärder de sju myndigheterna på eget initiativ planerar att vidta för att höja informations- och cybersäkerheten i samhället inom ramen för sina befintliga ansvarsområden de kommande åren. Med en samlad handlingsplan kommer – enligt regeringen – styrningen av de sju myndigheterna för att genomföra strategin bli mer ändamålsenlig. Uppdraget bidrar till att ge regeringen ett bättre underlag för att kunna analysera om myndigheternas planerade åtgärder är tillräckliga för att nå målsättningarna i strategin och vilka ytterligare åtgärder regeringen behöver vidta. Myndigheten för samhällsskydd och beredskap (MSB) ska vara sammanhållande för en årlig redovisning av den samlade handlingsplanen.[24]

Regeringen anger vidare att utöver uppdraget om en samlad handlingsplan avser den att återkomma med specifika uppdrag som myndigheterna ska utföra i samverkan. Ett prioriterat uppdrag är framtagandet av en nationell modell för systematiskt informationssäkerhetsarbete

[23] *Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022*, regeringsbeslut 2018-07-12, Ju2018/03737/SSK.

[24] Myndigheten för samhällsskydd och beredskap ska vara sammanhållande för en årlig redovisning till Regeringskansliet (Justitiedepartementet, Försvarsdepartementet och Näringsdepartementet) av dessa myndigheters arbete med att genomföra handlingsplanen. Den första redovisningen lämnades i mars 2020 till Regeringskansliet (Justitiedepartementet, Försvarsdepartementet och Näringsdepartementet). En redovisning ska därefter lämnas den 1 mars varje år fram till att uppdraget slutredovisas den 1 mars 2023. I samband med de årliga redovisningarna bör myndigheterna vid behov uppdatera handlingsplanen så att den ger en rättvisande bild av myndigheternas huvudsakliga aktiviteter.

som utgör en av målsättningarna i den nationella strategin för samhällets informations- och cybersäkerhet. Den nationella modellen syftar till att utgöra en gemensam plattform för det systematiska informationssäkerhetsarbetet genom at samordna och samla regelverk, metoder, verktyg, utbildningar med mera på ett lättillgängligt sätt.

Regeringen anger att strategin ger uttryck för regeringens övergripande prioriteringar och målsättningar och syftar till att utgöra en plattform för Sveriges fortsatta utvecklingsarbete. Ingen aktör kan ensam lösa utmaningarna på detta område. När flera aktörer arbetar mot samma mål är det särskilt viktigt med samverkan och en gemensam riktning. Tillsammans med strategin bidrar den samlade handlingsplanen till en sådan riktning och risken minskar för till exempel överlappande arbete eller att centrala behov inte tillgodoses.[25] Regeringen framhåller att myndigheterna i detta uppdrag har centrala ansvarsområden i arbetet för en god informations-och cybersäkerhet i samhället. För ett effektivt genomförande av strategin krävs att myndigheterna i detta uppdrag i så stor utsträckning som möjligt samordnar sitt arbete. Myndigheterna ska därför i sin egen planering och prioritering av verksamheten när så är relevant för myndigheten beakta arbetet med handlingsplanen för att ta tillvara effektivitets- och kvalitetsnyttor i arbetet med hela samhällets informations- och cybersäkerhet. Löpande arbete med informations- och cybersäkerhet i den egna organisationen ska dock i enlighet med ansvarsprincipen bedrivas kontinuerligt och självständigt. Den typen av åtgärder ska inte ingå i handlingsplanen.

De berörda myndigheterna offentliggjorde i mars 2021 en samlad informations- och cybersäkerhetshandlingsplan för 2019–2022.[26] Denna samlade informations- och cybersäkerhetshandlingsplan innehåller åtgärder som berörda myndigheter enskilt, tillsammans eller i samverkan med andra aktörer avser att vidta för att höja informations- och cybersäkerheten i samhället. I 2021 års redovisning har ett antal åtgärder avslutats, vissa har uppdaterats och ett fåtal har tillkommit. Åtgärderna i handlingsplanen ligger inom ramen för de an-

[25] Försvarsberedningen har i sin rapport *Motståndskraft, Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025* (Ds 2017:66) betonat vikten av ett kontinuerligt och systematiskt arbete med informations- och cybersäkerhet för en trovärdig totalförsvarsförmåga. För att öka förmågan inom totalförsvaret är det enligt Försvarsberedningen centralt att bygga vidare på arbetet inom krisberedskapen och de strukturer för samhällets informations- och cybersäkerhet som redan är etablerade.

[26] *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022 – redovisning 2021*, publikationsnummer: MSB1635 – mars 2021.

svarsområden och uppdrag som myndigheterna har. Handlingsplanen ska dock inte ses som en komplett redovisning av alla de åtgärder som de olika myndigheterna avser att genomföra inom sina respektive verksamheter på informations- och cybersäkerhetsområdet. Samtliga åtgärder i handlingsplanen ansluter till någon eller några av de sex strategiska prioriteringar som regeringen beslutat i den nationella strategin för samhällets informations- och cybersäkerhet (skr. 2016/17:213). Huvuddelen av åtgärderna syftar till att:

– säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet,
– öka säkerheten i nätverk, produkter och system,
– stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter, och
– öka kunskapen och främja kompetensutvecklingen.

Av redovisningen framgår vilken myndighet som är ansvarig för respektive åtgärd, vilka som deltar i arbetet samt vad åtgärden omfattar.

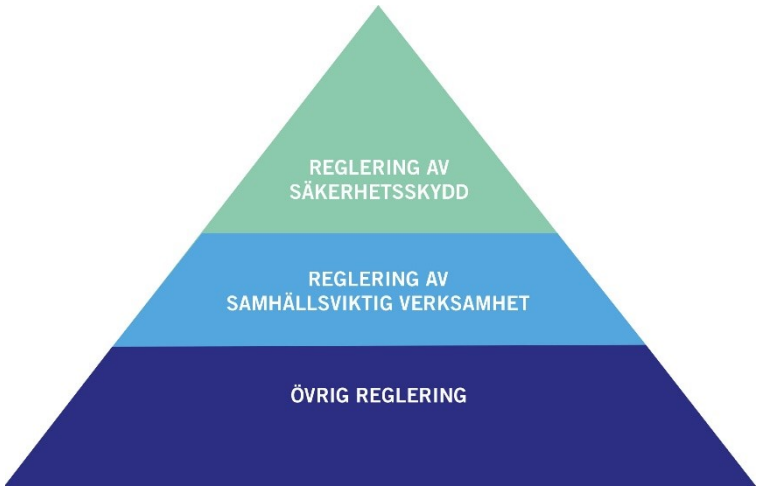
3.5 Författningsbestämmelser om informations- och cybersäkerhet

Bestämmelser om myndigheters och övriga aktörers ansvar för informationssäkerhet och säkerhetsskydd finns i flera olika former av författningar. Vissa typer av regleringar som avser ansvar för information utgår från att skydda eller tillvarata särskilda intressen, bl.a. informationssäkerhet, offentlighet, sekretess, integritetsskydd, effektiv förvaltning, m.m. Här finns anledning att även nämna dataskyddsreglernas krav på säkerhet vid behandling av personuppgifter liksom arkivregleringens krav rörande bevarande av handlingar och uppgiftssamlingar över lång tid. Vidare kan sektorsspecifik reglering om hantering av information också innehålla bestämmelser om informationssäkerhet.

Bestämmelser som reglerar *informationssäkerhet* återfinns i flera olika regelverk. I huvudsak reglerar författningarna antingen skydd för information i viss typ av verksamhet eller särskilt skydd för viss typ av information samt skydd av nätverks- och informationssystem

i vissa typer av verksamheter. Reglering finns i huvudsak inom områdena för säkerhetskänslig verksamhet (säkerhetsskydd) respektive annan samhällsviktig verksamhet, dvs. närmare angivna samhällsviktiga och digitala tjänster. I övrigt finns reglering om informationssäkerhet inom bl.a. området för skydd av personuppgifter (dataskyddsförordningen).

Figur 3.1 **I figuren finns en översiktlig skiss över indelning i de verksamhetsområden som innehåller reglering av informations- och cybersäkerhet**



Nedan följer översiktlig redogörelse av regleringen av nätverks- och informationssäkerhet som är av mer central betydelse för den fortsatta analysen av utredningsfrågorna.

3.5.1 Säkerhetsskydd

En ny säkerhetsskyddslag (2018:585) och den till lagen anslutande säkerhetsskyddsförordningen (2018:658) har trätt i kraft den 1 april 2019. I lagen och förordning finns bestämmelser som ställer krav på särskilda skyddsåtgärder (säkerhetsskydd) för den information och informationssystem som kan påverka rikets säkerhet. Med säkerhetsskydd avses bl.a. skydd av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen jämte skydd av informations-

system i övrigt som rör Sveriges säkerhet. Informationssäkerhet är en av tre grundläggande säkerhetsskyddsåtgärder i säkerhetsskyddslagen och ska förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Vilka uppgifter som en myndighet ska hålla hemliga med hänsyn till rikets säkerhet avgörs efter en säkerhetsanalys hos respektive myndighet. Ytterligare bestämmelser om kraven på informationssäkerhet finns i säkerhetsskyddsförordningen.

Lagen gäller vid verksamhet hos staten, regioner och kommunerna, men även aktiebolag, handelsbolag, föreningar och stiftelser över vilka staten, regionerna och kommunerna utövar ett rättsligt bestämmande inflytande. Lagen gäller också för enskilda om verksamheten är av betydelse för rikets säkerhet. Lagstiftningen har därefter kompletterats med bestämmelser om skärpt kontroll av statliga myndigheters utkontraktering och överlåtelse av säkerhetskänslig verksamhet. Säkerhetsskyddslagstiftningen genomgår fortsatt ett omfattande reformarbete (se kapitel 6, 8 och 13).

Försvarsmakten, Säkerhetspolisen och andra tillsynsmyndigheter ansvarar för tillsyn och kontroll av säkerhetsskyddet hos myndigheter och andra som lagen gäller för.

3.5.2 Samhällsviktiga och digitala tjänster

NIS-direktivet[27] ställer krav på säkerhet i nätverk och informationssystem i vissa angivna samhällsviktiga verksamheter.[28] Reglerna omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster. Dessa leverantörer kan finnas i både offentlig och privat sektor. Tjänster som omfattas av NIS-direktivet delas in i samhällsviktiga tjänster och digitala tjänster. Samhällsviktiga tjänster är tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. De är indelade i sju sektorer:

[27] Europaparlamentets och Rådets direktiv (EU) 2016/1148 av den 6 juli 2016 *om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen*.
[28] Samhällsviktig verksamhet är ett samlingsbegrepp som omfattar de verksamheter, anläggningar, noder, infrastrukturer och tjänster som är av avgörande betydelse för att upprätthålla viktiga samhällsfunktioner.

– bankverksamhet,
– digital infrastruktur,
– energi,
– finansmarknadsinfrastruktur,
– hälso- och sjukvård,
– leverans och distribution av dricksvatten,
– transport.

I NIS-direktivet används begreppet ”samhällsviktiga tjänster” vilket har ett snävare fokus än ”samhällsviktig verksamhet”. Det är verksamhetsutövaren själv som ansvarar för att identifiera sig som en samhällsviktig tjänst under NIS, och att anmäla detta till berörd tillsynsmyndighet.

Lagen (2018:1174) respektive förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster om informationssäkerhet för samhällsviktiga och digitala tjänster trädde i kraft den 1 augusti 2018. Den angivna lagen ställer krav på leverantörer av samhällsviktiga tjänster inom de sju utpekade sektorerna samt, under vissa förutsättningar, leverantörer av digitala tjänster.

Myndigheten för samhällsskydd och beredskap (MSB) har meddelat föreskrifter om vilka tjänster inom dessa sektorer som ska anses som samhällsviktiga. Leverantörer av samhällsviktiga tjänster ska vidta adekvata åtgärder för att skydda de nätverks- och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.[29] De ska även rapportera till MSB om incidenter som har en betydande inverkan på kontinuiteten i tjänsterna. Ett antal myndigheter har genom föreskrift fått i uppgift att bedriva tillsyn över regelverket inom sina respektive sektorer. En sådan tillsynsmyndighet ska ha befogenhet och medel för att kontrollera att leverantörerna uppfyller sina skyldigheter samt fastställa regler om sanktioner vid överträdelse av regelverket. Den nya lagen gäller även för digitala tjänster

En leverantör av samhällsviktiga tjänster ska arbeta systematiskt och riskbaserat med sitt informationssäkerhetsarbete. Kraven för leverantörer av samhällsviktiga tjänster beskrivs mer detaljerat i Myn-

[29] Myndigheten för samhällsskydd och beredskaps föreskrifter *om informationssäkerhet för leverantörer av samhällsviktiga tjänster* (MSBFS 2018:8).

digheten för samhällsskydd och beredskaps (MSB) föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8). I föreskrifterna beskrivs hur leverantören ska gå tillväga för att bedriva ett effektivt informationssäkerhetsarbete. Föreskrifterna ger bland annat kunskap, och stöd, om resurser för att identifiera, införa och utvärdera ändamålsenliga och proportionerliga organisatoriska och tekniska säkerhetsåtgärder.

Den angivna regleringen ställer således krav på att verksamhetsutövare som omfattas av regleringen ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete i sin verksamhet.,

I detta sammanhang kan noteras att NIS-direktivet är föremål för översyn och att kommissionen i december 2020 har offentliggjort ett utkast till ett nytt NIS2-direktiv, som bl.a. utökar tillämpningsområde till fler sektorer i samhällsverksamheten (se kapitel 12

3.5.3 Det europeiska ramverket för cybersäkerhetscertifiering

Utredningen lämnade delbetänkandet *EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering* (SOU 2020:58) till regeringen i september 2020. I delbetänkande lämnar utredningen förslag om att Försvarets materielverk ska utses till nationell cybersäkerhetsmyndighet med uppgift att fullgöra de skyldigheter som följer av EU:s cybersäkerhetsakt. Vidare lämnades förslag om författningsbestämmelser avseende tillsyn, sanktioner, sekretess, m.m. Delbetänkandet har remissbehandlats under 2021.

Regeringen överlämnade den 29 april 2021 till riksdagen propositionen *Kompletterande bestämmelser till EU:s cybersäkerhetsakt* (prop. 2020/21:186) med anledning av utredningens delbetänkande. Utredningen har tagit del av vad regeringen anför i propositionen och kommer på motsvarande sätt som gäller för remissinstansernas synpunkter att beakta vad som anförs i propositionen i den utsträckning det har betydelse för utredningsarbetet.

I EU:s cybersäkerhetsakt anges att regleringen i akten inte påverkar medlemsstaternas befogenheter i fråga om verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på straffrättens område, dvs. verksamheter som till stor del bedöms utgöra säkerhetskänslig verksamhet enligt den nationella säkerhetsskyddslagstiftningen.

Utredningen har i delbetänkandet gjort bedömningen att många av de IKT-produkter, -tjänster och -processer som kan komma att omfattas av regleringens tillämpningsområde även kommer att användas i verksamheter som berör samhällsviktiga tjänster och i verksamhet som berör säkerhetskänslig verksamhet och därför även det svenska totalförsvaret, såväl det militära som det civila försvaret.[30]

En av utgångspunkterna för utredningens arbete i denna del har därför varit – på motsvarande sätt som i delbetänkandet – att i de analyser och de överväganden som gjorts i olika frågor avseende den säkerhetskänsliga verksamheten även beakta hur utredningens ställningstaganden och förslag kan komma att beröra informations- och cybersäkerhet inom tillämpningsområdet för EU:s cybersäkerhetsakt.

3.5.4 Regleringen avseende statliga myndigheter

Grundläggande krav på statliga myndigheters informationssäkerhet finns i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Av förordningen framgår att varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt.[31] Behovet av säkra ledningssystem för informationssäkerhet ska särskilt beaktas. Vidare regleras en skyldighet för myndigheterna att rapportera it-incidenter till Myndigheten för samhällsskydd och beredskap (MSB). Förordningen kompletteras av myndighetens föreskrifter om statliga myndigheters informationssäkerhet[32], föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter[33] och om statliga myndigheters rapportering av it-incidenter.[34] I anslutning till föreskrifterna har myndigheten tagit fram allmänna råd som förtydligar innebörden av bestämmelserna i föreskrifterna och ger generella rekommendationer om tillämpningen.

[30] Se avsnitt 2.4 i delbetänkandet.
[31] 19 och 20 §§ förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.
[32] Myndigheten för samhällsskydd och beredskaps föreskrifter *om informationssäkerhet för statliga myndigheter* (MSBFS 2020:6).
[33] Myndigheten för samhällsskydd och beredskaps föreskrifter *om säkerhetsåtgärder i informationssystem för statliga myndigheter* (MSBFS 2020:7).
[34] Myndigheten för samhällsskydd och beredskaps föreskrifter *om rapportering av it-incidenter för statliga myndigheter* (MSBFS 2020:8).

3.5.5 Regioner och kommuner

För regioner och kommuner gäller lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap. Bestämmelserna i lagen syftar till att regioner och kommuner ska minska sårbarheten i sin verksamhet och ha en god förmåga att hantera krissituationer i fred. Regioner och kommuner ska därigenom också uppnå en grundläggande förmåga till civilt försvar. Regioner och kommuner ska analysera vilka extraordinära händelser i fredstid som kan inträffa i kommunen respektive regionen och hur dessa händelser kan påverka den egna verksamheten. Resultatet av arbetet ska värderas och sammanställas i en risk- och sårbarhetsanalys. Regioner och kommuner ska vidare, med beaktande av risk- och sårbarhetsanalysen, för varje ny mandatperiod fastställa en plan för hur de ska hantera extraordinära händelser. Regeringen eller den myndighet som regeringen bestämmer får meddela närmare föreskrifter om risk- och sårbarhetsanalyser samt planer för hanteringen av extraordinära händelser. Regleringen omfattar emellertid inte specifika bestämmelser med krav på eller om informationssäkerhet.[35]

3.6 Offentliga utredningar och rapporter

Under den senaste femårsperioden har ett antal offentliga utredningar och myndighetsrapporter offentliggjorts som berör informations- och cybersäkerhet och, till viss del, säkerhetsskydd i olika verksamheter. Både utredningar och rapporter visar det finns besvärande brister i informations- och cybersäkerheten i många offentliga aktörers verksamhet och att det därför finns befogad anledning anta att även informations- och cybersäkerheten i den säkerhetsskyddade verksamheten kan vara bristfälligt. En redogörelse för vad som framkommer av utredningarna och rapporterna finns i kapitel 8.

[35] Det kan dock nämnas att vissa föreskrifter som gäller hälso- och sjukvården anger krav på informationssäkerhet när vårdgivare behandlar patienters personuppgifter (HSLF-FS 2016:40).

3.7 Digitaliseringen och kraven på informations- och cybersäkerhet

Utredningen kan konstatera att digitaliseringen och hanteringen av information i nätverks- och informationssystem ökar i alla delar av samhället och inom alla samhällsverksamheter. I takt med att den digitala utvecklingen skapar nya möjligheter uppstår nya säkerhetsutmaningar och hela samhället behöver därför kunna hantera både nationella och globala säkerhetsutmaningar. När det uppkommer sårbarheter och brister i olika nätverks- och informationssystem riskerar det att få omfattande säkerhets- och integritetsmässiga konsekvenser för samhället i stort och för enskilda. En betryggande nätverks- och informationssäkerhet på alla samhällsområden och på alla nivåer är därför grundläggande för den fortsatta utvecklingen av en säker, innovativ och effektiv digital samhällsverksamhet och förvaltning. Den påverkan som den mer generella utvecklingen av samhällets digitalisering, och därtill kopplade krav på bl.a. säkra nätverks- och informationssystem, medför går inte att bortse från när en analys ska göras av behovet av att stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet. Detta blir även en utgångspunkt för utredningens fortsatta analys och överväganden i de frågor som tas upp i utredningsdirektiven.

4 Digitalisering och informations- och cybersäkerhet

Bedömning: Digitaliseringen i samhället sker snabbt och i stor omfattning inom de flesta samhällssektorer. Digitalisering medför nya arbetssätt, som bygger på nya tekniska möjligheter att samla in stora mängder data. Förändringsfaktorer, bl.a. utvecklingen av ny teknik, medför att nya sårbarheter och risker uppstår. Informations- och cybersäkerhet i samhället i stort och inom olika samhällsviktiga områden utvecklas inte i motsvarande grad vilket innebär att gapet mellan digitalisering och informations- och cybersäkerhet ökar över tiden. Detta medför även ökade risker för cyberangrepp mot eller it-incidenter i säkerhetskänsliga och andra samhällsviktiga verksamheter.

4.1 Inledning

Den pågående digitala utvecklingen i Sverige och i världen går på många plan mycket fort och statliga myndigheter, regioner, kommuner och aktörer i näringslivet bedriver sedan många år olika digitaliseringsarbeten. Digitaliseringen påverkar hela samhället och området kan beskrivas som horisontellt, bl.a. för att det omfattar alla samhällssektorer. På samma sätt som utvecklingen av digitaliseringen kan föra med sig fördelar kan den också föra med sig nya eller förändrade hot och sårbarheter. Covid-19-pandemin under 2020 är ett exempel som har tydliggjort detta genom att många anställda, både i offentlig sektor och i näringslivet, mot bakgrund av rådande omvärldsläge har behövt utföra sina arbetsuppgifter på annan plats än den ordinarie arbetsplatsen. Det har fört med sig att myndigheter och företag i större omfattning behövt nyttja internet och olika system

för fjärruppkoppling, anskaffa teknisk utrustning och nyttja olika tekniska tjänster.

Mot bakgrund av utvecklingen av digitalisering inom olika samhällsverksamheter, bl.a. säkerhetskänslig verksamhet, och betydelsen av stärkt informations- och cybersäkerhet behandlas dessa frågor översiktligt i detta kapitel. Syftet är att belysa betydelsen av informations- och cybersäkerhet när frågor om digitaliseringen behandlas, med fokus bl.a. på olika förändringsfaktorer som utgör utmaningar och ökade sårbarheter och risker för denna säkerhet.

4.2 Bakgrund

Riksdagen har vid åtskilliga tillfällen fått ta ställning till propositioner och skrivelser om digitaliseringen och informationsteknikens betydelse för samhällets utveckling inom många olika områden. Regeringen har lämnat förslag till mål, strategier och ett antal andra åtgärder, lagförslag, lägesrapporter om den digitala utvecklingen och lyft fram statens och den offentliga förvaltningens ansvar och uppgifter i denna utveckling, m.m. Regeringen har även tillsatt utredningar i kommittéväsendet för att utreda och lämna förslag om olika frågor som har med digitalisering och it att göra inom olika samhällsområden och om förvaltningens digitala organisering och utveckling. Regeringen har också tillsatt utredningar i kommittéväsendet med operativa uppgifter att utveckla e-förvaltningen. Regeringen har dessutom tillsatt arbetsgrupper, som har utrett olika frågor om e-förvaltning och tillsatt olika så kallade råd för att utveckla e-förvaltningen i samverkan med aktörerna i den offentliga sektorn och med näringslivet.

Samtidigt har myndighetsansvaret för digitaliserings- och it-frågorna, och då även informations- och cybersäkerheten, skiftat under åren. Regeringen har gett olika myndigheter uppgifter som har med samhällets och det offentliga åtagandet för förvaltningens digitalisering att göra samt inrättat och lagt ner flera myndigheter med uppgifter att utveckla och stödja förvaltningens användning av it. De organisatoriska lösningarna har varit tillfälliga och kortsiktiga. Regeringen har även gett statliga myndigheter inom olika politikområden och sektorer uppdrag om förvaltningens digitalisering, bl.a. e-förvaltning, i regleringsbrev och i särskilda regeringsbeslut. Samman-

fattningsvis kan noteras att det har sedan 1970-talet nästan konstant funnits en kommitté, arbetsgrupp eller myndighetsuppdrag med uppgift att behandla digitalisering och it-frågor.[1]

Dagens digitaliseringsstrategier föregås en rad utredningar under 1980- och 1990-talen som har behandlat frågor om ADB (automatisk databehandling) och sedermera it. Bl.a. inrättade den så kallade IT-kommissionen ett ”observatorium för IT-infrastrukturfrågor” i slutet av 1990-talet i syfte att skapa ett forum för diskussioner och rekommendationer kring frågor rörande den grundläggande infrastrukturen för it.[2]

Digitaliseringskommissionen, som bildades av regeringen i juni 2012 och som utgjorde IT-kommissionens arvtagare, fick till uppgift att verka för att det it-politiska målet uppnås och att regeringens ambitioner inom området fullföljs.[3] Digitaliseringskommissionen har utkommit med en rad delbetänkanden på temat Sveriges digitala agenda.[4] Kommissionen arbete sammanfattades med slutbetänkandet *För digitalisering i tiden* (SOU 2016:89).

De rapporter som publicerats av Digitaliseringskommissionen och andra aktörer visar att analyserna har vidgats från ett infrastruktur- och teknikfokus till ett bredare samhällsperspektiv som betraktar digitaliseringen som en transformerande kraft som påverkar samhället på alla nivåer. Även begreppen förändras från ADB till IT till det nuvarande begreppet digitalisering.

[1] SOU 2017:23, s. 51 ff. I delbetänkandet lämnas en översiktlig redogörelse för regeringens ambitioner för utvecklingen och digitaliseringen av den offentliga förvaltningen och det organiserade stödet av denna utveckling under den senaste tjugoårs-perioden.
[2] Se t.ex. *Framtidssäker IT-infrastruktur för Sverige* (SOU 1999:134).
[3] *Digitaliseringskommissionen – en kommission för den digitala agendan*, Dir. 2012:61.
[4] *En digital agenda i människans tjänst – Sveriges digitala ekosystem, dess aktörer och drivkrafter* (SOU 2013:31); *En digital agenda i människans tjänst – en ljusnande framtid kan bli vår* (SOU 2014:13); *Gör Sverige i framtiden – digital kompetens* (SOU 2015:28); *Om Sverige i framtiden – en antologi om digitaliseringens möjligheter* (SOU 2015:65); *Digitaliseringens transformerande kraft – vägval för framtiden* (SOU 2015:91) och *Digitaliseringens effekter på individ och samhälle – fyra temarapporter* (SOU 2016:85). Kommissionens arbete avslutades i och med slutbetänkandet *För digitalisering i tiden* (SOU 2016:89).

4.3 Politikens mål för digitalisering

4.3.1 Digitaliseringsstrategier

I Sverige har det tagits fram en rad strategier för att tillvarata digitaliseringens möjligheter. Det övergripande målet i den nuvarande digitaliseringsstrategin är, som tidigare berörts, att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. För att nå detta mål har ett antal delmål avseende digital kompetens m.m. formulerats (kapitel 3).

Regeringen inrättade i mars 2017 Digitaliseringsrådet – inom Regeringskansliet – som stöd i arbetet med att förverkliga dessa mål. Digitaliseringsrådets uppgift är att bidra till bättre samordning och ett effektivt genomförande av regeringens strategiska arbete med digitalisering. Digitaliseringsrådet är direktrapporterande till digitaliseringsministern. Rådets uppgift är i korthet att:

- följa och stödja regeringens arbete med digitalisering,
- följa digitaliseringen i Sverige,
- följa digitaliseringen i omvärlden och jämföra hur Sverige presterar mot andra länder, och
- lämna förslag till konkreta insatser samt samråda med andra funktioner som regeringen inrättat för att arbeta med samhällets digitalisering.

Den övergripande digitaliseringsstrategin är dock inte den enda strategin av relevans för digitaliseringsfrågor. I Digitaliseringsrådets rapport *En lägesbild av digital ledning*[5] 2018 ges en översikt av närliggande strategidokument som också har påverkan på digitaliseringsfrågorna.[6]

Digitaliseringsrådet lämnar i rapporten även en uppdaterad lägesbild av de fem delmål som anges i digitaliseringsstrategin. Lägesbilderna, tillsammans med Digitaliseringskommissionens slutbetänkande[7], utgör en bas för det vidare arbetet när gäller förståelse om viktiga utmaningar och möjligheter. Under 2019 inriktades rådets verksam-

[5] *En lägesbild av digital ledning,* Digitaliseringsrådet, 2018.
[6] Bl.a. *Nationell strategi för informations- och cybersäkerhet*, *Demokratistrategin*, *Regeringens strategi för standardisering*, *Bredbandsstrategin*, *Nationell inriktning för artificiell intelligens* (inte formellt en strategi), *Regeringens strategi för en digitalt samverkande statsförvaltning*, m.m.
[7] Digitaliseringskommissionens slutbetänkande *Digitaliseringens transformerande kraft – vägval för framtiden* (2015:91).

het på att fortsätta följa utvecklingen, där analysarbetet är en stor utmaning.[8]

4.3.2 Utvecklingen

Digitaliseringskommissionen konstaterar att digitaliseringen utgör katalysator och motor i samhällsutvecklingen sedan ett par decennier. Utvecklingen innebär helt nya förutsättningar för samhället och människan. Digitaliseringen och användningen av ny teknik förändrar förutsättningar och villkor för offentlig sektor och företag, för arbetsliv och utbildning och för tillit och social sammanhållning i samhället. Det som är särskilt kännetecknande för den av digitaliseringen drivna samhällsutvecklingen är hastigheten. Utvecklingen är exponentiell. Det beror på att informations- och kommunikationstekniken (IKT) kontinuerligt och snabbt utvecklar nya användningsområden och funktioner, högre prestanda samt att användarnas intresse för och kompetens att använda tekniken ständigt växer och driver utvecklingen.[9] Digitalisering innebär digital kommunikation och interaktion mellan människor, verksamheter och saker, dvs. möjligheten att samla in, tolka, tillämpa och utveckla allt större kvantiteter av data. Interaktionen via digitala plattformar gör att transaktionskostnaderna för kontakt och kommunikation, varor och tjänster blir låga. Det innebär en växande marknad även för digitala mellanhänder. Traditionell administrativ handläggning minskar betydligt i det digitala samhället. Eftersom allt som sker digitalt lämnar digitala spår möjliggörs insamling och tolkning av stora mängder data. Dessa data kan tillämpas för olika saker, såsom kunskapsuppbyggnad och analys, utveckling av tjänster och varor och för kvalitets- och förbättringsarbete inom de flesta områden. Analys av stora mängder data innebär att kunskap om och förståelse av människan, samhället och miljön kommer att förändras. Det påverkar sättet att arbeta med olika utmaningar inom de flesta samhällsområden.

Begreppet digitalisering har även blivit ett ledord för många aktörer som vill lyfta fram innovation, utveckling, framtid, förändring och – som det uttrycks – en pågående revolution. Kungl. Ingenjörsvetenskapsakademien (IVA) bedömer att

[8] https://digitaliseringsradet.se/vi-aer-digitaliseringsraadet/vaart-uppdrag/ (hämtad 2021-05-09).
[9] Digitaliseringskommissionens slutbetänkande *Digitaliseringens transformerande kraft – vägval för framtiden* (2015:91), s. 57.

> digitaliseringen innebär en mycket snabb och genomgripande samhällsförändring, en fjärde industriell revolution.[10]

Innebörden av denna revolution brukar beskrivas i termer av djupgående förändringar som påverkar såväl strukturer som individer. Digitaliseringens globala och gränsöverskridande karaktär påverkar alla samhällssektorer men begränsar samtidigt enskilda staters makt i förhållande exempelvis till globalt verkande företag. Det offentliga har dock fortfarande ett ansvar eftersom enskilda företag inte behöver eller förmår att ta ansvar för helheten eller konsekvenser av digitaliseringen som uppstår i andra eller tredje ledet.

I vid mening syftar begreppet digitalisering på processer som förändrar eller skapar något nytt genom användning och integrering av digital teknik. En förutsättning för att digitalisera är att information finns tillgänglig i digitalt format. Myndigheten för digital förvaltning (DIGG) bedömer att på senare tid har det skett en tydlig ambitionshöjning vad gäller den digitala förvaltningen i Sverige. Sedan bildandet av DIGG år 2018 har flera större projekt initierats. Det handlar framför allt om etablerandet av en förvaltningsgemensam digital infrastruktur för informationsutbyte, etableringen av flera nationella grunddatadomäner och ett intensifierat arbete med öppna data. Även styrningen av den offentliga sektorns digitalisering, som tidigare präglades av fragmentering och ett stort självbestämmande, har ändrat fokus och handlar i dag mycket om att öka helhetssynen och konsolidera och standardisera de komponenter och lösningar som behövs i hela eller stora delar av förvaltningen. Denna utveckling bedöms kunna ha stor positiv inverkan på den svenska förvaltningens förutsättningar att tillvarata digitaliseringens möjligheter.[11]

Arbetet med digital infrastruktur

Myndigheten för digital förvaltning (DIGG) leder ett arbete med att etablera en hållbar digital infrastruktur som ska möjliggöra ett effektivt och säkert utbyte av information inom och med det offentliga. Utvecklingen av infrastrukturen ska främja nya förvaltningsgemensamma tjänster och lösningar för framtiden. Om Sverige ska kunna

[10] *Digitalisering för ökad konkurrenskraft*, Kungl. Ingenjörsvetenskapsakademien (IVA), 2019, s. 7.
[11] www.digg.se/om-oss/nyheter/2021/sveriges-digitala-forvaltning-ar-bra-men-flera-andra-ar-battre (hämtad 2021-05-09).

möta kommande samhällsutmaningar, bibehålla välfärden och nå ekonomisk, social och ekologisk hållbarhet krävs det att svensk offentlig förvaltning utvecklar nya gemensamma lösningar, tillsammans. Digitalisering är det viktigaste verktyget för att skapa en effektiv och ändamålsenlig förvaltning för framtiden. Ökad tillgång till data och ett ökat informationsflöde mellan aktörer bäddar för stora effekthemtagningar i form av bl.a. tidsvinster, minskad administrativ börda och lägre kostnader inom det offentliga. Infrastrukturen möjliggör även att nya datadrivna tekniker, såsom artificiell intelligens (AI), kan användas för att öka innovationsförmågan och ge bättre service. En fullt utvecklad digital infrastruktur ska underlätta för medborgare och företagare i deras myndighetskontakter både nationellt och inom EU, där en uppgift till exempel bara ska behöva lämnas en gång.

DIGG har – inom ramen för två regeringsuppdrag – tillsammans med ett stort antal andra myndigheter påbörjat etableringen av de beståndsdelar som ska ingå i den digitala infrastrukturen. Under 2021 och framåt intensifieras arbetet med att bygga upp en hållbar infrastruktur som ska vara säker, enkel och effektiv att använda. Infrastrukturen består i sin enklaste form av ett antal så kallade byggblock som tillsammans utgörs av standarder, modeller, ramverk, strukturer och tjänster. Till detta finns även ett nationellt ramverk för grunddata och en struktur för styrning.[12]

4.4 Internationella jämförelser (index)

Digitaliseringsrådets uppgift är att följa Sveriges utveckling ur ett internationellt perspektiv. Det sker bland annat genom uppföljningen av ett antal internationella index. Indexen presenterar av olika internationella aktörer och uppdateras i regel en gång per år. Syftet med ett index är att på ett åskådligt sätt jämföra länder med varandra och är uppbyggt genom att mätpunkter inom utvalda områden sammanvägs för att ranka länder.

[12] De myndigheter som har uppdragen att etablera en förvaltningsgemensam digital infrastruktur och ett nationellt ramverk för grunddata är Bolagsverket, DIGG, Domstolsverket, E-hälsomyndigheten, Försäkringskassan, Lantmäteriet, Myndigheten för samhällsskydd och beredskap, Riksarkivet samt Skatteverket.

Sammanfattning av Sveriges placeringar

Sverige har under många år presterat bra i internationella jämförelser och rankas genomgående högt. Utifrån de index som redovisas presterar Sverige bra vad gäller infrastruktur och individers användning i form av till exempel internetanvändning. Några av indexen visar på en lägre rankning för företagens användning av digitalisering. Det område där Sverige presterar lägst är e-förvaltning, vilket går igenom alla index där det finns indikatorer som mäter detta. I varierande grad stämmer de internationella indexen med de fem delmål som den svenska digitaliseringsstrategin innefattar. I jämförelserna finns stor övervikt av indikatorer som mäter infrastruktur och kompetens ur ett globalt perspektiv. De indikatorer som försöker fånga aspekter av t.ex. innovation, ledning och trygghet bygger ofta på kvalitativa insamlingar vars metoder – enligt rådet – kan ifrågasättas. Ett annat generellt problem med indexen är att indikatorerna inte alltid mäter det som man avser att fånga.

Såväl Digitaliseringsrådet som Digitaliseringskommissionen anser att de internationella jämförelserna täcker endast in delar av de aspekter och trender som bör följas. Djupare kunskap behöver utvecklas för att få en adekvat uppfattning om hur Sverige ligger till i förhållande till det yttersta målet ”att bli bäst i världen att använda digitaliseringens möjligheter”. T.ex. behövs det tas fram nya indikatorer. Statistiken bör även kompletteras med andra typer av studier som ger kunskap om variationer, mönster och orsakssamband.

EU-kommissionens index, DESI, publiceras varje år och kartlägger EU-ländernas prestation inom digitalisering. Under 2020 publicerades nya beräkningar som placerar Sverige på en andra plats efter Danmark. Det är en förbättring med en placering sedan förra året. Sverige räknas tillsammans med Danmark, Finland, Nederländerna, Storbritannien, Luxemburg, Belgien och Estland som de högpresterande länderna i Europa.[13]

[13] Se https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi.

4.5 Digitala sårbarheter

De visioner och strategier som framhåller digitaliseringens möjligheter påpekar att utvecklingen i Sverige verkar gå långsammare jämfört med andra länder. Samtidigt finns risk för att digitaliseringen medför att säkerhetsfrågorna förs in alltför sent i processen, vilket negativt kan påverka olika digitaliseringssatsningar.

Regeringens delmål *digital ledning* pekar på vikten av att verksamheter effektiviseras, utvecklas och får högre kvalitet genom styrning, mätning och uppföljning. Digitaliseringsrådet menar att den svenska förvaltningen behöver moderniseras och effektiviseras och drar slutsatsen att offentlig sektor behöver kunna svara upp mot växande krav på både ökad informations- och cybersäkerhet och effektivitet i verksamheterna i förening med ökad servicegrad och digitala tjänster.

Digitaliseringens möjligheter beror även på i vilken grad metoderna, bl.a. tillämpning av AI och automatisering, kommer att leda fram till målen om ökad kvalitet och effektivitet. Strävan att automatisera olika processer sker i syfte att uppnå ökad kostnadseffektivitet och besparingar. Många offentliga utredningar och rapporter framhåller att en ökad digitalisering kan skapa större kostnadseffektivitet. Forskning om kostnader för implementering av nya tekniska system visar dock att det kan dröja länge innan ny teknik ger avkastning i termer av ökad produktivitet och/eller minskade kostnader.[14] Vad gäller att digitalisering av komplexa verksamheter kan i själva verket kostnaden vara avsevärd, bl.a. genom att införandet av ny teknologi och nya arbetssätt och som medför en längre process där olika mål och behov behöver beaktas samtidigt.

Som tidigare berörts medför digitaliseringen såväl ökade tekniska möjligheter som nya risker och sårbarheter. I Digitaliseringsrättsutredningen betänkande 2018 konstaterades att den politiska inriktningen i Sverige är att den offentliga förvaltningen ska leda vägen när det gäller den digitala omvandlingen och att ny teknik gärna ska tas i bruk tidigt. I betänkandet påpekas att detta mål samtidigt medför att det kommer att finnas ett växande behov av ett informations- och cybersäkerhetsarbete i myndigheternas informationshantering. Ett ökande behov av arbete med informations- och cybersäkerhet med-

[14] *Vilse i lasagnen? – En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur*, s. 21, (FOI-R--4814--SE), Totalförsvarets forskningsinstitut, 2020.

för kostnader, vilket erfarenhetsmässigt dock många gånger inte beaktas när kostnader för verksamheten ska beräknas. Om kostnadsbesparingar utgör en drivande kraft för att digitalisera finns en tydlig risk för att bl.a. behovet av informations-och cybersäkerhet inte beaktas i tillräcklig utsträckning. Det finns således en risk att sådant som på kort sikt ses som kostnadsdrivande, som t.ex. säkerhetsaspekter, åsidosätts när nya digitaliseringsprojekt ska genomföras. Ur ett risk- och sårbarhetsperspektiv kan därmed åtgärder för att spara kostnader innebära en risk om säkerhetsarbetet prioriteras ned.

Ett argument för en ökad digitalisering av olika samhällsverksamheter är att ökad automatisering kan frigöra resurser från mer rutinartad administration och i stället tillföras verksamhetens kärnuppgifter. Automatisering brukar dock inte bara presenteras i termer av behov utan också i termer av nya möjligheter. Bl.a. Vinnova har i en rapport om artificiell intelligens (AI)[15] betonat att utvecklingen av nya systemlösningar, tjänster och varor inom både offentlig sektor och näringslivet rymmer en stor potential för bl.a. ökad effektivitet. Vinnova pekar även på ett antal utmaningar och risker, bl.a. risken att AI-lösningar baseras på bristfälliga eller felaktiga algoritmer och data och att säkerhetsrisker kan uppstå genom medvetet skadlig dataanvändning och datamanipulering.

I vilken grad digitalisering kan möta olika typer av utmaningar och t.ex. öka kvaliteten och effektiviteten i olika samhällsverksamheter är dock en fråga som inte är begränsad till enbart tekniska aspekter. Avgörande är samtidigt hur dessa utmaningar ser ut och vad som menas med begrepp som kvalitet och effektivitet i samhällets olika verksamheter samtidigt som säkerheten i nätverks- och informationssystem kan uppnås.

Ett grundläggande problem som uppkommer kan handla om underskattningar av den tid som krävs för att skapa säkra och användarvänliga system, vilket kan medföra bristfälliga lösningar. Detta kan få allvarliga följdverkningar genom sårbarheter och säkerhetsbrister byggs in i de nya systemen. Samtidigt som signalen från strategidokumenten är att myndigheterna ska vara drivande vad gäller digitalisering finns det ett gap mellan behovet av säkerhet och förutsättningarna att bedriva säkerhetsarbete.

[15] *Artificiell intelligens i svenskt näringsliv och samhälle – Analys av utveckling och potential*, Vinnova, 2018.

Sammantaget förmedlas dock i flera rapporter att möjligheterna för ökad effektivitet många gånger väger tyngre än riskerna, oavsett om det gäller digitalisering i allmänhet eller användningen av AI eller ökad automatisering.

Brister i styrningen och samordningen

Flera utredningar och rapporter har identifierat behovet i Sverige av att stärka styrningen och samordningen av digitaliseringen, särskilt när det gäller utbyggnad av infrastruktur och samordning av informationssäkerhetsarbetet.[16] Mot bakgrund av mängden offentliga aktörer är detta en uppgift av betydande omfattning då frågan berör bl.a. fler än 200 statliga förvaltningsmyndigheter, 21 länsstyrelser, 20 regioner, 290 kommuner, fler än 100 andra offentliga aktörer och cirka 40 helägda statliga bolag. Det är en omfattande förvaltning som kompliceras av stora skillnader mellan verksamheterna vad gäller storlek, geografi, uppdrag, finansiella resurser och kompetens. Alla ska dock med i den digitala transformationen.[17] Dessutom tillkommer alla de privata företag som på något sätt driver och förvaltar samhällets infrastruktur.

Kungl. Ingenjörsvetenskapsakademien (IVA) påpekar i rapporten *Digitalisering för ökad konkurrenskraft* att Sverige har en avreglerad marknad med olika skikt av infrastrukturproducenter, operatörer och tjänsteutvecklare, som å ena sidan har många fördelar men som å andra sidan lider av bristande helhetssyn och samordning. Sverige är mycket nära en situation där alla vitala samhällsfunktioner kräver en välfungerande digital infrastruktur. Denna förutsätts fungera minst lika säkert som annan infrastruktur men det saknas regler och planer för drift och utbyggnad. Ansvaret ligger i stället på många händer och samordningen brister på både statlig och kommunal nivå.

Enligt IVA är grundläggande infrastruktur för digital kommunikation i Sverige är av de viktigaste områdena att styra och samordna. Den svenska digitala infrastrukturen är, menar IVA, uppbyggd enligt en lasagnemodell med olika lager av verksamheter, men styrning och samordning är inte fullt ut anpassade till detta. Modellen för-

[16] *Digitalisering för ökad konkurrenskraft*, IVA, 2019, s. 49 och 50; *Vetenskapsrådets guide till infrastrukturen*, Vetenskapsrådet, 2018; *Digitalisering av det offentliga Sverige* (ESV 2018:31), Ekonomistyrningsverket (ESV), 2018.
[17] Digitaliseringsrådet, 2018, s. 48.

utsätter att statliga myndigheter och kommuner både investerar och utövar tillsyn, samtidigt som privata aktörer är ansvariga för vitala delar av infrastrukturen. Syftet med samordning och styrning är att se till att både befintliga och nya delar av infrastrukturen har tillräcklig säkerhet, robusthet och kapacitet. Styrningen och samordningen av digitaliseringsfrågorna är, menar IVA, dock svag och otillräcklig.[18]

I betänkandet *reboot – omstart för den digitala förvaltningen 2017* påpekas att risken för att de krav på informations- och cybersäkerhet som utfärdas i praktiken fördröjs eller aldrig blir utförda på grund av oklara ansvarsförhållanden.[19] Utredningen påpekar vidare att det finns en risk för ökad fragmentering av kravställningar när fler aktörer utan samordning utfärdar regler på området, något som kan leda till att samma typ av information riskerar att få helt olika skydd beroende på var i förvaltningssystemet som den hanteras.[20]

En fråga som kan uppkomma när behovet av digitalisering behandlas är skillnaden mellan förväntningar och verklighet. Förväntningar kan leda till missförstånd om vad digital teknik kan åstadkomma. För aktörerna på den öppna marknaden, som i många avseenden styr hur infrastrukturen och nätverks- och informationssystemen ska utveckla, strävar ofta efter låga kostnader och effektivitet snarare än säkerhet på samhällsnivå och genomtänkt systemfunktion för offentlig verksamhet. Detta leder till en betydande risk att behovet av säkerhet och tillförlitlighet på den högre systemnivån inte tillgodoses, bl.a. vad gäller stora system och i systemet ingående kommunikationer, elförsörjning och påverkan på samhällseffekter. Ett scenario med ett större cyberangrepp och sammanbrott i samhällets funktionalitet, t.ex. mot elförsörjningen, kan få mycket allvarliga och svåra följder för hela eller vitala delar av samhällets funktion.[21]

Brister i infrastrukturen och sårbarheter med ny teknik

Enligt IVA finns i dag ett gap mellan infrastrukturens kapacitet och de digitala tjänsternas faktiska behov av kapacitet. Hos viktiga beslutsfattare såväl som i samhället i stort saknas dock kunskap om att

[18] IVA, 2019, s. 49 och 50.
[19] SOU 2017:114, s. 164.
[20] A.a.
[21] SOU 2019:59, s. 19 (jfr även s. 22 och 23).

detta gap existerar.[22] Detta är allvarligt anser IVA, som menar att det saknas en omfattande kontroll av kvalitet och driftsäkerhet för den digitala infrastrukturen. Det innebär en mycket stor riskaggregering när man utgår från att många funktioner ska fungera. En bakgrund till dessa förhållanden är – enlig IVA – bristande samordning av utbyggnaden av infrastrukturen. Dagens nationella it-infrastruktur har byggts ut där det funnits affärsmässiga skäl som talat för detta, och bristande koordinering har medfört att det finns för få mötesplatser för fiber, vilket i sin tur leder till bristande redundans. Några få operatörer har etablerat redundanta vägar, men långt ifrån i den utsträckning samhället behöver.[23]

Nya tekniker medför ofta även brister i tekniken som i sig innebär sårbarheter. Ny teknik behöver därför testas i skyddade miljöer och introduceras med försiktighet och i lagom takt. För att åstadkomma en kontrollerad och strukturerad utbyggnad av ett nytt system, eller en ny teknik, krävs agenda och planering. Tekniska standarder kan fylla denna funktion och tillämpas ofta just med det syftet. En utmaning är att det kan finnas olika incitament att bygga ut eller exploatera teknik, och att alla incitament inte innebär att tekniken blir säker när den väl är på plats. Om teknik byggs ut i stor skala, med många latenta fel eller sårbarheter kan stora tekniska och säkerhetsmässiga utmaningar följa för att åtgärda problemen. Om tekniken, och därmed dess sårbarheter, sprids okontrollerat kan betydande problem uppstå. I bästa fall åtgärdas sårbarheterna löpande, men om utvecklingen är snabb kan detta vara svårt, särskilt om sårbarheterna initialt är okända. Ett exempel som framhålls är utvecklingen av IoT, vilket kommer att medföra stora utmaningar när det gäller säkra produkter och tjänster ur ett informations- och cybersäkerhetsperspektiv. Ett annat exempel är bristfälligt genomförda satsningar på ”smarta städer” som inte beaktar risker och sårbarheter med att koppla upp och ihop många olika typer av sensorer och funktioner. Denna typ av digitala tjänster möjliggör potentiellt effektiviseringar men också att många funktioner kan slås ut samtidigt. Om produkter förses med uppkopplingsmöjligheter ger det utrymme för tekniken att användas t.ex. i en säkerhetskänslig miljö. Om uppkopplingsmöjligheten till en början är okänd, t.ex. för att den införts

[22] IVA, 2019, s. 7.
[23] *Att motverka överbelastning av samhällsviktiga webbplatser – Slutrapport 2018 från projekt Särimner*, Vetenskapsrådet, 2018.

längre bak i leverantörskedjan, kan det initialt finnas svårigheter till spårbarhet I detta fall är risken att de tekniska installationerna, särskilt om de är mångfaldigade, kan bli en, vissa fall dold, hävstång för angrepp mot t.ex. kritisk infrastruktur eller i övrigt säkerhetskänsliga informationssystem.

En av de mer i dag uppmärksammade teknikerna är den femte generationens telekommunikation (5G). Tekniken innebär en kapacitetshöjning, dvs. högre dataöverföringshastigheter, större antal samtidigt anslutna enheter och kortare svarstider. Dessa tekniska förbättringar innebär i sin tur att förutsättningar för att bygga digitalt smarta hem och städer ökar då fler uppkopplade enheter kan anslutas. Risker och sårbarheter med tillämpningen av 5G har uppmärksammats i olika sammanhang, bl.a. av Enisa och olika medlemsstater.[24]

Andra exempel som medför risker och sårbarheter är produkter och tjänster med många användare, t.ex. operativsystem, molntjänster och sökverktyg. När många är beroende av funktion och säkerhet i en enda produkt eller tjänst kan en sårbarhet där orsaka stora konsekvenser om den nyttjas av en angripare eller på annat sätt utsätts för oväntade händelser.

När en ny eller befintlig teknik ska byggas ut för att tillgodose framtidens krav så måste även infrastrukturen och säkerheten, och den redundans som krävs, stärkas i motsvarande takt och omfattning. Det kan många gånger vara svårt för verksamheten att förstå hur system är uppbyggda och vilka beroenden som finns, speciellt om de upphandlas från en extern part. En enskild leverantör kan svara för funktioner hos många olika verksamheter, till exempel inom myndigheter och andra offentliga aktörer.

En annan utmaning i detta sammanhang är att det i dag är ett fåtal stora teknikföretag som tillsammans har stor makt över det som sker på t.ex. internet. Företagen står för står för en betydande del av den informationshantering och teknik som används i dag. Denna marknad fungerar i dag som ett oligopol, vilket bör beaktas när frågan om informations- och cybersäkerhet diskuteras och hanteras.

[24] Se bl.a. Enisa: *SECURITY IN 5G SPECIFICATIONS – Controls in 3GPP Security Specifications* (5G SA), 2021.

4.6 Digitalisering och informations- och cybersäkerhet i otakt

Informations- och cybersäkerhetsarbete är en stödjande verksamhet som syftar till att bl.a. öka säkerheten i nätverks- och informationssystem i olika samhällsverksamheter. I och med den ökande digitaliseringen är informations- och cybersäkerhet en förutsättning för att nya verksamheter som uppstår, och ny teknik som utvecklas, ska kunna fungera och användas på ett säkert sätt. Informations- och cybersäkerhet innebär en strävan efter att skydda information så att den alltid finns när den behövs (tillgänglighet), att det går att lita på att den är korrekt och inte manipulerad eller förstörd (riktighet), att endast behöriga personer får ta del av den (konfidentialitet) och att det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet). Den syftar även till att skydda nätverks- och informationssystem i övrigt.

Myndighetens för samhällsskydd och beredskap (MSB) övergripande arbete med att stödja och samordna arbetet med samhällets informations- och cybersäkerhet inriktas på strategisk nivå av den nationella informations- och cybersäkerhetsstrategin, som anger sex strategiska prioriteringar:

- Säkerställa en systematisk och samlad ansats i arbetet med informations och cybersäkerhet.
- Öka säkerheten i nätverk, produkter och system.
- Stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter.
- Öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet.
- Öka kunskapen och främja kompetensutvecklingen.
- Stärka det internationella samarbetet.

Förutom MSB finns en rad statliga aktörer som har olika roller för det nationella arbetet med informations- och cybersäkerhet, bl.a. Säkerhetspolisen Försvarsmakten, Försvarets radioanstalt (FRA), Försvarets materielverk (FMV), Post- och telestyrelsen (PTS) och Polismyndigheten. Myndigheternas arbete samordnas sedan 2020

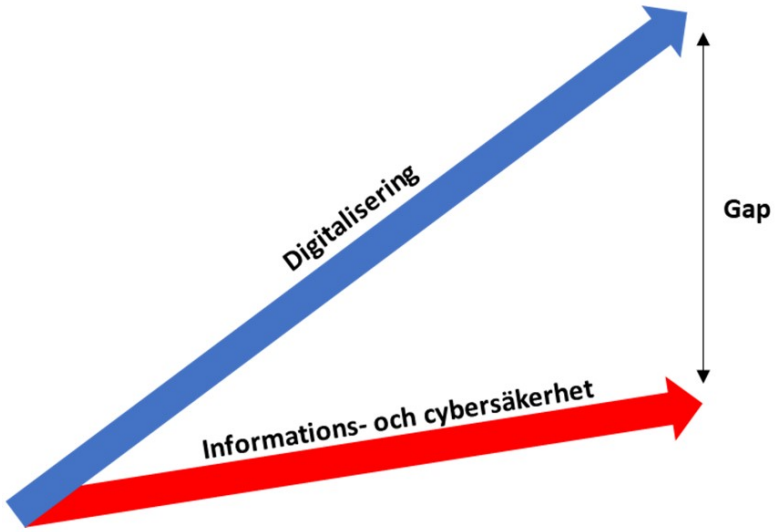
genom det nationella cybersäkerhetscentret. Regeringen har också gett berörda myndigheter uppdrag att ta fram en samlad handlingsplan med förslag på olika åtgärder som kan stärka Sveriges arbete med informations- och cybersäkerhet. Dessa förslag konkretiserar behov och rekommendationer som identifierats på en mer övergripande nivå i den nationella informations- och cybersäkerhetsstrategin.

Digitaliseringsrådet konstaterar att det ser ut ungefär på samma sätt i andra undersökta länder, dvs. att det finns en digitaliseringsstrategi men även ett antal andra strategier som berör specifika aspekter av digitaliseringen och ofta på liknande områden som i Sverige. Samtidigt kan noteras att det i Sverige finns en grupp av myndigheter som fokuserar på digitaliseringens möjligheter, t.ex. ur ett effektiviseringsperspektiv, och en annan grupp som fokuserar på olika typer av hot, risker och sårbarheter. I takt med ökad digitalisering kommer en ökad samverkan och samordning mellan dessa grupper att få stor betydelse för utvecklingen i sin helhet, annars riskerar gapet mellan digitalisering och informations- och cybersäkerhet att öka ytterligare (se nedan).

Gapet mellan digitalisering och informations- och cybersäkerhet ökar

Den digitala utvecklingen i samhället går snabbt men däremot ökar inte informations- och cybersäkerheten i samma takt. Det innebär att informations- och cybersäkerhetsgapet som uppstår ökar riskerna för att drabbas av ett cyberangrepp eller en it-incident, vilket illustreras nedan i figuren nedan.

Figur 4.1 Digitalisering och informationssäkerhet i otakt



Gapet kan dock minska genom olika åtgärder, bl.a. genom ett ökat systematiskt informationssäkerhetsarbete och åtgärder som stärker it-säkerheten.

Inom informations- och cybersäkerhetsområdet betonas ofta vikten av att verksamheter inför ledningssystem för informationssäkerhet (LIS). Ledningssystem för informations-säkerhet är ett stöd för hur informations- och cybersäkerhetsarbetet styrs i en verksamhet.[25] En central del är att verksamheten måste ha ledningens uttalade stöd i sitt arbete med informationssäkerhet. Det finns olika typer av svenska och internationella standarder som underlättar arbetet med ledningssystem för informationssäkerhet. Utifrån sådana standarder tar ledningssystem för informationssäkerhet sin utgångspunkt i en verksamhetsanpassad riskanalys och informations- och cybersäkerhetsarbetet följer en tydlig process.[26]

God informations- och cybersäkerhet bidrar till att en verksamhet kan bedrivas på ett säkert, ändamålsenligt och effektivt sätt, att risken för att drabbas av avbrott eller störningar i driftmiljön minskar. God informations- och cybersäkerhet är också en grundläg-

[25] MSB har utvecklat ett metodstöd för systematiskt informationssäkerhetsarbete. Metodstödet finns tillgängligt på webben: www.informationssakerhet.se.
[26] Se t.ex. den svenska och internationella standardserien SS-ISO/IEC 27000.

gande byggsten för den fortsatta utvecklingen av en säker, innovativ och effektiv digital förvaltning.

Samtidigt som digitaliseringens fördelar välkomnas står det klart att de risker och hot som behöver hanteras i dessa sammanhang är några av våra mest komplexa säkerhetsutmaningar. Säkerhetspolisen konstaterar att den största risken för samhället och totalförsvaret utgörs av bristande informationssäkerhet.[27] Försvarets radioanstalt (FRA) framhåller att säkerheten generellt hos myndigheter och statliga bolag inte är dimensionerad för den befintliga hotbilden.[28] Dessa uttalanden ska ses i ljuset av att det sker en ständigt växande hantering av information i nätverks- och informationssystem, både i offentlig och enskild verksamhet. Om det uppstår brister i hanteringen av information i nätverks- och informationssystem, och i skyddet av densamma, riskerar det att få omfattande konsekvenser både för samhället i stort och för enskilda. Brister i informations- och cybersäkerheten, t.ex. bristande säkerhetsrutiner, kan medföra allvarliga och upprepade störningar i myndigheters nätverks- och informationssystem som kan sprida sig till andra sektorer och aktörer.

Utvecklingen och användningen av ny teknik och nya innovationer innebär att nya hot och risker behöver hanteras. Hot och riskskalan inom det informationsteknologiska området spänner från mindre omfattande risker till väl planerade, och med precision riktade, angrepp mot vitala delar av samhällets funktionalitet. Även antagonistiska hot såsom informationsoperationer och elektroniska angrepp mot skyddsvärda nätverks- och informationssystem, t.ex. i form av dataintrång, sabotage eller spionage behöver mötas. Detsamma gäller olika former av störningar i mjuk- eller hårdvara eller störningar i driftmiljö. Yttre fysiska händelser som t.ex. bränder, avgrävda kablar, översvämningar och solstormar utgör också en del av hotbilden. I andra fall är det den mänskliga faktorn som kan utnyttjas vid cyberangrepp eller som ligger bakom it-incidenter.

[27] Säkerhetspolisens årsbok 2016, s. 40.
[28] FRA:s årsrapport 2016, s. 19.

Sammantaget finns således en rad inriktande initiativ och flera olika styrande dokument som anger vikten av att digitalisering sker i Sverige och att informations- och cybersäkerheten behöver stärkas på många olika verksamhetsområden. Sverige placerar också sig bra i internationella digitaliseringsindex samtidigt som det finns en bekymmersam bild över utvecklingen när det gäller informations- och cybersäkerheten inom många olika samhällssektorer (se även kapitel 8).

5 Utvecklingen av hot, sårbarheter och risker

5.1 Inledning

I detta kapitel lämnas en översiktlig redogörelse över hot, sårbarheter och risker som påverkar behov av stärkt informations- och cybersäkerhet, såväl allmänt som vad gäller säkerhet i nätverks- och informationssystem i säkerhetskänslig verksamhet. Syftet med redogörelsen är dock inte att beskriva alla olika typer av hot, risker och sårbarheter som föreligger då sådana sammanställningar redan finns tillgängliga.[1]

5.2 Hot, sårbarheter och risker

Digitaliseringen påverkar hela samhället och vår säkerhet och ekonomiska välstånd vilar allt mer på digitala grunder. I dag betraktar därför de flesta länder informations- och cybersäkerhet som en stor nationell utmaning och denna säkerhet anses vara av såväl säkerhetspolitisk som utrikespolitisk och därigenom även av strategisk betydelse. Flera av de samhällsviktiga system som är kritiska för att upprätthålla samhällets funktionalitet är redan i fredstid sårbara för angrepp och störningar. Den teknologiska utvecklingen, utbredningen av digitala lösningar och ökade datavolymer skapar stora möjligheter men innebär samtidigt sårbarheter och risker för såväl samhället i stort som för enskilda myndigheter och andra aktörer, bl.a. i näringslivet.

[1] Se bl.a. World Economic Forum, 2019. Hotbilden inom it-området beskrivs närmare av World Economic Forum som genomför en årlig undersökning över de största riskerna som världen står inför I rapporten för 2019 ligger cyberangrepp på femte plats när det gäller sannolikhet och sjunde plats när det gäller konsekvens (www.weforum.org/press/2019/10/cyberattacks-and-fiscal-crises-top-list-of-business-risks-in-2019/).

De hot, sårbarheter och risker som digitaliseringen medför utgör komplexa säkerhetsutmaningar. Hoten blir svårare att upptäcka, beroenden blir svårare att överskåda och sårbarheterna och riskerna blir mer svårbedömda. Exempel på sådana utmaningar är antagonistiska hot som informationsoperationer och cyberangrepp mot skyddsvärda nätverks- och informations, t.ex. i form av spionage, sabotage och dataintrång mot totalförsvarets verksamhet.

Ett cyberangrepp eller storskalig it-incident bedöms i dag kunna få allvarliga konsekvenser för såväl samhällsviktig och ekonomisk verksamhet som kritisk infrastruktur. Det kan även medföra påverkan på både militär och civil verksamhet inom totalförsvaret. Cyberangrepp för att bedöma, påverka eller störa samhällsviktiga funktioner som ett förstadium till en väpnad konflikt utgör ett allvarligt hot. Utflyttning av väsentliga funktioner i samhällsviktig verksamhet till utlandet, t.ex. inom energiförsörjningen, har också inneburit att sårbarheten har förändrats. När det uppstår brister i informations- och cybersäkerheten kan detta få omfattande konsekvenser både för samhället i stort och för olika samhällssektorer (se även kapitel 4 och 8).

Uppkopplad samhällsviktig verksamhet

Stora delar av den samhällsviktiga infrastrukturen, t.ex. energi, och kommunikationer, har industriella informations- och styrsystem[2] som är uppkopplade mot internet. Dessa system behöver inte alltid vara internetanslutna, men av effektivitetsskäl är de ofta uppkopplade mot internet, som ger åtkomst från distans. Många av dessa system är äldre och har därför ofta sårbarheter som en hotaktör kan utnyttja (se kapitel 8). Antalet sårbarheter som är specifika för industriella informations- och styrsystem har ökat kraftigt under senare år. Det är ofta en utmaning att på ett ändamålsenligt sätt säkerhetsuppdatera systemen då de inte är byggda för att regelbundet uppdateras. Detta förstärks av att verksamhetsutövare ofta inte har utrymme eller resurser att tillåta att dessa system får förändras, är avstängda eller att åtgärder som medför fördröjningar i datatrafiken införs. Dessa system och de processer de upprätthåller måste dock ha ett adekvat skydd över hela livslängden, som i vissa fall kan uppgå

[2] S.k. Industrial control systems/supervision control accusation data (ICS/SCADA).

till mer än 20 år, och verksamhetsutövarna måste ha kunskap om de hot, sårbarheter och risker mot säkerheten i systemen som finns.

Sårbarhet genom kritiska beroenden

Kritiska beroenden uppstår när funktionen i en samhällsviktig verksamhet kräver att en annan verksamhet fungerar och där det saknas alternativ. Sådana beroendeförhållanden är en orsak till att samhällsviktiga verksamheter är sårbara Flera av dessa viktiga funktioner styrs och övervakas med stöd av avancerade nätverks- och informationssystem. När ett cyberangrepp eller tekniskt fel inträffar kan det påverka flera delar av samhället samtidigt och konsekvenserna kan i vissa fall bli svåra att överblicka. Ett exempel på ett sådant förhållande är beroendet mellan elförsörjning och elektroniska kommunikationer. Det uppkopplade samhället är nämligen beroende av fungerande elförsörjning och elektroniska kommunikationer.

Att allt fler verksamhetsutövare digitaliserar hela eller delar av sin verksamhet innebär ökade krav på tillgänglighet av el och fungerande uppkoppling. En följd av digitalisering och effektivisering är att även förmågan att leverera el och upprätthålla kommunikationer är digitaliserad, och är därmed sårbar för samma svagheter och utsatt för liknande risker som övrig digitaliserad verksamhet. I de fall styr- och kontrollsystem är exponerade mot internet uppkommer risken för att hotaktörer att utnyttja sårbarheter i systemen för cyberangrepp med betydande konsekvenser för samhället som följd. Förutom de omedelbara konsekvenserna med omfattande strömavbrott så skulle många system som är beroende av fungerande informationsteknologi upphöra att fungera. Det skulle i dag leda till betydande problem på flera nivåer i samhället. Denna utveckling förstärks i och med det ökade utbudet av IoT. Det skapar stora vinster, men som en följd av detta ökar beroendet av el, och i viss mån ökar de sårbarheter som kommer ur det stora elberoendet.

Den internationella dimensionen får samtidigt en alltmer ökad betydelse. Infrastrukturen är i dag sammanflätad och korsar nationsgränser och många privata företag som driver och äger infrastrukturen är verksamma i flera länder. Störningar i informationssystem kan därför snabbt röra sig mellan nationell och internationell nivå. En annan sårbarhet i samhället är därför koncentrationen av ett begrän-

sat antal stora leverantörer som skapar nya sårbarheter i samhället. Vissa verksamheter tillhandahåller så väsentliga tjänster att när deras funktionalitet upphör eller kraftigt reduceras hotas möjligheten att värna samhällets grundläggande värden.

Digitaliseringen och teknikutvecklingen innebär även ändrade förutsättningar för säkerhetsskyddet och informations- och cybersäkerheten. Efter att regleringen av säkerhetsskydd trädde i kraft har informationstekniken och användningen av den genomgått en betydande utveckling. Den tekniska utvecklingen och informationstekniken påverkar i stort sett alla aspekter av säkerhetskänsliga och samhällsviktiga verksamheter.

I dag hanteras stora informationsmängder i såväl öppna som hemliga nätverks- och informationssystem. Den ökade öppenheten medför t.ex. större risk för att aktörer med antagonistiska avsikter utnyttjar de möjligheter som den brett åtkomliga informationen ger för hot och angrepp. Även tillgången till och öppenheten kring stora mängder av information på t.ex. myndigheters webbplatser kan ge användaren nya möjligheter att söka och sammanställa information på ett sätt som kan få konsekvenser för säkerhetsskyddet. Lagring av stora mängder uppgifter i digitala system har ökat kraftigt och fortsätter öka i takt med ökade tekniska möjligheter och ökade ambitioner i samhället. Sammanställningar över t.ex. känsliga anläggningar och objekt kan snabbt och enkelt tas fram genom effektiva sökmotorer. Effekten av detta kan bli att uppgifter, som var för sig inte är skyddsvärda, i aggregerad form kan komma att utgöra en stor sårbarhet. Skyddet av de egna informationstillgångarna, bl.a. nätverks- och informationssystemen, blir därför en grundläggande fråga för samhället i stort men även för många olika aktörer inom samhällsviktiga och säkerhetskänsliga verksamheter. Det är av även grundläggande betydelse att infrastrukturen med väl fungerande elektroniska kommunikationer är säker, tillgänglig och robust (se kapitel 4).

Som framgår av kapitel 4 är en av de stora utmaningarna som finns på informations- och cybersäkerhetsområdet att tekniken ofta utvecklas betydligt snabbare än säkerhetsarbetet. Den snabba tekniska utvecklingen på it-området i kombination med myndigheternas ökande nyttjande av teknik och privatägd infrastruktur innebär även en utmaning för myndigheter och andra aktörer att upprätthålla egen teknisk kompetens. Bristande kunskap och kontroll över vilka it-produkter som nyttjas i nationell infrastruktur och olika nätverks-

och informationssystem ger nya förutsättningar och möjligheter för olika aktörer att genom olika it-angrepp inhämta information om eller påverka nationella skyddsintressen och tillgångar av strategisk betydelse. Informations- och cybersäkerhet kräver därför i dag en helhetssyn eftersom det är ett komplext och gränsöverskridande område, såväl geografiskt som vad avser bl.a. teknik, administration, ekonomi och juridik.

5.3 Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden 2020

I den myndighetsgemensamma rapporten *Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden 2020* redogör Säkerhetspolisen, Försvarsmakten, Försvarets radioanstalt (FRA) och Myndigheten för samhällsskydd och beredskap (MSB) för den aktuella hotbilden.[3] Myndigheterna konstaterar att metoder och verktyg för cyberangrepp utvecklas ständigt och hotaktörernas agerande förändras i takt med teknikutvecklingen. Bland de svenska mål som utsätts för cyberangrepp finns verksamheter som är väsentliga för samhällets grundläggande funktioner. Att kunna skydda sig mot cyberangrepp från kvalificerade hotaktörer är därför en nationell angelägenhet.

Statliga aktörer

Av rapporten framkommer att ett stort antal stater bedöms ha förmåga att genomföra cyberangrepp och statliga aktörer använder cyberangrepp för att uppfylla olika nationella intressen. I de flesta länder är aktörerna nationella underrättelse- och säkerhetstjänster eller grupperingar som har kopplingar till dessa. Vissa statliga aktörer är mycket kvalificerade och genomför cyberangrepp på ett sätt som är storskaligt, systematiskt, uthålligt och globalt för att tillgodose

[3] Regeringen har uppdragit åt FRA, Försvarsmakten, MSB och Säkerhetspolisen att tillsammans vidta förberedande åtgärder och lämna förslag för att ett nationellt cybersäkerhetscenter ska kunna inrättas under 2020. Parallellt med detta sker en fördjupad myndighetssamverkan som syftar till att främja denna uppgift. Som en del i detta har myndigheterna tillsammans med Polismyndigheten gemensamt tagit fram denna rapport. Syftet är att tillsammans – utifrån de lägesuppfattningar som respektive myndighet har – sammanställa en lägesbild som på ett enkelt och tillgängligt sätt beskriver cybersäkerhet ur ett nationellt perspektiv.

det egna landets intressen.[4] Cyberangrepp erbjuder även goda möjligheter till anonymitet, förnekbarhet och vilseledning för den bakomliggande aktören jämfört med mer traditionella metoder. Detta öppnar upp för nya möjligheter att agera utan att hamna i öppna konflikter med andra länder. Myndigheterna konstaterar att cyberangrepp från statliga aktörer mot svenska mål sker hela tiden. Aktörerna utvecklar metodik och verktyg och blir allt mer sofistikerade. Samtidigt fortsätter de att använda sig av äldre kända metoder så länge dessa fortsatt ger resultat. Även cyberangrepp från statliga aktörer i syfte att inhämta underrättelser pågår ständigt mot svenska mål. De angriper bl.a. verksamheter som hanterar känslig eller skyddsvärd information som rör Sveriges säkerhet, men även öppen information kan vara av intresse. Det förekommer att cyberangrepp genomförs för att påverka skeenden i Sverige eller utomlands. Allt ifrån stulen information som används för att misskreditera makthavare och splittra landet, till angrepp som syftar till att slå ut infrastruktur, skada tilliten till institutioner, eller på annat sätt framtvinga eller förhindra att en stat agerar. Statliga aktörer genomför även angrepp för att få åtkomst till individers personliga information. Angreppen sker exempelvis i syfte att få fram känsliga uppgifter som kan användas i utpressningssyfte mot personer i maktposition eller personer som har tillgång till information som aktören vill åt. Det sker även i syfte att bedriva flyktingspionage för att kontrollera oppositionella eller tysta opinioner utomlands. För att komma åt information om individer kan verksamheter som hanterar stora mängder av denna typ av uppgifter angripas. Angrepp sker även direkt mot individers personliga it-utrustning.

Militär förmåga

Statliga aktörer studerar – som förberedelse för att använda cyberangrepp i konflikter – sårbarheter som kan utnyttjas och utvecklar därefter verktyg som behövs för att genomföra cyberoperationer. Sårbarheterna utnyttjas för att ta sig in i system och infektera dessa

[4] Det kan handla om att ge det egna landet utrikes- och säkerhetspolitiska fördelar, gynna det egna landets forskning och utveckling och skapa konkurrensfördelar för inhemska företag, eller skaffa fram underlag för att utföra påverkansoperationer. Det kan även handla om förberedande angrepp som genomförs i syfte att skapa förutsättningar att vid ett senare tillfälle kunna genomföra operationer vars syfte exempelvis kan vara att orsaka skada för den verksamhet som utsätts.

för att kunna slå ut systemet i det fall en konflikt uppstår. Attackerna förbereds i fredstid och kan sedan koordineras med konventionella stridsmedel om det gynnar operationen. Stater kan även genomföra angrepp som stör eller avbryter försvarsrelaterade eller samhällsviktiga funktioner i syfte att minska ett lands förmåga att stå emot ett kommande militärt angrepp eller försvaga ett lands motståndskraft mot påtryckningar. I konflikter mellan stater är cyberoperationer ett av de medel som kan användas för att minska ett lands försvarsvilja, bl.a. genom påverkansoperationer där information som stjäls genom cyberangrepp sedan kan manipuleras och publiceras för att påverka opinionen.[5]

I rapporten konstateras att många länder utvecklar förmåga att genomföra avancerade cyberoperationer, bl.a. i form av offensiva cyberangrepp. Statliga aktörer bedriver även underrättelseinhämtning mot svenska myndigheter och försvarsindustri, bl.a. söker man information genom cyberangrepp, i syfte att kartlägga Sveriges förmåga och sårbarheter med koppling till Sveriges försvarsförmåga. Den tekniska utvecklingen är hög och det upptäcks kontinuerligt nya sårbarheter, varför det pågår en ständig kapplöpning mellan medel och motmedel. Det krävs därför ett konstant utvecklingsarbete för att upprätthålla en förmåga till avancerade cyberoperationer.

Ekonomiska intressen

Kunskap och innovationer är stöldbegärliga för de stater som vill ta genvägar i sin egen teknikutveckling. Genom cyberangrepp och industrispionage uppvägs brister i det egna landets innovationsförmåga. Av rapporten framkommer även att vissa stater bedriver omfattande program som syftar till att stjäla företagshemligheter från andra länder. Cyberangrepp i syfte att genomföra industrispionage mot svenska mål är vanligt förekommande och innebär att svenska företag som utvecklar ny teknik kan komma att konkurreras ut av sina egna lösningar som stulits av statliga aktörer. Det finns även exempel där statliga aktörer har använt cyberangrepp för att skaffa

[5] Genom att välja vilka mål hotaktören inriktar sig mot och hur stor effekt som ska uppnås, finns möjlighet för en statlig aktör att operera i ett tillstånd av fred där krigets lagar inte är tillämpliga. Problematiken kring attribuering och förnekbarhet stärker denna möjlighet. I det fall ett cyberangrepp orsakar skada på samma sätt som ett konventionellt väpnat angrepp kan det under vissa förutsättningar vara att betrakta som ett väpnat angrepp.

sig monetära tillgångar, exempelvis genom att angripa banker för att stjäla pengar, kryptovaluta eller genom att angripa verksamheter och infektera dem med utpressningstrojaner (ransomware) för ekonomisk utpressning. I tider av sanktioner kan stater sättas under stor ekonomisk press och då kan cyberangrepp för att stjäla pengar vara en lösning för landets överlevnad.

Ideologiskt motiverade aktörer

I rapporten konstateras att det finns ideologiskt motiverade aktörer som betraktar angrepp mot svenska mål som legitima, även om förmågan inte motsvarar vilja och ambition att genomföra sådana angrepp. Försök till cyberangrepp med enklare metoder och tekniska medel bedöms dock fortsätta, t.ex. genom distribuerade överbelastningsattacker (DDoS) och kapade hemsidor.

Kriminella aktörer

I rapporten konstateras att cyberkriminalitet är en internationell och gräns- överskridande verksamhet som genomförs där det finns möjligheter till ekonomisk vinning. Vilket mål aktören väljer är vanligen inte intressant, utan det viktigaste är den vinst man kan räkna med. Ransomware, bedrägerier, stölder och liknande kriminella aktiviteter drabbar såväl företag som myndigheter och deras leverantörer, ofta verksamheter med höga skyddsvärden.

I rapporten konstateras att en tillbakablick på inträffade händelser visar att hotaktörer har en tendens att använda de verktyg som fungerar för stunden. I stället för att använda nya och avancerade metoder väljer de att förfina existerande metoder och det blir allt svårare för användare att upptäcka förfalskningar och bedrägerier. DDoS-angreppen fortsätter där det vanligaste motivet är utpressning men också många gånger med intentionen att endast orsaka målet skada. Spridningen av utpressningstrojaner har skiftat från att riktas brett och urskillningslöst, till att i stället riktas mot specifika företag. Kriminella hotaktörer fokuserar även på att in- hämta uppgifter som antingen används av dem själva, eller så säljs uppgifterna vidare på Darkweb. Tidigare har ett tillvägagångssätt varit att använda phishing av olika slag för att lura till sig sådana uppgifter direkt från

enskilda individer. Ett skifte är att aktörer flyttat fokus från angrepp direkt mot individer till att i stället angripa mindre e-handelsplatser där de får större effekt av sina cyberangrepp.

Metoder för initial åtkomst

Ett viktigt steg i ett cyberangrepp är den initiala kontroll angriparen behöver skaffa sig i systemet man vill få åtkomst till. Målsättningen med detta steg är vanligen att angriparen vill få möjlighet att exekvera skadlig kod i systemet för att på så sätt exempelvis erhålla möjligheter att påverka systemet i sig eller kunna nå priviligierad information i detsamma. För att dessa metoder ska kunna användas förutsätts att det finns en eller flera sårbarheter som kan utnyttjas av angriparen. I rapporten redogörs för vanliga eller effektiva metoder som används för att få initial kontroll, vilka ofta benämns attack- eller angreppsvektorer. Dessa metoder används ofta vid cyberangrepp men ska inte betraktas som en uttömmande lista, utan en delmängd av de metoder som ofta används av flera typer av aktörer (se även kapitel 6).

I rapporten konstateras vidare att det pågår ständig forskning i jakt på nya och okända sårbarheter, s.k. zero-day-sårbarheter. Okända sårbarheter som upptäcks av hotaktörer kan utnyttjas utan omvärldens vetskap och utan skydd mot dessa sårbarheter. Till följd av detta har det uppstått en marknad för zero-days där både statliga och kriminella aktörer utgör köpare och säljare. På denna marknad säljer individer och företag sårbarheter till mäklare, som sedan säljer vidare till andra tillverkare, kriminella eller statliga aktörer.

5.4 Cyberangrepp mot myndigheter

Myndigheten för samhällsskydd och beredskap (MSB) presenterar årligen en sammanställning och analys av de rapporter om allvarliga it-incidenter som mottagits från statliga myndigheter sedan april 2016. Myndigheterna ska skyndsamt rapportera it-incidenter som inträffat i myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation.

MSB mottog under 2020 sammanlagt 286 rapporter från 93 myndigheter. Den vanligaste incidentkategorin var handhavandefel, följt av angrepp, störning i mjukvara eller hårdvara samt störning i driftmiljö. I ungefär hälften av fallen angavs incidenten ha fått begränsade konsekvenser och i ungefär en fjärdedel angavs incidenten ha fått stora konsekvenser.[6]

Förutom redogörelse för de incidenter som inkommit innehåller rapporten även ett antal lärande exempel på incidenter som inträffat och rekommenderade åtgärder.

En analys av de rapporterade incidenterna visar att:

- Covid-19-pandemin förefaller inte bara ha påverkat informations- och cybersäkerheten genom hur och var vi arbetar utan även incidentrapporteringen.
- Andelen rapporterade angrepp har minskat medan andelen incidenter relaterade till störningar i driftmiljö, mjuk- eller hårdvara eller rena handhavandefel har ökat.
- Komplexa system och miljöer får större konsekvenser.

Baserat på den inkomna rapporteringen bedömer MSB att myndigheterna bl.a. behöver höja lägstanivån, analysera beroendet till externa leverantörer samt se över sin incidenthantering och incidentrapportering.

5.5 Cyberangrepp mot företag

I rapporten *Cyberhoten mot Sverige 2019 – En undersökning om hur 100 större svenska bolag ser på cyberbrott nu och i ett framtidsperspektiv*[7] redovisas en helhetsbild över hur 100 större svenska bolag ser på cyberhot i dag och i framtiden. Av rapporten framkommer att när det gäller det egna företaget så väntas allt fler attacker mot den egna verksamheten och att cyberbrottsligheten förväntades öka markant under 2019. Närmare hälften (49 procent) av företagen blev utsatta för en cyberattack under 2018, vilket var i nivå med det föregående årets undersökning (47 procent). 65 procent av företagen räknade

[6] MSB:s årsrapport *Statliga myndigheters it-incidentrapportering 2020 – Utmaningar för en säker och robust informationshantering.*
[7] *Cyberhoten mot Sverige 2019 – En undersökning om hur 100 större svenska bolag ser på cyberbrott nu och i ett framtidsperspektiv, PricewaterhouseCoopers (PwC), 2020.*

med att 2019 skulle bli ett besvärligare år med fler cyberattacker mot den egna organisationen. Vidare ansåg 81 procent av företagen att ny teknik som robotik och automatisering ökar riskerna för cyberattacker. Närmare hälften (48 procent) av företagen ansåg att tredjepartsrisker, dvs. risker som uppkommer till följd av tekniksamarbeten, samarbeten med leverantörer och andra former av samarbeten, ökade under 2018.

Av rapporten framkommer vidare att en majoritet av företagen anser att Sverige är inte tillräckligt rustat för att möta de ökade cyberhoten. Undersökningen visar tydligt att de ökade hotbilderna när det gäller cyberbrott har en stor påverkan på hela samhället och att det finns en enighet i näringslivet om problemets omfattning.

Enligt rapporten visar resultaten från undersökningen att det återstår mycket arbete när det gäller prioritering av frågorna om cybersäkerhet i de svenska storföretagen. Undersökningen visar att få företag inser att cybersäkerhet är en verksamhetskritisk fråga med påverkan på hela företagets existens. T.ex. rapporterar endast 28 procent av informationssäkerhetscheferna (CISO) direkt till verkställande direktören eller styrelse och av dessa är det endast fyra procent som rapporterar till styrelsen. I rapporten framhålls att skillnaden är markant i jämförelse med omvärlden, t.ex. visade den globala undersökning *Global State of Information Security Survey 2018* att 67 procent av företagens CISO:s rapporterar direkt till vd eller styrelse och 27 procent till styrelsen. Anmärkningsvärt är även att närmare hälften (43 procent) av företagen inte tycker eller inte vet om styrelsen är tillräckligt engagerad i cybersäkerhetsfrågorna. 43 procent av företagen tycker inte att eller vet inte om styrelsen är tillräckligt engagerad i cybersäkerhetsfrågorna.

Av rapporten framkommer även att 83 procent av företagen anser även att det svenska samhället inte är tillräckligt rustat för att klara av de ökade cyberhoten. Många företag anser att det görs för få insatser från politiskt håll. 76 procent av tillfrågade företag anser att svenska politiker inte tar cybersäkerhet som samhällsutmaning på tillräckligt stort allvar i dagsläget, andelen som ansåg att politikerna tar cybersäkerhet som samhällsutmaning på tillräckligt stort allvar i dagsläget minskade också från 22 procent till 14 procent. Företagen anser vidare att politikerna gör för lite för att möta den här negativa utvecklingen.

5.5.1 CYBERHOTEN – Så ser hotbilden och attackerna ut mot svenska teknikföretag (2019)

I rapporten *CYBERHOTEN – Så ser hotbilden och attackerna ut mot svenska teknikföretag*[8] framhålls att industrin och företag i Sverige genomgår en omfattande digitalisering. Utvecklingen innebär att utrustning och verktyg både kan kopplas upp och kopplas ihop till en rimlig kostnad, samt att data som skapas i olika processer kan fångas upp och användas. Detta ger möjlighet till ökad produktivitet, nya affärsmöjligheter och en ökad miljömässig hållbarhet. Parallellt med dessa möjligheter så har också förväntningarna och kraven ökat från kunder och leverantörer att tjänster ska finnas att tillgå digitalt. Med digitaliseringen kommer samtidigt en ökad sårbarhet som gäller alla företag, oavsett storlek. Digitaliseringen ger upphov till stora risker som måste hanteras. För mindre teknikföretag och underleverantörer är det tre faktorer som, enligt rapporten, är särskilt utmanande:

– frekvensen, såväl som konsekvensen, av cyberattacker har ökat,
– attackerna har även blivit diversifierade, mer sofistikerade och riktade mot specifika sektorer, samt
– mindre teknikföretag och underleverantörer är numera primära måltavlor.

Hälften av teknikföretagen har angripits det senaste året

I rapporten anges att antalet cyberattacker mot olika företag och myndigheter i Sverige har ökat och uppgår till över 100 000 per år. Angreppen mot företagen sker i olika former. I början av 2020 var över 17 000 datorer infekterade i Sverige, dvs. de var bl.a. angripna av virus eller utgjorde delar av ett botnät. Motsvarande siffra för mobila enheter uppskattas till omkring 400 000. Denna mängd datorer och mobiler kan sedan användas för koordinerade attacker mot enskilda företag eller specifika branscher och riskerar då att slå ut exempelvis kritiska produktionssystem. Den mest frekventa formen av angrepp som företagen identifierat sker genom elakartad programvara som virus och trojaner samt genom att sårbarheter i de digitala systemen utnyttjas för intrång.

[8] *CYBERHOTEN – Så ser hotbilden och attackerna ut mot svenska teknikföretag*, Teknikföretagen, 2019.

Av rapporten framkommer vidare att bland Teknikföretagens medlemmar, dvs. tillverkande företag och industrinära tjänsteföretag, uppgav nära hälften att de blev utsatta för cyberangrepp under 2018–2019. Andelen för företag i övriga sektorer i näringslivet var knappt 25 procent. En särskild utmaning är att cyberattackerna som riktas mot företagen bedrivs långsiktigt och systematiskt där bitar av information läggs samman. I detta perspektiv är mindre teknikföretag och underleverantörer nyckelkomponenter för att komma över uppgifter.

Olika aktörer utför olika typer av angrepp

Av rapporten framkommer att sedan ett antal år tillbaka kommer cyberhoten som möter industrin i Sverige i stor utsträckning från främmande makter. Dessa stater utför själva attackerna eller ger direkt stöd åt kriminella grupperingar för riktade intrångsförsök. Sammantaget är det ett femtontal länder som aktivt opererar med sikte på svenska företag. Attackerna kombineras med påverkansoperationer, traditionella underrättelseaktiviteter och strategiska uppköp, vilket riktas mot bl.a. företag inom elektronik, kommunikationsteknik och industriella produkter. I sammanhanget kan noteras att en del av de företag som är måltavlor, tillhandahåller civila komponenter och produkter, som har dubbla användningsområden. Genom att produkterna även kan användas för militära ändamål är de av särskilt intresse för främmande makter.

Angrepp för miljarder och stort mörkertal

Av rapporten framkommer även att på samma sätt som attackerna varierar, på samma sätt skiftar konsekvenserna. För Teknikföretagens medlemmar innebar cyberattackerna under 2019 att system blev otillgängliga och att data blev publikt eller att affärshemligheter stulits. Bedömningen var att denna utveckling skulle fortsätta med ökande styrka även under år 2020. Samtidigt kan noteras att företag ogärna offentliggör när de blivit attackerade, varför redovisade uppgifter – enligt rapporten – sannolikt döljer ett stort mörkertal. Dessutom förblir många företag ovetandes om att de överhuvudtaget har blivit utsatta för angrepp.

I rapporten anges att en rimlig uppskattning är att de samlade direkta kostnaderna uppgår till cirka 16 miljarder kronor för svenska företag, vilket främst drabbar de forskningsintensiva industriföretagen och företag som arbetar med dem, exempelvis underleverantörer. Även störningar och avbrott som följer av cyberattacker är riskabla och kan bli kostsamma. Under 2019 rapporterades exempelvis 50 allvarliga och betydande incidenter. Kostnaden för dessa har inte bl.a. uppskattats, men totalt beräknas en nedstängning eller blockering av datatrafiken i Sverige generera en kostnad för samhället på omkring 6 miljarder kronor om dagen.

5.5.2 Cybersäkerhet – En kartläggning av Sveriges nuläge 2020 och framtidsutsikter för branschen

I studien *Cybersäkerhet – En kartläggning av Sveriges nuläge 2020 och framtidsutsikter för branschen*[9] redovisas bl.a. nuläget och framtidsutsikter för cybersäkerhetsbranschen vad gäller utbildning, företag och kompetens inom området.[10] Sammanfattningsvis framkommer av studien att den snabba och omfattande digitaliseringen driver utvecklingen av cybersäkerhetsmarknaden framåt. Det finns dock ett stort behov av kompetens på området, både när det gäller utbildningar och när det gäller den interna kompetensen hos anställda på myndigheter och företag. Cybersäkerhet är dessutom ett brett område som sträcker sig utanför it-avdelningar och rena teknikbolag och därför krävs också olika kompetenser i kombination med cybersäkerhet. Det saknas dock teknisk kompetens i form av ingenjörer men också inom andra yrken som jurister och statsvetare.

I studien lyfter respondenterna[11] genomgående människan som den största risken när det kommer till cybersäkerhet, liksom brist-

[9] Kartläggningen utfördes av Unitalent på uppdrag av Linköpings Science Park, Tillväxtverket och Security Link, en centrumbildning vid Linköpings universitet, KTH, Chalmers och FOI.
[10] Kartläggningen är avgränsad till att undersöka den svenska marknaden för cybersäkerhet. etta görs främst ur ett nationellt perspektiv, i viss mån sker även en internationell utblick. Begreppet cybersäkerhet är i vissa sammanhang synonymt med it-säkerhet och informationssäkerhet – i den här rapporten särskiljs dock begreppen. Cybersäkerhet definieras som en delmängd av it-säkerhet och informationssäkerhet, där det finns ett fokus på att skydda den digitala informationen i system och processer mot ett antagonistiskt hot. Vidare är cybersäkerhet något som berör många olika typer av verksamheter, med cybersäkerhetsmarknaden respektive cybersäkerhetsbranschen avses i det här fallet de företag och organisationer som arbetar direkt med frågor, produkter eller tjänster gällande cybersäkerhet.
[11] Kartläggningen är baserad på aktuell litteratur, rapporter från myndigheter, medierapportering samt semi-strukturerade intervjuer med erfarna personer med kunskaper inom olika områden kopplat till cybersäkerhet.

fälliga riskanalyser och bristande, kontinuerligt säkerhetsarbete. Därtill lyfts att utvecklingen av nya tekniker såsom AI och IoT skapar nya möjligheter men också risker. Enligt studien visar kartläggningen på att det finns stora utvecklingsområden och behov av insatser på området.

6 Säkerhetskänslig verksamhet

6.1 Inledning

I säkerhetsskyddslagen (2018:585) finns bestämmelser om säkerhetsskydd i säkerhetskänslig verksamhet. Säkerhetsskyddsförordningen (2018:658) innehåller kompletterande bestämmelser till säkerhetsskyddslagen.[1]

I direktiven framhålls att för *informationssystem* som används i eller har betydelse för säkerhetskänslig verksamhet finns särskilda krav i säkerhetsskyddsförordningen (2018:658). Det rör sig dels om förberedande åtgärder inför driftsättning av sådana informationssystem, dels om säkerhetskrav som kontinuerligt ställs på informationssystemen.

Bestämmelserna innebär att det är *verksamhetsutövaren* som *ansvarar* för att se till att informationssystemen upprätthåller kraven på informationssäkerhet.

Bestämmelserna innehåller även krav på *samråd* med Säkerhetspolisen eller Försvarsmakten i vissa fall. Detta gäller för informationssystem som kan komma att behandla säkerhetsskyddsklassificerade uppgifter av visst slag och informationssystem där obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är obetydlig.

Enligt direktiven finns det anledning att överväga om *ytterligare krav* bör införas för att säkerställa att *nätverks- och informationssystem* som ska användas i *säkerhetskänslig verksamhet* uppfyller de krav som behövs för att upprätthålla skyddet av sådana verksamheter.

I detta avsnitt redogörs översiktligt för relevanta bestämmelser om säkerhetsskydd i säkerhetsskyddslagen respektive den anslutande förordningen. I efterföljande kapitel 7 lämnas en närmare redogörelse för det nationella regelsystemet för *informationssäkerhet* i *säkerhets-*

[1] Ord och uttryck som används i förordningen har samma innebörd som i lagen.

känslig verksamhet, som är det begrepp som används i regleringen för att beskriva åtgärder som syftar till säkerhet i bl.a. nätverks- och informationssystem (informationssystem). I 1 kap. 5 § angivna förordning anges att med informationssystem avses ett *system av sammansatt mjuk- och hårdvara som behandlar information*.

6.2 Säkerhetsskyddslagen

Säkerhetskänslig verksamhet är enligt 1 kap. 1 § säkerhetsskyddslagen (2018:585)[2] sådan verksamhet

- som är av betydelse för *Sveriges säkerhet*, eller
- som omfattas av ett för Sverige förpliktande *internationellt åtagande* om säkerhetsskydd.

Säkerhetsskyddslagens bestämmelser gäller för den som till någon del bedriver säkerhetskänslig verksamhet (*verksamhetsutövare*).

6.2.1 Sveriges säkerhet

Säkerhetsskydd har traditionellt uttryckts som olika åtgärder för att skydda totalförsvaret eller rikets säkerhet i övrigt. Uttrycket rikets säkerhet är i säkerhetsskyddslagen numera ersatt av *Sveriges säkerhet* men liksom tidigare finns ingen tydlig definition angiven i säkerhetsskyddslagen. Uttrycket förekommer dock även i annan lagstiftning och kan sammanfattas som Sveriges oberoende – i betydelsen självständighet och suveränitet – och bestånd. Detta innefattar rätt till okränkta landsgränser, ett bevarande av det svenska självstyret och det demokratiska statsskicket samt av nationens grundläggande funktionalitet.

Såväl myndigheter som enskilda driver ett stort antal samhällsviktiga verksamheter som i helhet eller delar kan vara av större eller mindre betydelse. Detta brukar illustreras med en pyramid där den översta delen utgörs av de verksamheterna som är av betydelse för Sveriges säkerhet ur ett nationellt perspektiv (se figuren i avsnitt 3.5).

[2] I lagen finns också bestämmelser som gäller den som avser att överlåta aktier eller andelar i säkerhetskänslig verksamhet och om internationell samverkan på säkerhetsskyddsområdet.

Dessa verksamheter har ett *kvalificerat skyddsbehov* och omfattas av säkerhetsskyddslagen.

Uttrycket ”Sveriges säkerhet” tar sikte på sådant som är av grundläggande betydelse för Sverige. I detta ingår bland annat det militära och civila försvaret, den nationella ekonomin, de brottsbekämpande myndigheterna, domstolarna och sådana leveranser av exempelvis livsmedel, elkraft, dricksvatten och drivmedel som är nödvändiga för samhällets funktionalitet på nationell nivå. Anläggningar, objekt, system och liknande verksamhet identifieras och graderas utifrån vilken typ och grad av skada som direkt eller uppenbart indirekt kan uppstå för Sveriges yttre säkerhet, för Sveriges inre säkerhet, på nationellt samhällsviktig verksamhet och för Sveriges ekonomi. Detsamma gäller för anläggningar och objekt där det bedrivs verksamhet som vid en antagonistisk handling kan generera skadekonsekvenser på nationell nivå på andra säkerhetskänsliga verksamheter (s.k. skadegenererande verksamhet).

Vad som är av betydelse för Sveriges säkerhet kan *förändras över tid* och i takt med att samhället utvecklas. Ett exempel är hur samhällets funktionalitet de senaste åren blivit mer beroende av datasystem och mobiltelefoni. Av denna anledning är det viktigt att verksamhetsutövare med regelbundenhet uppdaterar sin *säkerhetsskyddsanalys* (se nedan) och bedriver ett fortlöpande *säkerhetsskyddsarbete*.

6.2.2 Internationellt åtagande om säkerhetsskydd

Med internationellt åtagande om säkerhetsskydd avses att Sverige förbundit sig att *skydda* något åt en annan stat eller mellanfolklig organisation, t.ex. *uppgifter* som utbytts inom militära samarbeten eller samarbeten mot terrorism.

6.3 Vad som avses med säkerhetsskydd

I 1 kap. 2 § säkerhetsskyddslagen anges att med *säkerhetsskydd* avses:

- Skydd av säkerhetskänslig verksamhet mot *spionerі*, *sabotage*, *terroristbrott och andra brott* som kan hota verksamheten samt
- Skydd i *andra fall* av säkerhetsskyddsklassificerade uppgifter.

Säkerhetsskydd behövs för att skydda säkerhetskänsliga verksamheter mot olika typer av *antagonistiska* handlingar från hotaktörer med varierande avsikt och förmåga (se kapitel 5).

Säkerhetsskydd som ett system av samverkande åtgärder

Säkerhetsskydd kan övergripande beskrivas som ett system av samverkande åtgärder som syftar till att skapa ett heltäckande skydd. Olika verksamhetsutövare har många gånger olika förutsättningar för verksamheten och säkerhetsskyddsåtgärderna måste därför anpassas efter den säkerhetskänsliga verksamhetens förutsättningar. Detta gör säkerhetsskydd till ett många gånger komplext område där olika åtgärder måste fogas samman för att värna Sveriges säkerhet eller det Sverige åtagit sig att skydda åt andra stater och mellanfolkliga organisationer.

Säkerhetsskydd kan beskrivas som ett system av åtgärder som utifrån säkerhetsskyddsanalysen tillsammans skyddar den säkerhetskänsliga verksamheten. Merparten av åtgärderna inom säkerhetsskydd kan sorteras in i någon av de tre säkerhetsskyddsåtgärderna *informationssäkerhet*, *fysisk säkerhet* och *personalsäkerhet*. Andra åtgärder som ingår i systemet av säkerhetsskydd är exempelvis anmälan av säkerhetshotande händelser och säkerhetsskyddsavtal med leverantörer.

En grundförutsättning för ett heltäckande säkerhetsskydd är samspelet mellan olika typer av åtgärder som överlappar varandra. Exempelvis räcker det inte att enbart skydda ett informationssystem med informationssäkerhet som hindrar intrång via internet. Det krävs även fysisk säkerhet för att förhindra att obehöriga kommer åt datautrustningen samt personalsäkerhet för att förebygga att personer som inte är pålitliga ur säkerhetssynpunkt får arbeta med systemet.

Utöver samspelet måste hela kedjan av åtgärder vara jämnstark så att det inte finns några svaga länkar. Om exempelvis personal reser med säkerhetsskyddsklassificerade uppgifter mellan arbetsplatser måste transporten regleras så den inte utgör en sårbarhet. I annat fall kan en angripare utnyttja detta och slå till på en plats där nivån av säkerhetsskydd är lägre än på arbetsplatserna.

Begreppet säkerhetskänslig verksamhet omfattar således såväl militär som civil verksamhet och är oberoende av om verksamheten bedrivs av det offentliga eller av enskilda aktörer. Inom många verk-

samheter är endast *en viss del*, *tillgång* eller *funktion* av betydelse för Sveriges säkerhet. Verksamhetsutövaren måste då analysera vilka delar som är säkerhetskänsliga så att säkerhetsskyddsåtgärderna inte görs onödigt omfattande men inte heller missar delar som omfattas av säkerhetsskyddslagens krav.

Utgångspunkten är att verksamheten ska ha direkt betydelse för Sveriges säkerhet men även verksamhetsutövare som t.ex. levererar driftstjänster såsom data och telekommunikation, kan anses bedriva verksamhet som är av betydelse för Sveriges säkerhet. Det kan då vara den *samlade betydelsen* som indirekt aktualiserar behovet av säkerhetsskydd även om de enskilda uppdragen sedda var och en för sig inte är säkerhetskänsliga.

Den som hanterar *säkerhetsskyddsklassificerade uppgifter* anses redan på den grunden bedriva säkerhetskänslig verksamhet eftersom uppgifterna i sig är av betydelse för Sveriges säkerhet. Detta oavsett om uppgifterna rör den egna verksamheten eller härrör från någon annan verksamhetsutövare, t.ex. vid arkivförvaring av handlingar. Även verksamheter som hanterar *allmänt åtkomlig information* såsom meteorologiska data och kartor *kan* vara säkerhetskänsliga. Uppgifterna kan exempelvis behöva vara tillgängliga för nationell flygtrafikledning eller olika former av beredskap för reparationer av nationellt viktig infrastruktur.

De internationella åtagandena om säkerhetsskydd som staten Sverige har åtagit sig omfattar framför allt *hantering av uppgifter*.

Sverige har förbundit sig att skydda säkerhetsskyddsklassificerade uppgifter för ett trettiotal andra stater och mellanfolkliga organisationer, bl.a. EU och NATO.

Därutöver har Sverige även andra internationella åtaganden gällande exempelvis luftfartsskydd. *Verksamheter som omfattas av sådana åtaganden* är att anse som *säkerhetskänsliga*. Det förekommer att myndigheter vid samarbete med utländska myndigheter självständigt kommer överens om olika typer av skyddsåtgärder. Denna typ av egna överenskommelser gör dock inte att verksamheten omfattas av säkerhetsskyddslagen.

Säkerhetsskyddsanalys är grunden för säkerhetsskydd. Själva bedömningen av om en verksamhet är säkerhetskänslig eller inte har sin grund i verksamhetens säkerhetsskyddsanalys. Efter det initiala

konstaterandet att verksamheten är säkerhetskänslig följer en mer detaljerad analys av på vilket sätt och i vilken utsträckning.[3]

Skillnaden mellan säkerhetsskydd och andra säkerhetsåtgärder[4]

Utöver behovet av säkerhetsskydd försöker de flesta verksamheter skydda sig mot olika risker för att inte drabbas av exempelvis produktionsavbrott. I många fall är skyddet inriktat på olyckor, men det kan även i likhet med säkerhetsskydd ta höjd för antagonistiska handlingar såsom anlagda bränder eller industrispionage. Säkerhetsskyddet och andra säkerhetsåtgärder kan mycket väl sammanfalla men det är i så fall viktigt att klargöra vilka perspektiv som är grunden för respektive åtgärd.

Säkerhetsåtgärder som utgår från verksamhetens egna krav och incitament är valfria, medan skyddet av det som faller inom ramen för säkerhetsskydd är tvingande genom lag. Denna skillnad i perspektiv påverkar det grundläggande arbetet med analyser och efterföljande val av åtgärder och hur omfattande dessa behöver vara. I exempelvis en affärsriskanalys kan den bedömda sannolikheten för olika händelser vägas mot kostnaden för åtgärder och vilka möjliga förluster organisationen är beredd att acceptera.

I en säkerhetsskyddsanalys beaktas inte sannolikheten, utan utgångspunkten är i stället de *konsekvenser* som måste undvikas. Utrymmet att själv välja vad som är en lagom skyddsnivå är begränsat eftersom principen är att skyddet för en säkerhetskänslig verksamhet ska vara detsamma oavsett vem som är verksamhetsutövare.

Säkerhetsskyddets huvudsakliga inriktning att *skydda mot antagonistiska handlingar* gör att säkerhetsåtgärder som renodlat syftar till att minska konsekvenserna av olyckor i regel inte utgör fullgoda säkerhetsskyddsåtgärder. Det finns vissa åtgärder som är förbehållna säkerhetskänslig verksamhet. Merparten av dessa finns inom personalsäkerhetsområdet i form av de registerkontroller som ska utföras innan och under anställning. Med detta perspektiv blir det ännu tydligare hur viktigt det är att hålla isär åtgärder som vidtas med avseende på säkerhetsskydd från verksamhetens övriga behov.

[3] För dessa moment har Säkerhetspolisen gett ut en separat vägledning, *Säkerhetsskyddsanalys*, där begreppen utvecklas.
[4] 1 kap. 2 § säkerhetsskyddslagen.

6.4 Konsekvenskategorier

Verksamhetsutövare ska *identifiera anläggningar, objekt, system eller liknande verksamhet* som har betydelse för Sveriges säkerhet utifrån vilken typ av skada en antagonistisk handling direkt eller uppenbart indirekt skulle kunna medföra. Identifieringen ska göras enligt följande konsekvenskategorier[5]:

- *Skada för Sveriges yttre säkerhet*: Sveriges yttre säkerhet kan delas in i förmågan att upprätthålla nationellt försvar (territoriell suveränitet) samt Sveriges integritet, oberoende och handlingsfrihet (politisk självständighet). Utöver Försvarsmakten finns andra verksamheter, till exempel vissa myndigheter och enskilda inom försvarsindustrin, som är viktiga för det militära försvarets förmåga att utföra sitt uppdrag inom ramen för totalförsvaret.
- *Skada för Sveriges inre säkerhet*: Sveriges inre säkerhet rör förmågan att upprätthålla och säkerställa grundläggande strukturer i form av det demokratiska statsskicket, rättsväsendet och den brottsbekämpande förmågan på nationell nivå. Säkerhetsskyddet för Sveriges inre säkerhet handlar till stor del om att skydda särskilt kritiska anläggningar, funktioner och informationssystem.
- *Skada på nationellt samhällsviktig verksamhet*: Verksamheter som rör leveranser, tjänster och funktioner som är nödvändiga för samhällets funktionalitet på nationell nivå. Dessa verksamheter finns ofta inom, men är inte begränsat till, sektorerna energiförsörjning, livsmedelsförsörjning, elektroniska kommunikationer, vattenförsörjning, transporter och finansiella tjänster.
- *Skada för Sveriges ekonomi*: Verksamheter som är nödvändiga för den nationella betalningsförmågan och där en ekonomisk skada kan få negativa konsekvenser för Sveriges suveränitet, handlingsfrihet och oberoende.
- *Skadegenererande verksamhet*: Verksamheter som, om de utsätts för antagonistisk handling, kan generera direkta eller uppenbara indirekta skadekonsekvenser på andra säkerhetskänsliga verksamheter på nationell nivå genom påverkan på liv, hälsa och infrastruktur.

[5] 2 kap. 2 § Säkerhetspolisens föreskrifter om säkerhetsskydd.

6.4.1 Konsekvensnivåer

Säkerhetskänslig verksamhet som identifierats tillhöra en konsekvenskategori enligt ovan ska därefter *graderas* utifrån *konsekvensnivåer* beroende på hur allvarlig skada en antagonistisk handling skulle kunna medföra.[6] Till skillnad från konsekvenskategori kan en verksamhet som helhet bara tillhöra en konsekvensnivå. Om verksamheten återfinns i flera konsekvenskategorier väljs den konsekvensnivå där den potentiella graden av skada för Sveriges säkerhet är som störst.

Indelningen i konsekvensnivåer sker enligt följande:

- Nivå 5: Synnerligen allvarlig skada för Sveriges säkerhet.
- Nivå 4: Allvarlig skada för Sveriges säkerhet.
- Nivå 3: Inte obetydlig skada för Sveriges säkerhet.
- Nivå 2: Ringa skada för Sveriges säkerhet.
- Nivå 1: Inte mätbar eller inte relevant konsekvens med bäring på Sveriges säkerhet.

De verksamheter som bedöms tillhöra konsekvensnivåerna 4 och 5 benämns *särskilt säkerhetskänslig verksamhet* och omfattas av särskilda bestämmelser (se nedan). Verksamheter som vid ett angrepp endast bedöms kunna medföra skada enligt nivå 1 omfattas inte av kraven på säkerhetsskydd.

6.4.2 Särskilt säkerhetskänslig verksamhet

Verksamhet som tillhör de ovannämnda konsekvensnivåerna 4 och 5 benämns som särskilt säkerhetskänsliga verksamheter och omfattas av två särskilda krav:[7]

– rapportering till tillsynsmyndighet,
– dimensionering med hjälp av dimensionerande hotbeskrivning (DHB).

[6] 2 kap. 3 § Säkerhetspolisens föreskrifter om säkerhetsskydd.
[7] 2 kap. 6 och 8 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd.

Rapportering till tillsynsmyndighet

Verksamhetsutövare som bedriver *särskilt säkerhetskänslig* verksamhet ska *rapportera* till respektive tillsynsmyndighet att sådan verksamhet bedrivs. Syftet med rapporteringen är att tillsynsmyndigheterna ska kunna ha en samlad bild över vilka verksamhetsutövare som är verksamma inom respektive tillsynsmyndighets ansvarsområde. Detta så att såväl tillsyn som rådgivning ska kunna prioriteras för de verksamheterna som är av störst betydelse för Sveriges säkerhet. De verksamhetsutövare som står direkt under Säkerhetspolisens tillsynsansvar ska rapportera dit.[8] De verksamhetsutövare som står direkt under Försvarsmaktens tillsynsansvar ska rapportera dit.

Dimensionerande hotbeskrivningar (DHB)

Säkerhetspolisen tar i samråd med tillsynsmyndigheterna fram *dimensionerande hotbeskrivningar* (DHB) till de verksamhetsutövare som bedriver särskilt säkerhetskänslig verksamhet. En DHB syftar till att ge en långsiktigt hållbar beskrivning av en antagen angripares förmåga, oberoende av om det för stunden föreligger ett konkret hot mot verksamheten. Verksamhetsutövaren ska använda den DHB:n för att dimensionera sitt säkerhetsskydd vilket innebär att DHB i praktiken utgör en lägstanivå för vad säkerhetsskyddet ska klara av att skydda mot.[9]

6.5 Grundläggande bestämmelser om säkerhetsskydd

Skyldigheter för den som bedriver säkerhetskänslig verksamhet

I 2 kap. 1 § säkerhetsskyddslagen anges att den som bedriver säkerhetskänslig verksamhet ska utreda behovet av säkerhetsskydd (*säkerhetsskyddsanalys*). Säkerhetsskyddsanalysen ska dokumenteras.

Med utgångspunkt i analysen ska verksamhetsutövaren planera och vidta de *säkerhetsskyddsåtgärder* som behövs med hänsyn till verk-

[8] Se vidare information på Säkerhetspolisens webbplats.
[9] Närmare beskrivning av DHB finns i Säkerhetspolisens vägledning *Säkerhetsskyddsanalys*.

samhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.

Verksamhetsutövaren ska även kontrollera säkerhetsskyddet i den egna verksamheten, anmäla och rapportera sådant som är av vikt för säkerhetsskyddet och i övrigt vidta de åtgärder som krävs enligt den angivna lagen. Så långt det är möjligt ska säkerhetsskyddsåtgärderna utformas så att de inte medför någon skada eller annan olägenhet för andra allmänna eller enskilda intressen.

Säkerhetsskyddsåtgärder

Med *säkerhetsskyddsåtgärder* avses i den angivna lagen åtgärder som syftar till informationssäkerhet, fysisk säkerhet och personalsäkerhet.

I 2 kap. 2 § samma lag anges att *informationssäkerhet* ska

1. förebygga att säkerhetsskyddsklassificerade uppgifter *obehörigen röjs, ändras, görs otillgängliga eller förstörs*, och
2. förebygga skadlig inverkan *i övrigt på uppgifter* och *informationssystem* som gäller säkerhetskänslig verksamhet.

I 3 § anges att f*ysisk säkerhet* ska

1. förebygga att obehöriga får *tillträde till områden, byggnader och andra anläggningar eller objekt* där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där säkerhetskänslig verksamhet i övrigt bedrivs, och
2. förebygga skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt som avses i 1.

I 4 § anges att *personalsäkerhet* ska

1. förebygga att personer som *inte är pålitliga från säkerhetssynpunkt* deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av någon annan anledning är säkerhetskänslig, och
2. säkerställa att de som deltar i säkerhetskänslig verksamhet har *tillräcklig kunskap* om säkerhetsskydd.

Som inledningsvis nämnts kan säkerhetsskydd övergripande beskrivas som ett system av samverkande åtgärder som syftar till att skapa ett heltäckande skydd. Merparten av åtgärderna inom säkerhetsskydd kan sorteras in i något av de tre huvudområdena informationssäkerhet, fysisk säkerhet och personalsäkerhet vilka här förklaras översiktligt. Säkerhetsskyddslagen benämner dessa tre områden säkerhetsskyddsåtgärder och för respektive område har Säkerhetspolisen gett ut specifika vägledningar.

6.5.1 Informationssäkerhet

Alla verksamheter är beroende av att kunna inhämta, lagra, bearbeta och kommunicera information i olika former. Den tekniska utvecklingen har på senare år gjort informationssystem till viktiga verktyg i hanteringen, men även pappersdokument används fortfarande. Säkerhetsskyddsåtgärden informationssäkerhet syftar till att skydda information oavsett form och förekomst, elektronisk såväl som fysisk. Informationssäkerhet ska förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs.[10]

Informationssäkerhet ska även förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet.

I likhet med fysisk säkerhet är informationssäkerhet inte begränsat till tekniska åtgärder utan inkluderar även bl.a. rutiner och är beroende av en god personalsäkerhet med relevanta utbildningar. Säkerhetsskyddsklassificerade uppgifter kan förekomma i pappersform som utskrivna dokument, fotografier, ritningar etc. Informationssäkerhet kan då exempelvis innebära att dokumenten förses med anteckning om aktuell säkerhetsskyddsklass och att förvaring sker på ett betryggande sätt i brandskyddade och låsbara skåp. Behovet av samordning mellan olika säkerhetsskyddsåtgärder blir tydligt i detta exempel. Personalen som hanterar dokumenten behöver utbildas i anteckningens innebörd och förvaringsskåpen måste dimensionerats i förhållande till den fysiska säkerheten i övrigt. Rutiner för hantering, delning, kopiering och destruktion är andra exempel på åtgärder.

Hantering av säkerhetsskyddsklassificerade uppgifter sker i dag ofta i informationssystem. De flesta verksamhetsutövare använder

[10] 2 kap. 2 § säkerhetsskyddslagen.

e-post och digitala meddelandetjänster för kommunikation samt olika former av dataprogram för textbehandling och dokumenthantering. Informationssystemen kan på detta sätt komma att innehålla stora mängder säkerhetsskyddsklassificerade uppgifter vilket gör dem skyddsvärda.

Ett informationssystem behöver dock inte innehålla säkerhetsskyddsklassificerade uppgifter för att vara skyddsvärt. Även informationssystem som t.ex. samlar in väderdata till flygledning eller styrsystem på kraftverk kan vara viktiga för säkerhetskänslig verksamhet.

I fråga om informationssystem kan informationssäkerhet exempelvis bestå av att systemen ska separeras från andra informationssystem med logiska funktioner såsom t.ex. brandväggar som hindrar kommunikation eller genom att ha fysiskt avskilda nätverk som inte kan kommunicera med varandra eller internet.

En vanlig åtgärd är att använda kryptografiska funktioner, s.k. signalskydd, då säkerhetsskyddsklassificerade uppgifter överförs mellan informationssystem. Då informationssäkerhet inte bara handlar om skydd mot att uppgifter röjs behöver informationssystemen också skyddas mot olika former av hot som är inriktande på att störa eller förstöra och sådana som är inriktade mot att obehörigen ändra informationen. Exempel på sådana säkerhetsskyddsåtgärder kan vara säkerhetskopiering, s.k. backup, för att säkerhetsställa tillgänglighet och digitala signaturer som ett sätt att kontrollera så att uppgifter inte obehörigen ändrats.

I 7 kapitel behandlas närmare begreppen *skyddsvärda uppgifter* och *informationssäkerhet* när det gäller regleringen om säkerhetsskydd.

6.5.2 Fysisk säkerhet

Fysisk säkerhet ska förebygga obehörigt tillträde till och skadlig inverkan på områden, byggnader och andra anläggningar eller objekt där säkerhetsskyddsklassificerade uppgifter finns eller där säkerhetskänslig verksamhet bedrivs.[11] Fysisk säkerhet är även en viktig förutsättning för att obehöriga inte på annat sätt ska få insyn i verksamheten eller ta del av säkerhetsskyddsklassificerade uppgifter.

[11] 2 kap. 3 § säkerhetsskyddslagen.

6.5.3 Personalsäkerhet

Personalsäkerhet består av två delar, säkerhetsprövning och utbildning. Säkerhetsprövning syftar till att förebygga att personer som inte är pålitliga ur säkerhetsynpunkt deltar i säkerhetskänslig verksamhet eller på annat sätt ges tillgång till säkerhetsskyddsklassificerade uppgifter. Utbildning syftar till att säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd för att uppfylla det krav på behörighet och kompetens som deltagandet kräver.[12] Säkerhetsprövningen görs för att klargöra om en person kan antas vara lojal mot de intressen som ska skyddas och i övrigt pålitlig ur säkerhetssynpunkt. Viktiga aspekter att utreda är eventuella dubbla lojaliteter, intressekonflikter, bristande säkerhetsmedvetandet och andra sårbarheter.

6.5.4 Behörighet att delta i säkerhetskänslig verksamhet

I 1 kap. 3 § säkerhetsskyddsförordningen anges att behörig att *ta del av säkerhetsskyddsklassificerade uppgifter* eller *i övrigt delta i säkerhetskänslig verksamhet* är, om inte något annat följer av bestämmelser i lag, endast den som

1. har bedömts pålitlig från säkerhetssynpunkt,
2. har tillräckliga kunskaper om säkerhetsskydd, och
3. behöver uppgifterna eller annan tillgång till verksamheten för att kunna utföra sitt arbete eller på annat sätt delta i den säkerhetskänsliga verksamheten.

6.6 Särskild säkerhetsskyddsbedömning

Inom säkerhetsskydd förekommer uttrycket *särskild säkerhetsskyddsbedömning* vid vissa upphandlingar, driftsättning eller ändringar i informationssystem och förändringar i hotbild eller verksamhet.[13]

[12] 2 kap. 4 § säkerhetsskyddslagen.
[13] Se Säkerhetspolisens vägledning Säkerhetsskyddsanalys om metod för särskild säkerhetsskyddsbedömning.

6.6.1 Statliga myndigheter vid upphandling

Statliga myndigheter ska vid vissa upphandlingar samråda med Säkerhetspolisen.[14] Innan samrådet kan ske ska en *särskild säkerhetsskyddsbedömning* göras för att identifiera och dokumentera vilka säkerhetsskyddsklassificerade uppgifter eller säkerhetskänsliga informationssystem som leverantören kan få del av och som kräver säkerhetsskydd.

6.6.2 Inför driftsättning av informationssystem

Verksamhetsutövare, oavsett om det är en myndighet eller enskild, ska *innan* ett informationssystem som har betydelse för säkerhetskänslig verksamhet *tas i drift* genomföra och dokumentera en särskild säkerhetsskyddsbedömning.[15]

Genom den särskilda säkerhetsskyddsbedömningen ska verksamhetsutövaren ta ställning till vilka säkerhetskrav som är motiverade och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses. I vissa fall ska även samråd med Säkerhetspolisen ske.[16]

6.6.3 Vid förändringar av hotbild eller verksamhet

Vid *förändringar i hotbilden* eller om verksutövaren genomför *en förändring som kan antas få betydlig påverkan på verksamheten* ska en särskild säkerhetsskyddsbedömning genomföras.[17] En förändring av hotbild kan identifieras av såväl tillsynsmyndigheten som verksamhetsutövaren vid exempelvis säkerhetshotande händelser eller genom omvärldsbevakning. Exempel på förändringarna i verksamheten är upphandlingar, nyetablering, förändringar av säkerhetskänsliga system eller flytt till nya lokaler.

[14] 2 kap. 6 § säkerhetsskyddsförordningen.
[15] 3 kap. 1 § säkerhetsskyddsförordningen.
[16] Se avsnitt 6.7.2 om samråd gällande informationssystem samt Säkerhetspolisens *Vägledning i säkerhetsskydd – Informationssäkerhet*, juni 2019.
[17] 2 kap. 12 § Säkerhetspolisens föreskrifter om säkerhetsskydd.

6.7 Samråd

Inom säkerhetsskydd finns olika situationer som medför *skyldighet* att samråda mellan myndigheter, verksamheter och Säkerhetspolisen respektive Försvarsmakten.

6.7.1 Upphandling av myndigheter

Statliga myndigheter som avser genomföra en upphandling som innebär krav på säkerhetsskyddsavtal ska *innan förfarandet inleds* samråda med Säkerhetspolisen eller Försvarsmakten. Innan samrådet kan ske ska verksamhetsutövaren genomföra en särskild säkerhetsskyddsbedömning. Säkerhetspolisen respektive Försvarsmakten kan inom ramen för samrådet förbjuda myndigheten att genomföra upphandlingen.

6.7.2 Samråd avseende informationssystem

Verksamhetsutövare ska i vissa fall skriftligen samråda med Säkerhetspolisen respektive Försvarsmakten innan ett informationssystem tas i drift eller i väsentliga avseenden förändras.[18] Kravet gäller oavsett om det är en myndighet eller enskild som är verksamhetsutövare.

Samråd ska ske vid driftsättning eller väsentlig förändring av:

– informationssystem som behandlar eller kan komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *konfidentiell* eller *högre*, eller

– andra informationssystem om det vid obehörig åtkomst till systemet kan *medföra en skada* för Sveriges säkerhet som *inte är obetydlig*.

6.7.3 Samråd och information vid registerkontroll

En tillsynsmyndighet som beslutar om placering i säkerhetsklass eller ansöker om registerkontroll för personal hos en enskild verksamhetsutövare ska vid behov samråda med verksamhetsutövaren i fråga om säkerhetsprövningsåtgärder.

[18] 3 kap. 2 § säkerhetsskyddsförordningen.

Samråd ska ske löpande under hela den tid som deltagandet i den säkerhetskänsliga verksamheten pågår. Det är särskilt viktigt att samråd sker i de fall det vid registerkontroll framkommer uppgifter som kan antas ha betydelse för säkerhetsprövning.

6.7.4 Samråd avseende ytterligare föreskrifter och undantag

En tillsynsmyndighet som avser meddela föreskrifter som kompletterar eller ger undantag från bestämmelser i Säkerhetspolisens föreskrifter om säkerhetsskydd ska innan beslut fattas samråda med Säkerhetspolisen.[19]

Samrådet är en del i att koordinera kravbilden så att en myndighet inte fattar beslut som leder till en obalans i skyddet för Sveriges säkerhet. Denna obalans kan uppstå om en säkerhetskänslig verksamhet bedrivs i en sektor men påverkar verksamheten i en annan. Så är exempelvis förhållandet i fråga om elförsörjningsverksamhet och elektronisk kommunikation som hanteras av Affärsverket Svenska kraftnät respektive Post- och Telestyrelsen (PTS).

6.7.5 Samråd vid sänkning av säkerhetsskyddsklass

Om det finns skäl att omklassificera en handling med kvalificerat hemlig uppgift krävs samråd innan så sker.[20] Samråd ska ske med verksamhetens högsta chef eller motsvarande organ och med den som upprättat handlingen.[21] Samråd kan även vara lämpligt i fråga om uppgifter i lägre säkerhetsskyddsklass än kvalificerat hemlig men detta är inget krav.[22]

6.8 Säkerhetsskyddsavtal

Av 2 kap. 6 § säkerhetsskyddslagen följer att *statliga myndigheter, regioner och kommuner* som avser att genomföra en *upphandling* och ingå ett avtal om bl.a. varor och tjänster ska se till att det i ett säker-

[19] 7 kap. 8 § säkerhetsskyddsförordningen och 9 kap. 1 § Säkerhetspolisens föreskrifter om säkerhetsskydd.
[20] 3 kap. 8 § Säkerhetspolisens föreskrifter om säkerhetsskydd.
[21] Anteckning om samrådet ska göras på handlingen.
[22] Samråd och hantering av säkerhetsskyddsklassificerade handlingar utvecklas ytterligare i Säkerhetspolisens *Vägledning i säkerhetsskydd, Informationssäkerhet*, 2020.

hetsskyddsavtal anges hur kraven på säkerhetsskydd enligt 2 kap. 1 § ska tillgodoses av leverantören om

– det i upphandlingen förekommer säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *konfidentiell* eller *högre*, eller
– upphandlingen i övrigt avser eller ger leverantören tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Dessa bestämmelser gäller även för *enskilda verksamhetsutövare* som ingår avtal om bl.a. varor och tjänster med utomstående leverantörer. Verksamhetsutövaren ska kontrollera att leverantören följer säkerhetsskyddsavtalet.

6.9 Roller och ansvar

Då säkerhetsskydd omfattar flera typer av verksamheter hos såväl myndigheter som enskilda finns ett stort antal aktörer med olika roller och ansvar.[23] Säkerhetspolisen och Försvarsmakten är som tillsynsmyndigheter övergripande ansvariga för att bl.a. utöva tillsyn och meddela föreskrifter. Försvarsmakten ansvarar för den egna myndigheten, Fortifikationsverket, Försvarshögskolan samt de myndigheter som ligger under Försvarsdepartementets ansvarsområde. Säkerhetspolisen ansvarar för övriga myndigheter samt regioner och kommuner.

Utöver Säkerhetspolisen och Försvarsmakten finns ett antal ytterligare tillsynsmyndigheter vilka redogörs för nedan.

Tillsynsmyndigheterna får meddela kompletterande föreskrifter inom sitt respektive ansvarsområde. Därutöver har vissa myndigheter rätt att meddela föreskrifter inom speciella områden, exempelvis Försvarsmakten om kryptografiska funktioner och Regeringskansliet samt Försvarets materielverk om utfärdande av säkerhetsintyg för personer respektive leverantörer.

[23] 7 kap. 1–11 §§ säkerhetsskyddsförordningen, 9 kap. 1 § Säkerhetspolisens föreskrifter om säkerhetsskydd.

6.9.1 Säkerhetspolisens roll och uppgifter

Säkerhetspolisen är Sveriges nationella säkerhetstjänst med ansvar för Sveriges inre säkerhet. En av myndighetens uppgifter är enligt 3 § polislagen (1984:387) att fullgöra uppgifter enligt säkerhetsskyddslagen.

Säkerhetspolisen utövar tillsyn av säkerhetsskydd i syfte att kontrollera att verksamhetsutövare följer lag och annan författning. Vidare har Säkerhetspolisen rätt att meddela föreskrifter inom säkerhetsskyddsområdet och ett uppdrag att lämna råd till Regeringskansliet, Justitiekanslern, riksdagen och dess myndigheter.

När Säkerhetspolisen lämnar råd kan detta t.ex. bestå av utbildningar, föreläsningar och tester av säkerhetsskyddsåtgärder. Det är viktigt i sammanhanget poängtera att det alltid är verksamhetsutövaren som har ansvaret för sina skyddsvärden och de åtgärder som vidtas för att skydda dessa.

Säkerhetspolisen har även en central roll att verka som samrådsmyndighet, exempelvis i vissa upphandlingssituationer och vid förändring och idrifttagande av informationssystem (se avsnitt 6.7 Samrådsdialoger). Vidare är det Säkerhetspolisen som tar emot anmälningar vid säkerhetshotande händelser och verksamhet, bl.a. it-incidenter eller om säkerhetsskyddsklassificerade uppgifter kan ha röjts.

Säkerhetspolisen ansvarar även för att utföra registerkontroll vid säkerhetsprövning av de personer vars anställning eller deltagande i säkerhetskänslig verksamhet har placerats i säkerhetsklass.[24]

6.9.2 Försvarsmaktens roll och uppgifter

Försvarsmakten har motsvarande uppgifter och roll som Säkerhetspolisen inom myndighetens eget ansvarsområde.

6.9.3 Tillsynsmyndigheternas roll

Utöver de två huvudaktörerna Säkerhetspolisen och Försvarsmakten finns ytterligare ett antal tillsynsmyndigheter som utövar tillsyn över enskilda verksamhetsutövare inom en avgränsad sektor eller ett geo-

[24] Kontrollen innebär slagning mot bland annat belastningsregistret och misstankeregistret. Registerkontroll beskrivs mer utförligt i Säkerhetspolisens vägledning Personalsäkerhet.

grafiskt område. Följande myndigheter har ansvar för respektive område:

- Affärsverket Svenska kraftnät: elförsörjning.
- Post- och Telestyrelsen (PTS): elektronisk kommunikation och posttjänst.
- Transportstyrelsen: civil flygtrafiktjänst, militär flygtrafikledningstjänst och verksamhet som i övrigt är av betydelse för luftfartsskydd, hamnskydd och sjöfartsskydd.
- Länsstyrelserna: andra enskilda verksamhetsutövare än de som täcks in av ovanstående myndigheters ansvar.

Det bör förtydligas att tillsynsmyndigheterna endast har ansvar för tillsyn av enskilda verksamhetsutövare inkluderat statliga, kommunala och regionala bolag.

Säkerhetspolisen utövar tillsyn av tillsynsmyndigheterna samt andra myndigheter som tangerar en sektor, t.ex. Trafikverket och Energimyndigheten.

Tillsynen får även utövas hos leverantörer som omfattas av ett säkerhetsskyddsavtal och hos enskilda verksamhetsutövare som leverantören i sin tur anlitat inom ramen för avtalet.

I det fall en tillsynsmyndighet vid tillsyn upptäcker allvarliga brister som trots tidigare påpekanden inte rättats till ska myndigheten informera Säkerhetspolisen och Försvarsmakten.

Undantag från informationsplikten finns gällande vissa verksamhetsutövare som är leverantörer.[25]

Säkerhetspolisen och Försvarsmakten kan utöva tillsyn även i de fall en verksamhet sorterar under en tillsynsmyndighets ansvarsområde.

Tillsynsmyndigheterna har utöver tillsyn ett ansvar för rådgivning och är den huvudsakliga kontakten för enskilda verksamhetsutövare vid frågor om säkerhetsskydd och tillämpning av bestämmelser. Det är tillsynsmyndigheterna som beslutar om placering i säkerhetsklass för enskilda verksamhetsutövare.[26] Tillsynsmyndigheterna har även rätt att efter samråd med Säkerhetspolisen medge undantag

[25] Se Säkerhetspolisens vägledning *Säkerhetsskyddad upphandling*.
[26] Se Säkerhetspolisens vägledning *Personalsäkerhet*.

från Säkerhetspolisens föreskrifter om säkerhetsskydd och inom respektive område meddela ytterligare kompletterande föreskrifter.

6.9.4 Närmare om verksamhetsutövarens ansvar

Den som bedriver säkerhetskänslig verksamhet har grundläggande skyldigheter att utreda behovet av säkerhetsskydd, planera och vidta säkerhetsskyddsåtgärder samt kontrollera det egna säkerhetsskyddet.[27] Det finns dock ingen förteckning, tillståndsprövningsprocess eller liknande som tydligt pekar ut vilka som bedriver säkerhetskänslig verksamhet. Det är i stället, i likhet med vad som gäller inom många andra lagreglerade områden, varje verksamhetsutövares egna ansvar att hålla sig informerad, göra bedömningar och bedriva sin verksamhet enligt de författningar som gäller på säkerhetsskyddsområdet.

Arbetet med säkerhetsskydd behöver inledas med ett aktivt ställningstagande om huruvida en verksamhet till någon del är säkerhetskänslig. I praktiken medför detta att verksamhetsutövare, om svaret inte är uppenbart, behöver genomföra det första steget av processen för säkerhetsskyddsanalys.

Säkerhetsskyddsanalys är grunden för säkerhetsskydd. För den som bedriver säkerhetskänslig verksamhet är ansvaret långtgående. Verksamhetsutövaren ska planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.[28]

Om säkerhetskänslig verksamhet utkontrakteras sträcker sig ansvaret även utanför den egna organisationen, i och med behovet av att reglera och kontrollera säkerhetsskyddet hos den anlitade leverantören. Även om verksamhetsutövarens ansvar är långtgående finns utrymme att utforma och bedriva säkerhetsskyddsarbetet på det sätt som passar den egna organisationen, detta så länge en tillräcklig nivå av säkerhetsskydd uppnås enligt principen att skyddet bör vara detsamma oavsett var, hur och av vem som verksamheten bedrivs.

[27] 2 kap. 1 § säkerhetsskyddslagen.
[28] I Säkerhetspolisens vägledning *Säkerhetsskyddsanalys* finns ett antal indikatorer att använda som grund för en initial bedömning.

6.10 Säkerhetsskyddsregleringen och NIS-direktivet

Den som bedriver säkerhetskänslig verksamhet behöver ofta förhålla sig till krav även i annan lagstiftning. Detta kan i likhet med behovet av säkerhetsskydd och andra säkerhetsåtgärder (se ovan). Skillnaden mellan säkerhetsskydd och andra säkerhetsåtgärder, innebära såväl utmaningar som möjligheter till synergieffekter. Verksamhetsutövare bör därför på ett eller annat sätt inventera och bedöma vilka lagkrav som ställs på verksamheten för att få en samlad bild och kunna skapa ett effektivt säkerhetsskydd.

Vissa lagkrav kan uppfyllas med samma eller liknande typer av åtgärder som behövs för säkerhetsskydd, exempelvis skydd mot intrång i informationssystem som hanterar personuppgifter eller skydd mot otillbörligt tillträde i hamnar och på kärnkraftverk. I andra fall finns motstridiga syften som måste uppfyllas, exempelvis krav skydd mot olika former av angrepp samtidigt som viss tillgänglighet måste säkerställas. I vissa fall framgår gränsdragningar och undantag av författning vilket gör det tydligt om ett krav står över ett annat. Ett sådant exempel är de regler som implementerats i svensk rätt till följd av det så kallade NIS-direktivet. I Sverige har NIS-direktivet implementerats genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Lagen gäller för leverantörer inom sju sektorer som tillhandahåller samhällsviktiga tjänster som är centrala för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet samt vissa leverantörer av digitala tjänster.[29] Genom lagen ställs krav på bland annat *skydd av informationssystem* och incidentrapportering till Myndigheten för samhällsskydd och beredskap (MSB). Verksamhetsutövare i de sju sektorerna eller verksamhetsutövare som levererar digitala tjänster bedriver i vissa fall även säkerhetskänslig verksamhet vilket kan skapa en möjlig konfliktsituation med krav från olika lagar. Det finns dock ett undantag i lagen om informationssäkerhet för samhällsviktiga och digitala tjänster, som gör att den lagen inte gäller för verksamhet som omfattas av krav på säkerhetsskydd enligt säkerhetsskyddslagen. För verksamhetsutövare som endast till någon del bedriver säkerhetskänslig verksamhet innebär det att vissa delar av verksamheten kan då omfattas av kraven på säkerhetsskydd och andra delar av lagen om informationssäkerhet för samhällsviktiga och digitala tjänster. Detta kan ha betydelse vid

[29] 8 § lagen (2018:1174) om informationssäkerhet i samhällsviktiga och digitala tjänster.

exempelvis anmälan av säkerhetshotande händelser så att känslig information om en sårbarhet i informationssystem kommuniceras på ett tillräckligt säkert sätt och till rätt myndighet.

7 Informationssäkerhet

7.1 Inledning

Informationssäkerhet handlar om att skydda information ur olika aspekter. I och med den ökade digitaliseringen ökar informationsmängderna och olika verksamheter är beroende av fungerande nätverks- och informationssystem (informationssystem). Information kan inhämtas, lagras, kommuniceras och bearbetas i olika former. En verksamhet har i allmänhet stora mängder information som av olika anledningar kan vara skyddsvärd. Detta innebär att en verksamhetsutövare kan behöva identifiera och skydda den information som är värdefull (skyddsvärd information)[1]. Det kan uppstå stora negativa konsekvenser för en verksamhet, och i vissa fall även för samhället i stort, om skyddsvärd informationen blir röjd för obehörig, om den obehörigen förändras eller om den inte finns till hands när den behövs. Att säkerställa en tillräcklig informationssäkerhet innebär att vidta åtgärder för att skydda informationen så att negativa konsekvenser inte uppstår. För att få en effektiv och säker informationshantering är en förutsättning att informationssäkerhetsarbetet bedrivs systematiskt.[2] Som framgår av kapitel 6 ska den informationssäkerhet som bedrivs inom ramen för säkerhetsskyddarbetet samordnas med det *övriga* informationssäkerhetsarbetet i verksamheten.

7.2 Informationssäkerhet

Begreppet *informationssäkerhet* infördes i 1996 års lagstiftning om säkerhetsskydd som en ersättning till det tidigare begreppet sekretesskydd. I dag är termen informationssäkerhet allmänt spridd och accep-

[1] 2 kap. 2 § säkerhetsskyddslagen (2018:585).
[2] På bl.a. webbplatsen www.informationssakerhet.se finns stöd i hur ett systematiskt informationssäkerhetsarbete kan bedrivas.

terad, och den används inom skilda verksamheter där kraven och behoven av skydd skiljer sig åt. Begreppet avser skydd av olika slag av information hos såväl myndigheter som enskilda. Åtgärder som avser informationssäkerhet enligt säkerhetsskyddslagen kan inte särskiljas från informationssäkerhet i en vidare bemärkelse. Exempel på detta är skydd mot skadlig kod och användarautentisering som är relevanta åtgärder även för nätverks- och informationssystem (informationssystem) som inte är av betydelse för Sveriges säkerhet.[3]

7.2.1 Informationssäkerhetens beståndsdelar

Informationssäkerhet enligt regleringen om säkerhetsskydd innebär åtgärder av olika slag för att skydda information som är av betydelse för säkerhetskänslig verksamhet. Sådan information förekommer i olika miljöer och verksamheter och hanteras och används på flera olika sätt. Därför måste säkerhetsskyddsåtgärderna anpassas för att passa för dessa skiftande förutsättningar. Uppgifternas form saknar i sammanhanget betydelse och åtgärderna måste avse såväl elektroniskt lagrade och kommunicerade uppgifter som uppgifter på papper samt uppgifter som kan läsas ut ur t.ex. bilder eller materiel.

Man kan beskriva informationens livscykel från det att den skapas till det att den upphör eller förstörs och att utifrån denna beskrivning identifiera moment som har betydelse för säkerheten. Dessa moment i informationshanteringen kan skyddas genom administrativa, fysiska eller tekniska säkerhetsskyddsåtgärder eller genom en kombination av dessa. För att beskriva åtgärdernas karaktär kan de indelas i tre kategorier:[4]

– administrativ informationssäkerhet,
– it-säkerhet,
– kommunikationssäkerhet.

[3] Redogörelsen för Informationssäkerhet i detta kapitel grundas bl.a. på uppgifter som finns i Säkerhetspolisens *Vägledning i säkerhetsskydd*, *Informationssäkerhet*, 2020. Motsvarande uppgifter finns även i Försvarsmaktens *Handbok Försvarsmaktens säkerhetstjänst*, *Informationssäkerhet*, *H Säk Infosäk* 2013.
[4] Indelningen följer i princip *Rådets beslut av den 23 september 2013 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter* (2013/488/EU).

Syftet med denna kategorisering är dels att åtgärderna riktar sig mot olika målgrupper, dels att genomförandet av åtgärderna kräver olika typer av kompetens.

Administrativ informationssäkerhet

Till de *administrativa* informationssäkerhetsåtgärderna hör åtgärder som tar sikte på rutiner, arbetsflöden och arbetsledning. Här kan nämnas bestämmelser om registrering, distribution, kopiering, kvittering och inventering av handlingar som innehåller säkerhetsskyddsklassificerade uppgifter. Ett exempel på en sådan bestämmelse är att handlingar som placerats i informationssäkerhetsklass *konfidentiell* eller *högre* ska kvitteras av den som tar del av handlingen. En för säkerhetsskyddet central fråga är reglerna om behörighet till säkerhetsskyddsklassificerade uppgifter. Behörighetskriteriet innebär att en person för att vara behörig till hemliga uppgifter ska vara pålitlig från ett säkerhetsperspektiv, ha relevanta kunskaper om säkerhetsskyddet och ha behov av uppgifterna för sin tjänst eller för sitt uppdrag.

It-säkerhet

It-säkerheten innefattar regler om handhavande och rutiner för informationssystem (nätverks- och informationssystem) jämte tekniska krav på säkerhetsfunktioner i systemen och komponenter. För att även säkerställa att tillgängligheten är i enlighet med verksamhetens krav bör informationssystem som används i säkerhetskänslig verksamhet vara föremål för kontinuitetsplanering. Säkerhetskopiering är också en viktig åtgärd som ger ett skydd i termer kring tillgänglighet och riktighet. Till it-säkerheten hör även bestämmelser som rör krav på säkerhetsgodkännande av it-system inför driftsättning. Ett exempel på en säkerhetsskyddsbestämmelse inom it-säkerheten är att lagringsmedia som innehåller säkerhetsklassificerade uppgifter ska förvaras och hanteras på samma sätt som säkerhetsskyddsklassificerade handlingar. Åtgärder som behörighetskontroll och skydd mot obehörig avlyssning är också viktiga beståndsdelar av it-säkerheten.

Kommunikationssäkerhet

Termen *signalskydd* används för att beskriva det i huvudsak kryptografiska skyddet för information i s.k. signalskyddssystem. Bestämmelser om signalskydd och kryptografiska funktioner förekommer i dag i flera olika författningar. Försvarsmakten har i uppgift att leda och bedriva militär säkerhetstjänst samt leda och samordna signalskyddstjänsten. Det innebär arbete med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information samt även biträda Regeringskansliet i frågor som rör kryptoverksamhet och annan signalskyddsverksamhet. Bestämmelsen om vad säkerhetsskyddslagen ska skydda mot.

Syftet med informationssäkerhet

I säkerhetsskyddslagen anges att säkerhetsskyddsåtgärden *informationssäkerhet* ska:

1. förebygga att säkerhetsskyddsklassificerade uppgifter *obehörigen röjs*, *ändras*, *görs otillgängliga* eller *förstörs*, och
2. *förebygga skadlig inverkan i övrigt på uppgifter* och *informationssystem* som gäller säkerhetskänslig verksamhet.

Även om det finns flera olika definitioner av begreppet informationssäkerhet så är tre kriterier vanligen återkommande: *konfidentialitet*, *riktighet* och *tillgänglighet*.

Konfidentialitet

Informationssäkerhet syftar till att förhindra att information *röjs för obehöriga*.

Riktighet

Informationen som är av betydelse för en verksamhet behöver ofta även skyddas så att den *inte kan förändras av obehöriga*. I många fall är en behörighetsstyrning som säkerställer att endast behörig person kan förändra informationen en tillräcklig skyddsåtgärd. En annan

säkerhetsskyddsåtgärd för att skydda information där riktigheten är kritisk, kan vara att använda kryptografiska funktioner så som exempelvis elektronisk signering.[5] Även här handlar det i en säkerhetsskyddskontext om att skydda uppgifter och informationssystem som är av betydelse för en säkerhetskänslig verksamhet mot antagonistiska hot.

Tillgänglighet

Förutom att säkerställa att information inte röjs för obehöriga, syftar också informationssäkerhetsarbetet till att säkerställa att informationen finns *tillgänglig* när den behövs. I en säkerhetsskyddskontext handlar det om att säkerställa att skyddet av uppgifter och informationssystem som är av betydelse för säkerhetskänslig verksamhet skyddas så att en antagonist inte kan göra dessa otillgängliga. En säkerhetsskyddsåtgärd kan inriktas mot att skydda verksamheten, snarare än ett informationssystem, med så kallade *kontinuitetsåtgärder*. Sådana åtgärder kan exempelvis vara så enkla som att se till att skyddsvärd information finns utskriven på papper, eller finns tillgänglig i flera informationssystem. Sådana alternativa åtgärder måste dock utformas så att eventuella säkerhetsskyddsklassificerade uppgifter ges ett erforderligt säkerhetsskydd.[6]

Standarder till stöd för informationssäkerhet

I syfte att öka informationssäkerheten finns flera etablerade svenska standarder, bl.a.:

- SS-ISO/IEC 27000,
- SS-ISO/IEC 27001,
- SS-ISO/IEC 27002,
- SS-ISO/IEC 27003.

Standarderna i ISO 27000-serien är framtagna av internationella expertgrupper inom ISO/IEC (International Organization for Standardiza-

[5] 4 kap. 22 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.
[6] 2 kap. 19 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

tion/International Electrotechnical Commission) där Sverige medverkar genom SIS, (Swedish Standards Institute). SIS deltar aktivt i det internationella arbetet i såväl ISO/IEC som på europeisk nivå inom CEN-CENELEC (European Committee for Standardization – European Committee for Electrotechnical Standardization).

7.2.2 Säkerhetsskyddsklassificerade uppgifter

Säkerhetsskyddsklassificerade uppgifter är uppgifter som rör säkerhetskänslig verksamhet och som *omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400)* eller som skulle *omfattas av sekretess om lagen var tillämplig*.[7] För verksamheter där offentlighets- och sekretesslagen inte är tillämplig behöver verksamhetsutövaren således göra en fiktiv sekretessprövning.

Säkerhetsskyddsklassificerade uppgifter kan också vara uppgifter som *omfattas av ett internationellt åtagande om säkerhetsskydd*. Sådana avtal har Sverige ingått med ett antal olika länder och mellanfolkliga organisationer. Det kan t.ex. röra sig om EU-klassificerad information. Hur och i vilken nivå en klassificering sker regleras vanligen i bi- eller multilaterala avtal om säkerhetsskydd.

7.2.3 Indelning i säkerhetsskyddsklasser

Säkerhetsskyddsklassificerade uppgifter ska delas in i *säkerhetsskyddsklasser* utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet.[8] Indelningen i säkerhetsskyddsklasser ska göras enligt följande:

- kvalificerat hemlig vid en synnerligen allvarlig skada,
- hemlig vid en allvarlig skada,
- konfidentiell vid en inte obetydlig skada, eller
- begränsat hemlig vid endast ringa skada.

[7] 1 kap. 2 § andra stycket säkerhetsskyddslagen (2018:585).
[8] 2 kap. 5 § första stycket säkerhetsskyddslagen (2018:585), 3 kap. 7 § säkerhetsskyddsförordningen (2018:658) och 2 kap. 2 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

I förarbetena till den nya säkerhetsskyddslagen ges ingen närmare förklaring till vad som avses med respektive skadenivå. Det är därför ytterst upp till rättstillämpningen att avgöra vad som utgör en skada för Sveriges säkerhet.

Vid indelningen av uppgifter i säkerhetsskyddsklasser bör eventuella konsekvenser av ett röjande som framstår som helt orimliga inte beaktas. Bedömningen bör ske utifrån vad som är det rimliga scenariot om uppgifterna röjs.[9] Att klassificeringen ska ske utifrån den skada som ett röjande kan medföra för Sveriges säkerhet innebär dock att det inte ska beaktas vilken skada det kan medföra om uppgifterna blir otillgängliga för verksamhetsutövaren eller om de manipuleras och inte längre kan anses riktiga.

Syftet med indelningen av uppgifter i säkerhetsskyddsklasser är att fastställa en korrekt *lägsta skyddsnivå* för uppgifterna i respektive säkerhetsskyddsklass.[10] En verksamhetsutövare som tar emot en säkerhetsskyddsklassificerad handling av en annan verksamhetsutövare är inte bunden av den tidigare säkerhetsskyddsklassificeringen av uppgifterna i handlingen, förutom när det gäller uppgifter som omfattas av ett internationellt åtagande om säkerhetsskydd.

Utgångspunkten bör dock ändå vara att den ursprungliga säkerhetsskyddsklassificeringen ska godtas om det inte tillkommit några nya omständigheter sedan indelningen i säkerhetsskyddsklass gjordes. Det är normalt den verksamhetsutövare som upprättat handlingen som har bäst förutsättning att bedöma vilken skada ett röjande skulle medföra för Sveriges säkerhet, särskilt om uppgifterna rör verksamhetsutövarens egen verksamhet.

7.2.4 Uppgifter som omfattas av ett internationellt åtagande om säkerhetsskydd

Säkerhetsskyddsklassificerade uppgifter som omfattas av *ett internationellt åtagande om säkerhetsskydd* ska delas in i säkerhetsskyddsklass, om de inte redan har klassificerats av en annan stat eller en mellan-

[9] Enligt samma princip bör man inte heller beakta vad som skulle hända om andra uppgifter skulle röjas vid samma tidpunkt. I annat fall riskerar indelningen i säkerhetsskyddsklasser att leda till att i princip samtliga uppgifter delas in i någon av de högre klasserna, vilket inte är syftet med lagstiftningen.

[10] Indelningen i säkerhetsskyddsklass är därför inte avgörande vid en prövning av om sekretessen hindrar ett utlämnande av en säkerhetsskyddsklassificerad handling.

folklig organisation.[11] En befintlig klassificering ska då godtas, om det inte tillkommit några nya omständigheter sedan indelningen i säkerhetsskyddsklass gjordes, och ligga till grund för bestämmande av skyddsnivå.[12]

I vissa internationella samarbeten förekommer det att en svensk verksamhetsutövare upprättar handlingar som innehåller uppgifter som omfattas av ett internationellt åtagande om säkerhetsskydd. I sådana fall ska uppgifterna delas in i säkerhetsskyddsklass utifrån den skada ett röjande av uppgiften kan medföra för Sveriges förhållande till den andra staten eller den mellanfolkliga organisationen.

7.2.5 Aggregerade och ackumulerade uppgifter

Aggregerade uppgifter innebär att *olika* typer av uppgifter samlas och tillsammans utgör ett *nytt skyddsvärde*, medan *ackumulerade uppgifter* betyder en *ökad volym* av samma typ av uppgifter.

Om enskilda uppgifter som saknar säkerhetsskyddsklass eller är indelade i en av säkerhetsskyddsklasserna *begränsat hemlig*, *konfidentiell* eller *hemlig* samlas, kan det i vissa fall medföra att en *högre* säkerhetsskyddsklass ska tillämpas på uppgiftssamlingen. Så är fallet om den aggregerade eller ackumulerade informationen gör att en antagonist kan dra andra, nya slutsatser av uppgiftssamlingen än av varje enskild uppgift.[13]

Av förarbetena till säkerhetsskyddslagen framgår att en klassificering av en samling av uppgifter inte bör göras i större utsträckning och med placering i högre klass än vad som är nödvändigt. Detta för att bl.a. begränsa onödiga administrativa kostnader och onödiga ingrepp i enskildas integritet. Endast i undantagsfall, där det finns ett tydligt samband mellan uppgifterna som gör att skadan av ett röjande skulle bli mer allvarlig, bör det vara aktuellt att höja klassificeringen på en sammanställning av uppgifter.

[11] 2 kap. 5 § andra stycket säkerhetsskyddslagen (2018:585).
[12] Se Säkerhetspolisens vägledning *Introduktion till säkerhetsskydd* för mer information om internationella åtaganden om säkerhetsskydd och de internationella motsvarigheterna till de svenska säkerhetsskyddsklasserna.
[13] 4 kap. 6 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

7.3 Hantering av säkerhetsskyddsklassificerade uppgifter

Nedan följer en översiktlig sammanställning av hanteringsreglerna för säkerhetsskyddsklassificerade uppgifter i respektive säkerhetsskyddsklass. Dessa utgör minimikrav och en verksamhetsutövare kan komplettera reglerna i interna styrdokument.

7.3.1 Anteckning om säkerhetsskyddsklass

En säkerhetsskyddsklassificerad handling ska förses med en anteckning om vilken säkerhetsskyddsklass uppgifterna i handlingen har, i syfte att klargöra vilka hanteringsregler som gäller för handlingen.[14] Kravet på anteckning gäller både för fysiska och elektroniska säkerhetsskyddsklassificerade handlingar. Om det i samma handling förekommer uppgifter som är indelade i olika säkerhetsskyddsklasser ska den högsta säkerhetsskyddsklassen anges. Anteckningen bör vara röd och omgärdas av en enkel ram upp till och med säkerhetsskyddsklassen hemlig. För säkerhetsskyddsklassen kvalificerat hemlig bör anteckningen omgärdas av en dubbel ram.[15] För elektroniska handlingar eller uppgiftsamlingar där formatet inte stödjer en anteckning kan uppgift om säkerhetsskyddsklass i stället anges i filnamnet.

Även enskilda verksamhetsutövare kan behöva hänvisa till tillämpliga sekretessbestämmelser i offentlighets- och sekretesslagen, detta för att underlätta hanteringen av handlingar som distribueras mellan enskilda och offentliga verksamhetsutövare och för att åstadkomma transparens i säkerhetsskyddsklassificeringen.

Om en säkerhetsskyddsklassificerad handling inte längre ska vara indelad i säkerhetsskyddsklass eller ska delas in i annan säkerhets-

[14] 5 kap. 5 § offentlighets- och sekretesslagen (2009:400), 1 § offentlighets- och sekretessförordningen (2009:641), 3 kap. 7 § säkerhetsskyddsförordningen (2018:658) och 3 kap. 4–6 §§ Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

[15] Anteckningen bör även innehålla hänvisning till tillämplig sekretessbestämmelse i offentlighets- och sekretesslagen, datum då anteckningen gjordes, samt vilken verksamhetsutövare som har gjort anteckningen. På så sätt uppfyller även anteckningen kriterierna för en sekretessmarkering. För allmänna handlingar i säkerhetsskyddsklassen kvalificerat hemlig ska det på anteckningen även framgå om det är chefen för Justitie-, Utrikes-, eller Försvarsdepartementet som prövar om handlingen efter begäran kan utlämnas till en enskild.

skyddsklass än vad som anges på handlingen, ska detta antecknas på handlingen.[16]

7.3.2 Förvaring

En säkerhetsskyddsklassificerad handling ska förvaras i ett förvaringsutrymme med säkerhet som motsvarar den skyddsnivå som skyddsdimensioneringen kräver.[17]

7.3.3 Märkning av lagringsmedium

Lagringsmedium för säkerhetsskyddsklassificerade uppgifter i säkerhetskyddsklass *konfidentiell* eller *högre* ska märkas med säkerhetsskyddsklass och identifieringsuppgift. Om lagringsmediet är fast monterat i annan utrustning ska i stället utrustningen märkas så att det fortfarande framgår att lagringsmediet innehåller säkerhetsskyddsklassificerade uppgifter. Om ett sådant lagringsmedium i efterhand avlägsnas från utrustningen ska lagringsmediet märkas.[18] Med den fastställda identiteten kan en förteckning över verksamhetsutövarens lagringsmedia avseende säkerhetsskyddsklassificerade uppgifter upprättas, utifrån vilken en inventering kan ske.

7.3.4 Distribution

Verksamhetsutövaren ska som en del i säkerhetsskyddsarbetet upprätta dokumenterade rutiner över hur denne avser att i säkerhetsskyddsklass *konfidentiell* eller *högre* distribuera säkerhetsskyddsklassificerade

[16] Det bör i anteckningen framgå vem som har fattat beslut om att ändra säkerhetsskyddsklass och datum för beslutet. Om handlingen är allmän ska beslutet om att säkerhetskyddsklassen ändrats antecknas i det register där handlingen är diarieförd. För säkerhetsskyddsklassificerade handlingar i säkerhetsskyddsklassen kvalificerat hemlig ska ett sådant beslut föregås av samråd med den som har upprättat handlingen och med verksamhetsutövarens högsta chef eller motsvarande organ, eller den som sådan chef eller organ bestämmer.

[17] 3 kap. 10 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd. Se även Säkerhetspolisens *Vägledning i säkerhetsskydd – Fysisk säkerhet*, 2020, för mer information om förvaring.

[18] 3 kap. 13 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd. Märkningen med säkerhetsskyddsklass syftar till att uppmärksamma den som hanterar lagringsmediet på att det innehåller säkerhetsskyddsklassificerade uppgifter samt i vilken säkerhetsskyddsklass. Märkning med identifieringsuppgift syftar till att fastställa en specifik identitet för ett lagringsmedium som innehåller säkerhetsskyddsklassificerade uppgifter.

fysiska handlingar och lagringsmedia med säkerhetsskyddsklassificerade elektroniska handlingar.[19]

För försändelser av säkerhetsskyddsklassificerade handlingar till och från utlandet ska Utrikesdepartementets kurirförbindelse anlitas, såvida inte handlingen skyddas av kryptografiska funktioner som har godkänts av Försvarsmakten. Tillsynsmyndigheterna får medge undantag från detta krav.

7.3.5 Förstöring

Säkerhetsskyddsklassificerade uppgifter ska förstöras på ett sätt som omöjliggör åtkomst och återskapande av uppgifterna. Metoder för förstöring är t.ex. dokumentförstörare eller bränning. Vid användning av dokumentförstörare ska verksamhetsutövaren säkerställa att spånet efter förstöring inte går att utläsa och att det inte går att återskapa handlingen.[20]

Förstöring av en säkerhetsskyddsklassificerad allmän handling i säkerhetsskyddsklassen *hemlig* eller *kvalificerat hemlig* ska dokumenteras.

Förstöring av säkerhetsskyddsklassificerade uppgifter kan även utföras av en leverantör. Verksamhetsutövaren behöver då reglera de säkerhetsskyddsåtgärder som leverantören behöver vidta i ett säkerhetsskyddsavtal.

7.4 Säkerhetsskyddsanalys

En verksamhetsutövare som utvecklar ett informationssystem som har betydelse för säkerhetskänslig verksamhet är ansvarig för att säkerhetsskyddet kring ett sådant informationssystem utformas så att författningarna avseende säkerhetsskydd efterlevs. Säkerhetsskyddsåtgärden informationssäkerhet ska, utöver att skydda *säkerhetsskyddsklassificerade uppgifter*, också skydda *andra uppgifter* samt själva *informationssystemen* som hanterar uppgifter i en säkerhetskänslig verksamhet. Sådana skyddsåtgärder tar framför allt sikte på att tillgodose behovet

[19] 3 kap. 10 § säkerhetsskyddsförordningen (2018:658). 3 kap. 14 och 16 §§ Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.
[20] 3 kap. 25 och 26 §§ Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

av tillgänglighet och riktighet.[21] Vilka åtgärder som är motiverade att vidta ska analyseras och bedömas i verksamhetens *säkerhetsskyddsanalys*[22] samt i förekommande fall i ett informationssystems *särskilda säkerhetsskyddsbedömning*.

Verksamhetsutövaren ska vid en särskild säkerhetsskyddsbedömning enligt 3 kap. 1 § säkerhetsskyddsförordningen (2018:658) beakta såväl de *enskilda* säkerhetsskyddsklassificerade uppgifterna som den *totala mängden* sådana uppgifter som kan komma att behandlas i informationssystemet, dvs. *aggregerad* och *ackumulerad* information i systemet.

7.5 Särskild säkerhetsskyddsbedömning

7.5.1 Allmänt om särskild säkerhetsskyddsbedömning

Av 3 kap. 1 § säkerhetsskyddsförordningen (2018:658) framgår att *innan* ett informationssystem som har betydelse för säkerhetskänslig verksamhet *tas i drift* ska verksamhetsutövaren genom en *särskild säkerhetsskyddsbedömning* ta ställning till vilka säkerhetskrav i systemet som är motiverade och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses. Den särskilda säkerhetsskyddsbedömningen utgör grunden för det säkerhetsskyddsarbete som ska bedrivas för ett informationssystem av betydelse för säkerhetskänslig verksamhet. Då den särskilda säkerhetsskyddsbedömningen ska klargöra vilka säkerhetskrav som är motiverade för ett sådant informationssystem blir den ett viktigt stöd för verksamhetsutövaren under utvecklingsprocessen. Säkerhetsskyddsbedömningen ska *dokumenteras*.

Den särskilda säkerhetsskyddsbedömningen bör kunna ge svar på ett antal frågor:

- hur ska informationssystemet användas och av vem?
- på vilket sätt är informationssystemet av betydelse för säkerhetskänslig verksamhet?
- hur exponeras informationssystemet mot andra informationssystem?
- vilka säkerhetskrav gäller för informationssystemet?

[21] 2 kap. 2 § säkerhetsskyddslagen (2018:585).
[22] Se bl.a. Säkerhetspolisens *Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys*, 2019.

– vilka säkerhetsskyddsåtgärder behöver införas i och kring informationssystemet?

7.5.2 Hur ska informationssystemet användas?

En särskild säkerhetsskyddsbedömning för ett informationssystem ska klarlägga vad informationssystemet ska användas till och av vem det ska användas, detta gäller också om informationssystem är avsett att användas i flera verksamheter. I vissa fall sker utveckling av informationssystemet för en specifik verksamhet, men det är inte ovanligt att informationssystem över tid kan komma att användas i andra verksamheter där behovet av säkerhetskyddsåtgärder är annorlunda. Förändringar av säkerhetsskyddsåtgärder som behöver ske i efterhand kan medföra betydande kostnader och det är därför många gånger en fördel att verksamhetsutövaren har ett långsiktigt perspektiv och vid behov planerar för ett bredare användningsområde.

7.5.3 På vilket sätt är informationssystemet av betydelse för säkerhetskänslig verksamhet?

En verksamhetsutövare behöver även klarlägga på vilket sätt informationssystemet har betydelse för säkerhetskänslig verksamhet. I denna bedömning kan olika frågeställningar bli aktuella för att identifiera berörda skyddsvärden:

– ska säkerhetsskyddsklassificerade uppgifter behandlas i systemet?

– vilken skada för Sveriges säkerhet kan uppstå om uppgifterna som informationssystemet behandlar röjs?

– ska informationssystemet behandla uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd?

– vilken skada för Sveriges säkerhet kan uppstå om uppgifterna som informationssystemet ska behandla görs otillgängliga eller obehörigen förändras?

Säkerhetsskyddsklassificering och vad som framgår av verksamhetsutövarens säkerhetsskyddsanalys är viktiga ingångsvärden för bedömningen.

7.5.4 Hur exponeras informationssystemet mot andra informationssystem?

I bedömningen kan verksamhetsutövaren även behöva analysera hur informationssystemet kan komma att exponeras mot och interagera med andra informationssystem. Verksamhetsutövaren kan dokumentera detta genom att ta fram en övergripande design som beskriver hur informationssystemet ska kommunicera med andra informationssystem och andra logiska samband som finns till informationssystemet.

7.5.5 Vilka säkerhetskrav gäller för informationssystemet?

När samtliga skyddsvärden är identifierade och bedömda ska kraven på säkerhet fastställas för skyddet av informationssystemet. Dessa krav framgår främst av bestämmelserna i säkerhetsskyddslagen (2018:585), säkerhetsskyddsförordningen (2018:658) och i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd samt Försvarsmaktens föreskrifter om säkerhetsskydd (FFS 2019:2) Fortsättningsvis refereras i första hand till Säkerhetspolisens föreskrifter om informationssäkerhet i säkerhetskänslig verksamhet. I Försvarsmaktens förskrifter finns i allt väsentligt motsvarande bestämmelser om informationssäkerhet och de gäller inom myndighetens tillsynsområde.

Vilka krav som är tillämpliga beror på vilken typ av säkerhetsskyddsklassificerade uppgifter som ska hanteras i informationssystemet. Om informationssystemet även ska behandla uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd måste också de krav som följer av den internationella överenskommelsen identifieras och dokumenteras.

7.5.6 Vilka säkerhetsskyddsåtgärder behöver införas i och kring informationssystemet?

När säkerhetskraven är identifierade måste verksamhetsutövaren analysera vilka *säkerhetsskyddsåtgärder* som är motiverade att vidta i och kring informationssystemet.

De krav på säkerhetsskyddsåtgärder som följer av bestämmelserna i de angivna författningarna kräver ofta en bredare analys för att fastställa på vilket sätt de ska tillämpas. Det framgår t.ex. inte av bestämmelserna var i ett informationssystem säkerhetskyddsåtgärderna ska appliceras och hur de ska dimensioneras.

Huvudprincipen är att säkerhetsskyddsåtgärderna ska anpassas utifrån det *högsta* identifierade *skyddsvärdet* som informationssystemet avser att hantera, vilken *hotbild* som föreligger mot dessa skyddsvärden, *hur* och av *vem* informationssystemet ska *användas* samt *hur* det ska *exponeras*. Det kan därutöver finnas skäl till att vidta ytterligare säkerhetsåtgärder än vad som framgår av författningarna.

När behovet av säkerhetsskyddsåtgärder analyseras bör en utgångspunkt vara att de utformas så att de kompletterar och överlappar varandra, dvs. säkerhetsskyddsåtgärderna bör byggas i *flera lager*. Fördelen med detta är att även om en säkerhetsskyddsåtgärd visar sig vara otillräcklig, finns flera andra säkerhetsskyddsåtgärder som kan träda in och exempelvis förhindra ett försök till intrång.[23]

I följande avsnitt redogörs översiktligt för några olika säkerhetsskyddsåtgärder som kan implementeras i ett informationssystem som har betydelse för säkerhetskänslig verksamhet.[24]

7.6 Omvärldsbevakning

7.6.1 Allmänt om omvärldsbevakning

En verksamhetsutövare måste förhålla sig till de *hot* som ett informationssystem kan vara exponerat mot och de *sårbarheter* som finns i och kring informationssystemet. För att en verksamhetsutövare ska kunna få en uppfattning om nya eller förändrade hot, uppkomst av nya sårbarheter, t.ex. i programvaror som används, behöver verk-

[23] Inom engelsk facklitteratur brukar denna princip beskrivas som *defence in depth*.
[24] Se Säkerhetspolisens *Vägledning i säkerhetsskydd*, *Informationssäkerhet*, 2020, och Försvarsmaktens *Handbok Försvarsmaktens säkerhetstjänst*, *Informationssäkerhet*, *H Säk Infosäk*, 2013.

samhetsutövaren löpande bevaka händelser i omvärlden som kan påverka säkerheten i verksamhetsutövarens informationssystem.

Bestämmelser om omvärldsbevakning finns i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd. I 4 kap. 2 § anges att verksamhetsutövaren ska kontinuerligt anpassa säkerhetsskyddsåtgärder i informationssystem för att möta förändringar av hot och sårbarheter. Verksamhetsutövaren ska även fastställa hur detta ska genomföras och vem som ansvarar för att identifiera förändringarna. Denne behöver därför ha förmåga att bedöma hur en sårbarhet, t.ex. i en programvara, kan påverka säkerheten i verksamhetsutövarens informationssystem och därefter ta ställning till om sårbarheten behöver åtgärdas omgående eller inte.

De stora tillverkarna av programvara publicerar normalt säkerhetsuppdateringar (s.k. säkerhetspatchar) när en sårbarhet i en programvara blir känd. Tillverkaren har ofta redan gjort någon form av värdering av hur allvarlig sårbarheten är som säkerhetsuppdateringen ska åtgärda, vilket kan ligga till grund för verksamhetsutövarens bedömning av hur sårbarheten kan påverka verksamhetsutövarens informationssystem.

Information om nya attackmetoder och sårbarheter i hård- och mjukvara publiceras löpande i omvärlden och det kan därför vara svårt att manuellt inhämta och distribuera denna typ av information. Som stöd i detta kan en verksamhetsutövare behöva använda ett system som automatiskt hämtar in och distribuerar relevant information till berörd personal. Oavsett om omvärldsbevakning sker manuellt eller med ett tekniskt stöd är det av vikt att verksamhetsutövaren har en inventarieförteckning för den mjuk- och hårdvara som förekommer i verksamhetsutövarens informationssystem eftersom det annars kan uppstå problem för verksamhetsutövaren att veta vilka sårbarheter som är relevanta att ta ställning till.

7.6.2 Kompetens och resursplanering

Om en verksamhetsutövare ska ha förutsättningar att kunna hålla ett informationssystem i drift och upprätthålla säkerheten krävs både resurser och kompetens. Utan en planering för detta riskerar säkerhetsarbetet att åsidosättas. Bestämmelser relaterade till kompetens

och resursplanering återfinns i Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2).

Av bestämmelserna i 2 kap. 16 § PMFS 2019:2 framgår att verksamhetsutövaren ska säkerställa att det finns resurser och kompetenser tillgängliga i den utsträckning som krävs för att upprätthålla säkerhetsskyddet.

Av bestämmelserna i 4 kap. 3 § PMFS 2019:2 framgår att verksamhetsutövaren ska se till att den som deltar i *utveckling*, *framtagning av arkitektur*, *testning* och *drift* av informationssystem som har betydelse för säkerhetskänslig verksamhet har tillräcklig kompetens avseende informationssäkerhet och sårbarheter i aktuellt informationssystem.

Utveckling av informationssystem eller mjukvara i ett informationssystem kan ske i olika plattformar och baseras på en mängd olika programmeringsspråk. Var och en av dessa it-plattformar kan ha inneboende sårbarheter som både kan nyttjas av en hotaktör vid ett angrepp och som kan påverka driftsäkerheten i informationssystemet. Den som deltar i utveckling av informationssystem måste av därför ha adekvat och aktuell kompetens om de sårbarheter som finns i de plattformar där utveckling sker för att sårbarheter ska kunna omhändertas. Motsvarande förhållningssätt till kompetens gäller även för den som arbetar med drift av informationssystem. Utveckling av informationssystem är ett arbete som ofta bedrivs i projektform av ett utvecklingsteam som är skräddarsytt för det specifika utvecklingsprojektet. Inte sällan är den personal som utvecklar informationssystemet inhyrd eller i övrigt organisatoriskt frånskild från den personal som ska arbeta med drift och förvaltning av informationssystemet. Av denna anledning är det av vikt att den mottagande organisationen (driftorganisationen) som ska arbeta med drift och förvaltning av informationssystemet har rätt kompetenser och resurser innan informationssystemet tas i drift. Detta bidrar även till att driftorganisationen kan upprätthålla tillräcklig funktionalitet och säkerhetsskydd för informationssystemet över tid. Verksamhetsutövaren bör därför innan ett informationssystem av betydelse för säkerhetskänslig verksamhet tas i drift planera för drift och förvaltning av informationssystemet. I detta ligger att fastställa vilka resurser och kompetenser som erfordras för drift och förvaltning av informationssystemet. Att utbildning av personal eller nyrekryteringar tar tid och

är ytterligare aspekt, varför planeringen för drift och förvaltning bör ske på ett tidigt stadium.

I 8 § anges att verksamhetsutövaren även ska – innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift – *dokumentera* de *resurser* och *kompetenser* som krävs för att bibehålla fastställt säkerhetsskydd under informationssystemets förväntade livstid.

7.7 Utveckling av informationssystem

7.7.1 Allmänt om utveckling av informationssystem

Att utveckla ett informationssystem som har betydelse för säkerhetskänslig verksamhet kan vara en resurs- och tidskrävande aktivitet. Det kräver en tydlig *kravbild* utifrån en *särskild säkerhetsskyddsbedömning*, men också ett *strukturerat arbetssätt* och *god kompetens* om de risker och sårbarheter som kan kopplas till de plattformar i vilket utvecklingen sker.

7.7.2 Behovet av process för utveckling av informationssystem

Utveckling av informationssystem som ska användas i säkerhetskänslig verksamhet är en aktivitet som kräver noggrann planering och ett systematiskt arbetssätt. Om verksamhetsutövaren inte tar fram en egen process för utvecklingen, finns vedertagna koncept och processer för hur utveckling av ett informationssystem kan genomföras. Oavsett vilken metod eller process som används vid utveckling behöver verksamhetsutövaren planera med ett långsiktigt perspektiv för hanteringen av informationssystemet, dvs. från utvecklingen av systemet till avveckling av detsamma (systemets livscykel).[25] En sådan process bör bl.a. innefatta:

– planering,

– utveckling,

[25] Ett exempel på en sådan process utgör *Software Development Life Cycle* (SDLC), som är en vedertagen term för att beskriva en utvecklingsprocess där säkerhet tas i beaktande genom utvecklingsprocessens alla faser.

– testning,
– implementation,
– drift, och
– avveckling av ett informationssystem.

Oavsett val av modell för utveckling är det viktigt att verksamhetsutövaren säkerställer en integration av säkerhetsarbetet som en naturlig del av utvecklingsprocessen för att tillvarata säkerhetsskyddskraven i hela livscykelperspektivet för informationssystemet.

7.7.3 Systemdesign och systemutveckling

Allmänt om systemdesign och systemutveckling

Genom att införa olika säkerhetsrelaterade aktiviteter i varje steg under en utvecklingsprocess för ett informationssystem ökar möjligheterna att uppnå en ändamålsenlig och kostnadseffektiv säkerhet. För att uppnå en säker *systemdesign* och *systemutveckling* behöver ett antal aktiviteter genomföras, t.ex.:

– utbildning av utvecklare i säker systemutveckling (kodning, kodhantering och ramverk),
– hotmodellering,
– statisk och dynamisk kodanalys.

Verksamhetsutövaren bör även upprätta en separation av utvecklingsmiljön från test- och produktionsmiljöerna.[26]

Hotmodellering

Hotmodellering är en process där potentiella tillvägagångssätt som en hotaktör kan tänkas nyttja för att angripa ett informationssystem identifieras.[27] Syftet med hotmodellering är att utifrån en systematisk

[26] 4 kap. 4 och 5 §§ Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.
[27] Organisationen MITRE har tagit fram ett ramverk (ATT&CK framework) som beskriver olika attackmetoder, vilka kända aktörer som använt dessa och hur de kan motverkas eller upptäckas.

analys få en bild av vilka typer av angrepp en verksamhetsutövare kan drabbas av. Vid genomförandet av en hotmodellering identifieras systemets olika komponenter, kommunikationsvägar, flöden av data och potentiella hot samt attacker mot dessa. Detta arbete ska resultera i en lista med säkerhetsfunktioner som ska implementeras och potentiella säkerhetsbrister som ska hanteras i den fortsatta utvecklingen av informationssystemet. En sådan hotmodellering kan t.ex. göras i samband med framtagandet av den *särskilda säkerhetsskyddsbedömningen* för informationssystemet.

Säker kodning och kodhantering

Vid *systemutveckling* bör man utveckla arbetssätt som ger *god kodkvalitet* och *stabil funktionalitet*, t.ex. kan det ske i testdriven utveckling, där koden kontrolleras löpande för att upptäcka säkerhetsbrister. En verksamhetsutövare kan t.ex. använda automatiserad statisk kodanalys för att identifiera enklare säkerhetsbrister i koden. Utvecklaren får då information om vilka problem som upptäckts i källkoden och hur dessa kan åtgärdas. Verksamhetsutövaren kan även genomföra återkommande kodgranskning under hela utvecklingsprocessen.

Proprietära[28] säkerhetslösningar tenderar ofta att bli sårbara. Av denna anledning bör standardiserade och väletablerade produkter, protokoll och algoritmer i den omfattning det är möjligt användas. Vid utveckling av informationssystem bör även standardiserade och välbeprövade programvarubibliotek användas.

Tredjepartsbibliotek används ofta i utvecklingsprojekt för att skynda på utvecklingen, då dessa kan erbjuda en genväg för att uppnå en viss funktionalitet. Dessa bibliotek bör dock granskas innan de inkluderas i projektet då de kan innehålla sårbarheter. Har biblioteket hunnit användas brett i projektet kan det vara svårt att ta bort eller byta ut biblioteket i efterhand. Det är även viktigt att alla tredjepartsbibliotek som används i projektet kontinuerligt uppdateras, så att eventuella säkerhetsuppdateringar som publiceras inkluderas i projektet.

[28] Proprietär *programvara* är programvara som har restriktioner, t.ex. satta av ägaren, vad gäller att använda, modifiera eller kopiera.

7.7.4 Allmänt om arkitektur

Med begreppet *arkitektur* i ett informationssystem avses vanligen en detaljerad specifikation över vilka ingående komponenteter ett informationssystem ska bestå av och gränssnitten mellan dessa. Komponenter kan exempelvis utgöras av hårdvara, t.ex. infrastrukturkomponenter, eller mjukvara i form av applikationer och plattformar. Ett gränssnitt kan t.ex. vara kommunikationsprotokoll eller hur komponenterna ska sammankopplas rent fysiskt.

Med begreppet arkitektur avses även uppbyggnaden inom ett informationssystem, exempelvis i fråga hur olika entiteter inom informationssystem tillåts kommunicera med varandra, samt beroenden mellan entiteter.

7.7.5 Separation

Allmänt om separation

Ett informationssystem och programvaror och komponenter som ingår i det innehåller i regel både kända och okända sårbarheter som under vissa omständigheter kan nyttjas av en hotaktör. Vilken insats som krävs av en hotaktör för att utnyttja en sådan sårbarhet är till stor del beroende av hur informationssystemet exponeras.

Ett informationssystem som *inte kommunicerar* med något annat informationssystem har generellt sett en låg grad av exponering gentemot externa hotaktörer. Ett informationssystem som *kommunicerar* med ett eller flera andra informationssystem har däremot en högre exponering, vilket också öppnar upp fler möjliga vägar till angrepp.

För att minska exponering av informationssystem som innehåller säkerhetsskyddsklassificerade uppgifter är separation mellan informationssystem en viktig säkerhetsskyddsåtgärd.

Bestämmelser relaterade till separation av informationssystem återfinns i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

Av bestämmelserna i 4 kap. 20 § i PMFS 2019:2 framgår att verksamhetsutövaren ska se till att informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen begränsat *hemlig* eller *konfidentiell*, *logiskt* separeras från infor-

mationssystem eller nätverk som inte omfattas av motsvarande krav på säkerhetsskydd.

Av 21 § samma föreskrifter framgår att verksamhetsutövaren ska se till att informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *hemlig* eller *kvalificerat hemlig*, *fysiskt* separeras från informationssystem eller nätverk som inte omfattas av motsvarande krav på säkerhetsskydd. Informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *hemlig* eller *kvalificerat hemlig*, ska tillåta endast envägskommunikation vid import respektive export av data.

Logisk separation

Med logisk separation avses att möjligheten till kommunikation mellan informationssystem förhindras med stöd av mjuk- eller hårdvara. En verksamhetsutövare ska säkerställa att ett informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *begränsat hemlig* eller *konfidentiell*, logiskt separeras från informationssystem eller nätverk som inte omfattas av motsvarande krav på säkerhetsskydd.

Ett informationssystem avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *begränsat hemlig* eller *konfidentiell* kan i vissa fall *dela* infrastrukturkomponenter med ett informationssystem som inte omfattas av säkerhetsskydd. De tekniska lösningar som finns tillgängliga för att dela infrastruktur medför både risker och sårbarheter som en verksamhetsutövare behöver hantera. Att dela infrastrukturkomponenter mellan sådana informationssystem bör därför ske restriktivt.

Vid logisk separation föreligger bl.a. följande risker:

- sårbarheter i tekniken,
- sårbarheter i implementationen av tekniken,
- felaktiga konfigurationer.

Om den virtuella infrastrukturen delas mellan ett informationssystem som behandlar säkerhetsskyddsklassificerade uppgifter och ett informationssystem som inte omfattas av säkerhetsskydd kan en hotaktör

angripa den virtuella infrastrukturen och får åtkomst till det andra informationssystemet med hjälp av en sårbarhet i det ena informationssystemet.

Även om informationssystem avsedda för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *begränsat hemlig* eller *konfidentiell* inte ska kommunicera med informationssystem eller nätverk som saknar motsvarande krav på säkerhetsskydd, föreligger ibland behov av sådan kommunikation. Om sådan kommunikation ska kunna realiseras måste verksamhetsutövaren *ansöka om undantag*. Både Säkerhetspolisen och tillsynsmyndigheterna har möjlighet att medge undantag från bestämmelserna i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd. Innan en tillsynsmyndighet fattar beslut om undantag ska myndigheten *samråda* med Säkerhetspolisen.

Fysisk separation

Med fysisk separation avses att ett informationssystem inte har några fysiska sammankopplingar med ett annat informationssystem, om det inte omfattas av motsvarande krav på säkerhetsskydd.

En verksamhetsutövare ska se till att informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *hemlig* eller *kvalificerat hemlig*, fysiskt separeras från informationssystem eller nätverk som inte omfattas av motsvarande krav på säkerhetsskydd.

7.7.6 Import och export av data

Om data ska importeras till informationssystem avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *begränsat hemlig* eller *konfidentiell*, från ett informationssystem som inte omfattas av säkerhetsskydd, behöver verksamhetsutövaren tillse att import görs på ett sådant sätt att informationssystemen inte kan kommunicera med varandra. En metod för genomföra sådan import kan vara att importera data via bärbar lagringsmedia.

För informationssystem avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *hemlig* eller *kvalificerat hemlig*, får import och export av data endast ske via *envägskom-*

munikation. Med envägskommunikation avses att information enbart kan flöda åt ett håll. Om import och export behöver utföras samtidigt ska dessa funktioner, så långt det är möjligt, *separeras* för att göra det svårt att öppna upp en *dubbelriktad kommunikationskanal*.

Vid import av data kan verksamhetsutövaren behöva en funktion som kan detektera förekomst av skadlig kod, eller på annat sätt verifiera integriteten i data som importeras. Ett tillvägagångsätt kan vara att exekvera data i ett fristående informationssystem, s.k. sandlåda (sand box). Med denna metod kan verksamhetsutövaren kontrollera innehållet och i förkommande fall ”tvätta” filerna eller förhindra filerna från att importeras.

7.7.7 Säkerhetszoner och kontrollerad kommunikation

Allmänt

Ett sätt att minska exponeringen av ett informationssystem är att säkerställa att det kommunicerar på ett *kontrollerat* sätt. Ett informationssystem av betydelse för säkerhetskänslig verksamhet bör därför utformas enligt principen om kontrollerad kommunikation. Med detta avses att verksamhetsutövaren först fastställer hur och på vilket sätt ett sådant informationssystem får kommunicera. Därefter bör verksamhetsutövaren införa lämpliga säkerhetskyddsåtgärder som säkerhetsställer att informationssystem endast tillåts kommunicera på ett kontrollerat sätt.

Bestämmelser relaterade till kontrollerad kommunikation återfinns i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd. Av bestämmelserna i 4 kap. 19 § framgår att verksamhetsutövaren ska se till att informationssystem som har betydelse för säkerhetskänslig verksamhet kommunicerar på ett kontrollerat sätt med komponenter eller delsystem inom samma informationssystem, och kommunicerar på ett kontrollerat sätt med informationssystem eller nätverk som inte omfattas av krav på säkerhetsskydd.

7.7.8 Säkerhetszoner

Ett teoretiskt koncept som brukar användas för att åskådliggöra olika principer för att minska exponeringen av ett informationssystem är att modellera *olika säkerhetszoner*. I denna kontext placeras ett informationssystem i en säkerhetszon baserat på hur skyddsvärt det är. Säkerhetskyddsåtgärder bör säkerställa att endast tillåten kommunikation kan ske från en zon till en nästliggande zon.[29] Informationssystem som omfattas av motsvarande krav på säkerhetsskydd kan placeras i samma säkerhetszon.

En hotaktör med ett slumpmässigt mål har oftast inte kunskap och resurser som krävs för att få åtkomst till de mest skyddsvärda zonerna. En målinriktad hotaktör med mer kunskap och resurser kan försöka komma åt de mer skyddsvärda informationssystemen. En avancerad hotaktör kan förfoga över stora resurser, vilket kan möjliggöra kompromettering av det mest skyddsvärda informationssystemen.

Informationssystem kan i vissa fall vara placerade inom samma säkerhetszon och kan kommunicera direkt med varandra och dela infrastrukturkomponenter. Kommunikation mellan dessa bör dock ske på ett kontrollerat sätt, t.ex. med hjälp av brandvägg.

7.7.9 Nödvändig kommunikation

För att fastställa *vilken* kommunikation som ska *tillåtas* i ett informationssystem och vilka skyddsåtgärder som är lämpliga för att förhindra otillåten kommunikation kan en verksamhetsutövare genomföra en hotmodellering.

Kommunicering på ett kontrollerat sätt

Ett informationssystem innehåller flera olika entiteter (användare, funktioner m.m.), som kommunicerar med varandra för att utbyta information. När en entitet tillåts att kommunicera med en annan öppnas möjliga vägar till angrepp som kan nyttjas av en hotaktör. Ett annat sätt att beskriva detta är att entiteterna exponerar en angreppsyta.

[29] Det bör därför exempelvis inte vara möjligt att upprätta kommunikation direkt från zon 4 till zon 2 eller 1, utan att passera mellanliggande zon(er) där data verifieras innan de skickas vidare.

Med begreppet kommunicerar på ett kontrollerat sätt avses att verksamhetsutövaren har gjort ett medvetet ställningstagande kring hur entiteter tillåts kommunicera sinsemellan, samt hur dessa får kommunicera med entiteter i andra informationssystem. Med begreppet avses även att verksamhetsutövaren har infört säkerhetsskyddsåtgärder som förhindrar kommunikation som inte är tillåten. En viktig princip att beakta för att kunna uppnå kontrollerad kommunikation är att endast nödvändig kommunikation mellan entiteter ska tillåtas, och övrig kommunikation förhindras.

För att minska exponering av angreppsytor bör verksamhetsutövaren tillse att informationssystem som har betydelse för säkerhetskänslig verksamhet endast kommunicerar på ett kontrollerat sätt med komponenter eller delsystem inom samma informationssystem, samt kommunicerar på ett kontrollerat sätt med informationssystem eller nätverk som inte omfattas av krav på säkerhetsskydd. Åtkomstkontroll avgör vilka funktioner som får kommunicera med varandra, vilket medför att möjliga vägar till angrepp kraftigt reduceras. Endast specifikt utpekade funktioner bör kunna kommunicera med varandra.

Kommunikation mellan entiteter kan även begränsas genom exempelvis VLAN och brandväggar som endast tillåter godkänd kommunikation mellan olika nätsegment. Stödjande eller säkerhetsrelaterade funktioner i ett informationssystem, t.ex. administration (management), loggning eller säkerhetskopiering bör utföras och hanteras i avskilda nätsegment. Syftet med detta är att minska exponering av angreppsytor och begränsa möjligheter för en hotaktör att få åtkomst till känsliga resurser som kan ge administrativa behörigheter eller påverka spårbarheten. Vidare bör kommunikation till sådana nätsegment, när så är möjligt, krypteras för att förhindra obehörig insyn och påverkan.

Vid kommunikation av säkerhetsskyddsklassificerade uppgifter över förbindelser utanför verksamhetsutövarens kontroll, krävs kryptografiska funktioner som har godkänts av Försvarsmakten.

7.7.10 Kryptering

Allmänt om kryptering

Datakommunikation som inte är krypterad kan med enkla medel avlyssnas av någon som har tillgång till kommunikationen. Detsamma gäller för information på lagringsmedia. Kryptering är därför en viktig åtgärd för att skydda information från obehörig åtkomst när den transporteras i ett nätverk, eller när den lagras. Kryptering kan även användas för att skydda information mot förändring genom så kallad elektronisk signering, vilket också kan användas för att bevisa en identitet (autentisering) med exempelvis smarta kort.

Av bestämmelserna i 3 kap. 5 § och 7 kap. 5 § i säkerhetsskyddsförordningen (2018:658) framgår att innan säkerhetsskyddsklassificerade uppgifter behandlas i ett informationssystem utanför verksamhetsutövarens kontroll ska denne försäkra sig om att säkerhetsskyddet för uppgifterna i systemet är tillräckligt. Om säkerhetsskyddsklassificerade uppgifter ska kommuniceras till ett informationssystem utanför verksamhetsutövarens kontroll ska uppgifterna skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten.

Bestämmelser om kryptering finns även i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.[30]

Av bestämmelserna i 4 kap. 22 § i PMFS 2019:2 framgår att verksamhetsutövaren ska analysera behovet av användning av kryptografiska funktioner till skydd för säkerhetsskyddsklassificerade uppgifter och uppgifter som behöver skyddas från ett riktighetsperspektiv. En verksamhetsutövare behöver analysera behovet av kryptografiska funktioner för data i vila och data under transport och därefter införa de skyddsåtgärder som är motiverade. Med data i vila menas att den lagras på ett lagringsmedium såsom exempelvis en hårddisk eller en mobil enhet. Med data under transport menas att den rör sig mellan olika komponenter i ett datanätverk.

För att kryptering av information ska bli robust krävs en kedja av fungerade åtgärder. I detta ingår bl.a. säker hantering av kryptonycklar, skydd av kryptografisk utrustning och teknisk implementation av den kryptografiska funktionaliteten i informationssystemet.

[30] 3 kap. 21 § och 4 kap. 22 och 28 §§ Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

Chiffersviter

Chiffersviter används bl.a. vid handskakning i *kommunikationsprotokollet Transport Layer Security (TLS)*, som är vanligt förekommande för kryptering av datakommunikation. Vid handskakningen förhandlar parterna om vilka algoritmer som ska användas vid kommunikationen. I detta sammanhang är det viktigt att handskakningen endast tillåter *algoritmer* som verksamhetsutövaren har godkänt för ändamålet. Med jämna mellanrum upptäcks sårbarheter i de algoritmer som används för kryptografi. Att genomföra omvärldsbevakning för att inhämta av information om sådana sårbarheter är därför viktigt för att verksamhetsutövaren ska ha möjlighet att byta ut bristfälliga algoritmer eller implementationer i god tid.

Public Key Infrastructure (PKI)

För att användare och komponenter inom ett informationssystem på ett enkelt sätt ska kunna verifiera identiteter och andra entiteter i informationssystemet kan s.k. *Public Key Infrastructure (PKI)* användas. PKI innebär att verksamhetsutövaren implementerar en infrastruktur för *certifikat* och *nyckelhantering*, där en eller flera certifikatutfärdare[31] är utgivare av digitala certifikat. Digitala certifikat knyter en publik nyckel till ett subjekt, t.ex. ett användarnamn, på certifikatet och signeras elektroniskt av certifikatutfärdaren. Förlitande parter kan sedan verifiera att en motpart har en privat nyckel som står i relation till en publik nyckel och som i sin tur är elektroniskt signerad av, en av dem, betrodd certifikatutfärdare.

PKI-infrastrukturen kan användas för olika tillämpningar, bl.a. krypterade anslutningar mellan klienter och servrar, signerad och/eller krypterad e-post eller tvåfaktorsinloggning med s.k. smarta kort.[32]

Krypteringsnyckel

Hur krypteringsnycklar skyddas är avgörande för hur säker en funktion för kryptering kan anses vara. Att säkerställa att ingen obehörig kan få åtkomst till de nycklar som används vid kryptering, och i före-

[31] Certificate Authority.
[32] Hantering av PKI-miljön och rutiner kring utfärdande av digitala certifikat beskrivs i ett så kallat Certificate Practice Statement (CPS).

kommande fall signering, är därför viktigt. En verksamhetsutövare kan behöva reglera nyckelhantering både ur administrativt och tekniskt perspektiv, t.ex. genom bestämmelser om hur och när krypteringsnycklar utfärdas, byts ut och förstörs.

Krypteringsnycklar bör säkerhetskopieras centralt så att dekryptering är möjlig även om originalnyckeln har försvunnit.[33] Signeringsnycklar bör dock inte säkerhetskopieras då det påverkar signeringens oavvislighet, d.v.s. att innehavaren av signeringsnyckel kan hävda att någon annan har signerat ett objekt i dennes namn.

Kryptografiska funktioner som godkänts av Försvarsmakten

Om säkerhetsskyddsklassificerade uppgifter ska *kommuniceras* till ett informationssystem *utanför verksamhetsutövarens kontroll*, ska uppgifterna skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten.

Med begreppet kontroll menas att verksamhetsutövaren ska ha sådan kontroll över den förbindelse som används för att överföra (kommunicera) de säkerhetsskyddsklassificerade uppgifterna, att obehörig avlyssning kan sägas vara utesluten.

Om verksamhetsutövaren saknar sådan kontroll ska i stället kryptografiska funktioner som har godkänts av Försvarsmakten användas för att skydda de säkerhetsskyddsklassificerade uppgifterna vid överföring. I praktiken innebär begreppet kontroll att verksamhetsutövaren ska besitta både administrativ kontroll över informationssystemet/datanätet och fysisk kontroll över förbindelsen så att obehörig åtkomst för avlyssning kan förhindras.

Försvarsmakten är den myndighet som får utfärda föreskrifter om kryptografiska funktioner som är avsedda för skydd av säkerhetskänslig verksamhet. Vid behov av kryptografiska funktioner som godkänts av Försvarsmakten kan en verksamhetsutövare i första hand kontakta Myndigheten för samhällsskydd och beredskap (MSB) som har i uppdrag att samordna beställningar av signalskydd.

[33] S.k. Key Escrow.

7.7.11 Identitets- och behörighetshantering

Allmänt

För att säkerställa att endast behöriga får åtkomst till ett informationssystem och spårbarhet till olika händelser är en verksamhetsutövares identitets- och behörighetshantering ett viktigt arbete. Detta arbete innefattar många delar, allt från ID-kontroll för att verifiera identiteten på en person som ska tilldelas ett användarkonto i ett informationssystem, till att följa upp och säkerställa att en användare har rätt behörigheter över tid.

Bestämmelser om identitets och behörighetshantering återfinns bland annat i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

Behörighetsstyrning

Åtkomst inom ett informationssystem baseras som regel på en användare (eller ett användarkonto) till vilket det tilldelas behörigheter som styr vad användaren kommer åt. Med behörighetsstyrning avses främst administrativa åtgärder för att styra och hantera åtkomst till och inom ett informationssystem. De administrativa åtgärderna handlar främst om processer, rutiner och regler som beskriver hur verksamhetsutövarens ska hantera användare och deras behörigheter i ett informationssystem. Viktiga perspektiv att beakta vid behörighetsstyrning är tilldelning, förändring och uppföljning av användare och behörigheter.

Huvudprincipen vid behörighetsstyrning för ett informationssystem av betydelse för säkerhetskänslig verksamhet är att en användare av ett sådant informationssystem endast tilldelas de behörigheter som denne behöver för att kunna utföra sina arbetsuppgifter.[34] En annan viktig princip att beakta vid behörighetsstyrning är att tilldelade behörigheter bör tidsbegränsas.

[34] Denna princip beskrivs bl.a. i internationella standarder och facklitteratur. I engelsk facklitteratur används begreppet ”least privileged access” som benämning för denna princip.

Identitetshantering och spårbarhet över tid

En digital identitet kan beskrivas som en representation av en fysisk individ i ett informationssystem. För att en individ ska kunna använda ett informationssystem skapas en digital identitet, i de flesta fall i form av ett användarkonto. Ett användarkonto tilldelas i sin tur behörigheter som ger åtkomst till olika resurser i informationssystemet.

Alla utställda identiteter i ett informationssystem som har betydelse för säkerhetskänslig verksamhet ska vara unika över tid, det vill säga över hela informationssystemets livstid. Anledningen till detta är att identiteten ska kunna knytas till en unik fysisk person under hela informationssystemets livstid, samt att spårbarheten för vad olika individer gjort i informationssystemet ska vara tillförlitlig.

Åtkomst inom ett informationssystem ska vara spårbar till antingen individ, system eller resurs. Spårbarheten till individ är viktigt vid brottsutredningar samt för att kunna upptäcka och utreda incidenter. Det finns dock ofta konton i informationssystem som inte kan kopplas till en fysisk individ, t.ex. tjänstekonton som används främst för att utföra automatiserat bakgrundsarbete i ett informationssystem. Även om tjänstekonton inte går att koppla till en fysisk individ är det lika viktigt att dessa identiteter är och förblir unika över tid.

Identiteter kan ställas ut på många sätt och i olika former. När verksamhetsutövare tar fram processer, rutiner och regler inom ramen för sin behörighetsstyrning är det viktigt att säkerställa att:

- användarkonton inte återanvänds under informationssystemets livstid,
- användarkonton aldrig tas bort från ett informationssystem, utan i stället avaktiveras om de inte används,
- det sker kontinuerlig uppföljning av tilldelade användarkonton och deras behörighet.

Det är även viktigt att verksamhetsutövaren har processer som säkerhetsställer att alla identiteter i ett informationssystem har utgivits på ett tillförlitligt sätt.

Behörighetskontrollsystem

En teknisk funktion som styr användarnas åtkomst i ett informationssystem, eller mellan informationssystem, benämns behörighetskontrollsystem. Ett behörighetskontrollsystem baseras ofta på olika roller som kan tilldelas till användarna. Dessa roller styr användarnas skriv- och läsrättigheter till den information som finns i informationssystemet. För att förenkla hantering samt uppföljning av behörigheter hanteras detta många gånger i en central funktion, ofta benämnd centralt behörighetskontrollsystem.

Ett centralt behörighetskontrollsystem kan utgöra ett intressant angreppsmål. Det är därför viktigt att verksamhetsutövaren vidtar adekvata säkerhetsskyddsåtgärder för att förhindra att systemet utgör den svagaste kedjan i länken, i fråga om kontrollen av åtkomst till information.

Ett centralt behörighetskontrollsystem ska ges ett säkerhetsskydd som motsvarar det högsta säkerhetsskydd som de anslutna informationssystemen omges av. Vid val av skyddsåtgärder för ett centralt behörighetskontrollsystem blir därför säkerhetsskyddsklassificeringen av informationen i de anslutna informationssystemen ett viktigt ingångsvärde. Skyddsåtgärderna bör omfatta såväl tekniska som administrativa säkerhetsåtgärder.

7.7.12 Intrångsskydd och intrångsdetektering

Allmänt

Intrångsskydd beskrivs som administrativa eller tekniska åtgärder som vidtas för att skydda informationssystem mot obehörig åtkomst.[35] Bestämmelser om intrångsskydd och intrångsdetektering finns i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd. I föreskrifterna beskrivs intrångsdetektering som administrativa eller tekniska åtgärder som vidtas för att detektera intrång eller försök eller förberedelse till intrång i informationssystem.

Av bestämmelserna i 4 kap. 29 § i PMFS 2019:2 framgår att verksamhetsutövaren ska förse ett informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskydds-

[35] 3 kap. 4 § säkerhetsskyddsförordningen (2018:658) och 4 kap. 29–30 §§ Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

klassen *konfidentiell* eller *högre* och som *kommunicerar med andra informationssystem*, med funktioner för intrångsskydd och intrångsdetektering.

Av 30 § framgår att verksamhetsutövaren även ska förse ett informationssystem som *kommunicerar med andra informationssystem* och där en incident kan medföra *mer än ringa skada för Sveriges säkerhet* med funktioner för intrångsdetektering och intrångsskydd.

Tekniska hjälpmedel

Intrångsskydd (Intrusion Prevention) har som funktion att stoppa eller blockera oönskade aktiviteter som pågår i ett nätverk eller i ett informationssystem.

Syftet med *intrångsdetektering* (Intrusion Detection) är att identifiera och göra verksamhetsutövaren uppmärksam på oönskade aktiviteter som pågår i ett nätverk eller i ett informationssystem.

Funktioner för och intrångsskydd och intrångsdetektering kan i praktiken se ut på olika sätt, från nätverksbaserade produkter[36] till programvara som installeras i någon del av informationssystemet[37]. Det är viktigt att de system som avses användas kan analysera de protokoll som används inom systemet samt identifiera angrepp på dessa protokoll eller tjänster. En verksamhetsutövare måste således analysera var informationssystemet är exponerat och var sådana säkerhetsfunktioner ska implementeras.

Nätverksbaserade produkter för intrångsdetektering och intrångsskydd kan dock bli mindre effektiva till följd av den tekniska utvecklingen, där en stor del av all nätverkstrafik är krypterad och därmed svårare att inspektera. I vissa fall är det möjligt att t.ex. placera servertjänster bakom en lastbalanserare som handhar kryptering gentemot klienter. Dekryptering av nätverkstrafiken sker då innan denna skickas vidare till servern, vilket möjliggör inspektion av nätverkstrafiken.

Systemnära intrångsskydd och intrångsdetektering kan ge bättre skydds- och detekteringsförmåga än nätverksbaserade motsvarigheter,

[36] Nätverksbaserade produkter tar oftast sikte på att upptäcka skadliga aktiviteter i nätverkstrafik benämns *Network Intrusion Detection System* (NIDS). Produkter som även förhindrar skadliga aktiviteter i nätverkstrafik benämns vanligen *Network Intrusion Prevention System* (NIPS).

[37] Operativsystemnära mekanismer för detektion eller prevention benämns *Host Intrustion Detection System* (HIDS) respektive *Host Intrusion Prevention System* (HIPS). Utöver dessa finns även applikationsnära skydd som är specialiserade på vissa nätverksprotokoll, t.ex. *Web Application Firewalls* (WAF) för webbaserad kommunikation.

eftersom de ligger närmare systemet där händelsen sker. Det är dock av vikt att även implementera säkerhetsövervakning som kan agera på larm då en hotaktör i de flesta fall kan ta sig runt dessa skydd om tid ges.

7.7.13 Granskning vid anskaffning och utveckling

Under arbetet med anskaffning eller utveckling av ett informationssystem av betydelse för säkerhetskänslig verksamhet är den *särskilda säkerhetsskyddsbedömningen* central. Genom denna fastställer verksamhetsutövaren vilka säkerhetsskyddsåtgärder *(säkerhetskrav)* i informationssystemet som är motiverade utifrån hur informationssystemet ska användas. Den särskilda säkerhetsskyddsbedömningen blir därefter ett stöd för verksamhetsutövaren när säkerhetsskyddet ska utformas och granskas så att dessa krav tillgodoses.

I 4 kap 4 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd anges att verksamhetsutövaren ska se till att *egenutvecklad programvara* i informationssystem som har betydelse för säkerhetskänslig verksamhet *granskas* för att upptäcka och åtgärda säkerhetsbrister och sårbarheter.

I 5 § anges att verksamhetsutövaren ska se till att *tredjepartsprogramvara* i informationssystem som har betydelse för säkerhetskänslig verksamhet *granskas* för att upptäcka och åtgärda säkerhetsbrister och sårbarheter, eller att programvaran på annat sätt bedöms vara tillförlitlig från säkerhetsskyddssynpunkt.

7.7.14 Drift- och testmiljö

Om ett informationssystem ska implementeras i en befintlig it-miljö (driftmiljö) bör *testning* av informationssystemet utföras i åtskild it-miljö (testmiljö), som på ett realistiskt sätt efterliknar den it-miljö där informationssystemet ska implementeras. Syftet med testmiljön är att säkerställa att sårbarheter inte införs i driftmiljön, att undvika störningar i driftmiljön, samt att testerna i övrigt blir tillförlitliga.

Förutom att driftmiljön bör vara separerad från testmiljön, bör även testmiljön vara separerad från den it-miljö där utveckling sker. Verksamhetsutövaren bör således även upprätta en så kallad utvecklingsmiljö.

7.8 Säkerhetskonfiguration av informationssystem

7.8.1 Allmänt om säkerhetskonfiguration

Säkerhetskonfigurering, s.k. härdning, innebär att operativsystem, nätverkskomponenter, andra komponenter, inbyggda programvaror, databaser och andra applikationer som ingår i ett informationssystem konfigureras på ett så säkert sätt som möjligt.[38] Exempelvis kan åtkomsträttigheterna i systemet och de delar som ingår begränsas, möjliga vägar till angrepp via sårbara funktioner i infrastrukturkomponenter och applikationer skäras av och exponering mot andra informationssystem eller externa enheter förhindras.

Bestämmelser om säkerhetskonfigurering återfinns i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd. Av bestämmelserna i 4 kap. 23 § i PMFS 2019:2 framgår att verksamhetsutövaren ska för informationssystem som har betydelse för säkerhetskänslig verksamhet tillämpa konfiguration som använder lämpliga säkerhetsfunktioner, stänger av funktioner som inte används och även i övrigt reducerar sårbarheter.

S.k. härdning utgår från principen att det som inte behövs för informationssystemets definierade funktion ska vara begränsat avseende åtkomst, avstängt eller borttaget ur informationssystemet. I arbetet med härdning behövs dock en avvägning av vilka åtgärder som ska vidtas, där man särskilt bör beakta hur informationssystemet exponeras samt vilken hotbild verksamhetsutövaren har att förhålla sig till. Härdning bör ske utan att informationssystemets stabilitet påverkas och därutöver kan användarvänligheten vara en aspekt att beakta. Härdning bör vara en del av en standardkonfiguration och automatiseras så långt det är möjligt för att minimera risken för felkonfigurationer.

För att härda ett informationssystem finns det olika *rekommendationer* från både tillverkare och andra aktörer på marknaden. Tillverkarspecifika rekommendationer eller andra allmänt kända och verifierade inställningar bör i första hand användas om sådana finns. Kvaliteten på rekommendationerna kan dock vara svår att bedöma, och varierar från tillverkare till tillverkare.

[38] 3 kap. 4 § säkerhetsskyddsförordningen (2018:658) och 4 kap. 23 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

Som alternativ till dessa finns olika *standarder* utgivna av olika *oberoende organisationer*. Dessa är oftast mer konceptuella och omfattar de vanligaste delarna i ett informationssystem.

För att säkerställa att en hotaktör inte ska kunna påverka ett informationssystem behöver säkerhetsskyddsåtgärderna utformas så att de kompletterar och överlappar varandra. Ett sätt att åstadkomma detta är att säkerhetsskyddsåtgärderna *byggs i flera lager.*[39]

7.8.2 Skydd mot skadlig kod

Allmänt om skydd mot skadlig kod

Skadlig kod är ett samlingsnamn för olika typer av programvaror som orsakar avsiktlig störning eller skada.[40] I begreppet skadlig kod ingår bl.a. virus, maskar, trojaner, exploits och rootkits.

Skydd mot skadlig kod syftar till att skydda informationssystemet mot programkod som är tänkt att användas för att otillbörligt ändra, röja, exfiltrera, förstöra eller avlyssna uppgifter, filer eller programvara som lagras eller kommuniceras till eller från ett informationssystem.

Bestämmelser om skydd mot skadlig kod finns i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.[41] Av bestämmelserna i 4 kap. 27 § i PMFS 2019:2 framgår att verksamhetsutövaren ska för informationssystem som har betydelse för säkerhetskänslig verksamhet analysera behovet av och i förekommande fall besluta att använda de funktioner för skydd mot skadlig kod som är nödvändiga från säkerhetsskyddssynpunkt.

---

[39] Säkerhetsskyddåtgärder att implementera kan t.ex. vara:
– fysisk plombering för att upptäcka eventuell manipulation av hårdvara,
– Secure Boot för verifiering av uppstartsprocess,
– hårddiskkryptering,
– skydd av systemfiler (åtkomstkontroll),
– vitlistning av godkända hårdvaruenheter,
– vitlistning och signering av godkända applikationer,
– användning av lokal brandvägg,
– skydd mot skadlig kod,
– detektering och skydd mot skadliga aktiviteter (intrångsdetektering/intrångsskydd).

[40] I engelsk facklitteratur används begreppet *malicious code* eller kortformen *malware*.

[41] 3 kap. 4 § säkerhetsskyddsförordningen (2018:658) och 4 kap. 27 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

Tekniska hjälpmedel

En verksamhetsutövare som har ett informationssystem som är av betydelse för säkerhetskänslig verksamhet behöver i första hand göra en analys av vilka funktioner för skydd mot skadlig kod som är lämpliga utifrån hur informationssystemet ska användas. Därefter behöver verksamhetsutövaren besluta vilka funktioner som ska användas, och slutligen införa dessa funktioner till skydd av informationssystemet.[42]

Det vanligaste skyddet mot skadlig kod är antivirusprogramvara, som med hjälp av signaturer söker efter hela eller delar av filer som kan ha ett skadligt beteende. Det är dock enkelt för en hotaktör att skapa nya versioner av skadlig kod som inte upptäcks av antivirusprogramvaran då signaturen inte längre matchar. Antivirusprogramvara kan därför vara ett svagt skydd mot en kvalificerad aktör, men ska ses som ett grundläggande skydd av informationssystem.

Utöver antivirusprogramvaror finns olika säkerhetsprodukter som ytterligare kan stärka skyddet. Initialt bör dock inbyggda funktioner användas så långt det är möjligt för att minimera kostnader och komplexitet. Vidare bör rutiner för att kontrollera att skyddet mot skadlig kod är aktivt tas fram och dokumenteras.

7.9 Funktionstester och säkerhetsgranskning

7.9.1 Allmänt om funktionstester och säkerhetsgranskning

Funktionstester och *säkerhetsgranskning* syftar till att säkerhetsställa att informationssystemet lever upp till den kravställning som ställs på systemet.[43]

Funktionstester kan säkerställa att systemet är robust och att informationen i systemet är tillgänglig och korrekt. Med säkerhets-

[42] Effektivt skydd mot skadlig kod kan bestå av:
– programexekveringskontroll (så kallad vitlistning) så att enbart godkända program kan exekveras,
– behörighetsstyrning (begränsning av administratörsrättigheter),
– begränsning av möjlighet att exekvera scriptkod inom olika dokumenttyper såsom exempelvis Microsoft Office dokument och PDF-filer,
– lokala brandväggar som hindrar skadlig programvara från att sprida sig vidare till andra system,
– funktioner som försvårar att exploatera sårbarheter, exempelvis buffertöverskridning, och
– antivirusprogramvara.

[43] 3 kap. 1 och 4 §§ säkerhetsskyddsförordningen (2018:658), 2 kap. 17 § och 4 kap. 12–17 §§ Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

granskning utökas detta till att även säkerhetsställa att informationssystemet kan motstå angrepp och andra incidenter som kan utsätta systemet eller informationen för exponering. Dessa tester och granskningar bör genomföras löpande under utvecklingsarbetet för att minimera arbetet med rättningar av avvikelser vid driftsättning.

I detta avsnitt beskrivs åtgärder som en verksamhetsutövare bör vidta vid funktionstester och säkerhetsgranskning av ett informationssystem som har betydelse för säkerhetskänslig verksamhet.

7.9.2 Funktionstester

Bestämmelser om *granskning* av informationssystem återfinns bl.a. i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd. Av bestämmelserna i 4 kap. 4 § i PMFS 2019:2 framgår att verksamhetsutövaren ska se till att *egenutvecklad programvara* i informationssystem som har betydelse för säkerhetskänslig verksamhet granskas för att upptäcka och åtgärda säkerhetsbrister och sårbarheter.

Av 5 § följer att verksamhetsutövaren ska se till att *tredjepartsprogramvara* i informationssystem som har betydelse för säkerhetskänslig verksamhet granskas för att upptäcka och åtgärda säkerhetsbrister och sårbarheter, eller att programvaran på annat sätt bedöms vara tillförlitlig från säkerhetsskyddssynpunkt.

För att säkerställa att programvaran eller systemet fungerar enligt kravställning bör därför *tester* utföras för att säkerställa att *integritet* och *tillgänglighet* kan garanteras.

Funktionstester kan bestå av t.ex. belastningstester, redundanstester och verifiering av indata. Funktionsrelaterade tester av ett informationssystem benämns ofta acceptanstest. Acceptanstest innebär att informationssystemet testas mot olika fördefinierade testfall som beskriver en händelse och hur informationssystem ska bete sig vid givna parametrar. Under sådana tester är säkerhetsfunktionerna ofta bara en delmängd av flera funktioner som testas.

7.9.3 Säkerhetsgranskning

Säkerhetsgranskning kan bestå av:

– granskning av *styrning* i fråga om *rutiner* och *regelverk*,
– teknisk granskning som syftar till att *verifiera säkerheten* i olika *tekniska* implementationer i ett informationssystem.

Vid *utveckling av egen programvara* bör tekniska säkerhetsgranskningar genomföras löpande under utvecklingsprocessen för att enklare kunna upptäcka och åtgärda säkerhetsproblem i ett tidigt skede. Verksamhetsutövaren kan därför behöva ta fram rutiner och metodstöd för ändamålet så att tekniska säkerhetsgranskningar blir en naturlig del av utvecklingsprocessen.

Även om granskning av delkomponenter genomförs under en utvecklingsprocess bör en sammantagen säkerhetsgranskning genomföras, där alla komponenter i informationssystemet testas tillsammans. Detta kan lämpligen ske i slutskedet av utvecklingsprocessen, t.ex. genom ett penetrationstest (se nedan).

Efter att upptäckta brister och sårbarheter har åtgärdats kan ytterligare en granskning behöva ske för att verifiera att dessa i praktiken är åtgärdade, eller på annat sätt motverkats. Säkerhetsgranskningar bör därutöver även genomföras löpande efter att driftsättning har skett.

Granskning av programvara från tredje part

Vid användning av programvara som inte utvecklats av verksamhetsutövaren (*s.k. tredjepartsprogramvara*), är det viktigt att verksamhetsutövaren undersöker om denna programvara har oönskad funktionalitet som negativt kan påverka säkerheten i ett informationssystem där programvaran ska användas. Om det kan antas att tredjepartsprogramvara inte granskats av en part som verksamhetsutövaren bedömer som tillförlitlig, bör verksamhetsutövaren själv genomföra en grundlig säkerhetsgranskning av programvaran innan den implementeras i ett informationssystem. Syfte med en sådan grundlig säkerhetsgranskning är att upptäcka oönskad funktionalitet samt skydda informationssystemet mot exempelvis dolda kanaler och skadlig kod som kan finnas i tredjepartsprogramvaran. Där det är lämpligt bör även

säkerhetskonfigurationen granskas så att produkten implementeras på ett korrekt sätt.

7.9.4 Sårbarhetsskanning

En *sårbarhetsskanning* är en metod som används för att automatiskt kontrollera att säkerhetsuppdateringar är installerade på en it-infrastruktur, system och applikationer. En sårbarhetsskanner kan även hitta enklare brister i konfiguration.

En sårbarhetsskanning är ofta ett verktyg som används under ett penetrationstest, men kan även automatiseras för regelbunden kontroll av applikationer och infrastruktur i it-miljön i syfte att över tid ha kontroll över uppdaterings- och säkerhetsnivån i nätverken. En sårbarhetsskanning kan genomföras både med och utan inloggning i målsystemen.[44]

7.9.5 Penetrationstest

Ett *penetrationstest* är en metod som används för att säkerställa att it-infrastruktur, system och applikationer kan stå emot ett angrepp genom att använda samma metoder som en hotaktör.

Penetrationstester kan utföras med olika metodik och det finns ett antal standarder att använda som stöd i testningen samt i bedömningen av brister. Ett penetrationstest kan utföras på allt från en hel it-infrastruktur till enskilda system eller applikationer. Metoderna kan skilja sig mellan olika testscenarier. Det finns i huvudsak tre vanligt

[44] Flertalet sårbarhetsskannrar erbjuder möjlighet att genomföra aggressiva tester som t.ex. *Denial-of-Service-attacker* (DoS-attacker). Flertalet sårbarhetsskanners erbjuder även möjlighet att genomföra webbapplikations-skanningar. Det finns också lösningar som enbart genomför skanningar på webbapplikationer. Dessa kan ses som ett komplement till renodlade penetrationstester.

förekommande koncept för penetrationstester som benämns *blackbox*[45], *whitebox*[46] och *greybox*[47].

Ett penetrationstest med godkänt resultat kan dock *inte ses som en garant för att inte bli utsatt för obehörigt intrång*, eftersom det inte finns några garantier att samtliga sårbarheter upptäckts under testet. Ett penetrationstest ger däremot en indikation av hur väl säkerhetsarbetetsarbetet fungerar.

De brister som upptäcks vid granskning bör dokumenteras och graderas.[48] Graderingen kan sedan ligga till grund för i vilken ordning säkerhetsbristerna ska åtgärdas eller på annat sätt motverkas. Efter åtgärdens införande bör ytterligare test ske för att säkerställa att åtgärden har gett avsedd effekt. Rapportering och dokumentation efter ett penetrationstest bör delges berörda inom en organisation så att de får en djupare kunskap om bl.a. upptäckta sårbarheter.

7.10 Inför driftsättning

7.10.1 Allmänt om åtgärder inför driftsättning

Innan ett informationssystem tas *i drift* behöver verksamhetsutövaren säkerställa att informationssystemet är färdigställt och att det kan användas operativt i den säkerhetskänsliga verksamheten. Detta innefattar bl.a. att *verifiera funktions-* och *säkerhetskrav*, tillse att relevant *systemdokumentation är upprättad*, genomföra ett eventuellt *samråd*

[45] *Blackbox* är ett koncept där de penetrationstestare som ska utföra testerna inte får någon förhandsinformation om organisationens it-miljö. Även om detta koncept är realistiskt i förhållande till de förutsättningar en hotaktör har används konceptet väldigt sparsamt. Anledning till detta är att ett penetrationstest enligt konceptet black-box är extremt tidsödande och sällan ger heltäckande resultat då ett penetrationstest vanligtvis genomförs inom en begränsad tidsperiod.

[46] *Whitebox* är ett koncept där de penetrationstestare som ska utföra testerna får fullständig tillgång till information om organisationens it-miljö innan testet påbörjas. Vanligtvis ges penetrationstestarna även fullständig åtkomst till nätverk, konton, applikationer samt eventuell källkod. Denna metodik är vanligtvis mest effektiv och ger ofta ett heltäckande resultat då tiden kan nyttjas mer effektivt och fler sårbarheter kan upptäckas och graderas.

[47] *Greybox* är ett koncept som utgör en kombination av blackbox och whitebox. Här kan informationstilldelning och åtkomst anpassas efter behov och förutsättningar. Denna metodik används ofta i övningar med s.k. blue- och red-team mellan säkerhetsövervakning och penetrationstestare för att testa upptäckandeförmågan och rutiner för incidenthantering inom organisationen.

[48] Gradering av säkerhetsbrister kan ske med hjälp av t.ex. *Common Vulnerability Scoring System* (CVSS). CVSS beaktar olika aspekter av en sårbarhet som t.ex. attackvektor, komplexitet och påverkan på konfidentialitet, riktighet och tillgänglighet. Baserat på dessa parametrar räknas ett värde från 0 till 10 fram, där 0 innebär låg risk för informationssystemet och 10 innebär kritisk risk.

med Säkerhetspolisen samt fatta *beslut om driftgodkännande*.[49] Driftsättning är det sista steget i en utvecklingsprocess innan ett informationssystem kan börja användas operativt av verksamhetsutövaren.

Bestämmelser om driftsättning finns bl.a. i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd. Av bestämmelserna i 4 kap. 7 § i PMFS 2019:2 framgår att verksamhetsutövaren ska, innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift, genomföra *tester av säkerhetsskyddsåtgärderna*. Resultatet ska dokumenteras och jämföras med de säkerhetskrav som gäller för informationssystemet. Den särskilda säkerhetsskyddsbedömningen ska uppdateras med eventuella avvikelser och de kompensatoriska åtgärder som måste vidtas.

Av bestämmelserna i 4 kap. 9 § i PMFS 2019:2 framgår att verksamhetsutövaren ska, innan samråd enligt 3 kap. 2 § säkerhetsskyddsförordningen (2018:658) sker med Säkerhetspolisen, kontrollera och dokumentera att de säkerhetskrav som identifierats i den särskilda säkerhetsskyddsbedömningen har implementerats och att säkerhetsskyddsåtgärderna ger avsedd effekt.

Av bestämmelserna i 4 kap. 25 § i PMFS 2019:2 framgår att verksamhetsutövaren även ska ha dokumentation som visar logiska samband och inbördes beroenden mellan komponenter som används i informationssystem som har betydelse för säkerhetskänslig verksamhet.

Av 26 § följer att verksamhetsutövaren ska för informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *kvalificerat hemlig*, dokumentera vilken hård- och mjukvara som används i informationssystemet och deras inbördes beroenden. Kraven gäller *även informationssystem* där en incident kan medföra *synnerligen allvarlig skada* för Sveriges säkerhet.

I nästa avsnitt beskrivs närmare de åtgärder som en verksamhetsutövare behöver genomföra innan driftsättning sker av informationssystem som har betydelse för säkerhetskänslig verksamhet.

[49] Se 3 kap. 1–3 §§ säkerhetsskyddsförordningen (2018:658) och 3 kap. 1 § och 4 kap. 7–9, 25 och 26 §§ Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

7.10.2 Dokumentation

Upprättad *systemdokumentation* är normalt en förutsättning för att få översikt över ett informationssystem. Det är också en förutsättning för att effektivt kunna hantera driftrelaterade problem och incidenter. Systemdokumentationen är även ett hjälpmedel för att identifiera vilka delar av informationssystemet som berörs av en säkerhetsuppdatering som ska installeras, vilka delar som berörs av en inträffad incident samt i övrigt för att kunna identifiera beroenden mellan olika komponenter i ett informationssystem.

Verksamhetsutövaren ska upprätta systemdokumentation för informationssystemet innan det driftsätts. Systemdokumentation kan behövas i olika delar av en organisation, och den måste därför utformas på ett sådant sätt att den är till nytta för de olika avsedda mottagarna.[50] Systemdokumentation bör även finnas i pappersform så att den är möjlig att ta del av även om den elektroniskt lagrade dokumentationen är otillgänglig, t.ex. vid större störningar i nätverken.

7.10.3 Verifiering av funktions- och säkerhetskrav

För att en verksamhetsutövare ska kunna säkerhetsställa att ett informationssystem som har betydelse för säkerhetskänslig verksamhet uppfyller säkerhetskraven och att de säkerhetskyddsåtgärder som identifierats i den särskilda säkerhetsskyddsbedömningen ger önskad effekt, behöver informationssystemet ha genomgått *testning* innan driftsättning. Resultatet av dessa ska jämföras mot verksamhetsutövarens funktionella och säkerhetsrelaterade krav för informationssystemet. Detta är ett sätt att verifiera att informationssystemet uppfyller de krav som verksamhetsutövaren fastställt. Kraven identifieras och fastställs av verksamhetsutövaren i den särskilda säkerhetsskyddsbedömningen, och i förkommande fall genom hotmodellering. Den särskilda säkerhetsskyddsbedömningen är ett styrande dokument för alla delar i utvecklingen av ett informationssystem som ska användas i säkerhetskänslig verksamhet. Detta gäller inte minst i den

[50] Systemdokumentation kan innehålla bl.a.:
– beskrivningar av informationssystemets arkitektur med ingående hård- och mjukvara (Solution Architecture Document, SAD),
– förklaring av hur varje komponent inom systemet fungerar, och
– beskrivningar av hur systemet bör underhållas och vad som ska göras vid vissa kända problem.

del i utvecklingsprocessen där en verksamhetsutövare ska genomföra tester och säkerhetsgranskningar.

7.10.4 Driftgodkännande

Av 3 kap. 3 § säkerhetsskyddsförordningen framgår att ett informationssystem som ska användas i säkerhetskänslig verksamhet inte får tas i drift förrän det har *godkänts* ur säkerhetsskyddssynpunkt *av verksamhetsutövaren*. Godkännandet ska dokumenteras.

Under vissa omständigheter är en verksamhetsutövare skyldig att även samråda med Säkerhetspolisen innan ett informationssystem tas i drift eller i väsentliga avseenden förändras.

7.11 Drift och underhåll

7.11.1 Allmänt om drift och underhåll

Arbetet med *drift* och *underhåll* av informationssystem avser dels att hantera olika driftrelaterade problem som kan uppstå, dels att tillse att säkerheten i informationssystemet upprätthålls över tid. Viktiga delar i detta arbete är att tillse att informationssystemet hålls uppdateras, att föråldrad programvara byts ut samt att förändringar och avveckling genomförs på ett kontrollerat sätt.[51]

Bestämmelser relaterade till drift och underhåll finns bl.a. i Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2).

7.11.2 Styrning av drift och underhåll

För att tillgodose att säkerheten i ett informationssystem upprätthålls över tid är det viktigt att en verksamhetsutövare har en tydlig *styrning* av hur *drift* och *underhåll* av ett informationssystem ska hanteras. Om drift och underhåll av ett informationssystem inte hanteras på ett medvetet och strukturerat sätt av verksamhetsutövaren, kan det leda till att systemets tillförlitlighet påverkas, t.ex. genom tillgänglighetsrelaterade problem eller andra sårbarheter i informationssystemet.

[51] Se 3 kap. 4 § säkerhetsskyddsförordningen (2018:658) och 3 kap. 3, 25–27 §§ och 4 kap. 2, 10, 24, 34 och 38 §§ Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

Av bestämmelserna i 4 kap. 10 § i PMFS 2019:2 framgår att verksamhetsutövaren ska *fastställa rutiner* för hanteringen av informationssystem som har betydelse för säkerhetskänslig verksamhet under systemets förväntade livstid.

Traditionellt styrs drift och underhåll av ett informationssystem med stöd av ett skriftligt ramverk som innehåller både över gripande principer och anvisningar för hur olika driftrelaterade frågor ska hanteras i praktiken. Oavsett styrmodell är det viktigt att styrdokumenten anpassas utifrån den egna verksamhetens förutsättningar och informationssystemets komplexitet och omfattning. En allt för detaljreglerad styrning kan i vissa fall medföra att driften blir för svårhanterad, och en allt för svag reglering kan medföra att kontrollen över informationssystemet blir bristfällig.

Vid framtagande av styrning för hur drift av informationssystem bör verksamhetsutövaren bl.a. beakta perspektiven:

- felhantering,
- förändringshantering,
- uppdateringar,
- incidenthantering,
- kontinuitetshantering.

Det är av vikt att verksamhetsutövaren etablerar tydliga roller med beskrivning av vem som gör vad, vem som har vilket ansvar och vem som har vilka befogenheter. I sammanhanget är det även av vikt att ansvaret för säkerheten i ett informationssystem tydligt anges. Förändringar i styrande dokument för drift bör endast genomföras efter att de har godkänts av en kompetent och specifikt utpekad person eller funktion hos verksamhetsutövaren. Den praktiska hanteringen av driften av ett informationssystem bör, där det är tekniskt möjligt, hanteras konsekvent med samma verktyg och hjälpmedel.

Förändringshantering

En grundläggande princip är att informationssystem som används i säkerhetskänslig verksamhet ska hållas uppdaterade så att säkerhetsbrister och sårbarheter motverkas. I praktiken innebär detta att verk-

samhetsutövaren måste förse både mjuk- och hårdvaran i informationssystemet med de säkerhetsuppdateringar som publiceras av tillverkaren, samt i övrigt byta ut äldre versioner av programvara som inte längre kan förses med säkerhetsuppdateringar. Större förändringar i ett informationssystem, särskilt när ny programvara implementeras, kan påverka både säkerheten och tillgängligheten. Förändringar av befintlig programvara eller implementation av ny programvara som kan komma att påverka informationssystemet bör därför ske under kontrollerade former. En annan viktig aspekt att beakta vid förändringar i ett informationssystem är att förändringar inte genomförs på ett sådant sätt som åsidosätter säkerhetsfunktioner i informationssystemet, antingen tillfälligt eller permanent.

Säkerhetsuppdatering

Informationssystem som innehåller programvara som inte är uppdaterad är i många fall ett tacksamt mål för en hotaktör. Sårbarheter i programvaror identifieras löpande och blir ibland publikt kända redan innan tillverkaren av programvaran hunnit åtgärda sårbarheten och publicerat en säkerhetsuppdatering. Regelbunden uppdatering av programvara genom säkerhetsuppdateringar (s.k. säkerhetspatchar) är en åtgärd som utgör en del av det grundläggande skyddet av ett informationssystem.

Syftet med säkerhetsuppdateringar är att användaren ska ha en möjlighet att åtgärda publikt kända sårbarheter i programvaran och på så sätt minska risker för att drabbas av ett angrepp via dessa. Hur en känd sårbarhet i programvara kan nyttjas av en hotaktör skiljer sig naturligtvis åt och beror till stor del på hur programvaran är implementerad och konfigurerad av användaren.

Säkerhetsuppdateringar publiceras inte bara för mjukvara såsom applikationer och operativsystem, utan även för hårdvara i infrastruktur såsom exempelvis switchar, routrar och servrar.

Utbyte av programvara

Av bestämmelserna i 4 kap. 24 § i PMFS 2019:2 framgår att verksamhetsutövaren ska se till att *programvara* i informationssystem som har betydelse för säkerhetskänslig verksamhet hålls *uppdaterad* så att

säkerhetsbrister och sårbarheter motverkas. Om det finns särskilda skäl får verksamhetsutövaren besluta om undantag från dessa krav.

Informationssystem som innehåller föråldrade versioner eller utgåvor av programvara är också ett tacksamt mål för en hotaktör. När en tillverkare släpper en ny version eller utgåva av en programvara upphör ofta publiceringen av säkerhetsuppdateringar till äldre versioner av programvaran. Äldre versioner av programvaran kan ha tillgång till support under en övergångsperiod som fastställs av tillverkaren. Det är därför av vikt att verksamhetsutövaren har kännedom om när tillverkarens support för en programvara upphör (s.k. ”end-of-life”) och har en plan för när avveckling av den föråldrade programvaran ska ske. Programvara som inte längre erhåller säkerhetsuppdateringar från tillverkaren bör därför avvecklas och ersättas.

Ett informationssystem som hanterar säkerhetsskyddsklassificerade uppgifter får inte anslutas direkt mot internet för hämtning av uppdateringar. Säkerhetsuppdateringar behöver därför hämtas till ett separat informationssystem och därefter, på ett kontrollerat sätt, föras över till informationssystemet som hanterar de säkerhetsskyddsklassificerade uppgifterna.

Om möjligt bör *ny programvara testas* i ett informationssystem som är separerat från det informationssystem där programvaran ska installeras och användas. Detta ger verksamhetsutövaren möjlighet att testa och granska hur den nya programvaran beter sig, utan att det kan påverka informationssystemet som är i drift. Samma testförfarande bör om möjligt även tillämpas vid *uppdatering* av och *utbyte* av befintlig programvara. Informationssystem som beskrivs ovan benämns ofta i termer av testmiljö respektive driftsmiljö.

7.11.3 Beslut om undantag av säkerhetsuppdateringar

En grundläggande princip är att informationssystem som används i säkerhetskänslig verksamhet ska hållas uppdaterade så att säkerhetsbrister och sårbarheter motverkas. Som ovan framgår innebär detta att verksamhetsutövaren måste förse både mjuk- och hårdvaran i informationssystemet med de säkerhetsuppdateringar som publiceras av tillverkaren, samt i övrigt byta ut äldre versioner av programvara som inte längre kan förses med säkerhetsuppdateringar.

Om det finns särskilda skäl får en verksamhetsutövare besluta om *undantag* från *kravet på att programvara* i ett informationssystem som har betydelse för säkerhetskänslig verksamhet hålls *uppdaterad*. Så kan vara fallet om det inte är tekniskt möjligt att installera säkerhetsuppdateringarna eller i det fall verksamhetsutövaren konstaterat att det uppenbarligen är obehövligt då andra kompenserade åtgärder har vidtagits.

7.11.4 Säkerhetskopiering

Säkerhetskopiering är många gånger en livlina och det kan få stora konsekvenser om den är bristfällig, eftersom information som regel är en verksamhetsutövares viktigaste resurs. Brister i säkerhetskopieringen kan vid dataförlust åsamka verksamhetsutövaren stor skada. Även förlust av till synes ganska oviktig information kan skada verksamheten. Verksamhetsutövaren bör därför ta fram rutiner för hur säkerhetskopiering ska hanteras.

7.12 Allmänt om operativ säkerhet

Med *operativ säkerhet* avses det operativa arbete som syftar till att upptäcka, försvåra och hantera skadlig inverkan på informationssystemet samt obehörig avlyssning av, åtkomst till och nyttjande av informationssystemet. Inom detta område är *säkerhetsloggning*, *logguppföljning*, *säkerhetsövervakning* och *incidenthantering* viktiga områden. Bestämmelser relaterade till operativt säkerhetsarbetet återfinns i säkerhetsskyddsförordningen.

Av bestämmelserna i 3 kap. 4 § säkerhetsskyddsförordningen framgår att en verksamhetsutövare som ansvarar för ett informationssystem som ska användas i säkerhetskänslig verksamhet ska vidta lämpliga skyddsåtgärder för att kunna *upptäcka*, *försvåra* och *hantera skadlig inverkan* på informationssystemet samt *obehörig avlyssning av*, *åtkomst till* och *nyttjande* av informationssystemet. Verksamhetsutövaren ska också se till att *spårbarhet* finns för händelser som är av betydelse för säkerheten i systemet.

7.12.1 Säkerhetsloggning

Allmänt om säkerhetsloggning

Loggning kan göras med olika syften. En verksamhetsutövare som är ansvarig för ett informationssystem av betydelse för säkerhetskänslig verksamhet bör primärt logga händelser med syfte att kunna upptäcka och utreda skadlig eller otillåten påverkan, obehörig åtkomst och funktionsstörningar i informationssystemet.[52]

En logg kan beskrivas som insamlad information om en händelse och om när händelsen inträffat i ett informationssystem. Loggar är ett hjälpmedel för att kunna veta vad som hänt i ett informationssystem vid ett givet tillfälle.

Loggar är en förutsättning för att en verksamhetsutövare kunna uppnå spårbarhet till olika händelser som inträffar i ett informationssystem. Spårbarhet är i sin tur en förutsättning för att en verksamhetsutövare ska kunna leda i bevis vem som har gjort vad i ett informationssystem vid ett givet tillfälle, t.ex. vem som haft åtkomst till säkerhetsskyddsklassificerade uppgifter. Detta är viktigt vid misstanke om brott. Vid en eventuell misstanke om brott måste en verksamhetsutövare kunna försäkra sig om vem som gjort vad i informationssystemet och där är loggar en viktig förutsättning. I övrigt är loggar även ett hjälpmedel för att i efterhand kunna identifiera orsaken till incidenter av olika slag.

Bestämmelser om loggning återfinns i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd. Av bestämmelserna i 4 kap. 31 § i PMFS 2019:2 framgår att verksamhetsutövaren ska logga händelser som kan påverka säkerheten i informationssystem som har betydelse för säkerhetskänslig verksamhet (säkerhetsloggning).

Av 32 § framgår att verksamhetsutövaren ska ha rutiner för loggning av händelser som kan påverka säkerheten i informationssystem som har betydelse för säkerhetskänslig verksamhet. Rutinerna ska omfatta hur verksamhetsutövaren ska kunna upptäcka skadlig eller obehörig åtkomst eller påverkan samt funktionsstörningar. Rutinerna ska även omfatta vad som behövs i övrigt samt vilka åtgärder som ska vidtas vid upptäckta händelser.

Av 33 § framgår att för informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter ska rutinerna om-

[52] Se 3 kap. 4 § säkerhetsskyddsförordningen (2018:658) och 4 kap. 31–35 §§ Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

fatta loggning av användning och ändring av behörigheter med systemadministrativ åtkomst och av roller med särskild behörighet i informationssystemet.

Av 34 § framgår att verksamhetsutövaren ska bevara säkerhetsloggar i minst 10 år. För informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen kvalificerat hemlig ska säkerhetsloggar bevaras i minst 25 år.

Av 35 § framgår att verksamhetsutövaren ska vidta åtgärder för att skydda säkerhetsloggar mot obehörig åtkomst, ändring eller förstöring.

Vad ska loggas?

Vad som ska loggas i ett informationssystem är beroende av flera olika faktorer, bl.a. hur och av vilka informationssystemet ska användas och hur det exponeras samt syftet med loggningen.

Loggar kan generas från olika typer av loggkällor. Loggning kan t.ex. ske i en programvara, i ett operativsystem eller i olika komponenter i infrastrukturen för ett informationssystem. Vad som ska loggas och vilka loggkällor som ska användas behöver verksamhetsutövaren fastställa innan ett informationssystem tas i drift.

Logguppföljning och åtgärder vid upptäckta händelser

Logguppföljning är en viktig åtgärd för att kunna upptäcka skadlig eller otillåten påverkan, obehörig åtkomst och funktionsstörningar i ett informationssystem. Logguppföljning kan ske med jämna intervaller eller i realtid som en del av en funktion för säkerhetsövervakning. För att arbetet med logguppföljning ska ge önskad effekt behöver verksamhetsutövaren ta fram rutiner som beskriver hur verksamhetsutövarens personal ska arbeta med logguppföljning. Det är även viktigt att rutinerna innehåller en tydligt beskriven eskaleringsordning som stöd i beslut om åtgärd vid en upptäckt händelse, t.ex. att incidenthantering ska påbörjas.

Hantering av säkerhetsloggar

Att upprätthålla tillförlitligheten till de loggar som genereras är en mycket viktig aspekt som en verksamhetsutövare behöver beakta. En av anledningarna till detta är att loggar ofta används som underlag i internutredningar som kan leda till disciplinära åtgärder eller vid bevisföring i brottsmål. Om riktigheten i loggarna kan ifrågasättas kan det leda till att ansvar inte kan utkrävas av den som gjort sig skyldig till brott. En annan aspekt som en verksamhetsutövare behöver beakta är att loggar kan innehålla skyddsvärda uppgifter och att konfidentialiteten för loggarna därmed behöver upprätthållas.

Loggar kan skyddas på flera olika sätt, där en grundläggande åtgärd för att skydda både riktigheten i loggarna och samtidigt upprätthålla konfidentialiteten är att begränsa åtkomsten till loggarna genom en strikt behörighetshantering. Tillförlitligheten kan stärkas ytterligare med hjälp av kryptografiska funktioner, t.ex. genom elektronisk signering.[53]

7.13 Säkerhetsövervakning

7.13.1 Allmänt om säkerhetsövervakning

Med *säkerhetsövervakning* avses en funktion som arbetar med *aktiv* övervakning av ett informationssystem med syfte att kunna upptäcka, försvåra och hantera skadlig inverkan på informationssystemet samt obehörig avlyssning av, åtkomst till och nyttjande av ett informationssystem.

Säkerhetsövervakning är en funktion där personal med hjälp av olika tekniska hjälpmedel aktivt söker efter oönskade aktiviteter i ett informationssystem. Vid upptäckt agerar funktionen genom att försöka förhindra t.ex. ett intrångsförsök. Skulle ett intrångsförsök lyckas utreder funktionen hur, var och varför intrånget skedde samt vad som behövs för att förhindra framtida intrång.

[53] För att kunna använda loggar vid en utredning är det viktigt att säkerställa att informationssystemen och dess loggar har korrekta tidsangivelser. Ett sätt att hantera detta är att använda standardprotokollet Network Time Protocol (NTP) för synkronisering mot gemensamma tidkällor.

Bestämmelser om säkerhetsövervakning återfinns i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.[54]

Av bestämmelserna i 4 kap. 36 § i PMFS 2019:2 framgår att verksamhetsutövaren ska använda funktion för säkerhetsövervakning av informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *hemlig* eller *kvalificerat hemlig*. Kraven gäller även informationssystem där en incident kan medföra *allvarlig* eller *synnerligen allvarlig skada* för Sveriges säkerhet.

Av 37 § framgåratt verksamhetsutövaren ska ha *rutiner för säkerhetsövervakning* enligt 36 §. Rutinerna ska omfatta vad som ska övervakas och vem som ansvarar för övervakningen. Rutinerna ska även omfatta vad som behövs i övrigt samt vilka åtgärder som ska vidtas vid upptäckta händelser.

En funktion för säkerhetsövervakning är beroende av både en teknisk plattform och av kompetent personal. Personal som arbetar med säkerhetsövervakning tillhör ofta en del i en verksamhet som benämns *Security Operations Center* (SOC). Vid sidan av en SOC finns ofta även en funktion för driftövervakning som benämns *Network Operations Center* (NOC). En NOC fokuserar oftast på övervakning av informationssystem med syfte att upprätthålla tillgänglighet och prestanda. Båda dessa funktioner kompletterar varandra och utgör sammantaget en viktig funktion för att upprätthålla säkerheten i ett informationssystem.

Hur arbetet med säkerhetsövervakning ska genomföras behöver verksamhetsutövaren fastställa och därefter reglera i interna styrdokument. Styrdokumenten bör innehålla en beskriven eskaleringsordning som stöd i beslut om åtgärd när ett potentiellt intrång eller en annan oönskad händelse upptäcks.

7.13.2 Åtgärder vid upptäckta händelser

När funktionen för säkerhetsövervakning upptäcker ett potentiellt intrång eller en annan oönskad händelse i ett informationssystem bör det även finnas en tydlig beskriven eskaleringsordning att ta stöd

[54] 3 kap. 4 § säkerhetsskyddsförordningen (2018:658) och 4 kap. 36 och 37 §§ Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

av. Utifrån denna kan de som arbetar med säkerhetsövervakning fatta beslut om vidare åtgärd. Fortsatta åtgärder kan exempelvis vara:

– att inleda fördjupad analys av händelsen, eller
– incidenthantering.

En fördjupad analys kan bestå av granskning av loggar i en loggkälla, t.ex. ett operativsystem, en programvara eller i infrastrukturkomponenter.[55] Även analys av minnesavbilder, nätverkstrafik och eventuell skadlig kod kan vara en del av den fördjupade analysen.

7.13.3 Tekniska hjälpmedel

Som ett stöd för arbetet med säkerhetsövervakning finns olika programvaror anpassade för ändamålet. *Security Information and Event Management* (SIEM) är en vanlig benämning på en sådan programvara som kan vara ett stöd vid säkerhetsövervakning av skyddsvärda system.

SIEM sköter insamling och aggregering av loggar som genererats av olika loggkällor i ett informationssystem. Baserat på innehållet i loggarna identifierar och kategoriserar SIEM möjliga incidenter och händelser som skett i informationssystemet och gör sedan en automatisk analys av dem. SIEM har därefter två syften:

– Tillhandahålla rapporter gällande säkerhetsrelaterade incidenter och händelser såsom förekomst av skadlig kod, misslyckade inloggningsförsök, avaktiverade användarkonton som återaktiveras och andra potentiellt skadliga aktiviteter i informationssystemet.
– Generera larm, om det under den automatiska analysen visar att sig att det förekommer potentiellt skadliga aktiviteter i informationssystemet (den automatiska analysen utgår från ett fördefinierat regelverk där det framgår vilka parametrar och tröskelvärden som ska generera ett larm).

Att bygga upp en funktion för säkerhetsövervakning, t.ex. SOC, är ett tidskrävande arbete. För att minska risken för inlåsningseffekter

[55] Fördjupad analys kan även göras i switchar, routrar, brandväggar, VPN-koncentratorer och i de inbyggda skyddsfunktionerna i samma komponenter, t.ex. intrångsdetektering eller innehållsfiltrering.

kan verksamhetsutövaren, innan tekniska hjälpmedel införskaffas, definiera hur säkerhetsövervakningen ska bedrivas både under en uppbyggnadsfas och på sikt.

7.13.4 Övning och utvärdering

Ett sätt att testa och utvärdera styrdokument, personella resurser och tekniska hjälpmedel som används i en funktion för säkerhetsövervakning är att genomföra övningar. Genom samarbete med penetrationstestare kan funktionen för säkerhetsövervakning öva olika angreppsscenarion i informationssystemet, vilket gör att t.ex. tröskelvärden för generering av larm kan testas och finjusteras. Genom ett oannonserat angrepp med hjälp av penetrationstestare kan även verksamhetsutövarens incidenthantering sättas på prov och utvärderas.

7.14 Uppföljning och kontroll

7.14.1 Allmänt om uppföljning och kontroll

Uppföljning och kontroll är viktiga verktyg för att kunna säkerhetsställa att säkerhetsskyddet för ett informationssystem upprätthålls över tid och ger avsedd effekt. Ett viktigt förhållningssätt som verksamhetsutövaren bör tillämpa i fråga om uppföljning och kontroll är att det sker med ett organisatoriskt *oberoende* mot den som utför drift, förändringar och underhåll i informationssystemet. Detta för att uppföljning och kontroll ska kunna ske med ett oberoende. Bestämmelser relaterade uppföljning och kontroll finns i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.[56]

Av bestämmelserna i 2 kap. 26 § PMFS 2019:2 framgår att verksamhetsutövaren ska regelbundet

– utvärdera om säkerhetsskyddsåtgärderna ger avsedd effekt,
– identifiera brister och sårbarheter i säkerhetsskyddet och genomföra förbättringar,
– kontrollera och följa upp det säkerhetsskyddsarbete som bedrivs på uppdrag av verksamhetsutövaren hos externa aktörer, och

[56] Se 2 kap. 13 och 26 §§ och 4 kap. 2, 11 och 13 §§ Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

– i övrigt kontrollera och följa upp att verksamheten följer regelverket för säkerhetsskydd.

Verksamhetsutövaren ska dokumentera åtgärderna i en plan som ska uppdateras löpande. I planen ska det anges vilken funktion som är ansvarig för åtgärderna.

Av bestämmelserna i 4 kap. 11 § PMFS 2019:2 framgår att verksamhetsutövaren ska årligen granska säkerheten i informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig eller i informationssystem där en incident kan medföra allvarlig eller synnerligen allvarlig skada för Sveriges säkerhet.

Uppföljning och granskning av säkerheten i ett informationssystem bör vara av såväl *administrativ* som *teknisk* karaktär.

Administrativ säkerhetsgranskning kan exempelvis ta sikte på:

– att identifiera brister i verksamhetens efterlevnad av den styrning som reglerar drift, förändring och underhåll av informationssystemet, eller
– att identifiera brister i användarnas efterlevnad av de regler och rutiner som reglerar hur informationssystemet får användas.

En teknisk säkerhetsgranskning kan exempelvis ta sikte på:

– att identifiera generella brister och sårbarheter i funktioner i och kring informationssystemet,
– att granska om informationssystemet är skyddat mot publikt kända sårbarheter som borde vara omhändertagna inom ramen för verksamhetsutövarens omvärldsbevakning, eller
– att identifiera brister i efterlevnad av den styrning som reglerar drift och underhåll av informationssystemet, exempelvis gällande hantering av tjänstekonton och användarkonton med systemadministrativ åtkomst.

7.14.2 Efterlevnad av kravställning

De säkerhetskrav som identifierats i den särskilda säkerhetsskyddsbedömningen bör följas upp med regelbundna kontroller. Dessa kontroller kan t.ex. vara i form av säkerhetsgranskningar, sårbarhetsskanningar och penetrationstester. Syftet med dessa kontroller är att verifiera att de säkerhetsfunktioner och den säkerhetskonfiguration som initialt applicerades vid driftsättning upprätthålls över tid. Säkerhetsarbetet måste kontinuerligt revideras och skyddet blir oftast mest effektivt om det iterativt anpassas och uppdateras.

Nya attackvägar och sårbarheter kräver att skyddet anpassas och det är inte ovanligt att säkerhetsåtgärder avaktiveras eller av andra orsaker blir ineffektiva med tiden.

Ny funktionalitet förs in, vilket både kan introducera nya sårbarheter och ändra hur verksamheten använder systemet. Därför är det en fördel om granskningar genomförs systematiskt och är årligt återkommande, men också att det rutinmässigt genomförs vid större förändringar.

7.14.3 Kontroll av åtkomst och behörigheter

Uppföljning av *åtkomst* och *behörigheter* är nödvändigt då:

- förändringar kan ske i användarens anställning (t.ex. kan användaren byta enhet eller arbetsuppgifter, vara tjänstledig under en längre tid eller lämna projektdeltagande i förtid),
- insiders kan ha tilldelat sig otillbörliga behörigheter,
- externa hotaktörer eller insiders kan ha skapat helt nya behörigheter, eller
- gamla användarkonton felaktigt kan ha återaktiverats (av misstag eller av en insider).

7.14.4 Uppdatering av dokumentation

Lika viktigt som att upprätta dokumentation vid driftsättning av ett nytt informationssystem, system eller applikation är arbetet med att se till att dokumentationen uppdateras över tid. Vid ny eller föränd-

rad funktionalitet i it- miljö, system eller applikation ska befintlig dokumentation ses över.[57]

7.15 Allmänt om incidenthantering

En it-incident kan bero på såväl ett avsiktligt som ett oavsiktligt agerande av egen personal eller av en hotaktör. De konsekvenser som kan uppstå vid en sådan incident är exempelvis att informationssystemet blir otillgängligt eller att information i systemet har förvanskats, förstörts eller röjts till obehörig. Oavsett orsak är det viktigt att incidenter hanteras på ett strukturerat sätt för att den säkerhetskänsliga verksamheten så snart som möjligt ska kunna återgå till normalläge.

Begreppet it-incident återfinns i 2 kap. 10 § säkerhetsskyddsförordningen (2018:658) där det av rubriksättningen framgår att en it-incident är en typ av säkerhetshotande händelse. Bestämmelser relaterade till hantering av säkerhetshotande händelser finns därutöver i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

Av bestämmelserna i 2 kap. 20 § PMFS 2019:2 framgår att verksamhetsutövaren ska ha rutiner för hantering av säkerhetshotande händelser som är av betydelse för verksamhetens säkerhetsskydd.

Av 21 § framgår att verksamhetsutövaren ska vid säkerhetshotande händelser som är av betydelse för verksamhetens säkerhetsskydd vidta åtgärder så att skadlig inverkan på den säkerhetskänsliga verksamheten minimeras och så att den säkerhetskänsliga verksamheten så snart som möjligt kan återgå till normalläge.

Av 22 § framgår att verksamhetsutövaren ska utvärdera inträffade säkerhetshotande händelser som är av betydelse för verksamhetens säkerhetsskydd. Utifrån utvärderingen ska verksamhetsutövaren införa de förbättringar som krävs för att minimera skadeeffekten av liknande händelser i framtiden.

I nästa avsnitt redogörs för åtgärder som en verksamhetsutövare ska och bör beakta i fråga om incidenthantering för ett informationssystem som har betydelse för säkerhetskänslig verksamhet.

[57] Det kan beröra policydokument, systemdokumentation, rutiner, driftsdokumentation, förvaltningsdokumentation, utvecklardokumentation, nätverkskartor, inventarielistor, m.m.

7.15.1 Grundläggande förutsättningar

För att en verksamhetsutövare ska kunna hantera it-incidenter på ett tillfredställande sätt krävs att två grundläggande komponenter finns på plats redan på förhand. Den viktigaste komponenten är att verksamhetsutövaren format en arbetsgrupp som är redo att ta sig an de utmaningar en it-incident medför. I en sådan grupp är god teknisk it- och säkerhetskompetens viktigt, likväl som insikt i och förståelse för it-miljön. En incidenthanteringsgrupp bör även bestå av personal som kan hantera rättsliga frågor, personal- och arbetsgivarfrågor samt kommunikationsfrågor.

Den andra viktiga komponenten är att verksamhetsutövaren tagit fram en incidenthanteringsplan. Syftet med planen är att den ska vara ett stöd i den praktiska incidenthanteringen. En incidenthanteringsplan bör vara konkret och kärnfull för att vara praktiskt användbar. En incidenthanteringsplan bör även innehålla beskrivningar av roller och ansvarsområden, mandat, prioriteringsordning, utredning, minimering av skador, återställning, dokumentering och rapportering.

7.15.2 Genomförande

Att hantera en it-incident kan vara komplicerat och tidskrävande och syftar till att:

- minimera skadeverkan i informationssystemet,
- utreda omfattning och orsak,
- återställa informationssysteminformationssystemet till normalläge,
- dokumentera och rapportera incidenten till berörda intressenter, och
- utvärdera och dra lärdom av incidenten för att kunna införa de förbättringar som krävs för att minska sannolikheten för, eller minimera skadeeffekten av, liknande händelser i framtiden.

7.16 Avveckling

7.16.1 Allmänt om avveckling

En vanligt förekommande orsak till avveckling är att ett befintligt informationssystem ska ersättas av ett annat. Att övergången från det befintliga till det nya kan ske utan oplanerade avbrott i den säkerhetskänsliga verksamheten, är ofta en viktig fråga att beakta i sådana sammanhang. Andra viktiga frågor som kan bli aktuella vid avveckling är migrering och arkivering av data. Att avveckla ett informationssystem är därför ett arbete som ofta kräver noggrann planering.

Utbyte och avveckling av komponenter i ett informationssystem är något som normalt sett sker mer frekvent än utbyte av hela informationssystem.

Av bestämmelserna i 4 kap. 10 § i PMFS 2019:2 framgår att verksamhetsutövaren ska fastställa rutiner för hanteringen av informationssystem som har betydelse för säkerhetskänslig verksamhet under systemets förväntade livstid.

Av bestämmelserna i 3 kap. 3 § i PMFS 2019:2 framgår att verksamhetsutövaren ska ha rutiner för behandling av säkerhetsskyddsklassificerade uppgifter och handlingar. Rutinerna ska reglera vad som gäller för spårbarhet, upprättande, kopiering, utskrift, utdrag, kvittering, förvaring, distribution, medförande, inventering och destruktion samt vad som behövs i övrigt för att upprätthålla ett fullgott säkerhetsskydd. Verksamhetsutövaren ska ha rutiner för behandling av uppgifter som behöver skyddas från ett tillgänglighets- eller riktighetsperspektiv.

Av bestämmelserna i 3 kap. 27 § i PMFS 2019:2 framgår att verksamhetsutövaren ska ha rutiner för avveckling eller återanvändning av lagringsmedium som används i säkerhetskänslig verksamhet. Rutinerna ska säkerställa att information på lagringsmediet inte kan återskapas.[58]

[58] Rutiner för avveckling av informationssystem bör omfatta hur:
– avveckling av lagringsmedier ska hanteras,
– avveckling av komponenter ska hanteras,
– migrering av säkerhetsskyddsklassificerade uppgifter och övrig data ska hanteras,
– arkivering av data ska hanteras samt hur länge data ska bevaras, och
– avvecklingen ska dokumenteras.

7.16.2 Avveckling av komponenter

Vissa komponenter som används inom ett informationssystem innehåller systemrelaterad information som beskriver hur säkerhetsåtgärder i informationssystemet, helt eller i vissa delar, är konfigurerade eller uppbyggda. Om en hotaktör får åtkomst till sådan information kan den i vissa fall användas för att underlätta ett angrepp på informationssystemet. Det är därför viktigt att verksamhetsutövaren gör en bedömning av om den typen av information är skyddsvärd och hur den i så fall ska hanteras vid avveckling av de komponenter där den förekommer.

Även om systemrelaterad information raderas, t.ex. genom en systemåterställning, är det inte alltid en heltäckande åtgärd då informationen kan finnas kvar i en minneskrets inom komponenten. Förekomst av minneskretsar bör därför beaktas särskilt vid avveckling av komponenter som innehåller säkerhetsskyddsklassificerad eller på annat sätt skyddsvärd information.

7.16.3 Avveckling och återanvändning av lagringsmedia

En verksamhetsutövare är skyldig att ta fram rutiner för avveckling eller återanvändning av *lagringsmedia* som använts i säkerhetskänslig verksamhet. Dessa rutiner ska säkerställa att information på lagringsmediet inte kan återskapas och bör beskriva vilket tillvägagångssätt som ska tillämpas för respektive säkerhetskyddsklass.

En vanlig metod för att förhindra möjligheten att återskapa information på lagringsmedia är överskrivning av data. Detta innebär att befintligt data vid upprepade tillfällen skrivs över och ersätts av annan data. En annan metod är att förstöra nyckeln till krypterade lagringsmedia. Båda dessa metoder har vid tillfällen visat sig innehålla sårbarheter som inneburit att den som har tillgång till lagringsmediet kunnat återskapa delar av informationen. Med anledning av detta bör återanvändning av lagringsmedia ske restriktivt och endast i de fall då lagringsmediet kommer att återanvändas i ett informationssystem som omfattas av säkerhetsskydd.

För lagringsmedia som inte ska återanvändas av verksamhetsutövaren bör avveckling ske genom fysisk destruktion.

7.17 Samråd om informationssystem[59]

7.17.1 Allmänt om samråd

Av bestämmelserna i 3 kap. 2 § säkerhetsskyddsförordningen (2018:658) framgår att innan ett informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre tas i drift, eller i väsentliga avseenden förändras, ska verksamhetsutövaren skriftligen samråda med Säkerhetspolisen.[60] Om verksamhetsutövaren hör till Försvarsmaktens tillsynsområde enligt 7 kap. 1 § första stycket 1, ska denne i stället samråda med Försvarsmakten.

Samrådsskyldigheten gäller även i fråga om *andra informationssystem* än sådana som anges i första stycket, om obehörig åtkomst till systemen kan medföra en *skada för Sveriges säkerhet* som *inte är obetydlig*. Vid ett sådant samråd lämnar Säkerhetspolisen ett *yttrande* kring de säkerhetsskyddsåtgärder verksamhetsutövaren har vidtagit, eller har för avsikt att vidta, samt hur dessa förhåller sig till bestämmelserna om säkerhetsskydd i författningarna.

7.17.2 Samråd inför driftsättning av ett informationssystem

Den särskilda säkerhetsskyddsbedömningen är central när en verksamhetsutövare ska *samråda* med Säkerhetspolisen. En verksamhetsutövare kan inleda ett samråd med Säkerhetspolisen redan vid framtagandet av design och arkitektur för ett informationssystem för att i ett tidigt skede få stöd i bedömningen av om säkerhetsskyddsåtgärderna för informationssystemet uppfyller bestämmelserna om säkerhetsskydd.

I de fall en verksamhetsutövare har för avsikt att *utveckla* ett informationssystem som ska nyttjas av andra verksamhetsutövare, föreligger samrådsskyldighet primärt för den verksamhetsutövare som utvecklar informationssystemet.

Ett samråd avslutas alltid med ett slutligt *yttrande* från Säkerhetspolisen till verksamhetsutövaren *inför driftsättning*. I yttrandet lämnar myndigheten synpunkter på de säkerhetsskyddsåtgärder verk-

[59] Se även kapitel 13.
[60] 3 kap. 2 § säkerhetsskyddsförordningen (2018:658) och 4 kap. 9 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

samhetsutövaren har vidtagit, eller har för avsikt att vidta, och hur dessa förhåller sig till bestämmelserna om säkerhetsskydd i författningarna.

Säkerhetspolisen anger att för myndigheten ska kunna lämna ett ”kvalitativt” yttrande förutsätts att verksamhetsutövaren har:

– genomfört tester och verifierat att de säkerhetsskyddsåtgärder (säkerhetskrav) som identifierats i den särskilda säkerhetsskyddsbedömningen har implementerats och att de ger avsedd effekt,
– säkerställt att samtliga identifierade sårbarheter och säkerhetsbrister i informationssystemet som kan medföra negativ påverkan för den säkerhetskänsliga verksamheten har omhändertagits, och
– säkerställt att eventuella undantag och kompenserande åtgärder som vidtagits i förhållande till säkerhetskraven i den särskilda säkerhetsskyddsbedömningen är dokumenterade.

7.17.3 Samråd vid väsentlig förändring av ett informationssystem

Vad som utgör en *väsentlig förändring* i ett informationssystem kan vara svårt att entydigt definiera. En väsentlig förändring kan ta sig uttryck på många olika sätt, t.ex. när:

– ett befintligt informationssystem ska hantera uppgifter med en högre säkerhetsskyddsklassificering än tidigare,
– ett befintligt informationssystem ska integreras eller kommunicera med andra informationssystem, eller när exponering av annat skäl väsentligen ökar, eller
– ett befintligt informationssystem ska användas i en annan säkerhetskänslig verksamhet.

En verksamhetsutövare ska göra en bedömning av vad som kan anses utgöra en *väsentlig förändring*. För stöd i en sådan bedömning kan verksamhetsutövaren samråda med Säkerhetspolisen. Innan en väsentlig förändring av ett informationssystem genomförs bör verksamhetsutövaren genomföra en *särskild säkerhetsskyddsbedömning*. Genom den särskilda säkerhetsskyddsbedömningen sätter verksamhetsutöva-

ren ramarna för vilka säkerhetsskyddsåtgärder som ska vidtas i och med att förändringen genomförs.

På motsvarande sätt som vid ett samråd innan ett informationssystem ska tas i drift, lämnar Säkerhetspolisen ett *skriftligt yttrande* till verksamhetsutövaren. I yttrandet lämnar myndigheten synpunkter på de säkerhetsskyddsåtgärder som verksamhetsutövaren har vidtagit, eller har för avsikt att vidta, och hur dessa förhåller sig till bestämmelserna om säkerhetsskydd i författningarna.

8 Offentliga utredningar och myndighetsrapporter

Bedömning: Av offentliga utredningar och myndighetsrapporter framkommer en mycket bekymmersam bild över nivån och omfattningen av informations- och cybersäkerhet i samhället allmänt och särskilt vad gäller i säkerhetskänslig verksamhet och annan samhällsviktig verksamhet. Av utredningarna och rapporterna framkommer bl.a.:

- att cybersäkerhet föreslås utgöra ett särskilt beredskapsområde och inte någon egen beredskapssektor då regeringen inte har utsett någon samordnande myndighet för cybersäkerhetsområdet,
- att det behöver etableras samverkansformer med övriga särskilda beredskapsområden,
- att det behöver finnas en nationell funktion med uppgift att stödja myndigheter och samhället i övrigt i arbetet med att förebygga och hantera angrepp inom informations- och kommunikationsområdet samt upprätthålla en aktuell lägesbild över samhällets digitala miljö, vilket är en viktig verksamhet för bl.a. det civila försvaret,
- att myndigheter som bedriver de mest skyddsvärda verksamheterna i många fall har svårt att bedöma vad som är skyddsvärt med hänsyn till Sveriges säkerhet,
- att myndigheter också vanligtvis har svårt att bedöma hotbilden mot den egna verksamheten,
- att myndigheter i stor utsträckning även saknar förmågan att bedöma den egna verksamhetens sårbarheter,

- att som en följd av dessa brister har många myndigheter svårt att vidta ändamålsenliga och kostnadseffektiva säkerhetsskyddsåtgärder,
- att det finns allvarliga brister i arbetet med informations- och cybersäkerhet samt att arbetet med informations- och cybersäkerhet och säkerhetsskydd dessutom inte är tillräckligt integrerade,
- att det på nationell nivå saknas enhetlig styrning och samordning av arbetet med informations- och cybersäkerhet,
- att det är svårt att få en sammanhängande bild av samtliga regelverk om informations- och cybersäkerhet samt säkerhetsskydd och hur de ska tolkas,
- att avsaknaden av en samlad statlig strategi leder till att varje myndighet gör egna utredningar, bedömningar och bygger egna lösningar för att uppfylla krav på informations- och cybersäkerhet,
- att krav på digitalisering och kostnadseffektiva lösningar ofta ställs mot höga krav på informations- och cybersäkerhet,
- att höga krav på informations- och cybersäkerhet påverkar i sig möjligheterna att nyttja kostnadseffektiva it-driftstjänster,
- att det finns svårigheter med att formulera ändamålsenliga krav för it-drift som påverkar kostnadseffektiviteten,
- att informations- och cybersäkerhet inte prioriteras och att det inte avsätts tillräckligt med resurser för denna verksamhet hos många verksamhetsutövare,
- att det finns föråldrade nätverks- och informationssystem hos ett stort antal myndigheter som dessutom är verksamhetskritiska system,
- att teknikskulden avseende nätverks- och informationssystem påverkar förutsättningarna att arbeta med informations- och cybersäkerhet i systemen,
- att föråldrade nätverks- och informationssystem medför risker för bristande informations- och cybersäkerhet samt säker-

hetsskydd, vilket även medför bristande hushållning med statens medel,

- att det finns allvarliga brister i arbetet med systematisk informationssäkerhet hos många verksamhetsutövare,
- att det brister bl.a. i förmågan att genomföra informationsklassificering, som ligger till grund för säkerhetsskyddsåtgärder hos verksamhetsutövare,
- att det är svårt att finna personer med kompetens inom it, säkerhet och upphandling,
- att bristen på relevant kompetens upplevs som ett stort hinder för säker it-drift, och
- att myndigheterna har kommit olika långt i sitt informations- och cybersäkerhetsarbete.

8.1 Inledning

Ett antal offentliga utredningar och myndighetsrapporter samt andra rapporter som berör informationssäkerhet i olika verksamheter har offentliggjorts under den senaste femårsperioden. I några av utredningarna och rapporterna berörs även frågor om informationssäkerhet inom ramen för regleringen av säkerhetsskydd i olika verksamheter. I detta kapitel redogörs för ett urval av dessa utredningar och rapporter i de delar som behandlar frågor om informationssäkerhet mer allmänt och informationssäkerhet inom ramen för säkerhetsskydd, såväl i offentlig som enskild verksamhet.

Urvalet har skett med utgångspunkt i direktiven att utredningen ska analysera om det finns behov av att stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet. Urvalet grundas på behovet av att – om möjlig – få en översiktlig bild över nivån på och omfattningen av nätverks- och informationssäkerheten i angivna verksamheter, särskilt vad avser den säkerhetskänsliga verksamheten, men även hur arbetet med att stärka informationssäkerheten allmänt och i säkerhetskänslig verksamhet har utvecklats över tiden, eftersom dessa två frågor har beröringspunkter.

8.2 Offentliga utredningar och rapporter

År 2014

Informationssäkerheten i den civila statsförvaltningen (RiR 2014:223)

Riksrevisionen konstaterade i granskningsrapporten *Informationssäkerheten i den civila statsförvaltningen* (RiR 2014:223) att regeringen gett olika myndigheter flera uppdrag med stor betydelse för informationssäkerheten i statsförvaltningen men att regeringen i liten utsträckning hade informerat sig om status på informationssäkerheten. Man noterade att regeringen i regleringsbreven inte hade ställt krav på myndigheternas nivå för informationssäkerhet. I de fall regleringsbreven innehöll krav på it handlar det mer om effektivisering av myndighetens it eller krav på enskilda system. Vidare utgjorde enligt regeringen risk- och sårbarhetsanalyser samt förmågebedömningar viktiga underlag för att möjliggöra en effektiv uppföljning, styrning och inriktning av den sammantagna krisberedskapen i samhället. Påpekanden om brister i risk- och sårbarhetsanalyserna hade dessutom gjorts under flera år.

Riksrevisionens bedömning av den aktuella handlingsplanen för informationssäkerhet var att mål och åtgärder var av blandad karaktär. Det fanns heller ingen central funktion i Regeringskansliet med ett utpekat ansvar för att dels vara mottagare av strategiskt viktig information som underlag för styrning från regeringens sida, dels bereda ärenden som rör informationssäkerheten i statsförvaltningen. Riksrevisionen framhöll att den granskat om informationssäkerheten i den civila delen av statsförvaltningen är ändamålsenlig utifrån ökande hot. Riksrevisionens samlade slutsats av granskningen var att arbetet med informationssäkerheten inte är ändamålsenligt sett till de hot och risker som finns och påpekade att granskningen visade på omfattande brister i statsförvaltningen. Regeringen hade inte heller någon samlad lägesbild som inkluderar hot, i vilken omfattning och mot vilka hoten realiseras samt vilka skyddsåtgärder myndigheterna vidtar. Det hade inte heller någon av regeringens stöd- och tillsynsmyndigheter. Det innebar att den samlade förmågan att kunna hantera de konsekvenser som kan bli följden av en allvarlig incident till stora delar var okänd. Av det skälet var det nödvändigt att regeringen och dessa myndigheter vidtar åtgärder, så att det går att få en samlad

bild av läget och utifrån detta anpassa säkerheten till de behov som finns. Riksrevisionen framhöll att granskningen visade att

– regeringen inte utövat en effektiv styrning av informationssäkerheten i den civila statsförvaltningen och
– regeringens stöd- och tillsynsmyndigheter endast delvis hade vidtagit nödvändiga åtgärder för att informera sig och regeringen om vilka hot som finns mot den civila statsförvaltningen, i vilken omfattning de realiseras och vilka skyddsåtgärder som vidtas.

Riksrevisionen framhöll hade vidare att den som ett led i granskningen uppdragit åt Myndigheten för samhällsskydd och beredskap (MSB), Försvarets radioanstalt (FRA) och Säkerhetspolisen att hämta in och analysera uppgifter om läget för informationssäkerheten i statsförvaltningen. Redovisningen av dessa uppdrag innebar ny och väsentlig, ny information om läget. Vart och ett av myndigheternas yttranden pekade dessutom entydigt i samma riktning. Riksrevisionen drog till följd av granskningen slutsatsen att läget var allvarligt för de myndigheter som fått sina skydd testade mot intrång av FRA, och även för flera av de myndigheter vars säkerhetsskydd kontrollerats av Säkerhetspolisen. Enbart det faktum att myndigheterna har ett ansvar för sin informationssäkerhet verkar inte vara tillräckligt för att uppnå en god informationssäkerhet i statsförvaltningen. Säkerhetspolisen hade i sin tillsyn funnit systematiska brister i säkerhetsskyddsarbetet, framför allt i fråga om it- och informationssäkerhet hos de mest skyddsvärda myndigheterna. Det handlar till exempel om skadekonsekvensbeskrivningar som antingen saknas eller innehåller ekonomiska eller andra konsekvenser för den egna verksamheten i stället för de som rör rikets säkerhet eller terrorism. Det kan också handla om att det saknas förmågebedömningar av tänkta angripare, vilket medför att det blir oklart hur informationssäkerheten ska dimensioneras. Dessa brister ledde sammantaget till att dessa myndigheter inte kan ta fram ändamålsenliga kravspecifikationer för att värna de mest skyddsvärda informationstillgångarna.

Riksrevisionen betonade att det var betydande brister i säkerhetsarbetet som hade upptäckts. FRA:s penetrationstester som sker på begäran av en myndighet visade på att säkerhetsnivån är otillräcklig på flertalet av de myndigheter som blivit testade. FRA testar dessutom informationssäkerheten på en avgränsad del av statsförvaltningen,

vilket innebär att FRA saknar kännedom om statusen på informationssäkerhet för merparten av myndigheterna i statsförvaltningen. Om inte ens de mest skyddsvärda verksamheterna hade ägnat frågan tillräcklig uppmärksamhet var risken stor att motsvarande brister återfinns även i övriga förvaltningen.

Riksrevisionen konstaterade vidare att statusen på kunskapsläget för informationssäkerheten i statsförvaltningen var oklart. Varken regeringen eller någon av stöd- och tillsynsmyndigheterna hade en bra och systematiskt underbyggd lägesbild, vilket är en förutsättning för att kunna säkerställa att man vidtar rätt åtgärder. För att arbetet med informationssäkerhet i förvaltningen ska vara effektivt krävs kunskap om såväl hot och risker som vilka hot som förverkligas och vilka skyddsåtgärder myndigheterna vidtar. Regeringen hade organiserat arbetet på ett sätt som gör att man får kunskap om hot och risker på en övergripande nivå. Genom Säkerhetspolisens tillsyn får man även kunskap om realiserade hot och vidtagna skyddsåtgärder för de mest samhällskritiska verksamheterna. Vilka hot eller risker som realiseras mot de myndigheter som inte omfattas av säkerhetsskyddslagstiftningen eller vilka skyddsåtgärder dessa myndigheter vidtar fanns dock ingen myndighet som kontrollerar. Regeringen hade inte heller genom regleringsbrev eller på annat sätt krävt att myndigheterna lämnar sådan information. MSB och FRA hade i avrapporteringen av regeringsuppdragen om obligatorisk incidenthantering och ett tekniskt detektering- och varningssystem uttryckt att dessa åtgärder åtminstone delvis skulle kunna ge sådan information. Dessa frågor bereddes dock – flera år efter att behovet uttryckts – fortfarande i Regeringskansliet. Regeringen hade således i visst avseende styrt mot en förbättrad säkerhet genom att ge dessa myndigheter uppdrag. När sedan uppdragen redovisats blev de liggande länge i Regeringskansliet utan åtgärd, vilket försvårade att få till stånd en gemensam lägesbild att utgå från när säkerheten ska förbättras.

Riksrevisionen konstaterade även att eftersom varken regeringen eller stöd och tillsynsmyndigheterna hade den fulla bilden av i vilken omfattning hot realiseras eller vilka skyddsåtgärder myndigheterna vidtar saknades en nödvändig förutsättning för ett effektivt arbete med informationssäkerhet.

Riksrevisionen fann att även myndigheternas risk- och sårbarhetsanalyser hade omfattande brister när det gäller informationssäkerhet. Trots att det ställs uttryckliga krav på att informationssäkerhet ska

beaktas i analyserna, var det inte alla myndigheter som gjorde det. Det var dessutom stora variationer mellan myndigheter på hur analyserna struktureras. Av dessa skäl var det svårt att aggregera informationen från flera myndigheter, vilket gjorde det omöjligt att upprätta en gemensam lägesbild av informationssäkerheten på central nivå. Detta ledde i sin tur till att det blir svårt att analysera vilka brister som finns och därmed kunna göra en grundlig riskbedömning. Då blir det naturligtvis också svårt att vidta lämpliga åtgärder för att bygga upp nödvändig förmåga.

Riksrevisionen noterade vidare att både Säkerhetspolisen, genom sin tillsyn, och FRA, genom sin stödjande och rådgivande verksamhet, får kunskap om brister i enskilda myndigheters informationssäkerhet. Ingen av myndigheterna har dock lämnat någon mer aggregerad redovisning av bristerna och vilken status det är på myndigheternas informationssäkerhet till Regeringskansliet. Ett skäl som angavs till varför så inte har skett är att det saknas en naturlig mottagare i Regeringskansliet.

Riksrevisionen konstaterade vidare att MSB har inget mandat att utöva tillsyn över myndigheternas informationssäkerhet. Avsaknaden av dessa verktyg försvårar för MSB att arbeta effektivt. Det fanns sedan fem år föreskrifter för ledningssystem för informationssäkerheten (LIS) utfärdade av MSB. LIS-föreskrifterna ska stödja uppbyggnaden och vidmakthållandet av informationssäkerheten på myndigheterna. Efterlevnaden visade sig dålig när föreskrifterna 2014 hade utvärderats då inte ens hälften av myndigheterna – enligt Riksrevisionens bedömning – kunde anses uppfylla kraven i föreskrifterna, vilket talar starkt för att många myndigheter inte prioriterar informationssäkerheten. Det tyder också på att utfärdande av föreskrifter behöver kompletteras med ett uppföljnings- eller tillsynsansvar. Ett tydligt och väl anpassat regelverk är dessutom en förutsättning för att uppnå effektivitet i arbetet med informationssäkerhet. Riksrevisionen drog därför slutsatsen att det regelverk som styr myndigheternas arbete med informationssäkerhet bättre kan behöva anpassas till olika typer av statlig verksamhet för att kunna nå önskvärda mål.

Riksrevisionen konstaterade att även om frågan om informationssäkerhet i hög grad var aktualiserad av regeringen fanns det således stora brister. Ett skäl till problemen att få till stånd en bättre informationssäkerhet var sannolikt – enligt Riksrevisionen – att det

inte finns någon funktion som ansvarar för informationssäkerheten som helhet i statsförvaltningen, inklusive Regeringskansliet, och som är mottagare av viktig information om denna. Inte heller hade något av statsråden ett uttalat ansvar för just informationssäkerheten i statsförvaltningen. Frågor om informationssäkerhet hanterades antingen på det departement som respektive myndighet lyder under eller bereds i samråd med andra departement, även om informationssäkerhet är en dimension som spänner över hela statsförvaltningen och dessutom har bäring på flera funktioner såsom förvaltningspolitik, intern styrning och kontroll, krishantering samt brottsbekämpning. Beroende på vilken funktion som anses mest styrande kommer ansvaret för att samordna ärendet att variera mellan olika departement. Dessa förhållanden gör att i praktiken är det inget departement som har ett samlat ansvar för informationssäkerheten i statsförvaltningen. Det innebär att det inte finns en given funktion i Regeringskansliet som kan stå för styrning och samordning av informationssäkerheten, såsom fallet är med till exempel krisberedskap där ett visst departement har ett utpekat ansvar. Det betyder dessutom att det saknas en självklar mottagare av information i Regeringskansliet när det gäller informationssäkerhet. Riksrevisionen ansåg att detta var en brist som orsakar svårigheter att styra och följa upp statusen på myndigheternas informationssäkerhet.

Riksrevisionen noterade vidare att regeringens tillsyns- och stödmyndigheter, framför allt MSB, Säkerhetspolisen och FRA, är på olika sätt aktiva när det gäller informationssäkerhet. MSB verkar brett över hela den offentliga sektorn med uppdrag att främja en god informationssäkerhet, men har inte till uppgift att utöva tillsyn över informationssäkerheten i enskilda myndigheter. Dåvarande Rikspolisstyrelsen genom Säkerhetspolisen utövar tillsyn, men har av resursskäl inte möjlighet att göra det i hela förvaltningen utan har inriktat sin tillsyn på de myndigheter som har den allra mest skyddsvärda verksamheten. FRA agerar endast på begäran av enskilda myndigheter, och har i praktiken inte möjlighet att testa säkerheten på alla myndigheter. Dessa myndigheter samverkar också tillsammans med PTS, Försvarsmakten och Försvarets materielverk när det gäller informationssäkerhet (SAMFI). Trots dessa myndigheters verksamhet och samverkan visade granskningen att det skulle behöva göras mer, och att myndigheterna saknar mandat för det. Säkerhetspolisen bedriver viss tillsyn inriktad på särskilt skyddsvärd verksamhet, vilket utgör en

mindre del av den samlade statsförvaltningen. MSB utfärdar föreskrifter om ledningssystem för informationssäkerhet (LIS), men har inte till uppgift att utöva tillsyn över myndigheters arbete med informationssäkerhet. Riksrevisionen bedömde att resurser för tillsyn generellt inte har prioriterats i tillräcklig utsträckning.

Riksrevisionen ansåg vidare att när det gäller stödet till myndigheterna fanns resursaspekter som var värda särskild uppmärksamhet. Den första aspekten var att det saknas en samlad avvägning för staten hur mycket resurser som behöver satsas på skyddsåtgärder sett till de risker som finns. Det fanns inte en samlad riskvärdering, utan i stället råder osäkerhet om hur starkt skyddet är, vilka händelser som ägt rum och hur hoten utvecklas. En samlad lägesbild hade gett förutsättningar för en samlad värdering av riskerna och sannolikheten att hot realiseras. Detta hade i sin tur kunnat vägas mot hur omfattande stödet behöver vara. Inträffade händelser har visat att kostnaderna kan bli betydande dels för att hantera händelsen, dels för att ställa till rätta efteråt. Risker för informationssäkerheten kan således potentiellt leda till omfattande skada, inte minst i form av extra kostnader. Därför är det angeläget att åtgärder vidtas och prioriteras för att kontrollera dessa risker.

Den andra aspekten var att varje myndighet har ett eget ansvar för hela sin verksamhet i såväl normalläge som i krisläge, vilket är nödvändigt för att verksamheten ska kunna bedrivas effektivt. Det är dock sannolikt inte tillräckligt eftersom de flesta myndigheter har svårt att rekrytera och upprätthålla den kompetens som behövs för att möta behoven. De av regeringen utpekade stödmyndigheterna har dessutom begränsade resurser och saknar möjlighet att lämna operativt stöd till enskilda myndigheter i någon större utsträckning. Riksrevisionen menade att det fanns behov av ett bättre utbyggt stöd som riktar sig till hela statsförvaltningen, och som kompletterar de enskilda myndigheternas egen kompetens. Det skulle kunna leda till en bättre säkerhet totalt i statsförvaltningen, samtidigt som den totala kostnaden för informationssäkerhet borde bli väsentligt lägre än om varje myndighet håller sig med specialistkompetens.

Riksrevisionen konstaterade att granskningen visade att det råder oklarhet om läget i informationssäkerheten i statsförvaltningen och lämnade bl.a. följande rekommendationer till regeringen och regeringens stöd- och tillsynsmyndigheter:

– angivna brister förelåg redan 2007, och då bristerna fortfarande inte är åtgärdade är det angeläget med en skyndsam hantering,
– låt utreda om regelverket som styr arbetet med informationssäkerheten är ändamålsenligt i sin nuvarande utformning och om ansvaret för att utöva tillsyn över informationssäkerheten i den civila statsförvaltningen kan samlas och koordineras på ett bättre sätt än i dag,
– utöka tillsynen av informationssäkerheten i den civila statsförvaltningen, så att den omfattar väsentligt mer än endast de allra mest skyddsvärda delarna,
– överväg att låta tillsynsmyndigheten få mandat att utfärda sanktioner mot myndigheter som inte vidtar nödvändiga åtgärder efter en tillsyn som visat på brister,
– se till att det finns en funktion och en process i Regeringskansliet med syfte att samlat hantera informationssäkerheten och som även ska vara mottagare av information om en samlad lägesbild och annan nödvändig information om läget för informationssäkerheten i statsförvaltningen,
– Säkerhetspolisen och FRA bör var för sig systematiskt avge aggregerade rapporter om säkerhetsläget till Regeringskansliet och MSB.

En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter

Myndigheten för samhällsskydd och beredskap (MSB) genomförde 2014 även en kartläggning[1] (enkätundersökning) av hur statliga myndigheter tillämpar myndighetens föreskrifter om statliga myndigheters informationssäkerhet (2009:10) och i övrigt arbetar med informationssäkerhet. Enkäten lämnades till 351 myndigheter varav 334 myndigheter besvarade enkäten. Frågor om hur det praktiska informationssäkerhetsarbetet går till, och som redovisas i rapporten, ställdes till de 227 myndigheter som själva har hand om sitt informationssäkerhetsarbete. Enligt myndigheten gav kartläggningen en god

[1] En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter (MSB740).

bild av hur myndigheterna själva uppfattade sitt arbete med informationssäkerhet och hur de arbetar med föreskrifternas olika krav. Av resultaten från enkäten framkom bl.a. att 84 procent av myndigheterna har en informationssäkerhetspolicy men att 26 procent av myndigheterna kontrollerar inte efterlevnaden, dvs. att policyer och riktlinjer följs av medarbetarna. Vidare framkom att 38 procent av de som leder och samordnar informationssäkerhetsarbetet i myndigheterna uppges sakna tillräcklig kompetens, resurser eller mandat för att utgöra uppdraget på ett tillfredsställande sätt. Det fram gick även att 67 procent av myndigheterna har en informationsklassningsmodell för att identifiera informationstillgångarna och kunna ställa rätt krav på informationssäkerheten samtidigt som 41 procent av myndigheterna uppgav att det inte är tydligt uttalat vem som ansvarar för att informationsklassning genomförs och 59 procent av myndigheterna uppgav att det inte är fastslaget när informationsklassning ska ske.

Av resultaten framkom vidare att 78 procent av myndigheterna har en metod för riskanalys men att 42 procent saknar regler för vad riskanalyser ska omfatta eller när det ska ske, samtidigt som 35 procent av myndigheterna saknar ett uttalat ansvar för vem som ska initiera riskanalyserna. Det framkom också att 45 procent av de myndigheter som besvarat enkäten uppgav att myndighetens ledning i stor utsträckning löpande håller sig informerade om arbetet med informationssäkerhet medan 37 procent av myndigheterna har ingen eller en mycket begränsad utvärdering av informationssäkerhetsarbetet på myndigheten. I samband med enkäten angav myndigheterna de önskade mer stöd, bl.a. med kravställning, uppföljning, informationsklassning och kontinuitetsplanering.

År 2015

En bild av kommunernas informationssäkerhetsarbete 2015

Myndigheten för samhällsskydd och beredskap (MSB) redovisade i en rapport 2015 resultaten av en granskning av informationssäkerheten i kommunerna[2] varvid myndigheten fann att fler än 70 procent av kommunerna inte arbetade systematiskt med informationssäkerhet, att över 40 procent inte hade någon utpekad funktion för informa-

[2] *En bild av kommunernas informationssäkerhetsarbete 2015, Myndigheten för samhällsskydd och beredskap (MSB)*, 2015.

tionssäkerhet och att ungefär samma andel inte genomförde någon riskanalys i informationssäkerhetsarbetet.

År 2016

Informationssäkerheten i Sveriges kommuner – Analys och rekommendationer utifrån MSB:s kommunenkät 2015

Myndigheten för samhällsskydd och beredskap (MSB)[3] redovisade i en ny rapport en analys och rekommendationer av den enkätundersökning som gjordes 2015 (se ovan). MSB konstaterade i rapporten att resultatet tyder på att informationssäkerheten i kommunerna bör stärkas på flera områden. En klar majoritet av kommunerna arbetar inte systematiskt med informationssäkerhet. Kontroll och tillsyn av säkerheten i informationssystemen genomförs i liten omfattning. En majoritet av kommunerna saknar en plan för bortfall av information i kommunens kritiska verksamhetsprocesser. Övning och utbildning är eftersatta områden. Kommunerna har i och för sig påbörjat införandet av ett ramverk för informationssäkerhet och utsett ansvar, men har inte implementerat ett arbete med informationsklassning och riskhantering i någon större utsträckning. Enbart en tredjedel av kommunerna har ett systematiskt arbetssätt i sitt arbete med informationssäkerhet och huvuddelen av kommunerna har otillräcklig riskhantering. Sju av tio kommuner lägger tio procent eller mindre av en arbetskraft på att säkra informationen i kommunen. Enkätsvaren tyder vidare på att det finns ett gap mellan det som står i kommunens informationssäkerhetspolicy och det som operationaliseras i verksamheten. Det finns därmed sannolikt större verksamhetsrisker hos kommunerna avseende informationssäkerheten än de är medvetna om. När det gäller hur kommuner arbetar med informationssäkerhet är det mycket som liknar arbetet hos de statliga myndigheterna. En avgörande skillnad är dock att arbetet med informationssäkerhet vid myndigheterna med stor sannolikhet gynnats av att myndigheten har föreskriftsrätt inom området. Föreskrifterna innehåller en hänvisning till standarder inom området (SS-ISO/IEC 27001 och 27002) vilket troligen ytterligare fungerat som stöd för myndigheterna i arbetet med att driva informationssäkerhetsfrågor. Sveriges kommu-

[3] *Informationssäkerheten i Sveriges kommuner – Analys och rekommendationer utifrån MSB:s kommunenkät 2015*, Myndigheten för samhällsskydd och beredskap, december 2016, MSB1045.

ner har inte motsvarande informationssäkerhetsföreskrifter, vilket troligen bidragit till att det finns större brister i kommunerna, exempelvis i fråga om informationsklassning och riskanalyser.

Informationssäkerhetsarbete på nio myndigheter – En andra granskning av informationssäkerhet i staten (RiR 2016:8)

Riksrevisionen genomförde 2016 en andra granskning av informationssäkerhet i staten och granskade hur ett antal myndigheter arbetar med sin informationssäkerhet. Resultatet av granskningen redovisades i granskningsrapporten *Informationssäkerhetsarbete på nio myndigheter – en andra granskning av informationssäkerhet i staten* (RiR 2016:8). Syftet med denna granskning var att åter granska informationssäkerhetsarbetet vid de myndigheter som Riksrevisionen granskade 2005–2007[4] och undersöka om regeringen säkerställer att de granskade myndigheterna har en effektiv intern styrning och kontroll av sin informationssäkerhet. Granskningen omfattar de myndigheter vars arbete med informationssäkerhet granskades under åren 2005–2007.[5]

Riksrevisionen konstaterade i rapporten att granskningen visade att det ännu omkring tio år efter de granskningar Riksrevisionen då gjorde av informationssäkerhet fortfarande fanns allvarliga brister i myndigheternas arbete med informationssäkerhet.[6] Granskningen visade även att det fanns enskilda delar av arbetet som fungerar väl, vilket till stor del kan förklaras av vissa initiativ från enskilda individer eller delar av en verksamhet snarare än som ett resultat av ett systematiskt informationssäkerhetsarbete förankrat på ledningsnivå. Riksrevisionen framhöll att det fanns ett ansenligt behov av ännu fler insatser för att bygga upp och förvalta en informationssäkerhet som håller jämna steg med de ökande hoten som framkom genom Riksrevisionens förra granskning av informationssäkerhet.[7]

[4] Riksrevisionens granskningsrapport *Informationssäkerheten i den civila statsförvaltningen* (RiR 2014:23).
[5] Arbetsförmedlingen, Affärsverket svenska kraftnät, Bolagsverket, Försäkringskassan, Lantmäteriet, Migrationsverket, Post- och telestyrelsen, Sjöfartsverket och Statens tjänstepensionsverk. Regeringen, Regeringskansliet och Ekonomistyrningsverket har också ingått i granskningen.
[6] S. 4.
[7] Se Riksrevisionens granskningsrapport *Informationssäkerheten i den civila statsförvaltningen* (RiR 2014:23).

År 2017

Säkerhetspolisens rapport om generella brister i säkerhetsskyddet

Säkerhetspolisen fick 2016 i uppdrag av regeringen att redovisa dels en samlad bild av vilka generella brister som finns i säkerhetsskyddet hos de myndigheter Säkerhetspolisen har tillsyn över som bedriver mest skyddsvärd verksamhet, dels vilka ytterligare åtgärder som kan behöva vidtas för att hantera dessa brister.[8] I Säkerhetspolisens redovisning av inventeringen av säkerhetsskyddet hos myndigheter och institutioner som utifrån sin verksamhet är av högt skyddsvärde, t.ex. energiförsörjning, telekommunikation och finanssektor, framkom att ju mer frekvent en myndighet hanterar generella säkerhetsfrågor i sin kärnverksamhet, desto bättre är den på säkerhetsskydd. Hos ett flertal myndigheter fanns dock brister i arbetet med t.ex. den egna säkerhetsanalysen.

digitalforvaltning.nu (SOU 2017:23)

Regeringen beslutade i 2016 att tillkalla en särskild utredare för att analysera och lämna förslag till effektiv styrning av utveckling, införande och förvaltning av nationella digitala tjänster. I uppdraget ingick bl.a. analysera och lämna förslag till utformning av organisering och ansvarsfördelning för de nationella digitala tjänsterna, åtgärder och incitament för att uppnå en ökad användning av de nationella digitala tjänsterna, och samverkan mellan offentlig och privat sektor i tillhandahållandet av de nationella digitala tjänsterna. Regeringen beslutade i november 2016 att utvidga uppdraget och i tilläggsdirektivet fick utredaren även i uppdrag att analysera hur digitaliseringen i den offentliga sektorn kan stärkas genom att, inom ramen för den befintliga myndighetsstrukturen, samla ansvaret för dessa frågor till en myndighet. Den del av uppdraget som avsåg att samla ansvaret för digitaliseringen i den offentliga sektorn skulle redovisas senast den 15 mars 2017.

Utredningen om effektiv styrning av nationella digitala tjänster lämnade delbetänkandet *digitalforvaltning.nu* (SOU 2017:23) i mars 2017. I delbetänkandet konstaterade bl.a. att digitaliseringen av för-

[8] Säkerhetspolisens pressmeddelande den 16 mars 2017, www.sakerhetspolisen.se/ovrigt/pressrum/aktuellt/aktuellt/2017-03-16-sakerhets-skyddet-maste-starkas/gapet-mellan-hot-och-skydd-vaxer-sakerhetsskyddetmaste starkas.html.

valtningen inte en intern angelägenhet utan en vital del av arbetet med att utveckla den nationella digitala infrastrukturen. Digitalisering har därför inte bara som syfte att underlätta för enskilda (medborgare) och företag. Den syftar också till att främja konkurrenskraften. Med detta breda perspektiv finns det – enligt utredningen – också skäl att uppmärksamma de risker som följer av en alltmer utvecklad användning och spridning av individrelaterad information. Utredningen har därför valt att integrera frågor om bl.a. informationssäkerhet i utvecklingen och genomförandet av den digitala förvaltningen. Bl.a. denna fråga har därför kommit att ta en större plats i utredningsarbetet än direktivet gett uttryck för och utredningen lämnar även flera förslag som rör frågor om bl.a. informationssäkerhet. Utredningen påpekade att Sverige har halkat efter jämförbara länder när det gäller digital förvaltning. Orsaken är främst ett medvetet val att delegera ansvaret för arbetet med e-förvaltning till myndigheterna. Att arbetet varit framgångsrikt i många avseenden kompenserar inte för de begränsningar detta har inneburit. Utredningen fann att regeringen har avstått från att använda de styrinstrument som står till buds, t.ex. genom att inte förtydliga vilka uppdrag myndigheterna har när det gäller digitalisering. Vidare saknas styrande mål för vad som ska uppnås. Det är inte heller tydligt vad som ska anses vara offentliga åtaganden i den nationella digitala infrastrukturen.[9] Utredningen menade att politiken för digital förvaltning bör utformas mot bakgrund av dess roll i den nationella digitala infrastrukturen. En prioriterad fråga är vilket som ska vara det offentliga åtagandet i denna infrastruktur, både i principiella termer och vilka tjänster som det offentliga ska tillhandahålla.[10] Vidare behöver säkerhetsfrågorna integreras i digitaliseringen av den offentliga sektorn. Stödet till statliga och kommunala myndigheter behöver stärkas i dessa frågor. Detta inte minst för att informationssäkerhet täcks in av flera olika lagar som bitvis överlappar varandra. Detsamma kan – enligt utredningen – sägas om ansvaret för de myndigheter som har uppdrag inom områdena för bl.a. informationssäkerhet. Samtidigt skiljer sig myndigheternas befogenheter betydligt. Frågor om bl.a. informationssäkerhet har under utredningens arbete kommit upp i många sammanhang. Det är avgörande att myndigheternas informationssystem är uppbyggda för att klara av en ökad användning och är motstånds-

[9] S. 89 ff.
[10] S. 97 ff.

kraftiga mot eventuella angrepp.[11] Utredningen ansåg att det behövs en övergripande plan för att stärka digitaliseringen av den offentliga sektorn. Enligt planen, som enligt utredningen bör bestå av sju punkter varav en är att bl.a. informationssäkerhet ska beaktas i varje skede av arbetet med att bygga ut den digitala förvaltningen.

Utredningen ansåg vidare att eftersom frågan om bl.a. informationssäkerhet är av avgörande betydelse för att digitaliseringen ska lyckas bör området ska utgöra ett särskilt prioriterat område i uppdraget. Det behöver beaktas redan från början i förberedelserna inför att axla det samlade ansvaret för den offentliga sektorns digitalisering. Det ska då knytas sådan kompetens till den myndighet som får uppdraget, som behövs för att beakta bl.a. informationssäkerhetsskydd i ett tidigt skede av olika projekt och uppdrag. I uppdraget ska även ingå att ansvara för samverkan med bl.a. MSB och PTS för att säkerställa att frågorna om informationssäkerhet ständigt är närvarande när digitaliseringen genomförs. Utredningen föreslog vidare att det i uppdraget för den nya digitaliseringsmyndigheten ingå att bl.a. samverka med MSB och PTS för att underlätta myndigheternas arbete med bl.a. informationssäkerhet. Enligt utredningen behöver säkerhetsfrågorna integreras i digitaliseringen av den offentliga sektorn. Utredningens bedömning är att stödet till statliga och kommunala myndigheter därför behöver stärkas i dessa frågor.

Reboot – omstart för den digitala förvaltningen (SOU 2017:114)

Utredningen om effektiv styrning av nationella digitala tjänster framhöll i slutbetänkandet *reboot – omstart för den digitala förvaltningen* (SOU 2017:114) att för att digitaliseringen och dess effekter ska åtnjuta alla aktörers, inklusive individernas, förtroende och leva upp till förväntningarna om trygghet och säkerhet måste informationssäkerhetsarbetet inom offentliga myndigheter styras på ett mer kraftfullt sätt och därmed genomsyra samtliga digitaliseringsprocesser. En kombination av krav på ett systematiskt och riskbaserat informationssäkerhetsarbete, incidentrapportering och tillsyn tillsammans med ett ändamålsenligt stöd ska säkerställa att samhällets aktörer ges möjlighet att hantera och prioritera informationssäkerhetsbehoven. Utredningen konstaterade samtidigt att det ofta är svårt att motivera

[11] S. 102 ff.

investeringar i informationssäkerhet eftersom det sällan ger en synbar eller upplevd nytta direkt vid investeringstillfället. Informationssäkerhet kan t.o.m. av vissa betraktas som något som endast fördyrar, försvårar och riskerar att försena och till och med stoppa projekt. Många organisationer undviker därför att sätta sig in i vilka värden säker hantering av information ger på längre sikt. Inte sällan betraktas också informationssäkerhetsfrågor som enbart it-frågor vilket innebär att säkerhetsåtgärder av administrativ och organisatorisk art mer eller mindre förbises, exempelvis utformning och följsamhet till arbetssätt och rutiner. Dessutom hänvisas resursförfrågningar till att ingå i rådande it-budget som i sin tur inte behöver vara föremål för någon strategisk satsning. Utredningen framhöll att informationssäkerhet ska genomsyra alla processer som handlar om digitalisering, vilket även påpekats i tidigare utredningar och rapporter.[12] Utredningen noterade även att Riksrevisionen hade påpekat att det behövs en starkare styrning från regeringen gentemot myndigheterna, så att nödvändiga säkerhetsåtgärder verkligen blir genomförda. Att enbart ta fram ett övergripande regelverk är inte tillräckligt för att säkerheten ska bli god.[13]

Utredningen noterade att arbetet med informationssäkerhet är dag till stor del varje organisations eget ansvar. I och med att organisationer i dag är allt mer beroende av andra för sin informationshantering, exempelvis i de förvaltningsgemensamma digitala funktionerna, är det nödvändigt med samordnade åtgärder för att reducera risker och behålla säkerhetsnivån. Möjligheterna att ytterligare kraftigt öka resurser som läggs ned på informationssäkerhetsarbetet är dock begränsade inom många organisationer.

Utredningen konstaterade vidare att det nationella informationssäkerhetsarbetet är i dag uppdelat i olika, delvis överlappande, ansvarsområden, både på departements- och på myndighetsnivå. Detta gör att det i dag saknas ett enhetligt regelverk för och ett enhetligt arbetssätt med samhällets informationssäkerhetsarbete och att det finns få gemensamma krav på informationssäkerhet. Expert- och sektorsmyndigheter har, utifrån sitt specifika ansvarsområde eller expertområde, gett ut föreskrifter som i olika grad har bäring på informa-

[12] *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten* (SOU 2015:23), betänkande av NISU 2014. Utredningen föreslog bl.a. att det bör etableras en nationell modell för att styra samhällets informationssäkerhet.
[13] *Informationssäkerhetsarbete på nio myndigheter – En andra granskning av informationssäkerhet i staten* (RiR 2016:8).

tionssäkerhet. Genom att fler aktörer – utan samordning – utfärdar regler på området finns dessutom en stor risk att fragmenteringen av kravställningen på området ökar. Detta får inte sällan till resultat att erfarenheter och kunskap som finns inte nyttjas effektivt, att de resurser som allokeras inte används inom de områden där bristerna är som störst och att utfärdade informationssäkerhetskrav fördröjs eller aldrig blir utförda på grund av oklara ansvarsförhållanden.

Utredningen menade att det fragmenterade arbetet leder till att det saknas gemensamma riktlinjer för vilket skydd olika typer av informationstillgångar minst bör ha. Detta leder till att samma typ av information riskerar att få helt olika skydd beroende på var i förvaltningssystemet som den hanteras. Detta innebär inte sällan även effektivitetsbrister då lösningar får olika utformning vilket skapar en minskad interoperabilitet som i sin tur leder till en ökad kostnad.

Utredningen ansåg att även bristen av samordnat rättsligt stöd medför svårigheter att säkerställa att offentliga aktörer har rätt förutsättningar i sitt arbete med att genomföra och förvalta digitaliseringsarbetet på ett sådant sätt att de tjänster som erbjuds uppfyller tillräckliga krav på tillgänglighet, riktighet och konfidentialitet.

Utredningen noterade vidare att den inte har kunnat finna någon samordnad tillsyn av det systematiska informationssäkerhetsarbetet. Viss tillsyn finns, t.ex. Post- och telestyrelsen (PTS) inom området elektronisk kommunikation samt Försvarsmakten och Säkerhetspolisen gällande säkerhetsskyddet. När det gäller kommuner, de som kanske kommer att erbjuda flest digitala tjänster, finns dock inte några lagkrav på att arbeta systematiskt med informationssäkerhet, inga krav på att rapportera incidenter och inte heller någon tillsyn. Inom vissa delar av det offentligas verksamhet kommer tillsynen utökas genom NIS-direktivet, men den tillsynen är endast gentemot samhällsviktig verksamhet inom de sju sektorerna energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Detta är dock bara en delmängd av de elva sektorer som MSB identifierat som samhällsviktiga sektorer. Utöver de samhällsviktiga sektorerna finns all övrig offentlig verksamhet som i dagsläget i stort är helt utan tillsyn. Utredningen framhöll att vid införande av tillsyn är det viktigt att regleringens olika delar samspelar så att det inte uppstår en obalans mellan dem. Om t.ex. vissa delar av tillsynsverksamheten är detaljerat reglerad med avseende på vilka prestationer en tillsynsmyn-

dighet ska åstadkomma medan andra delar har mer övergripande målformuleringar finns en risk att den detaljerade regleringen får en starkt styrande inverkan på tillsynen, med den konsekvensen att annan mer strategiskt inriktad tillsyn får stå tillbaka. Det finns också en stor risk att organisationer som är utsatta för tillsyn fokuserar arbetet på de delar som granskas mer specifikt och att arbetet att jobba med informationssäkerhet över hela linjen får stå tillbaka. De uppföljningar som har gjorts inom området informationssäkerhet har bl.a. visat att myndigheternas granskning av sitt eget informationssäkerhetsarbete behöver effektiviseras. Granskningen kan bedrivas med olika metoder och på olika nivåer. Den kan också behöva kombineras med rapportering av resultatet av genomförda granskningar för att uppnå avsedd effekt. Olika alternativa vägar för att stärka både granskning och rapportering av informationssäkerhetsarbetet bör övervägas.

Utredningen föreslog mot den ovan angivna bakgrunden bl.a. att regeringen:

– inleder ett arbete att samordna och strukturera reglering inom informationssäkerhetsområdet,

– ger digitaliseringsmyndigheten i uppdrag att ta fram och mäta nyckeltal för informationssäkerhetsrelaterade aspekter i syfte att följa informationssäkerhetsmognaden i förhållande till digitaliseringen,

– tar fram rättsliga krav som omfattar samtliga offentliga myndigheter att införa ett systematiskt och riskbaserat informationssäkerhetsarbete, och

– ger MSB i uppdrag att utreda hur tillsyn över informationssäkerhetsområdet och incidentrapportering kan genomföras.

Länsstyrelsernas förutsättningar att stödja kommuner gällande informationssäkerhet

Myndigheten för samhällsskydd och beredskap (MSB) gav 2017 Högskolan i Skövde, institutionen för Informationsteknologi, i uppdrag att genomföra en studie med syfte att kartlägga länsstyrelsernas faktiska möjligheter och hur de arbetar med att samordna och stödja kommunernas arbete avseende informationssäkerhet. I rapporten

framhålls att resultatet visar att länsstyrelserna behöver ett tydligt uppdrag med tillhörande mandat och resurser för att ha förutsättningar att kunna samordna och stödja kommunerna i deras informationssäkerhetsarbete. Detta anser de involverade länsstyrelserna saknas i nuläget. Dessutom visar resultatet på att det finns omfattande kompetensbrist inom informationssäkerhetsområdet. Kompetensbristen finns såväl i det interna arbetet som i det externa arbetet ut mot kommunerna, allt från ledningsnivå till operativ nivå. Det finns även behov av tydligare roller både strategiskt och operativt för att sätta igång arbetet och möjliggöra en tydligare överblick. Detta behövs för att ge förutsättningar till länsstyrelserna för att kunna samordna och stödja kommunerna i informationssäkerhetsarbetet relaterat till kris och höjd beredskap men även för att erhålla en strategisk helhetssyn på informationssäkerhetsarbetet utifrån ett samhällsperspektiv.

Bevakningsansvariga myndigheters informations- och cybersäkerhet

Myndigheten för samhällsskydd och beredskap (MSB) fick 2017 i uppdrag av regeringen att, i samverkan med Försvarsmakten och Säkerhetspolisen, redovisa en sammanvägd rapport utifrån samtliga bevakningsansvariga myndigheters redovisningar av analyser och bedömningar av sin informationssäkerhet i de delar av den egna verksamheten som är nödvändiga för att myndigheten ska kunna utföra sitt arbete. Säkerhetspolisen och Försvarsmakten har i samverkan bidragit med sina respektive perspektiv på den bild och den analys som MSB sammanställt baserat på redovisningarna.

MSB konstaterade att redovisningarnas varierande kvalitet och omfattning beror på myndigheternas varierande mognad i informationssäkerhetsarbetet. En mogen organisation identifierar många risker som är relevanta och organisationen har ett systematiskt arbetssätt för att åtgärda bristerna. En mindre mogen organisation identifierar färre brister och inte nödvändigtvis de som är mest kritiska för verksamheten. Därutöver tenderar en mindre mogen organisation att inte heller precisera vilka åtgärder som ska genomföras för att minska de identifierade riskerna. Det är av största vikt att alla myndigheter uppnår en nivå av informations- och cybersäkerhet där de har förmåga att arbeta systematiskt så att de kan identifiera sina risker och

åtgärda brister på ett adekvat sätt. MSB drar bl.a. följande övergripande slutsatser av redovisningarna:

– det finns brister i koppling mellan verksamhetsansvar och informations- och cybersäkerhetsansvar,
– få myndigheter följer myndighetens föreskrifter i sin helhet,
– underlaget från bevakningsansvariga myndigheter kan förbättras gällande både omfattning och kvalitet,
– arbetet med informations- och cybersäkerhet och säkerhetsskydd är inte tillräckligt integrerat.

År 2018

Säkerhetspolisens offentliga redovisning – Säkerhetsskydd hos myndigheter med mest skyddsvärd verksamhet

Säkerhetspolisen rapporterade 2018 att de myndigheter som bedriver de mest skyddsvärda verksamheterna i många fall har svårt att bedöma vad som är skyddsvärt med hänsyn till Sveriges säkerhet. Enligt Säkerhetspolisen har myndigheter också vanligtvis svårt att bedöma hotbilden mot den egna verksamheten. I stor utsträckning saknar även myndigheter förmågan att bedöma den egna verksamhetens sårbarheter. Som följd av dessa brister har många myndigheter svårt att vidta ändamålsenliga och kostnadseffektiva säkerhetsskyddsåtgärder. Säkerhetspolisen finner det därför angeläget att alla myndigheter genomför säkerhetsanalyser och bedömer vilken information och verksamhet som är skyddsvärd. Dessutom framhålls att säkerhetsarbetet bör prioriteras högre.[14]

Granskning av Transportstyrelsens upphandling av it-drift (Ds 2018:6)

Regeringen beslutade den 3 augusti 2017 att en utredare skulle granska den upphandling av it-drift som gjordes av Transportstyrelsen under 2014 och 2015 och som har medfört att säkerhetskänslig och av

[14] Säkerhetspolisens offentliga redovisning *Säkerhetsskydd hos myndigheter med mest skyddsvärd verksamhet*, 2018-02-13.

andra skäl sekretessbelagd information har hanterats på ett sätt som strider mot svensk lag.[15]

Utredaren lämnade departementspromemorian *Granskning av Transportstyrelsens upphandling av it-drift* (Ds 2018:6) till regeringen i februari 2018. Utredaren konstaterade i promemorian att granskningen har funnit brister i Transportstyrelsens hantering av hemliga uppgifter och andra skyddsvärda uppgifter, bl.a. känsliga personuppgifter. Utredaren drog slutsatsen att den grundläggande orsaken till varför Transportstyrelsens upphandling och outsourcing kom att dras med dessa brister var att man i allt för hög grad saknade relevant kunskap om vilken information myndigheten hade och saknade kännedom om hur denna information ska hanteras. Utredaren konstaterade att arbetet med informationssäkerhet vid myndigheten var eftersatt under lång tid och att säkerhetsfunktionerna vid myndigheten var utspridda och saknade tillräcklig samordning. Vidare har de som haft kännedom och kunskap om säkerhetsfrågorna av säkerhetsskäl inte velat tala om dem. Man har även saknat tillräckliga kunskaper om relevanta regler och hur de ska tillämpas.

Utredaren bedömde vidare att den andra huvudsakliga orsaken till att upphandlingen av it-driften ledde till olyckliga konsekvenser var en orealistisk tidplan. Transportstyrelsen inledde tre upphandlingar samtidigt. Det fanns en snäv tidsgräns för leverantörens övertagande av it-driften och slutpunkten för Trafikverkets leverans. Vidare var dokumentation och analys av befintlig information i itsystemen bristfällig. Den tredje grundläggande orsaken var bristen på kommunikation, såväl inom myndigheten som med andra berörda aktörer. Organisationen kring upphandlingen var komplex och därför ett hinder för effektiv kommunikation inom myndigheten. Kontakterna med Trafikverket kunde ha varit mer omfattande och på högre nivå. Vidare verkar styrelsen endast ha fått översiktlig information om händelseförloppet och regeringen har inte involverats för att hantera de uppkomna svårigheterna.

Utredaren ansåg att när det gäller ansvarsfrågan kunde dessa tre huvudsakliga brister härledas främst till myndighetens ledning. Utredaren ansåg bl.a. att det innebar att styrelsen och de tidigare generaldirektörerna hade ett ansvar för hur myndigheten varit organiserad, prioriterat sina resurser och agerat i praktiken. Även andra befattningshavare bar också ett ansvar, bl.a. ansvariga avdelningschefer, projekt-

[15] N2017/04991/SUBT.

ledare och säkerhetsfunktioner, som alla brustit i olika hänseenden när det gäller de tre ovan angivna bristerna.[16]

Juridik som stöd för förvaltningens digitalisering (SOU 2018:25)

Digitaliseringsrättsutredningen lämnade betänkandet *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25) i mars 2018. Utredningen framhöll att av direktiven framgår att den ska särskilt beakta behovet av informationssäkerhet i sitt arbete. Utredningen noterade att under kartläggningsarbetet, och utifrån övriga kontakter den har haft inom ramen för utredningen, har det tydliggjorts att informationssäkerhet är en förutsättning för den fortsatta utvecklingen av en trygg, innovativ och effektiv digitalt samverkande förvaltning. I betänkandet framhöll utredningen att förvaltningens digitalisering inte kan diskuteras utan att frågor om informationssäkerhet belyses särskilt. Utredningen konstaterade att god informationssäkerhet behövs för att möta nya risker i verksamheten. Utredningen fann att i digitaliseringsarbetet står myndigheterna inför många gemensamma utmaningar. Det gäller inte minst informationssäkerheten. Flera aktörer har påtalat att ju mer information som samlas in och hanteras desto svårare blir det att leva upp till säkerhetskraven.[17] Varje myndighet ansvarar självständigt för att informationsklassa sin information.[18] Men när myndigheter samverkar och utbyter information framhålls att det behövs en enhetlig informationsklassning för att informationen ska få likvärdigt skydd hos alla myndigheter som hanterar den. Inom ramen för myndighetsgemensamma system uppstår dessutom ofta nya informationsmängder och även dessa måste kunna hanteras korrekt ur ett informationssäkerhetsperspektiv.

I utredningen kartläggningsarbete efterfrågande myndighetsrepresentanter mer styrande reglering kring myndigheternas informationssäkerhetsarbete. Man framförde att det vore lämpligt med en förvaltningsgemensam reglering av behörighetsstyrning. På så sätt skulle man kunna säkerställa tillgänglighet till information av god kvalitet till

[16] Departementspromemorian *Granskning av Transportstyrelsens upphandling av it-drift* (Ds 2018:6), s. 3 ff.
[17] *Ny finansieringsmodell för grunddatautbyte mellan statliga myndigheter samt kommuner och landsting* (ESV 2017:54).
[18] Med informationsklassning avses att genom konsekvensanalys identifiera skyddsbehovet för en viss informationsmängd. Se 4 § Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1).

dem som har ett konstaterat behov av att ta del av informationen från en viss källa. Vidare framfördes att ett bredare tillsynsuppdrag över myndigheters arbete med informations- och cybersäkerhet behövs. Vidare framhölls att varje myndighet ansvarar dessutom för sina bedömningar och informationssäkerhets-, dataskydds- och sekretessfrågor måste beaktas såväl ur ett individ- som ur ett samhällsperspektiv. Det finns en oro över att uppgifter som en myndighet publicerar på aggregerad nivå ska kunna återskapas till personuppgifter om de kombineras med uppgifter som t.ex. har hämtats från en annan källa, eller att något säkerhetsrelaterat hot kan uppstå som en enskild myndighet inte har överblick över. Ett par aktörer har därför uppmärksammat behovet av en central aktör som har överblick över samtliga öppna data som publiceras av myndigheterna. Myndigheterna måste också beakta eventuella verksamhetsrisker som kan uppstå till följd av publicering av öppna data som rör verksamheten.

Utredningen framhöll att den uppmärksammat att många av de utmaningar kring informationssäkerhet som myndigheterna står inför är gemensamma för hela förvaltningen. Det är en avgörande förutsättning för att informationssäkerhetsfrågorna ska få den uppmärksamhet de förtjänar att frågorna prioriteras av myndighetsledningen. Verksamheten behöver avsätta tillräckliga resurser, såväl tidsmässiga som personella, för att kunna arbeta aktivt och löpande med informationssäkerheten. Om det saknas tillräckliga resurser för informationssäkerhetsarbetet finns det en risk för att verksamhetens fokus läggs på leveranserna i kärnverksamheten i första hand och på säkerheten i andra hand.

Utredningen noterade att flera aktörer har framhållit behovet av att hantera frågor om informationssäkerhet vid myndighetssamverkan. Det gäller särskilt myndighetssamverkan eller som inkluderar informationsutbyten. Information som utbyts mellan myndigheter behöver ha ett tillräckligt skydd hos alla aktörer som hanterar den. Informationsutbyten kan också medföra att nya informationsmängder uppstår. Det behöver finnas en beredskap för att hantera dessa informationsmängder på ett säkert och ansvarsfullt sätt. Avsaknaden av reglering tenderar att medföra att varje myndighet uppfinner sina egna rutiner för informationssäkerhet när det gäller klassning av informationstillgångar, utformning av roller och behörighetstilldelning för åtkomst till information i it-system, val av tekniska, administrativa och organisatoriska säkerhetsåtgärder, m.m. En tydligare

reglering som lägger grunden till en förvaltningsgemensam syn på informationssäkerheten i den offentliga förvaltningen efterfrågas.

Utredningen konstaterade att reglering av informationssäkerhet som träffar olika aktörer och information, med delvis olika syften, finns spridd i olika föreskrifter. Utredningen menade att ett mer sammanhållet arbete med informationssäkerhet i den offentliga förvaltningen har potential att effektivisera den digitala utvecklingen utan att säkerheten åsidosätts. Det gäller inte minst när myndigheter samarbetar i gemensamma utvecklingsarbeten som innefattar informationsutbyten. Mot den bakgrunden bedömer utredningen att det även efter genomförandet av bl.a. NIS-direktivet och ikraftträdandet av en ny säkerhetsskyddslag, kommer att vara angeläget att utforma en generell informationssäkerhetsreglering som omfattar hela förvaltningen, dvs. också kommuner och regioner. I syfte att stärka informationssäkerheten i hela den offentliga förvaltningen föreslår utredningen därför att regeringen låter utreda förutsättningarna för att ta fram en kompletterande reglering om informationssäkerhet som omfattar hela den offentliga förvaltningen.

Utredningen framhöll att förutsättningarna att tillhandahålla viss samordnad it-drift till den offentliga förvaltningen i stort bör fortsatt övervägas. Behovet av författningsreglering avseende en sådan samordnad it-drift bör övervägas i detta sammanhang. Reglering torde bl.a. ge ökad rättslig tydlighet vad avser förhållandet till upphandlingsregelverket.

Utredningens påpekade samtidigt att inom informationssäkerhetsområdet saknas viss reglering som träffar hela den offentliga förvaltningen. För att uppnå nödvändig säkerhet och skydd för information och upprätthålla enskildas förtroende för den digitala utvecklingen i hela den offentliga förvaltningen är det angeläget att etablera ett gemensamt förhållningssätt till informationssäkerhetsfrågorna som omfattar den offentliga förvaltningen i stort. Informationssäkerheten bör som utgångspunkt angripas på ett enhetligt sätt av samtliga myndigheter. Ett mer sammanhållet arbete med informationssäkerhet i den offentliga förvaltningen har potential att effektivisera den digitala utvecklingen i offentlig förvaltning utan att säkerheten åsidosätts. Det gäller inte minst när myndigheter samarbetar i gemensamma utvecklingsarbeten som innefattar informationsutbyte. För att reducera risker och behålla en god säkerhetsnivå hos alla samverkande myndigheter är det angeläget att myndigheter vidtar samord-

nade informationssäkerhetsåtgärder. Regeringen bör därför låta utreda förutsättningarna för att ta fram en kompletterande reglering om informationssäkerhet som omfattar hela den offentliga förvaltningen.

Utredningen noterade i detta sammanhang vad *Utredningen om effektiv styrning av nationella digitala tjänster* föreslår i sitt slutbetänkande om att regeringen tar fram rättsliga krav för ett systematiskt och riskbaserat informationssäkerhetsarbete för samtliga offentliga myndigheter.[19] Utredningen uttalade att den ansluter till de bedömningar som den utredningen har gjort men anser att det finns skäl att utveckla förslaget ytterligare. Enligt utredningens bedömning behövs ett rättsligt styrmedel som utgör ett tydligt incitament för myndighetsledningar att prioritera och ge nödvändiga resurser till arbetet med informationssäkerhet, samtidigt som ledning ges i fråga om vilka åtgärder som behöver vidtas. Ytterligare förvaltningsgemensamma rättsregler kan ge såväl styrning som stöd inom informationssäkerhetsområdet. Vissa generella och grundläggande krav på informationssäkerhetsarbetet för hela den offentliga förvaltningen skulle kunna regleras i form av lag. En sådan informationssäkerhetslag, för den offentliga förvaltningen i stort, i kombination med föreskriftsrätt, kan – enligt utredningens uppfattning – vara en lämplig form för ytterligare styrning och stöd inom informationssäkerhetsområdet. En lag om informationssäkerhet har möjlighet att lägga grunden till en mer enhetlig ansats i informationssäkerhetsarbetet inom den offentliga förvaltningen. Ett större mått av enhetlighet ger bättre förutsättningar att t.ex. effektivisera gemensamma utvecklingsarbeten i den offentliga förvaltningen.

Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82)

Regeringen beslutade den 23 mars 2017 att tillkalla en särskild utredare med uppdrag att överväga vissa frågor i säkerhetsskyddslagstiftningen (dir. 2017:32). Förslagen skulle komplettera de förslag som lämnats i betänkandet *En ny säkerhetsskyddslag* (SOU 2015:25). Utredningen skulle enligt direktiven kartlägga behovet av att förebygga att säkerhetsskyddsklassificerade uppgifter eller i övrigt säkerhetskänslig verksamhet utsätts för risker i samband med utkontrak-

[19] SOU 2017:114, kapitel 9.

tering och upplåtelse. Utredningen lämnade betänkandet *Kompletteringar till den nya säkerhetsskyddslagen* (SOU 2018:82) i november 2018.

Utredningen konstaterade att det finns flera brister i säkerhetsskyddsarbetet som t.ex. yttrar sig vid utkontraktering av säkerhetskänslig verksamhet men också vid vissa upplåtelser och andra förfaranden där utomstående involveras i den säkerhetskänsliga verksamheten. Vissa av bristerna gäller säkerhetsskyddet generellt, t.ex. att verksamhetsutövaren inte tillämpar säkerhetsskyddsreglerna eller har bristande kunskap om sina skyddsvärden. Sådana brister accentueras när verksamhetsutövaren utkontrakterar en del av den säkerhetskänsliga verksamheten eller på annat sätt kopplar in utomstående i verksamheten. Andra brister handlar specifikt om olika förfaranden där utomstående involveras i den säkerhetskänsliga verksamheten, däribland utkontraktering och upplåtelse men också andra förfaranden. Bristerna handlar om att man inte alltid prövar om förfarandet är lämpligt eller att det är svårt att pröva lämpligheten, att säkerhetsskyddsavtal kan vara bristfälliga, att man inte följer upp förfarandet medan det pågår och att det saknas tillräckliga möjligheter för samhället att ingripa mot förfaranden som är olämpliga från säkerhetsskyddssynpunkt.

Utredningen konstaterade att stora konsekvenser kan uppstå när it-drift läggs ut hos privata företag. Utkontraktering kan innebära att flera kunders system och information samlas i samma lagringsmedium eller lagringsmiljö, vilket innebär en ökad exponering. Vissa företag ser ett bra säkerhetsarbete som en konkurrensfördel och satsar därför resurser på säkerhet. Andra företag har inga incitament för att investera i säkerhetshöjande åtgärder som ofta är kostsamma och produktionshämmande.

Utredningen noterade att det finns verksamhetsutövare som inte tillämpar säkerhetsskyddslagen. I betänkandet *En ny säkerhetsskyddslag* (SOU 2015:25) anges att det antagligen finns verksamheter av stor betydelse för Sveriges säkerhet som över huvud taget inte tillämpar säkerhetsskyddslagstiftningen (s. 477). Denna bild stöds av det som framkommit under utredningens möten med myndigheter, enskilda och utredningens experter. Att verksamhetsutövare som bedriver säkerhetskänslig verksamhet inte tillämpar säkerhetsskyddslagstiftningen är i sig allvarligt eftersom det innebär en sårbarhet för de värden som lagstiftningen ska skydda. Inte minst innebär det en

överhängande risk för att man inte gör en säkerhetsskyddsanalys, vilket i sin tur kan leda till bristande kunskap om de egna skyddsvärdena. Det framstår som särskilt allvarligt med brister i tillämpningen vid utkontraktering och upplåtelsen eftersom säkerhetskänslig verksamhet och säkerhetsskyddsklassificerade uppgifter därigenom kan utsättas för ytterligare sårbarheteter. En utebliven eller bristande säkerhetsskyddsanalys kan leda till att verksamhet utkontrakteras eller andra slags förfaranden inleds i fall där det av säkerhetsskyddsskäl inte borde ske. I andra fall kan det leda till att en i och för sig lämplig utkontraktering, upplåtelse eller något annat förfarande äger rum utan att det ingås ett säkerhetsskyddsavtal. Detta innebär också en ökad risk för att motparten i avtalet inte vidtar de säkerhetsskyddsåtgärder som behövs, vilket kan leda till sårbarheter och skador för Sveriges säkerhet. Den omständigheten att den nya säkerhetsskyddslagen i större utsträckning än tidigare kommer att gälla för enskilda verksamhetsutövare underströk – enligt utredningen bedömning – behovet av förebyggande åtgärder.

Utredningen ansåg vidare att det finns bristande kunskaper om egna skyddsvärden. En bild som tydligt framträdde under utredningens möten med experter, myndigheter och enskilda var att många verksamhetsutövare saknar tillräcklig kunskap om vilka skyddsvärden som finns i den egna verksamheten. Sådana brister har ofta blivit synliga inför och under utkontrakteringar. Utredningen framhöll att Säkerhetspolisen har bl.a. observerat att det har förekommit utkontraktering av säkerhetskänslig verksamhet utan säkerhetsskyddsavtal, att säkerhetsskyddet vid utkontraktering har dimensionerats på fel sätt och att verksamhetsutövare har saknat kunskap om verksamhetens roll i samhället, dess betydelse för Sveriges säkerhet och om beroenden mellan den utkontrakterade verksamheten och annan verksamhet av betydelse för Sveriges säkerhet. Bristerna kan i stor utsträckning härledas till bristande kunskaper om den egna verksamhetens skyddsvärden, bl.a. har verksamhetsutövare inte känt till vilka känsliga uppgifter som hanterats i verksamheten. Vidare har verksamhetsutövare inte varit medvetna om vilka beroenden som finns till den egna verksamheten och hur dessa beroenden påverkar Sveriges säkerhet. Sådana brister utgör ett påtagligt problem vid utkontrakteringar eftersom kunskap om egna skyddsvärden är en förutsättning för att verksamhetsutövaren ska kunna formulera krav på hur leverantören ska tillgodose kraven på säkerhetsskydd. Bristande kunskaper

om skyddsvärden utgör ett problem vid bl.a. utkontrakteringar. Utredningen menade det behöver införas förebyggande åtgärder som syftar till att höja verksamhetsutövarnas kunskap om egna skyddsvärden. Detta är inte bara viktigt för att förebygga negativa konsekvenser vid utkontraktering utan också vid upplåtelser, upphandlingar och andra förfaranden där utomstående får tillgång till säkerhetsskyddsklassificerade uppgifter eller i övrigt säkerhetskänslig verksamhet.

Med utgångspunkt i kartläggningen av utvecklingsbehovet föreslog utredningen en bred ansats och ett antal förebyggande åtgärder som inte enbart är inriktade på utkontraktering och upplåtelse, utan som kan aktualiseras även vid vissa andra förfaranden med utomstående parter.

Regeringen har i den påföljande lagstiftningsprocessen delat merparten av utredningens bedömningar (prop. 2020/21:194). I kapitel 13 redogörs närmare för regeringens lagförslag.

År 2019

Granskningsrapport: Föråldrade it-system – hinder för en effektiv digitalisering (RIR 2019:28)

Riksrevisionen har granskat förekomsten av föråldrade it-system hos ett drygt 60-tal större myndigheter. Fokus för granskningen har varit om myndigheterna och regeringen har gjort tillräckligt för att hantera de problem som föråldrade it-system innebär. Granskningen, som redovisades i granskningsrapporten *Föråldrade it-system – hinder för en effektiv digitalisering* (RIR 2019:28), visar att det finns föråldrade it-system hos ett stort antal myndigheter. Hos många myndigheter är det dessutom ett flertal av de verksamhetskritiska it-systemen som är föråldrade. Riksrevisionen bedömer att detta dessutom är ny kunskap. Det har således inte funnits någon bred bild av problemet med föråldrade it-system i förvaltningen. Digitaliseringen går fort och nya it-system utvecklas och blir ständigt mer effektiva. Föråldrade it-system är vanligen förknippade med risker för bristande informationssäkerhet. Det finns stor risk för att föråldrade it-system även innebär bristande hushållning med statens medel. Föråldrade it-system kräver även mycket resurser som innebär en undanträngning av myndighetens innovationsförmåga. Det blir färre resurser över till att ta till sig ny digital teknik och att utveckla och anamma nya och

mer effektiva it-system. Många föråldrade system gör det också svårt eller omöjligt att, baserat på det befintliga systemet, utveckla nya tjänster eller funktionalitet eller att förändra och utveckla befintliga verksamhetsprocesser. Därmed påverkar it-systemen också myndigheternas verksamhetsutveckling. Närmare hälften av myndigheterna uppger att myndighetens fortsatta digitaliseringsarbete i ganska eller mycket stor utsträckning försvåras av problem i enskilda it-system eller av it-miljön i stort. Ett föråldrat it-system och problem med det enskilda systemet hos en myndighet innebär stora konsekvenser för möjligheterna att bedriva verksamheten hos en annan myndighet eller privat aktör. It-kostnaderna för de myndigheter som var föremål för granskning är ungefär 19 miljarder. Den bristande effektiviteten som kan kopplas till föråldrade it-system är därmed väsentlig även ur ett budgetperspektiv. Vidare svararade ungefär 80 procent av myndigheterna att man har svårigheter att upprätthålla eftersträvad nivå av informationssäkerhet för något eller några verksamhetskritiska system och 12 procent svararade att det är ett problem för samtliga eller en majoritet av de verksamhetskritiska systemen. Föråldrade it-system innebär därmed även en väsentlig risk ur ett informationssäkerhetsperspektiv.

Riksrevisionens slutsats är sammantaget att problemet med föråldrade it-system är så allvarligt och utbrett att det innebär ett hinder för en fortsatt effektiv digitalisering av statsförvaltningen. Riksrevisionen drar även slutsatsen att en stor del av de undersökta myndigheterna inte har eller använder de verktyg som behövs. Det innebär i sin tur man får svårigheter att analysera och förstå hur förändringar påverkar verksamhetens mål och det blir därmed också svårare att definiera ett framtida önskvärt läge. Det kan noteras att ungefär 70 procent av myndigheterna svarade att it-miljön är komplex på grund av ett stort antal heterogena system. Mer än hälften har en arkitektur som strävar i flera olika riktningar till förfång för helheten (spretig arkitektur). Riksrevisionen bedömer vidare att frånvaron av målarkitektur och arkitekturstyrning är en av flera bakomliggande förklaringar till att många myndigheter i dag har it-system som kan anses vara föråldrade utifrån verksamhetens behov. En arkitekturstyrning utifrån en målarkitektur är därmed centralt för att vidmakthålla och utveckla en it-miljö som effektivt stödjer verksamhetens behov. Behovet av målarkitektur och arkitekturstyrning accentueras med storleken på myndighetens totala it-miljö. Riksrevisionen be-

dömer att myndigheternas bristande arbete med digitaliseringsstrategier kan även de vara en förklaring till att många myndigheter brottas med en it-miljö bestående av föråldrade it-system i varierande omfattning. En sådan strategi anger en riktning för vad myndigheten totalt sett vill uppnå med sin digitalisering. Det ger därmed en riktlinje som varje enskilt projekt som rör it-utveckling eller förvaltning i någon utsträckning behöver förhålla sig till. Omvänt blir det utan en strategi svårt att åstadkomma en effektivt fungerande helhet.

Kommunernas informationssäkerhetsarbete – en övergripande kartläggning av kommunernas systematiska informationssäkerhetsarbete

Sveriges Kommuner och Regioner (SKR) genomförde under våren 2019 en webbenkät om hur långt kommunerna kommit i sitt systematiska informationssäkerhetsarbete. SKR utarbetade webbenkäten tillsammans med MSB. Enkäten var utformad för att kartlägga om resurser avsatts för att driva informationssäkerhetsarbetet, om grundläggande åtgärder vidtagits och vilken mognadsgrad den svarande kommunen själv skattade att den nått. Sammanfattningsvis framkom av enkäten att det finns en djup och bred förståelse av hur viktigt ett grundläggande systematiskt informationssäkerhetsarbete är för all fortsatt digitalisering. Det som fortfarande återstår på många håll är styrning, ledning, avsatta medel och resurser för arbetets planering och genomförande samt en tydlig uppföljning som är integrerad i övrig verksamhetsuppföljning. Det återstår fortsatt arbete i införandet av ett systematiskt och riskbaserat informationssäkerhetsarbete, inom samtliga undersökta områden i enkäten, bl.a. informerar sig färre än 3 av 10 kommunledningar om statusen för informationssäkerhetsarbetet, i endast 2 av 10 kommuner omsätts ledningens mål i konkreta handlingsplaner. I strax över 5 av 10 kommuner finns en hantering av informationssäkerhetsriskerna. Strax över 5 av 10 kommuner har ett etablerat arbetssätt för klassning av informationstillgångar. I 6 av 10 kommuner finns ett etablerat arbetssätt för hantering av informationssäkerhetsincidenter/-avvikelser. I 4 av 10 kommuner finns ett etablerat arbetssätt för planering som säkerställer verksamhetens kontinuitet. Få kommuner uppger nya säkerhetsskyddslagen eller NIS-direktivet som en faktor till att informationssäkerhet hamnat högre på prioriteringsordningen. Av resultatet från undersökningen kan dras slutsatsen att ett införande av ett systematiskt och risk-

baserat informationssäkerhetsarbete beror ofta på ledningens aktiva engagemang, och här uppvisar många kommuner brister. Snarare förefaller ledningen delegera ned även styrningen av arbetet i organisationen. Vissa av de kommuner som själva skattat sitt arbete högt verkar ha kommit så långt tack vare intresserade och motiverade medarbetare som givits utrymme att utforma informationssäkerhetsarbetet. Vidare verkar det som om många kommuner själva tar fram sina arbetsmetoder. En gemensam nämnare bland de kommuner som inte skattat sitt arbete högt är att ledningen delegerat ansvaret för uppdraget, men inte tilldelat resurser. Att engagera ledningen verkar vara kopplat till frågan om medvetenhet. Det förefaller ofta saknas tillräcklig kunskap om den egna organisationens behov av informationssäkerhet hos såväl den politiska- som tjänstemannaledningen. Den ökade graden av digitalisering och högre krav från allmänheten att få ta del av information verkar driva arbetet med informationssäkerhet. De som lyckats med sitt arbete förefaller ha tagit ett enhetligt grepp om frågan och arbetat aktivt med att förenkla sina arbetssätt och anpassar dem efter lokala förhållanden. Avsaknaden av ett systematiskt angreppssätt verkar begränsande på kommunens arbete, även där medarbetare uppmärksammat behovet av informationssäkerhet. Här verkar det vanligare med ad hoc-insatser med situationsanpassade lösningar, som troligtvis kostar större resurser men inte nödvändigtvis med högre kvalitet.

En struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen – Redovisning av regeringens uppdrag

Myndigheten för samhällsskydd och beredskap (MSB) fick 2019 även regeringens uppdrag att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen.[20]

MSB redovisade myndighetens svar i skrivelsen *En struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen.* I svaret påpekade myndigheten att en uppföljning av informationssäkerhetsarbetet upplevs ofta som en utmaning, samtidigt som det är en förutsättning för att en organisation ska kunna uppnå

[20] Ju2019/03058/SSK, Ju2019/02421/SSK.

och bibehålla ett adekvat skydd. Målsättningen med uppföljningsstrukturen är att statliga myndigheter, kommuner och regioner ska erbjudas stöd i sitt uppföljnings- och förbättringsarbete och att regeringen ska få en samlad nivåbedömning av det systematiska informationssäkerhetsarbetet i offentlig förvaltning. Myndigheten utvecklade i samverkan med företrädare för målgruppen en uppföljningsmodell. Modellen delar in det systematiska informationssäkerhetsarbetet i fyra nivåer, som är tänkta att motsvara ett stegvis utvecklingsarbete. Genom att besvara uppföljningsmodellens frågeformulär får en organisation automatisk återkoppling om sin nivå, styrkor och utvecklingsområden. Kompletterande återkoppling (benchmarking) erhålls efter inrapportering till MSB. I analysen av det samlade underlaget kan MSB dra slutsatser om vad för stöd och satsningar som är påkallade på nationell nivå. Uppföljningsstrukturen löper över två år, med lansering planerad till 2021. Därefter kommer uppföljningen att genomföras regelbundet i tvåårscykler, vilket bl.a. ger möjlighet att identifiera utvecklingstrender över tid. MSB bedömer att myndighetens uppföljningsstruktur bör kunna bidra till ett förbättrat och mer enhetligt arbete med informationssäkerhet inom offentlig förvaltning. Detta förutsätter dock ett brett deltagande från den offentliga förvaltningen, främjande av en positiv och bejakande uppföljningskultur, samt resurssättning av identifierade förbättringsområden.

År 2020

Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden 2020

Försvarets radioanstalt (FRA), *Försvarsmakten*, *Myndigheten för samhällsskydd och säkerhet* (MSB) och *Säkerhetspolisen* har i en fördjupad myndighetssamverkan tillsammans med *Polismyndigheten* gemensamt tagit fram rapporten *Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden 2020.*[21] I rapporten påpekas att det finns en avsaknad av ett strukturerat säkerhetsarbete. Cybersäkerhet är en viktig del i nästan allt säkerhetsarbete eftersom digital information och digitala tjänster används i de flesta verksamheter. Samtidigt har det visat sig att arbetet med cybersäkerhet i Sverige går trögt, med brister i cyber-

[21] Rapporten är framtagen av Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap, Polismyndigheten och Säkerhetspolisen inom ramen för en fördjupad samverkan.

säkerheten som följd. Genomförda granskningar och tillsyner visar att arbetet med cybersäkerhet inte är ändamålsenligt sett till de hot och risker som finns.

I rapporten görs bedömningen att det är vanligt förekommande med brister i systematiskt cybersäkerhetsarbete. Planering och genomförande av säkerhetsarbete är en dynamisk process som kräver fortlöpande uppföljning och utvärdering. De framsteg som sker inom informationsteknik gör att samhället behöver förhålla sig till nya teknologier i samband med sin verksamhetsutövning. Dessa tekniksprång ställer krav på att verksamheterna förstår och kan bedöma förändringar i sin teknikanvändning. När ny teknik introduceras kan det ske gradvis och det kan vara svårt att fastställa en tidpunkt när man behöver revidera en säkerhetsanalys. Det är dock ofta svårt att tydligt definiera ett särskilt tillfälle när en verksamhet har infört ny teknik i sådan omfattning att den påverkar tidigare gjorda bedömningar.

I rapporten pekas också på förekomsten av bristande kravställning vid upphandling och utkontraktering. I Sverige är många verksamhetsutövare i hög utsträckning beroende av informationsteknologi. Kraven på hur en verksamhet ska hantera sin cybersäkerhet ställs genom reglering, men de finns även i form av marknadsmässiga krav på effektivitet, kvalitet och säkerhet för att kunna upprätthålla verksamhetens konkurrenskraft. Det är svårt för vissa verksamhetsutövare att helt på egen hand uppfylla de krav som ställs på säkerhet. En lösning för dessa verksamheter kan vara att utkontraktera sina behov till en tjänsteleverantör som har bättre möjligheter att möta säkerhetskraven. Genom att utkontraktera dessa delar av verksamheten kan verksamhetsutövarna lägga ett större fokus på sin kärnverksamhet samtidigt som cybersäkerheten blir bättre. En utmaning – som noteras i rapporten – är att väl beskriven kravställning är en förutsättning för en bra upphandling. Att kravställa cybersäkerhet kräver kompetens, både när det gäller anskaffning av varor, tjänster och vid utkontraktering. Det finns tillfällen där anskaffning av varor och tjänster som hanterar information med ett högt skyddsvärde har genomförts utan tillräcklig identifiering och värdering av systemets skyddsvärden. Det har skapat risker för den information eller verksamhet som systemet hanterar, vilket innebär att krav på säkerhet i stället arbetas in i efterhand, vilket medför risk för att upphandlingen kan behöva göras om. Även i de fall en helt ny upphandling inte behöver ske är säkerhet kostsamt och ibland svårt att arbeta in i

efterhand. Med en korrekt kravställning kan i vissa fall en utkontraktering av it-infrastruktur till tjänsteleverantörer vara en säkerhetshöjande åtgärd. Vid ett beslut om utkontraktering behöver beställaren emellertid förstå hur tjänsterna som ska levereras är konstruerade och vad en sådan lösning innebär ur säkerhetssynpunkt. För att avgöra om en utkontraktering ger ett tillräckligt skydd krävs att den som beställer har en förmåga att bedöma helheten i den lösning som erbjuds. Då krävs också en förståelse för hur olika tekniska säkerhetsfunktioner fungerar och hur de tillsammans skapar en sammanhållen säkerhetslösning, men dessa bedömningar sker ofta – enligt rapporten – på ett otillräckligt sätt. Det är vanligt att flera tjänsteleverantörer delar på hanteringen av utkontrakterad it-infrastruktur, exempelvis som underleverantörer.

I rapporten noteras att det kan vara svårare för kunden att ställa krav på en kontinuerlig säkerhetsnivå som följs av samtliga leverantörer. Större tjänsteleverantörer som erbjuder sina tjänster gentemot svenska verksamhetsutövare bedriver i regel sin verksamhet i flera länder och omfattas på så vis av en annan jurisdiktion än den svenska. Det medför att utländsk lagstiftning kan bli tillämplig för de tjänster man levererar i Sverige, och den ger i vissa fall leverantören – och dess underleverantörer – rätt att ta del av information som hanteras inom ramen för den tjänst som levereras.

I rapporten påpekas att utkontraktering av it-infrastruktur innebär även att det skapas ett beroende av tjänsteleverantören. När it-tjänster utkontrakteras sker det inte sällan till globala tjänsteleverantörer, vilket innebär att det beroende som uppstår är internationellt. Detta uttrycks ibland som en risk för förlust av digital suveränitet, ett begrepp som använts i EU-sammanhang och innebär att en stat förlorar delar av sin kontroll över sitt oberoende, självständighet och handlingsfrihet på det digitala området. En annan effekt av utkontraktering av it-tjänster är att tjänsteleverantörer samlar flera kunder med verksamheter som innehåller skyddsvärden. Det innebär att den samlade mängden av kundernas information och tjänster hos en tjänsteleverantör gör att leverantören behöver beakta om dess verksamhet – till följd av kundernas skyddsvärden – når en nivå där den i sig är att betrakta som säkerhetskänslig. För att detta överhuvudtaget ska vara möjligt för tjänsteleverantören måste dock kunden kommunicera detta, då leverantören inte som regel själv kan identifiera detta genom sin leverans av det avtalade uppdraget.

I rapporten noteras även att en vanlig form av utkontraktering sker via delade molntjänster, dvs. att en verksamhet i stället för att på egen hand investera i egen hård- och mjukvara hyr de resurser som behövs, vilket kan vara allt från enskilda applikationer till hela eller delar av efterfrågad it-infrastruktur. Det innebär dock säkerhetsutmaningar eftersom verksamhetsutövaren i praktiken lämnar över kontroll över system och information till en tjänsteleverantör. Användandet av molntjänster innebär dessutom att insynen försämras för verksamhetsutövaren jämfört med om man hade hanterat behovet inom den egna verksamheten. En annan utmaning med delade molntjänster är att informationen i de allra flesta fall är indirekt exponerade mot såväl andra kunder som övriga på internet. Med andra ord kan en sårbarhet, såväl administrativ som teknisk, eller en felaktig konfiguration innebära att informationen direkt blir exponerad och sannolikt snabbt spridd till obehöriga. Det innebär att verksamhetsutövare måste hantera problematiken kring överförda hotbilder. Hotbilden mot en molntjänst blir den sammanlagda hotbilden mot alla kunder som använder molntjänsten. Molnlösningar innebär också att en hotaktör inte längre enbart är hänvisad till att angripa ägaren till den information eller tjänst man vill påverka. Förutom molntjänstleverantören har alla övriga kunder en logisk access till den gemensamma it-infrastrukturen hos en leverantör. Det innebär att man är beroende av ett gott it-säkerhetsarbete hos såväl de andra kunderna som sin leverantör. Sådana hot är både svåra att bedöma och att hantera. Svårigheter att logga och spåra datatrafik i komplexa molnmiljöer kan dessutom göra det svårt att utreda incidenter ur såväl ett juridiskt som ett tekniskt perspektiv.

I rapporten påpekas att en annan samhällsutmaning är att molntjänsterna koncentreras till ett fåtal leverantörer. Det innebär att en hotaktör kan inhämta från eller slå ut flera samhällskritiska system samtidigt om man får tillgång till miljön. Den sammanlagda konsekvensen för samhället av ett angrepp blir i dessa fall högre än konsekvensen för ett angrepp mot ett enskilt system. Samtidigt kan en stor leverantör ha större resurser att fördela till sitt säkerhetsarbete, vilket kan göra dem svårare att angripa.

År 2021

Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering (SOU 2021:1)

Regeringen beslutade den 26 september 2019 att ge en särskild utredare i uppdrag att kartlägga och analysera statliga myndigheters behov av säker och kostnadseffektiv it-drift samt hur dessa behov tillgodoses. Utredaren ska också analysera säkerhetsmässiga och rättsliga förutsättningar för samordnad statlig it-drift och lämna förslag på mer varaktiga former för sådan it-drift, om det bedöms lämpligt ur ett säkerhetsperspektiv, och de författningsförslag som detta kräver. Utredaren ska även analysera de rättsliga förutsättningarna för statliga myndigheter, kommuner och regioner att med bibehållen säkerhet utkontraktera it-drift till privata leverantörer och vid behov lämna författningsförslag.

Genom tilläggsdirektiv den 2 juli 2020 förlängdes utredningstiden i den del som avser att föreslå mer varaktiga former för samordnad statlig it-drift till den 15 oktober 2021.

It-driftsutredningen lämnade i december 2020 sitt delbetänkande *Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering* (SOU 2021:1). I delbetänkande redogör utredningen bl.a. för kartläggningen av statliga myndigheters it-drift, omvärldsanalysen och analysen av de rättsliga förutsättningarna för utkontraktering av it-drift till privata tjänsteleverantörer. I slutbetänkande fokuserar utredningen på frågan om samordnad statlig it-drift, utvärderingen av Försäkringskassans uppdrag om samordnad it-drift, exempel på samordnad it-drift mellan myndigheter i Sverige, en analys av de säkerhetsmässiga och rättsliga förutsättningarna för samordnad statlig it-drift samt eventuella förslag om samordnad, säker och kostnadseffektiv statlig it-drift jämte en konsekvensanalys.

Utredningen redogör i delbetänkandet för ett antal kartläggningar som gjorts under de senaste åren och som rör frågor om säker och kostnadseffektiv it-drift i den offentliga förvaltningen. Med utgångspunkt i direktiven bedömer den att det finns behov av att dels följa upp några av de frågeställningar som ingått i tidigare kartläggningar, dels bredda och fördjupa kunskapen om it-driften i dag och behoven framåt liksom säkerhetsaspekter och hinder kopplade till statliga myndigheters it-drift.

I delbetänkandet redogörs för den första delen i kartläggningen som omfattar en enkät till 200 statliga myndigheter. I urvalet ingår myndigheterna i den statliga redovisningsorganisationen, exklusive försvarsmyndigheter, myndigheter med en värdmyndighet och små myndigheter med särskilt låg omsättning. Syftet med enkäten är att få en representativ bild av myndigheternas informationshantering och säkerhet, hur deras it-drift och kostnader för it-drift ser ut i dag, deras framtida behov och vilka eventuella hinder för säker och kostnadseffektiv it-drift som finns. Bakgrundsvariabler som myndighetsstorlek, finansieringsform och departementstillhörighet har ingått i analysen. Enkäten genomfördes mellan den 16 mars 2020 och den 30 juni 2020. Totalt förväntades 180 myndigheter inkomma med svar. Totalt har 158 myndigheter besvarat hela eller delar av enkäten, fyra myndigheter har meddelat att de avstår och 18 myndigheter har inte svarat. Svarsfrekvensen uppgår till 88 procent. En bortfallsanalys visar att de myndigheter som inte svarat omfattar såväl små som medelstora myndigheter och med olika typer av verksamhet och verksamhetsområden. Enkätens representativitet är därmed mycket god.

I delbetänkandet redovisar utredningen kartläggningen, fallstudier av fem myndigheter och en digital workshop med 16 myndigheter. I kartläggningen har frågor ställts om bl.a. verksamhet, informationssäkerhet och uppgiftshantering, it-drift och kostnader, hinder för it-drift samt behoven framåt. Parametrar för analysen har varit myndigheternas storlek, verksamhet och uppgiftshantering samt vilka krav som utifrån detta ställs på it-driften.

Utredningen konstaterar att olika verksamheter har olika behov av säker och kostnadseffektiv it-drift. För samhällskritisk verksamhet ställs högre krav på säkra it-driftslösningar än för verksamheter som inte är samhällskritiska. Icke samhällskritiska verksamheter kan dock hantera känsliga personuppgifter som i sig ställer krav på säkerhet. Myndigheternas verksamhet och vilka uppgifter de hanterar påverkar vilka krav som ställs på it-driften och i sin tur vilka behov av säker och kostnadseffektiv it-drift som finns i den statliga förvaltningen. Den första delen i enkäten hanterar denna typ av frågeställningar.[22]

Utredningen beskriver samhällsviktig verksamhet som ett samlingsbegrepp som omfattar de verksamheter, anläggningar, noder, infrastrukturer och tjänster som är av avgörande betydelse för att upp-

[22] S. 64 ff.

rätthålla viktiga samhällsfunktioner inom en samhällssektor. Med samhällsviktig verksamhet avses dels verksamhet som måste fungera för att inte dess bortfall ska leda till en samhällsstörning, dels verksamhet som måste finnas för att hantera en samhällsstörning när den väl inträffar. Ett drygt 20-tal myndigheter har ett särskilt utpekat ansvar för att inom olika samverkansområden planera och vidta förberedelser för att skapa förmåga att hantera en kris, förebygga sårbarheter och motstå hot och risker.[23] I detta ansvar ingår bl.a. att beakta behovet av säkerhet och kompatibilitet i de tekniska system som är nödvändiga för att myndigheterna ska kunna utföra sitt arbete. Samverkansområdena omfattar teknisk infrastruktur, transporter, farliga ämnen, ekonomisk säkerhet och skydd samt undsättning och vård. Övriga myndigheter, som inte har ett särskilt sektors- eller bevakningsansvar ska själva bedöma om de bedriver samhällsviktig verksamhet eller inte.

I enkäten fick myndigheterna ange om de bedriver verksamhet som kan bedömas vara samhällsviktig. 55 av 158 svarande myndigheter (35 procent) bedömer att de bedriver samhällsviktig verksamhet, medan 100 myndigheter (63 procent) bedömer att de inte gör det. Tre myndigheter anger att de inte vet om de bedriver samhällsviktig verksamhet.

Av kartläggningen framkommer att det finns ett visst samband mellan samhällsviktig verksamhet och storlek på myndighet. Större myndigheter bedriver i högre utsträckning samhällsviktig verksamhet jämfört med mindre myndigheter. Av svaren framgår att myndigheternas samhällsviktiga verksamhet finns inom flera samhällssektorer, med viss övervikt på skydd och säkerhet, offentlig förvaltning, hälso- och sjukvård och finansiella tjänster.

Av kartläggningen framkommer att en mindre andel av myndigheterna hanterar uppgifter som kräver den högsta formen av skydd, dvs. säkerhetsskyddsklassificerad information. Flertalet av myndigheterna (cirka 90 procent) hanterar någon form av skyddsvärd information i sin verksamhet. Endast 14 av 158 myndigheter bedömer att de inte hanterar någon form av skyddsvärda eller i övrigt känsliga uppgifter, varvid olika typer av sekretessreglerade uppgifter är vanligast förekommande liksom känsliga personuppgifter.

[23] Se förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

Av kartläggningen framgår att av 152 svarande myndigheter hanterar 61 myndigheter (40 procent) säkerhetsskyddsklassificerade uppgifter medan 85 myndigheter (56 procent) inte gör det. Större myndigheter hanterar i högre grad säkerhetsskyddsklassificerade uppgifter jämfört med mindre myndigheter. Myndigheternas säkerhetsskyddsklassificerade uppgifter fördelar sig på olika säkerhetsskyddsklasser. Ett fåtal myndigheter anger att de inte vet om de hanterar säkerhetsskyddsklassificerade uppgifter.[24] Majoriteten av myndigheterna hanterar säkerhetsskyddsklassificerad information som klassats som hemlig, konfidentiell eller begränsat hemlig. Ett fåtal myndigheter hanterar uppgifter i den högsta säkerhetsskyddsklassen. Några myndigheter anger att de inte vet vilka säkerhetsskyddsklasser uppgifterna ligger inom, alternativt att de inte vet om de har säkerhetsskyddsklassificerade uppgifter i verksamheten.

Av kartläggningen framkommer att drygt 123 myndigheter (80 procent) hanterar någon form av sekretessreglerade uppgifter i övrigt i kärnverksamheten. 29 myndigheter svarar att de inte gör det och fem myndigheter vet inte om de gör det. 90 myndigheter uppger att de hanterar uppgifter med absolut sekretess, vilket ställer särskilda krav på säkerhetslösningar i it-driften. 80 procent av myndigheterna hanterar sekretessreglerade uppgifter som omfattas av ett omvänt skaderekvisit, dvs. med en presumtion för sekretess.

Av kartläggningen framkommer även att myndigheterna kommit olika långt i arbetet med informationssäkerhet i verksamheten. I enkäten fick myndigheterna uppskatta hur långt de kommit i sitt informationssäkerhetsarbete. Detta utifrån en skala från 1–6, där nivå 1 innebär att myndigheten inte påbörjat något systematiskt informationssäkerhetsarbete och nivå 6 innebär att det finns ett systematiskt och dokumenterat informationssäkerhetsarbete i hela organisationen.[25]

Av kartläggningen framgår att framgår att medianen ligger på nivå 4. Flest antal myndigheter (43 av 158 svarande) har uppskattat att de ligger på nivå 4. Det finns därefter en övervikt för nivå 2 och 3 (totalt 64 av 158 myndigheter), dvs. den något lägre nivån. 13 myndigheter har angett att de ligger på nivå 1, och 12 myndigheter att de ligger på nivå 6. Informationsklassning ingår som en del i informationssäkerhetsarbetet enligt kategori 4 i enkäten. Knappt hälften av myndig-

[24] S. 67 f.
[25] Skalan utgick från de då gällande föreskrifterna och allmänna råden för myndigheters informationssäkerhetsarbete (MSBFS 2016:1).

heterna har angett att de ligger på nivå 1–3. Enligt svaren har hälften av myndigheterna således inte genomfört någon informationsklassning. Samtidigt har de flesta av myndigheterna kunnat svara på enkätfrågorna om vilken typ av uppgifter som de hanterar i verksamheten.

I delbetänkandet noteras att tidigare kartläggningar om myndigheters it-kostnader och it-mognad också har omfattat frågor om informationssäkerhet och hur långt myndigheterna bedömt att de kommit i sitt informationssäkerhetsarbete.[26]

Utredningen noterar att Myndigheten för digital förvaltning (Digg) redovisar i sin rapport *Myndigheters digitala mognad och it-kostnader* (2019) resultatet av en enkät till statliga myndigheter. 14 procent av de myndigheter som ingick i enkätundersökningen hade en väl fungerande informationssäkerhetsstrategi på plats som var införd och tillämpades fullt ut på myndigheten. 25 procent av myndigheterna hade implementerat en informationssäkerhetsstrategi i verksamheten som skulle utvärderas och utvecklas. Ungefär lika stor andel hade påbörjat implementeringen av en strategi, medan 30 procent antingen hade påbörjat ett arbete med att ta fram en strategi eller beslutat om en strategi. Knappt tio procent av myndigheterna uppgav att de endast påbörjat en diskussion om att göra något på området.

Utredningen konstaterar att även om svarsalternativen i Digg:s enkät skiljer sig åt jämfört med vad som redovisas i dess kartläggning är de någorlunda jämförbara. Vissa myndigheter har kommit långt i sitt informationssäkerhetsarbete, medan andra avser att påbörja arbetet inom kort eller arbetar med frågorna. En mindre andel myndigheter har inte gjort något alls på området.

Utredningen noterar att Digg:s enkät dock ger en något mer positiv bild av hur långt myndigheterna kommit i sitt arbete jämfört med utredningen enkät. I Digg:s enkät har myndigheterna även fått uppskatta hur arbetet med informationssäkerhet kommer att se ut på myndigheten år 2021 jämfört med 2019. Drygt 70 procent av myndigheterna har svarat att de bedömer att de år 2021 kommer att ha implementerat en informationssäkerhetsstrategi eller ha en väl fungerande informationssäkerhetsstrategi som tillämpas fullt ut på myndigheten, vilket skulle innebära nästan en dubblering jämfört med läget år 2019.

Utredningens kartläggning visar även att 77 procent av myndigheterna har svarat att de utgår från en standard som stöd för ett

[26] Kapitel 3 i delbetänkandet.

systematiskt informationssäkerhetsarbete. Bland dessa utgår alla myndigheter utom en från ISO 27001, vilket är en av de standarder som rekommenderas i de nya föreskrifterna från MSB. Knappt 20 procent av myndigheterna anger att de inte utgår från någon standard och sex myndigheter (4 procent) har svarat att de inte vet om de gör det.

Utredningen konstaterar att fallstudierna av de fem typmyndigheterna bekräftar till stora delar den bild som enkätundersökningen ger avseende verksamhet, uppgifter och informationssäkerhet. Av de fem fallstudiemyndigheterna bedriver såväl en stor som en mindre myndighet samhällsviktig verksamhet, vilket ställer särskilda krav på säkerhet och it-driftslösningar. Samtliga fem myndigheter hanterar i större eller mindre omfattning skyddsvärda uppgifter, där olika typer av sekretessreglerade uppgifter och känsliga personuppgifter är vanligast förekommande. Två av myndigheterna hanterar även säkerhetsskyddsklassificerade uppgifter. Några fallstudiemyndigheter lyfter svårigheten att bedöma skyddsvärdet på aggregerade uppgifter i verksamheten. De upplever också att det är svårt att få stöd i denna typ av bedömningar, t.ex. från expertmyndigheter.

Av kartläggningen framkommer att företrädare för några fallstudiemyndigheter anser att det kan vara svårt att avgöra vilka krav på it-driftslösningar som ställs för olika typer av uppgifter som hanteras i verksamheten. Det gäller framför allt känsliga personuppgifter och uppgifter som omfattas av ett omvänt skaderekvisit, dvs. där det finns en presumtion för sekretess. För att värna säkerheten hanterar de aktuella myndigheterna denna typ av uppgifter i egen regi.

Utredningen konstaterar vidare att fallstudiemyndigheterna har kommit olika långt i sitt informationssäkerhetsarbete. Det finns ingen tydlig koppling till myndighetsstorlek. Stora myndigheter hanterar i regel en större mängd uppgifter och måste därför lägga mer tid på informationsklassificering jämfört med mindre myndigheter. En av de mindre myndigheterna pekar på att informationssäkerhetsarbetet kräver att myndigheten har egen kompetens och förmåga att arbeta med informationssäkerhet, vilket kan vara svårt att uppnå.

I utredningens enkät fick myndigheterna även besvara ett antal frågor om informationssäkerhet vid it-upphandling. Myndigheterna har fått uppskatta var de står på en tre-gradig skala, där den lägsta nivån innebär att man inte reflekterat över frågan på myndigheten och den högsta att myndigheten har ett etablerat arbetssätt på plats. Svaren på de fyra frågorna visar i sig myndigheternas mognadsgrad i

olika steg i upphandlingsprocessen.[27] Av svaren framgår att en majoritet av myndigheterna har påbörjat en diskussion om kravkatalog eller har en kravkatalog med säkerhetskrav på plats som används vid upphandling och för att värdera anbudssvar. Av svaren framkommer att myndigheterna inte har kommit lika långt när det gäller att verifiera säkerhetskrav vid leverans och driftsättning eller att verifiera kraven under avtalets giltighetstid.[28]

Utredningen noterar att den sammantagna bilden är att kraven på it-drift styrs av vilken typ av verksamhet en myndighet bedriver och vilken typ av uppgifter myndigheten hanterar. Små myndigheter kan därmed behöva ställa lika höga krav på säkra it-driftslösningar som större myndigheter.

Utredningen noterar att det kan finnas flera hinder för myndigheter att säkerställa en säker it-drift. Hindren kan finnas både inom den egna myndigheten och utanför myndigheten. Hinder utgörs av bl.a.

– svårigheter att tolka lagstiftning,
– avsaknad av relevant kompetens inom verksamheten,
– bristande informationsklassificering,
– svårigheter att hitta lösningar som möter verksamhetens krav, och
– stora kostnader för de lösningar som verksamheten kräver.

Av utredningens kartläggning framkommer att 143 myndigheter uppger att svårigheter att tolka lagstiftning tillsammans med bristande informationsklassificering och avsaknad av relevant kompetens inom verksamheten utgör de största hindren för säker it-drift. Detta är särskilt tydligt för de stora myndigheterna. Mindre myndigheter anger i rangordning avsaknad av relevant kompetens, svårigheter att tolka lagstiftning och stora kostnader för de lösningar som verksamheten kräver som hinder. Myndigheternas uppgifter om bristande informationsklassificering överensstämmer med myndigheternas uppskattningar av det egna informationssäkerhetsarbetet.

[27] MSB har gett ut en särskild vägledning om att upphandla informationssäkert (MSB1177). I vägledningen beskrivs bl.a. aktiviteter för att uppnå informationssäkerhet i upphandlingens tre steg – förbereda, upphandla och realisera.
[28] S. 74 f.

Utredningen noterar att när det gäller bristande informationsklassificering pågår arbete på flera myndigheter. Myndigheterna har i flera fall klassat delar av informationen, men inte all information. Bristande kompetens och resurser lyfts fram som problem i sammanhanget, men även tidsbrist anges. En myndighet anger att de saknar systemstöd för informationsklassificering. En annan myndighet menar att det är svårt att översätta informationsklassificeringen till konkreta säkerhetsnivåer i både hård- och mjukvara. Ytterligare ett problem som lyfts fram är svårigheten att informationsklassa aggregerad information.

Utredningen noterar vidare att avsaknad av relevant kompetens upplevs som ett lika stort hinder för säker it-drift som bristande informationsklassificering. Flera små myndigheter uppger att det är svårt att som liten myndighet ha egen kompetens inom it, säkerhet och beställarkompetens. Det kan också vara svårt att hitta och rekrytera rätt kompetens, t.ex. när nyckelpersoner slutar. Enligt flera myndigheter ses kompetensbrist som en riskfaktor. Flera myndigheter köper in kompetens från antingen en annan myndighet eller från företag, vilket i sig innebär ett beroende av extern kompetens.

Av kartläggningen framgår att det tredje största hindret som myndigheterna ser är svårigheter att tolka gällande lagstiftning. Oklarheter vad gäller användning av molntjänster verkar vara vanligast. Svårigheten att göra bedömningar av säkerhetsskydd lyfts också fram som ett problem av flera myndigheter, liksom oklarheter kring krav på datalagring och dataskydd. En myndighet menar att det är svårt att få en sammanhängande bild av samtliga regelverk och hur de ska tolkas beroende på vilken tjänst som ska utvärderas. En annan myndighet pekar på att det är svårt att få juridik, it och informationssäkerhet att mötas. Ytterligare en myndighet lyfter fram att det inte är tolkningen av lagstiftningen som är problemet, utan snarare effekterna av tolkningen som medför svårigheter att genomföra upphandlingar och upprätthålla en stabil it-drift över tid.

Av kartläggningen framgår även att stora kostnader för de lösningar som verksamheten kräver utgör ytterligare ett hinder för säker it-drift. Flera myndigheter framhåller att säkerhet kostar och alternativet med egen drift bedöms som relativt kostsamt av flera myndigheter. Någon myndighet påpekar att även samordnad it-drift kan vara en relativt dyr lösning.

Även svårigheter att hitta lösningar som möter verksamhetens krav upplevs som ett hinder. När fler tjänster blir molnbaserade blir det svårare att hitta lösningar som uppfyller säkerhetskraven. Hårda säkerhetskrav påverkar i sig möjligheterna att nyttja billigare och effektiva it-driftstjänster. Flera myndigheter lyfter svårigheten att kravställa. Verksamhetens krav på digitalisering och kostnadseffektiva lösningar ställs ofta mot krav på säkerhet.

Andra hinder för säker it-drift som lyfts fram i enkäten är bl.a. att det finns för lite resurser för it och säkerhet och att säkerhet inte prioriteras tillräckligt i verksamheten. Några myndigheter lyfter att de har en teknikskuld att hantera, vilket påverkar förutsättningarna att arbeta med säkerhetsfrågor. En myndighet menar att avsaknaden av en samlad statlig strategi leder till att varje myndighet gör egna utredningar, bedömningar och bygger egna lösningar för att uppfylla säkerhetskraven.

Utredningen har också undersökt vilka hinder som myndigheterna ser för att kunna upprätthålla en kostnadseffektiv it-drift. Flera myndigheter upplever höga krav på säkerhet och leverantörsberoende eller andra inlåsningseffekter som hinder för en kostnadseffektiv it-drift. Stora myndigheter uppger även svårigheten att formulera ändamålsenliga krav på it-drift som ett hinder. Flera myndigheter anger att säkerhet kostar och att säkerhetskrav påverkar möjligheterna att använda kostnadseffektiva it-lösningar. Svårigheter att formulera ändamålsenliga krav för it-drift kan också påverka kostnadseffektiviteten. Att hitta rätt kravnivå som dessutom håller under hela avtalsperioden är en stor utmaning.

It-driftsutredningens delbetänkande *Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering* (SOU 2021:1) har remissbehandlats under arbetet med detta slutbetänkande och remissvar har lämnats i maj 2021. Uppdraget att föreslå mer varaktiga former för samordnad statlig it-drift ska redovisas utredningens slutbetänkande senast den 15 oktober 2021.

Struktur för ökad motståndskraft (SOU 2021:25)

Regeringen beslutade 2018 att tillsätta en utredning som ska analysera och föreslå en struktur för ansvar, ledning och samordning inom civilt försvar på central, regional och lokal nivå.[29] En viktig del av att stärka det civila försvaret är att skapa tydliga lednings- och ansvarsförhållanden för att åstadkomma samordning såväl inom det civila försvaret som mellan det civila och det militära försvaret, Denna struktur ska också stärka samhällets krisberedskap.

Utredningen lämnade sitt betänkande *Struktur för ökad motståndskraft* (SOU 2021:25) i mars 2021. Utredningen föreslår att samverkansområdena avvecklas och ersätts av tio beredskapssektorer och fyra särskilda beredskapsområden. I dessa ingår myndigheter med ansvar för verksamheter och funktioner som är särskilt viktiga att upprätthålla under kris, höjd beredskap och ytterst i krig. En myndighet i varje beredskapssektor föreslås få ett mandat att inrikta och samordna arbetet inom sektorn, en sektorsansvarig myndighet. Utredningens definition av begreppet samhällsviktig verksamhet är att med detta avses verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet. Med stöd av definitionen har utredningen identifierat vilka statliga myndigheter som ansvarar för samhällsviktig verksamhet och därefter sammanfört myndigheter med ansvar inom samma samhällssektor. Utredningen föreslår att tio sådana beredskapssektorer inrättas med var sin sektorsansvarig myndighet. Med en indelning av statliga myndigheter i sektorer skapas – enligt utredningen – en organisatorisk plattform för såväl planering som operativ hantering av fredstida kriser, höjd beredskap och ytterst krig. I princip samtliga viktiga samhällsfunktioner är direkt beroende av el, vatten och elektroniska kommunikationer. På samma sätt är de flesta beroende av transporter och fungerande betalningssystem. Arbetet i respektive beredskapssektor ska skapa förutsättningar för att kunna upprätthålla den samhällsviktiga verksamheten under svåra påfrestningar och därigenom stärka samhällets säkerhet. Det gemensamma arbetet i sektorerna ska bidra till ökad försvarseffekt i händelse av ett väpnat angrepp och en god förmåga att hantera fredstida kriser. Myndigheterna inom beredskapssektorerna ska arbeta tillsammans. Samtidigt betonar utredningen vik-

[29] Dir. 2018:79.

ten av samverkan mellan sektorerna. Sektorerna är ömsesidigt beroende av varandra.

Utredningen har – utöver de tio föreslagna sektorerna med sektorsansvariga myndigheter – identifierat fyra särskilda beredskapsområden som ska ses som en del av beredskapssystemet. Enligt utredningen är verksamheterna av en sådan karaktär att de inte kan utgöra beredskapssektorer med en sektorsansvarig myndighet. Några av dessa områden omfattar enbart en myndighet och i några av verksamheterna ingår myndigheter utanför det civila försvaret såsom Försvarsmakten och Försvarets radioanstalt (FRA). Samtidigt fyller dessa verksamheter en viktig funktion i beredskapssystemet som helhet, bl.a. cybersäkerhet.

Utredningen framhåller att den delar Försvarsberedningens bedömning att ett systematiskt arbete med informations- och cybersäkerhet spelar en avgörande roll för att en trovärdig totalförsvarsförmåga ska kunna uppnås. Detta gäller såväl hos staten, kommuner, regioner och näringsliv. Det behöver finnas en nationell funktion med uppgift att stödja myndigheter och samhället i övrigt i arbetet med att förebygga och hantera angrepp inom informations- och kommunikationsområdet samt upprätthålla en aktuell lägesbild över samhällets digitala miljö. Verksamheten är viktig för det civila försvaret. Utredningen föreslår att cybersäkerhet ska vara ett särskilt beredskapsområde. Utredningen bedömer att det inte är möjligt att föreslå verksamheten som en beredskapssektor eftersom både Försvarsmakten och FRA ingår i arbetet med cybersäkerhetscentret samt att regeringen hittills inte har pekat ut någon samordnande myndighet för cybersäkerhetsområdet. Det finns i dag ett etablerat samarbete och samverkan mellan myndigheterna inom cybersäkerhetsområdet genom bl.a. Samverkansgruppen för informationssäkerhet (SAMFI). Formerna för samverkan med de föreslagna beredskapssektorerna kommer att behöva byggas upp när dessa etablerats. Det behöver även etableras samverkansformer med de övriga tre särskilda beredskapsområdena.

Betänkandet är föremål för remissbehandling under utredningens arbete med detta slutbetänkande och remissinstansernas synpunkter har därför inte kunnat beaktas inom ramen för detta arbete.

9 Internationell utblick

9.1 Inledning

När det gäller utredningens uppdrag att överväga om det bör införas ytterligare krav på certifiering och godkännande till skydd för Sveriges säkerhet ingår att göra en internationell jämförelse. Jämförelsen ska avse lagstiftning som innebär särskilda krav med anledning av nationell säkerhet för IKT-produkter, -tjänster och -processer som ingår i ett nätverks- eller informationssystem i länder som utredaren bedömer vara av intresse. Utredningen har mot denna bakgrund sökt information om systemen i Danmark, Finland, Norge, Nederländerna, Frankrike, Tyskland, Storbritannien, USA, Kanada, Australien och Nya Zeeland.

Arbetet har bedrivits främst genom undersökning av lagstiftning och i förekommande fall förarbeten samt övrig information från officiella webbplatser. Vad gäller materialinsamlingen bör beaktas att materialet funnits tillgängligt på originalspråk, i något fall kompletterat av mer eller mindre officiella översättningar till engelska. Skriftliga frågor har ställts till nationella myndigheter i de undersökta länderna (se den formella skrivelsen i bilaga 3 till betänkandet) och svar har inkommit från merparten av de kontaktade myndigheterna. I ett par fall har de skriftliga svaren även kompletterats med uppgifter som lämnats vid digitala möten med företrädare för myndigheterna.[1]

Avsnitten för respektive land inleds med en beskrivning av centrala aktörer med särskilt ansvar för nationell informations- och cybersäkerhet. Efter denna redovisning av organisation m.m. redogörs för landets arbete med att stärka informations- och cybersäkerheten, med fokus på särskilda krav på godkännande och/eller certifiering av IKT i säkerhetskänslig verksamhet. En sammanfattning av sådana krav

[1] Australien och Nya Zeeland har emellertid inte inkommit med svar inom angiven tidsfrist. Utredningen har haft digitala möten med *Nasjonal sikkerhetsmyndighet* i Norge och *Traficom* i Finland (se nedan).

i andra länder lämnas också i kapitel 12 och 13. I de fall där den nationella regleringen är omfattande och/eller behandlar flera relevanta områden överlappande sammanfattas de särskilda kraven även i förevarande kapitel.

Det kan inledningsvis noteras att vissa länder i sin reglering av informationssäkerhet gör en tydlig distinktion mellan samhällsviktig och säkerhetskänslig verksamhet medan somliga nationella system behandlar kritisk infrastruktur och nationell säkerhet tillsammans. Vidare tillskriver länder dessa begrepp olika betydelser. I vissa länder definieras nationell säkerhet i författning medan somliga inte har någon vedertagen definition eller premierar annan begreppsanvändning på området. I flera länder använder man begreppet kritisk infrastruktur i stället för samhällsviktig verksamhet. Också användningen av tekniska termer varierar något mellan länderna, t.ex. i fråga om it- respektive IKT-säkerhet och -incidenter.

De flesta länderna har bestämmelser om informationssäkerhet som reglerar klassificeringen av skyddsvärd information, vilket motsvarar det svenska klassificeringssystemet i säkerhetsskyddslagen. Det föreligger emellertid inte full överensstämmelse mellan antalet klassificeringsnivåer.[2] När begreppet klassificerad (”Classified”) används avses i första hand skyddsvärd information.

Även om vissa säkerhetsskyddsrättsliga skillnader mellan länderna kan identifieras framgår inte av den öppet tillgängliga information som utredningen samlat in från andra länder närmare hur den faktiska tillämpligheten ser ut i respektive land och därmed inte heller i vilken utsträckning det i praktiken förekommer undantag från ordningarna och speciallösningar.

9.2 Finland

Aktörer inom informations- och cybersäkerhet

Transport- och kommunikationsverket (Traficom)

Det finska transport- och kommunikationsverket *Traficom* är en myndighet som ansvarar för nationella frågor som gäller tillstånd, registrering och övervakning inom trafik, transport och kommunikation. Verket främjar bl.a. cybersäkerheten i landet.

[2] Detta kan bl.a. skapa utmaningar när det gäller att dela skyddsvärd information mellan länder.

Nationellt cybersäkerhetscenter

Vid *Traficom* finns Finlands cybersäkerhetscenter.[3] Centret bedriver bl.a. verksamhet för nationell informations- och kommunikationssäkerhet (NCSA-FI, se nedan) och som ansvarar för säkerhetsfrågor vid elektronisk dataöverföring och hantering av säkerhetsklassificerat material. Cybersäkerhetscentret har till uppgift att se till att nationella författningar om informationssäkerhet, störningsfrihet och skydd vid konfidentiell kommunikation efterlevs. Centret utfärdar vidare föreskrifter och rekommendationer, genomför utredningar inom sina verksamhetsområden samt utövar tillsyn över berörda aktörer. Centret utvecklar och övervakar kommunikationsnätens och -tjänsternas[4] tillförlitlighet och säkerhet. Centrets verksamhetsområden innefattar bl.a. televerksamhet, digitala tjänster enligt NIS-direktivet, stark autentisering och betrodda elektroniska tjänster (eIDAS). Centret tar också fram lägesbilder inom cybersäkerhet.[5]

Vidare kan det nationella cybersäkerhetscentret bevilja det s.k. Cybersäkerhetsmärket som visar att en produkt eller tjänst som försetts med märket uppfyller kraven på informationssäkerhet. Märket används i smarta konsumentprodukter som kan ansluta till internet, s.k. IoT-enheter, och applikationer nära sammankopplade med sådana produkter.[6]

Centret har även en CERT-verksamhet (CERT-FI) med uppgifterna att undersöka hot och angrepp mot informationssäkerheten i nät- och kommunikationstjänster och informera om frågor som gäller informationssäkerhet.[7]

NCSA-FI är den nationella godkännandemyndigheten för säkerhetsackreditering (SAA)[8]. NCSA-FI arbetar med att stödja olika aktörers förebyggande säkerhetsarbete. Myndighetens uppgifter innefattar

[3] Cybersäkerhetscentret är en del av *Traficom* med vissa självständiga funktioner som styrs av lag.
[4] Ett kommunikationsnät är ett system för överföring av signaler som används för att tillhandahålla tillgängliga elektroniska kommunikationstjänster. Elektroniska kommunikationstjänster utgörs av överföring av signaler i elektroniska kommunikationsnät.
[5] I juni 2020 lämnade den finska regeringen en proposition till riksdagen med förslag till författningsändringar bl.a. med anledning av EU:s cybersäkerhetsakt (RP 98/2020 rd). I denna utnämns *Cybersäkerhetscentret* vid *Traficom* till nationell myndighet för cybersäkerhetscertifiering enligt cybersäkerhetsakten, både vad avser uppgiften att bevilja cybersäkerhetscertifiering och utövandet av tillsyn.
[6] *Traficom* definierar förfaringssätt för testningen. Standarden ETSI EN 303645, som beskriver grundläggande cybersäkerhetskrav på IoT, utgör här grunden varav *Traficom* valt ett antal krav att tillämpas.
[7] Utöver allmän information om informationssäkerhet kan CERT-FI bistå med teknisk utredning av allvarliga informationssäkerhetskränkningar.
[8] *Security Accreditation Authority*.

bedömning och godkännande av informationssystem som behandlar säkerhetsklassificerad information. Tjänsterna erbjuds åt myndigheter och företag som behandlar nationellt eller internationellt säkerhetsklassificerad information. NCSA-FI är även den nationella godkännandemyndigheten för krypteringsprodukter.

Övriga säkerhetsmyndigheter

Utrikesministeriet har det samlade ansvaret för internationella förpliktelser som gäller informationssäkerhet. Utrikesministeriet är den nationella säkerhetsmyndigheten (NSA)[9] som styr den nationella verksamheten i dessa frågor och bl.a. ansvarar för beredningen av internationella säkerhetsavtal samt övervakar att internationellt särskilt känslig information skyddas och hanteras korrekt.

Försvarsministeriet, Huvudstaben och Skyddspolisen är övriga utsedda säkerhetsmyndigheter (DSA)[10].

Nationell cybersäkerhetsstrategi och cybersäkerhetsdirektör

2013 antog Finland en nationell cybersäkerhetsstrategi.[11] Målsättningar med strategin är bl.a. att främja samverkan på området mellan dels myndigheter och andra aktörer, dels internationellt, samt att förbättra lägesbilden respektive kunskapen i fråga om cybersäkerheten. Att stärka förmågan att avvärja cyberhot mot samhällsviktig verksamhet är ett annat mål.

Den nationella cybersäkerhetsstrategin uppdaterades 2019 och inkluderade då inrättande av en nationell cybersäkerhetsdirektör. Uppdraget som statens cybersäkerhetsdirektör grundar sig på ett principbeslut som statsrådet godkände 2019, som en del av den nationella cybersäkerhetsstrategin. Enligt strategin ska cybersäkerhetsdirektören samordna utvecklingen, planeringen och beredskapen i fråga om cybersäkerheten. De tre strategiska riktlinjerna i principbeslutet är internationellt samarbete, ledning av cybersäkerhet, förbättrad samordning av planering och beredskap samt utveckling av kompetens inom cybersäkerhet.

[9] *National Security Authority*.
[10] *Designated Security Authority*. *Traficom* har också DSA-uppgifter.
[11] Se https://turvallisuuskomitea.fi/sv/strategi-for-cybersakerheten.

Förverkligandet av den nationella cybersäkerheten anknyter till *Säkerhetsstrategin för samhället* (2017) och till de i strategin beskrivna allmänna principerna om samordning av beredskapen och säkerheten. Strategin och genomförandet av den är också ett led igenomförandet av EU:s cybersäkerhetsstrategi. Den nationella cybersäkerhetsstrategin ska såväl granskas som utvärderas kontinuerligt.[12]

Övergripande reglering av informationssäkerhet

Lagen om informationshantering inom den offentliga förvaltningen (906/2019) beskriver de minimikrav på informationssäkerhet som ska iakttas inom den offentliga förvaltningen. I *lagen om tjänster inom elektronisk kommunikation* (917/2014) finns angivet vissa av Traficoms uppgifter samt skyldigheter för kommunikationsförmedlare att sörja för informationssäkerhet.[13]

Enligt *lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation* (1406/2011) har *Traficom* till uppgift att på begäran göra bedömningar av överensstämmelse med kraven på informationssäkerhet i informationssystem och datakommunikation som en myndighet innehar eller planerar att anskaffa. Statliga myndigheter får, för bedömning av informationssäkerheten i sina informationssystem och sin datakommunikation, bara använda sig av det förfarande som anges i lagen (*Traficoms* bedömning) eller av ett sådant bedömningsorgan som har godkänts av *Traficom* enligt *lagen om bedömningsorgan för informationssäkerhet* (1405/2011). *Traficom* gör utredningar om nivån på informationssäkerheten och utfärdar även intyg som visar att informationssystemet eller datakommunikationen godkänts. Bedömningsgrunderna för informationssäkerheten utgörs bl.a. av EU:s bestämmelser om informationssäkerhet eller informationssäkerhetskrav i en fastställd

[12] De nationella arrangemangen för cybersäkerhetsarbetet i Finland är för närvarande under granskning och kommer sannolikt att genomgå förändringar inom en snar framtid. Landet har två nyligen utvecklade program för cybersäkerhet som är relaterade till målet att förbättra cybersäkerheten: rapporten *Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla* och *Digital säkerhet inom den offentliga förvaltningen – Genomförandeplan Haukka 2020–2023*.

[13] *Traficom* får bl.a. meddela föreskrifter om kvalitetskrav på kommunikationsnät och kommunikationstjänster, om informationssäkerhet och om kompatibilitet gällande klassificering i viktighetsordning och säkrande, om elektroniskt och fysiskt skydd av kommunikationsnät och tillhörande utrustningsutrymmen samt om standarder som ska iakttas respektive andra jämförbara tekniska krav på kommunikationsnät och kommunikationstjänster.

standard. Bedömningen av informationssystemen ska göras i enlighet med nu nämnda lagar (1406/2011 respektive 1405/2011).

Lagen om bedömningsorgan för informationssäkerhet (1405/2011) innehåller bestämmelser om ett förfarande genom vilket företag tillförlitligt kan visa en utomstående att de i sin verksamhet sörjt för en viss informationssäkerhetsnivå. Enligt lagen godkänner *Traficom* bedömningsorganen för informationssäkerhet och övervakar deras verksamhet. Den i lagen angivna ackrediterings- och bemyndigandeprocessen avseende organen för bedömning av överensstämmelse motsvarar i allt väsentligt vad som anges i EU:s cybersäkerhetsakt. Kraven på dessa organ är dock delvis annorlunda, vilket betyder att ett organ för bedömning av överensstämmelse enligt den nationella lagen inte får ställning som ett organ för bedömning av överensstämmelse enligt EU-förordningen. Därför måste ackrediteringen och bemyndigandet enligt cybersäkerhetsakten genomföras separat.[14]

När det gäller behovet att använda cybersäkerhetscertifiering har verksamhetsutövaren själv att göra en riskbedömning och vidta åtgärder för att nå en tillräckligt säker nivå. Även andra sätt än certifiering kan användas för att uppnå tillräcklig säkerhet.

Särskilda krav på IKT i säkerhetskänslig verksamhet

I den nyss nämnda *lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation* (1406/2011) delegeras en rätt till statsrådet att föreskriva att en myndighet är skyldig att skaffa ett intyg om *godkännande* från *Traficom* i fråga om informationssystem där säkerhetsklassificerade handlingar behandlas (8 a §).[15] Detta gäller handlingar som hör till säkerhetsklass I eller II, dvs. på de två högsta nivåerna (av fyra) där störst skada för nationell säkerhet riskeras.[16] Den som önskar ett intyg om godkännande ska förbinda sig att upprätthålla informationssäkerhetsnivån och ge *Traficom*

[14] Se prop. RP 98/2020 rd s. 110.
[15] Några nationella krav på certifiering av sådana system har dock inte framkommit.
[16] Indelning i säkerhetsklass I ska ske om obehörigt röjande eller obehörig användning av sekretessbelagda uppgifter i handlingen kan orsaka särskilt stor skada för försvaret, för förberedelser inför undantagsförhållanden, för internationella relationer, för brottsbekämpningen, för den allmänna säkerheten eller för stats- och samhällsekonomins funktion, eller på något annat jämförbart sätt för Finlands säkerhet. Säkerhetsklass II aktualiseras om röjande eller användning kan orsaka betydande skada för ett sådant skyddat intresse som anges ovan. Det finns ytterligare två säkerhetsklasser som kan komma i fråga vid risk för skada respektive lindrig skada för skyddade intressen.

tillträde till informationssystemen för utredning. Den nu nämnda föreskriftsrätten har emellertid aldrig utnyttjats, vilket innebär att det i nuläget inte är obligatoriskt att skaffa godkännande för informationssystem i säkerhetskänslig verksamhet. I stället kan verksamhetsutövare frivilligt ansöka om ett sådant intyg. Eftersom förfarandet är frivilligt är något sanktionssystem inte knutet till det.[17]

Statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019) innehåller bestämmelser om säkerhetsklassificering av skyddsvärda handlingar och om informationssäkerhetsåtgärder som gäller behandlingen av sådana handlingar. I förordningen uppställs vissa säkerhetskrav på informations- och datakommunikationssystem som används för behandling av säkerhetsklassificerade handlingar.[18]

9.3 Norge

Aktörer inom informations- och cybersäkerhet

Ansvariga departement

I Norge har *Justitie- och beredskapsdepartementet* ett särskilt ansvar för nationell cybersäkerhet i den civila sektorn och ska forma regeringens politik för cybersäkerhet, inklusive upprättande av nationella krav och rekommendationer för offentliga och privata verksamheter. *Försvarsdepartementet* har det yttersta ansvaret för cybersäkerheten i försvarssektorn.[19]

Nasjonal sikkerhetsmyndighet (NSM)

Nasjonal sikkerhetsmyndighet (NSM) är en sektorsövergripande expert- och tillsynsmyndighet inom nationell säkerhet. NSM är underordnat *Justitie- och beredskapsdepartementet* och den ledande aktören i landet på informations- och cybersäkerhetsområdet. NSM tar emot anmälningar om allvarliga cyberattacker mot samhällsviktig verksamhet och IKT-säkerhetsincidenter samt rapporterar till ovan angivna

[17] Inom social välfärd och hälsovård.
[18] Bl.a. ska säkra krypteringslösningar användas.
[19] Departementen har ett brett spektrum av instrument för att ta hand om sitt respektive ansvar för cybersäkerhet, bl.a. genom utveckling av regelverk och kunskap, tillsynsverksamhet och rådgivning respektive vägledning.

departement.[20] NSM ger vidare information, råd och vägledning om förebyggande säkerhetsarbete. NSM utövar certifieringsverksamhet avseende it-säkerhet i produkter och system (SERTIT, se nedan) och ansvarar för det nationella cybersäkerhetscentret (NCSC, se nedan), som i sin tur inrymmer den nationella CERT-funktionen (se nedan).[21] Myndigheten har även en roll att *evaluera* respektive *godkänna* vissa produkter, tjänster och skyddsvärda informationssystem av avgörande betydelse för säkerhetskänslig verksamhet (se nedan).

Nasjonalt cybersikkerhetssenter (NCSC)

Nasjonalt cybersikkerhetssenter (NCSC) är en avdelning som ingår i NSM och har till uppgift att stärka landets motståndskraft och beredskap i den digitala domänen. Verksamheten bedrivs i nära samarbete med operatörer av infrastruktur och övriga aktörer i näringslivet.

NCSC hjälper till att skydda grundläggande nationella funktioner, offentlig förvaltning och företag mot cyberattacker. Centret ger råd och rekommendationer till såväl statliga myndigheter som privata företag, bl.a. när det gäller hantering av cyberattacker, samt uppställer informationssäkerhetskrav för IKT. Dessutom erbjuder centret en rad tekniska informationssäkerhetstjänster,[22] och det producerar även en gemensam lägesbild. IKT-säkerhetstjänsterna inbegriper tekniska säkerhetsutredningar, kartläggning av sårbarheter i offentlig verksamhet och kritisk infrastruktur, certifiering av it-säkerhet (SERTIT, se nedan)[23] samt penetrationstestning. Vissa av tjänsterna är endast tillgängliga för verksamheter som omfattas av den nationella säkerhetslagen (se nedan).[24]

[20] NSM får riktlinjer från både *Justitie- och beredskapsdepartementet* och *Försvarsdepartementet* på deras respektive områden.
[21] NSM har cirka 300 anställda.
[22] Se bl.a. NSM:s grundprinciper för IKT-säkerhet, den 15 april 2020, v. 2.0, som definierar en uppsättning principer och åtgärder för att skydda informationssystem och data.
[23] Certifieringen baseras på standardiserade krav och metoder som är internationella erkända, som *Common Criteria*.
[24] Med tekniska säkerhetstjänster avses ett antal för samhället centrala strategiska tjänster som NSM erbjuder till samhällets aktörer. Dessa är för det stora flertalet frivilliga men för de aktörer som omfattas av landets säkerhetsskyddslag obligatoriska, exempelvis ansvaret för nationella certifieringslösningar.

Centrets huvudsakliga operativa uppgifter kommer till uttryck genom CERT-arbetet[25] och genom *Varslingssystem for digital infrastruktur* (VDI, Nationellt sensorsystem)[26] och detektering respektive hantering av it-incidenter.

Nationellt certifieringsmyndighet för it-säkerhet – SERTIT

Den nationella säkerhetsmyndigheten NSM har ansvar att vara certifieringsmyndighet för it-säkerhet i produkter och system i Norge enligt *Common Criteria*. Certifieringsorganet vid NSM, SERTIT, som representerar Norge i det internationella arrangemanget CCRA, är också internationellt erkänt som certifikatutgivare inom CCRA. NSM, representerat av SERTIT, är också del av den europeiska överenskommelsen SOG-IS MRA[27].

Utöver att driva den *Common Criteria*-baserade nationella certifieringsordningen övervakar SERTIT den professionella statusen hos ackrediterade evalueringsföretags personal.

Nationell cybersäkerhetsstrategi

Norge antog en ny nationell cybersäkerhetsstrategi 2019.[28] Med strategin vill regeringen skapa en gemensam grund för att hantera digitala säkerhetsutmaningar. Vidareutvecklingen av strategin baseras på behovet av ett stärkt offentlig-privat, civil-militärt[29] och internationellt samarbete. Ett av de övergripande målen med strategin är att kritiska samhällsfunktioner ska stödjas av en robust och pålitlig digital infrastruktur. Delmål är att myndigheterna ska ha en överblick över nationell kritisk digital infrastruktur och ställa krav på säkerhet i denna.

[25] *Norwegian Computer Emergency Response Team* (NorCERT) är en funktion i NCSC som ansvarar för Norges nationella CERT-funktion och utgör bl.a. en koordinerande enhet för incidenter kring it-säkerhet. Enhetens verksamhetscenter hanterar allvarliga cyberattacker mot kritisk social infrastruktur och information.
[26] VDI drivs av NCSC och består av sensorer som används för verksamheter inom Norges kritiska infrastruktur. VDI är ett slags digitalt inbrottslarm som utlöses vid misstänkt aktivitet i nätverket.
[27] NSM är även certifikatutgivare under SOG-IS MRA.
[28] Se www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177.
[29] Strategin identifierar att också cyberattacker mot civil infrastruktur kan utmana landets förmåga att skydda nationell säkerhet.

Sektorslagstiftning

Norge har inte genomfört NIS-direktivet i nationell lag. För närvarande behandlas dock ett förslag till en lag om säkerhet i nätverk och informationssystem på området.[30]

I Norge finns ett flertal författningar om cybersäkerhet som gäller olika sektorer, däribland regleringar om användning av IKT i finanssektorn (FOR-2003-05-21-630), elektronisk kommunikation i telekomindustrin (LOV-2003-07-04-8 och FOR-2004-02-16-401), samt säkerhet och beredskap i energisektorn (FOR-2012-12-07-1157).

Informations- och cybersäkerhet inom nationell säkerhet

Nationell säkerhet

I Norge finns en lag om nationell säkerhet (*sikkerhetsloven*, LOV-2018-06-01-24). Begreppet nationell säkerhet[31] definieras i lagen och täcker Norges suveränitet, territoriella integritet och demokratiska statliga system och allmänna politiska säkerhetsintressen.

Varje nationellt säkerhetsintresse avser grundläggande nationella funktioner. Dessa funktioner är tjänster, produktion och andra typer av aktiviteter som är så viktiga att en helt eller delvis förlust av funktionen skulle få allvarliga konsekvenser för nationella säkerhetsintressen.

Departementen och NSM ska inom sina respektive ansvarsområden peka ut, klassificera och övervaka skyddsvärda infrastrukturer och objekt. Vid denna klassificering i enlighet med säkerhetslagen ska tonvikt läggas på i vilken utsträckning grundläggande nationella funktioner beror på den aktuella infrastrukturen eller objektet samt den berörda aktörens skadebedömning.

Säkerhetslagen gäller för:

– alla statliga myndigheter (och motsvarande) och kommuner,
– efter beslut av ansvarigt departement,[32] för privata aktörer som hanterar klassificerad information, informationssystem, föremål

[30] Se www.regjeringen.no/no/dokumenter/horing-nou-2018-14-ikt-sikkerhet-i-alle-ledd-og-utkast-til-lov-som-gjennomforer-nis-direktivet-i-norsk-rett/id2623252/?expand=horingsnotater.
[31] ”Nasjonale sikkerhetsinteresser”.
[32] Varje departement pekar således ut grundläggande nationella funktioner och identifierar verksamheter som är av avgörande betydelse för dessa funktioner.

eller infrastruktur, eller deltar i aktiviteter som är av avgörande betydelse för grundläggande nationella funktioner, och

– privata tillhandahållare av varor eller tjänster som kan medföra tillgång till klassificerad information eller kritiska objekt respektive infrastrukturer.[33]

Information, informationssystem, infrastruktur och objekt som omfattas av lagen ska förses med en lämplig nivå av säkerhet. Skyddsåtgärder ska identifieras utifrån en riskbedömning och med beaktande av tillämplig klassificeringsnivå.

Krav på evaluering och certifiering

I en föreskrift om verksamheters arbete med förebyggande säkerhet, *virksomhetsikkerhetsforskriften* (FOR-2018-12-20-2053)[34], uppställs olika säkerhetskrav på berörda aktörer, bl.a. för att skydda vissa informationssystem. Verksamheter som hanterar risker förknippade med skyddsvärda informationssystem ska uppnå en försvarlig säkerhetsnivå genom att data och tjänster skyddas mot oönskad påverkan (49 §). Vissa säkerhetsåtgärder ska genomföras och kontrolleras (jfr 9, 11 och 15 §§).

I nu nämnda föreskrift finns en allmän bestämmelse om evaluering respektive certifiering. När en verksamhet väljer säkerhetsåtgärder ska den använda evaluerade produkter och tjänster om dessas funktion är avgörande för att personer inte obefogat ska få tillgång till hemlig eller kvalificerat hemlig information och inte heller ska kunna påverka driften av kritisk infrastruktur. Evalueringen ska ske genom metodisk utveckling och testning av produkten eller tjänsten och vara verifierbar. Evalueringen ska utföras av den nationella säkerhetsmyndigheten, NSM, eller ett ackrediterat laboratorium som utsetts av NSM (16 §).[35] Kraven på evalueringen kan uppfyllas genom en certifiering utfärdat av NSM eller ett ackrediterat certifierings-

[33] Lagen ger kungen rätt att föreskriva om skyddsvärda informationssystem, utpekande av godkännandemyndigheter och krav för leverantörer.
[34] Ansvarigt departement är *Justitie- och beredskapsdepartementet*.
[35] Av NSM:s handbok framgår att behövliga säkerhetsåtgärder ska evalueras och certifieras i enlighet med NSM:s krav. NSM utgår från ISO-certifierade produkter och tjänster. Om tillfredsställande standarder inte finns kommer NSM att ställa uttryckliga krav anpassade till den aktuella klassificeringsnivån. Det kan tilläggas att evalueringsuppdrag kan tillställas SERTIT.

organ som utsetts av NSM.[36] NSM kan vidare godkänna användningen av produkter och tjänster som har evaluerats eller certifierats i andra länder (17 §).

Krav på godkännande av informationssystem

För att kunna använda informationssystem som antingen behandlar säkerhetsklassificerad information eller är av avgörande betydelse för grundläggande nationella funktioner ska en godkännandemyndighet bedöma om kraven på säkerhet i systemen är uppfyllda och meddela beslut om godkännande.

Säkerhetsåtgärder som skyddar ett informationssystem ska ha en acceptabel risk- och säkerhetsnivå för att erhålla ett säkerhetsgodkännande. För informationssystem som hanterar säkerhetsklassificerad information ska säkerhetsgodkännandet beslutas innan systemet kan tas i drift (6–3 § *sikkerhetsloven*). Ett beslut om säkerhetsgodkännande är giltigt i upp till fem år eller tills betydande ändringar av informationssystemet gjorts.

Säkerhetsåtgärder definieras i närmare detalj i föreskrifter som meddelats med stöd av säkerhetslagen och i allmänna råd som utfärdats av NSM. De åtgärder som ska vidtas differentieras av klassificeringsnivån för informationen som behandlas i informationssystemet, eller systemets klassificeringsnivå när själva systemet är att bedöma som infrastruktur av avgörande betydelse för grundläggande nationella funktioner.

När en verksamhet beslutat att utveckla ett skyddsvärt informationssystem ska den *informera* NSM. Skyldigheten att lämna information gäller dock bara om NSM behöver godkänna systemet. I annat fall måste verksamhetsutövarna se till att informationssystem som ska behandla säkerhetsklassificerad information är godkända innan de används. Andra skyddsvärda informationssystem ska godkännas så snart som möjligt (50 § *virksomhetsikkerhetsforskriften*).[37]

Verksamhetsutövaren ska dokumentera att den bedömt och hanterat risken på ett tillfredsställande sätt och i samband med detta

[36] NSM ställer således krav på aktörer som utför certifiering och utvärdering av produkter och tjänster. Ackreditering av laboratorier och certifieringsorgan ska ske i enlighet med ISO- och IEC-standarder. Organen för bedömning av överenstämmelse ackrediteras av *Norsk Akkreditering* som är Norges nationella ackrediteringsorgan i enlighet med EU-förordningen om krav för ackreditering (EG 765/2008).

[37] Det är verksamhetsutövaren som har att täcka kostnaderna för godkännandet.

– identifiera behovet av skydd utifrån informationssystemets funktion och driftsmiljö,
– fastställa säkerhetskrav baserade på behovet av skydd,
– etablera säkerhetsåtgärder som uppfyller säkerhetskraven under informationssystemets livstid, och
– kontrollera att säkerhetsåtgärderna fungerar som avsett.

Om verksamheter hanterar särskilt skyddsvärd information och säkerhetsklassificerade uppgifter ska åtgärderna säkerställa att informationen inte med enkla medel går förlorad, ändras eller görs oåtkomlig och inte heller kan offentliggörs för obehöriga. Om risken motiverar det måste informationen också skyddas mot avancerade attackmetoder. När det gäller konfidentiell, hemlig eller kvalificerat hemlig information förutsätter en tillräcklig säkerhetsnivå att obehöriga inte obemärkt kan komma åt informationen.

NSM genomför kontroller och utövar tillsyn[38] över efterlevnaden av säkerhetslagen. NSM ska på *förhand* godkänna informationssystem som behandlar säkerhetsklassificerad information och vilka

– ska användas utomlands eller har anslutning utanför den egna verksamheten,
– har användare som inte är säkerhetsgodkända för rätt nivå, respektive
– bearbetar kvalificerat hemlig (”strengt hemmelig”) eller hemlig information.

NSM godkänner vidare skyddsvärda informationssystem som är utpekade som, eller har avgörande betydelse för, infrastruktur eller objekt klassificerade som mycket kritiska eller kritiska.

Godkännandet av ett skyddsvärt informationssystem innefattar en planerad och systematisk granskning av om verksamheten upp-

[38] Tillsyn enligt lagen kan också utföras av sektorsmyndigheter efter beslut av berört departement. Som tidigare berörts ger NSM även verksamheter vägledning om identifiering av risker och sårbarheter. Om behövliga säkerhetsåtgärder inte vidtagits kan NSM förelägga verksamhetsutövaren att åtgärda bristerna, t.ex. en undermålig riskanalys, vid äventyr av vite. Administrativa sanktioner är en annan ingripandemöjlighet som står till buds vid överträdelser. I sista hand anmäler NSM brott mot säkerhetsregleringen till *Politiets sikkerhetstjeneste en* varpå en process förs vid domstol.

nått en rimlig säkerhetsnivå.[39] Processen utgörs av en dokumentationsgenomgång som bl.a. tar fasta på om och hur IKT-incidenter hanteras. Vid granskningen utvärderas vidare informationssystemets operativa miljö, dess behov av skydd och om föreslagna säkerhetsåtgärder är tillräckliga för att uppnå lämpligt skydd.

Även kryptosystem som ska användas för att skydda säkerhetsklassificerad information ska godkännas av NSM. Kraven på beslut av NSM om förhandsgodkännande av informationssystem gäller således även på försvarsområdet.[40] Som en del av godkännandeprocessen finns som sagt också krav på evaluering av komponenter (se ovan).

Behörigt departement kan bestämma att godkännande av informationssystemet ska göras av en tillsynsmyndighet. Vidare kan NSM bestämma att en tillsynsmyndighet eller verksamhetsutövare ska godkänna berört informationssystem. En verksamhetsutövare som har ett skyddsvärt informationssystem och som inte omfattas av nämnda krav på förhandsgodkännande ska godkänna systemet själv (51 §).[41]

Överträdelser av skyldigheterna enligt säkerhetslagen är straffbelagda. Till detta kommer att NSM har ett antal undersökningsbefogenheter och möjlighet att besluta åtgärdsföreläggande vid vite.

Kontaktpersoner på NSM har framfört att en av de största fördelarna med det nationella godkännandeförfarandet är att det skapar en minimistandard för kontroll av säkerhet och mer enhetliga säkerhetskrav hos verksamhetsutövarna på de aktuella nivåerna. Vidare anser man att då det rör sig om de största riskerna för nationell säkerhet finns ett större behov av en oberoende tredjepartsbedömning (av en central myndighet).

[39] Om det finns ett särskilt behov av att använda ett skyddsvärt informationssystem innan det godkänts kan godkännandemyndigheten bevilja ett tillfälligt tillstånd vid behov och om det finns särskilda skäl.
[40] NSM har alltså ansvar för godkännanden inom samtliga sektorer. Försvaret har flest system som behandlar säkerhetsklassificerad information och är den sektor som har störst behov av NSM:s godkännanden.
[41] NSM och relevanta tillsynsmyndigheter ska informeras om sådana informationssystem.

9.4 Danmark

Aktörer inom informations- och cybersäkerhet

Nationellt cybersäkerhetscenter

Center for Cybersikkerhed är Danmarks nationella it-säkerhetsmyndighet och har i uppdrag att stödja en hög nivå av informationssäkerhet i den informations- och kommunikationsteknologiska infrastruktur som kritiska funktioner är beroende av. En del av uppdraget är att ge råd om cybersäkerhet till nationella samhällsviktiga myndigheter och privata företag. Centret är en del av Försvarets underrättelsetjänst och hör till Försvarsministeriet.

Cybersäkerhetscentret tillhandahåller en nätverkssäkerhetstjänst som innefattar analys och hantering av säkerhetsincidenter hos myndigheter och företag som anslutit sig till tjänsten. Centret har distribuerat intrångsdetekteringssystem för ett antal nätverk i verksamheter som avser kritisk infrastruktur och där känslig myndighetsinformation förekommer, inklusive försvar. De högsta statliga organen och myndigheterna kan på begäran anslutas till tjänsten. Regioner, kommuner och företag inom samhällsviktig verksamhet kan anslutas till tjänsten om centret bedömer att det kommer att bidra till en högre nivå av informationssäkerhet i samhället.[42] Centret övervakar också nätkommunikationen i samhällsviktig verksamhet och kritisk infrastruktur.

Säkerhets- och underrättelsetjänst

Den danska säkerhets- och underrättelsetjänsten, *Politiets Efterretningstjeneste* (PET), är ansvarig för att identifiera, förhindra, utreda och svara på hot mot friheten, demokratin och säkerheten i det danska samhället. PET ger rådgivning inom ett antal områden, däribland informationssäkerhet.

[42] Försvarsministeriet kan fastställa närmare regler om villkoren för anslutning samt föreläggande om medverkan (vid äventyr av böter).

Reglering av informations- och cybersäkerhet

Allmänt

Graden av digitalisering i Danmark är mycket hög. I landet finns ingen nationell övergripande säkerhetslagstiftning. Det finns emellertid en regeringsförordning som reglerar informationssäkerhet inom statliga myndigheter samt särskilda krav på säkerhet i nätverks- och informationssystem i vissa sektorer (se nedan).

Nationell cybersäkerhetsstrategi

Danmark har antagit en nationell strategi för informations- och cybersäkerhet för åren 2018–2021.[43] Under dessa år ämnar regeringen att markant öka investeringarna i landets informations- och cybersäkerhet. Genom den nationella strategin lanserar regeringen även 25 initiativ och 6 riktade strategier för de mest kritiska sektorernas informationssäkerhetsarbete, med fokus på att öka den tekniska motståndskraften i den digitala infrastrukturen och den allmänna medvetenheten samt stärka nationell samordning och samarbete på området. Enligt den nationella strategin är följande områden s.k. kritiska sektorer som ska ta fram egna informations- och cybersäkerhetsstrategier:

– telekommunikation,
– hälsa,
– energi,
– ekonomi,
– sjöfart, och
– transport.[44]

Med den nationella strategin har det således blivit ett krav att en dedikerad informations- och cybersäkerhetsenhet skapas för var och en av de kritiska sektorerna i samhället – och central finansiering ges för detta. Varje sektor måste utveckla en specifik strategi med hänsyn till de specifika hot och sårbarheter som gäller i sektorn. Sektors-

[43] Se https://digst.dk/media/16815/national_strategi_for_cyber-_og_informationssikkerhed_ pdfa.pdf.
[44] Samtliga sektorer förutom telekommunikation täcks av NIS-direktivet.

strategierna ska godkännas av en central statlig kommitté. Respektive sektor har vidare inrättat en decentraliserad cyber- och informationssäkerhetsenhet (DCIS).[45]

Cybersäkerhetscentrets befogenheter

Bekendtgørelse af lov om Center for Cybersikkerhed är en lag som reglerar det nationella cybersäkerhetscentrets uppgifter och befogenheter. Bl.a. får centrets nätverkssäkerhetstjänst, utan föregående domstolsbeslut, behandla en mängd olika uppgifter som härrör från berörda organisationer samt vidta diverse utredningar.

Informationssäkerhet hos myndigheter i säkerhetskänslig verksamhet

Det finns en regeringsförordning (”sikkerhedscirkulæret”) som reglerar informationssäkerhet inom statliga myndigheter, inklusive krav på ackreditering av informationssystem som används för klassificerad information. Sådana system kan vara föremål för certifiering och/eller godkännande. Ärenden som rör nationell säkerhet samordnas av en ministerkommitté för säkerhet medan hanteringen av större cyberincidenter samordnas av cybersäkerhetscentret.

Säkerhet i nätverk och informationssystem i vissa sektorer

Lov om sikkerhed i net- og informationssystemer i transportsektoren (LOV nr 441, 2018-05-08) reglerar bl.a. säkerhetskrav för tillhandahållare av viktiga transporttjänster. Dessa ska vidta lämpliga och proportionerliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten i sina nätverk och informationssystem. *Transport-, byggnads- och bostadsministern* fastställer närmare regler om nödvändiga åtgärder och att dokumentation ska ske genom ackrediterad certifiering i enlighet med reglerna och en internationellt erkänd standard för kontroll av säkerheten i nätverk och informationssystem. Ministern kan slutligen fastställa regler om den information som han eller hon ska få om valet av certifieringsordning.

[45] Den danska näringsmyndigheten och *Rådet för Digital Sikkerhed* har inlett en säkerhetskontroll baserad på standarden ISO 27001 som genererar en översikt och riktmärke för företags digitala säkerhet och riktlinjer för hur man kan förbättra den.

I 3 kap. 5 § *Bekendtgørelse om sikkerhed i net- og informationssystemer i transportsektoren* (verkställande order: BEK nr 1042, 2018-08-06) anges att tillhandahållare av viktiga transporttjänster inom två år från sin utnämning ska dokumentera till *Transport-, byggnads- och bostadsverket* att tillhandahållaren har erhållit en ackrediterad certifiering i enlighet med den verkställande ordern och en internationellt erkänd standard för kontroll av säkerheten i nätverk och informationssystem., t.ex. DS/EN ISO/IEC 27001 eller motsvarande.

Bekendtgørelse om sikkerhed i net- og informationssystemer af betydning for skibes sikkerhed og deres sejlads (verkställande order: BEK nr 46, 2019-01-15) föreskriver att tillhandahållare av sjöfartstjänster, inom två år efter det att de utsetts, måste vara certifierade i enlighet med en internationellt erkänd standard för kontroll av säkerheten i nätverk och informationssystem, t.ex. DS/EN ISO/IEC 27001 eller motsvarande. Certifieringen ska omfatta den del av operatörens nätverk och informationssystem som operatören är beroende av för att tillhandahålla sjötjänsten och där en händelse kan komma att ha en betydande inverkan på fartygssäkerhet och dess navigering. Certifieringen måste utföras som en ackrediterad certifiering av ett certifieringsorgan som är ackrediterat enligt relevant standard. Ackrediteringen måste i sin tur göras av antingen det nationella ackrediteringsorganet DANAK eller ett liknande ackrediteringsorgan, som är medsignatär till EA:s (European cooperation for Accreditation) eller IAF:s (International Accreditation Forum) multilaterala avtal om ömsesidigt erkännande som täcker relevant certifieringsstandard (se 4 kap. 6 och 7 §§).

Sammanfattning av särskilda krav på IKT i säkerhetskänslig verksamhet

I *Danmark* finns krav på cybersäkerhetscertifiering i fråga om säkerheten i nätverks- och informationssystem främst i vissa sektorer (såsom transport och sjöfart). För statliga myndigheter finns också krav på ackreditering av informationssystem som används för skyddsvärd information. Sådana system kan vara föremål för certifiering och/eller godkännande.

9.5 Nederländerna

Aktörer inom informations- och cybersäkerhet

Justitiedepartementet och nationellt cybersäkerhetscenter

Justitie- och säkerhetsdepartementet, *Ministerie van Justitie en Veiligheid*, har det övergripande ansvaret för informationssäkerheten i Nederländerna.

Nederländerna har valt att samla huvuddelen av sin IKT-säkerhetsexpertis och incidenthantering på nationell nivå i ett nationellt cybersäkerhetscenter, *Nationaal Cyber Security Centrum* (NCSC). Detta inkluderar både en nationell rapporteringspunkt, CERT-funktion, samordningsansvar för IKT-händelser, övervakning och informationsutbyte (se nedan). I landet hanteras således cybersäkerhetsrelaterade ärenden centralt hos NCSC. NCSC driver också ett offentligt anmälningssystem riktat till mindre verksamheter och allmänheten. Centret fungerar som en kontakt mellan de olika ansvariga organen inom cybersäkerhet och ska därmed säkerställa samordning av de olika aktiviteterna. NCSC utgör en del av Justitie- och säkerhetsdepartementet.

NCSC:s lagstadgade uppgifter på cybersäkerhetsområdet anges i den nationella lagen om säkerhet i nätverk och informationssystem (*Wet beveiliging netwerk- en informatiesystemen*, Wbni). Centret tar fram olika riktlinjer för it-säkerhet.[46] Centret samlar även in och delar med sig av kunskap om cyberhot och -sårbarheter. Centret har vidare till uppgift att ge råd till industrin inom de samhällsviktiga sektorerna. Råden till allmänheten avser främst it-säkerhetshot och incidenthantering.

Myndigheter och organisationer inom samhällsviktig sektor är skyldiga att rapportera allvarliga cybersäkerhetsincidenter till NCSC. I lagen anges att NCSC även är CSIRT för leverantörer av samhällsviktiga tjänster[47].

När det gäller implementeringen av det kommande NIS2-direktivet är avsikten att *National Coordinator for Security and Counterterrorism*, som är en del av säkerhets- och justitiedepartementet, ska ansvara för samordning av tillsynen.[48]

[46] Säkerhetsriktlinjerna avser bl.a. mobilapplikationer och transportlagersäkerhet (TLS).
[47] Se NIS-direktivet.
[48] Ansvar för regleringen av och tillsyn över sektorerna vattenhantering, transport och hamnar ska ligga hos *Ministeriet för infrastruktur och vattenhantering* (*Infrastructuur & Waterstaat*).

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) – den allmänna underrättelse- och säkerhetstjänsten

Nederländernas allmänna underrättelse- och säkerhetstjänst, *Algemene Inlichtingen- en Veiligheidsdienst* (AIVD), är ett generaldirektorat vid inrikesministeriet (*ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, BZK) och lyder under inrikesministern. AIVD spelar en viktig roll för den nationella säkerheten och försöker identifiera risker och hot mot nationell säkerhet så tidigt som möjligt.

NBV – nationell byrå för kommunikationssäkerhet

Den nationella byrån för kommunikationssäkerhet, *Nationaal Bureau voor Verbindingsbeveiliging* (NBV), är en enhet vid AIVD som evaluerar och utvecklar tekniska säkerhetsprodukter för skydd av känslig, sekretessbelagd, information av avgörande betydelse för regeringen. NBV har till uppgift att evaluera säkerhetsprodukter innan dessa ska godkännas för att skydda särskild information. De kriterier som tillämpas vid evalueringen beror främst på klassificeringen av den särskilda information[49] som utrustningen måste kunna bearbeta och säkra. NBV ger också råd om säkerhetsprodukternas användning till potentiella användare och organisationer. Med sin expertkompetens om informationssäkerhet bidrar NBV till nationell säkerhet i Nederländerna. NBV ansvarar vidare för produktion och distribution av nyckelmaterial för olika kryptografiska utrustningar.[50]

NBV har till uppgift att lämna råd i fråga om it-produkter och -tjänster relaterade till nationell säkerhet. Om NBV bedömer att en utvärderad produkt är lämplig utfärdar man ett särskilt råd till en arbetsgrupp för särskild informationssäkerhet, *Werkgroep Bijzondere Informatiebeveiliging* (WBI, se nedan), som fattar beslut om att god-

Ekonomiministeriet (*Economische Zaken*) svarar för sektoriell reglering och tillsyn avseende energi, olja och digitala tjänster. Övervakningen för dessa sektorer genomförs av *Agentschap Telecom*.

[49] Informationen inbegriper statshemligheter och annan speciell information som, hos obehöriga, kan påverka statens, dess allierades eller ett eller flera ministeriers intressen negativt.

[50] NBV kan hjälpa regeringen med utformningen av en säker och högkvalitativ IKT-infrastruktur. NBV kan också arbeta med andra ämnen som påverkar viktiga delar av den nederländska infrastrukturen.

känna produkten. Råden innehåller samtliga förutsättningar för säker användning av produkten.[51]

WBI – arbetsgrupp för informationssäkerhet

WBI är en arbetsgrupp för informationssäkerhet i vilken försvars-, inrikes-, justitie- och säkerhets- samt utrikesministerierna ingår.[52] Ministerier vänder sig till WBI för råd om speciell informationssäkerhet.[53] WBI får i sin tur instruktioner från en kommitté för underrättelsetjänst, *Comité Verenigde Inlichtingendiensten Nederland* (CVIN).

WBI:s uppgifter inbegriper

- politisk rådgivning avseende särskild informationssäkerhet,
- råd till inrikesministeriet om att – efter evalueringsundersökningar – bevilja godkännande av användning av tekniska informationssäkerhetssystem eller komponenter av dessa för att skydda särskild information,
- råd till AIVD när det gäller tillhandahållande av nationellt utvecklade tekniska informationssäkerhetssystem eller -komponenter till tredje part som godkänts eller kommer att godkännas efter evaluering av säkerheten för särskild information, och
- rådgivning om nationell kryptoverksamhet.[54]

Nationellt cybersäkerhetsråd

Det nederländska cybersäkerhetsrådet *Cyber Security Raad* (CSR), inrättat av NCSC, är ett nationellt oberoende organ som har till uppgift att tillhandahålla strategiska råd om cybersäkerhet till den nederländska regeringen och näringslivet samt att övervaka utvecklingen

[51] Det yttersta ansvaret för installation av en säkerhetsprodukt ligger inte på NBV eller WBI utan hos en avdelnings generalsekreterare, och en säkerhetschef ansvarar för genomförandet av en säkerhetspolicy. Nu nämnda personer kan avvika från NBV:s råd men avdelningen får då ta ansvar för eventuellt tillkommande risker.
[52] Även en representant från AIVD ingår i WBI. Denna representant är också ordförande för WBI.
[53] Medlemmarna i WBI har rätt att inspektera säkerhetsklassificerade dokument.
[54] Se den nederländska förordningen nr 2350225/01 om inrättandet av arbetsgruppen för särskild informationssäkerhet den 27 juni 2005 (*Instellingsregeling WBI*).

på cybersäkerhetsområdet. Rådet levererar även olika typer av produkter.

Certifieringsorgan

TÜV Rheinland Nederland B.V. (TÜV Rheinland) ansvarar för att implementera och driva den nederländska certifieringsordningen för it-säkerhet (NSCIB). TÜV Rheinland är ett certifieringsorgan ackrediterat av det nederländska ackrediteringsrådet *RvA*[55] som certifierar säkerheten i it-produkter och -system i enlighet med de förfaranden som anges i NSCIB-dokumentationen och *Common Criteria* (CC) respektive *The Common Evaluation Methodology* (CEM). I detta sammanhang är certifieringsorganet ansvarigt för att utfärda samtliga produktcertifikat, och organet offentliggör alla certifikat utfärdade enligt NSCIB i enlighet med villkoren i CCRA och SOG-IS MRA för internationellt erkännande.[56]

TÜV Rheinland har också till uppgift att licensiera evalueringsföretag enligt NSCIB och bedöma dessa företags tekniska rapporter. Personalen vid evalueringsföretagen måste genomgå en utbildning godkänd av TÜV Rheinland för att bli licensierade.

Agentschap Telecom

Den övergripande implementeringen av EU:s cybersäkerhetsakt handhas av *Ministeriet för Ekonomi och Klimatpolitik* som utsetts till nationell myndighet för cybersäkerhetscertifiering i enlighet med akten. De uppgifter som följer av cybersäkerhetsakten har ministeriet delegerat till landets telestyrelse, *Agentschap Telecom*. *Agentschap Telecom* kommer därmed att certifiera och utöva tillsyn enligt cybersäkerhetsakten.[57]

[55] Registrerat enligt C078 för *Common Criteria*.
[56] Beroende på mandat kan tillsynsmyndigheter och regelgivare ingripa i vissa stadier av produktlivscykeln.
[57] *Agentschap Telecom* föreslås vidare ha ansvaret för tillsyn enligt NIS2-direktivet över sektorer inom energi, olja och tillhandahållande av digitala tjänster.

Övergripande reglering av informations- och cybersäkerhet

Nationell cybersäkerhetsstrategi

I sin nationella cybersäkerhetsstrategi från 2018 konstaterar Nederländerna att cybersäkerhet är nära kopplad till nationell säkerhet till följd av digitaliseringen i samhället. I strategin anges att förmågan ska förbättras för att kunna hantera IKT-överträdelser som hotar den nationella säkerheten. Vidare finns intresse av att tillsammans med privata aktörer bevaka utvecklingen av en certifieringsordning för leverantörer av cybersäkerhetstjänster.[58]

I cybersäkerhetsstrategin presenteras sju mål och nödvändiga åtgärder för att uppnå dessa mål. Bland dessa åtgärder ingår obligatorisk rapportering av cyberhot och incidenter samt krav på att kritiska processer utvecklar sin förmåga att stå emot cyberattacker.[59]

Det kan konstateras att Nederländerna lägger särskilt stort fokus på att förbättra cybersäkerheten i landet genom att upprätta informationsdelningsstrukturer och samarbete mellan offentlig och privat sektor. Det senaste årtiondet har allt fler nya aktörer, från både offentlig och privat sektor involverats i arbetet med att utveckla den nationella strategin.

Färdplan för cybersäkerhet i hård- och mjukvara

I det strategiska dokumentet *Roadmap for Digital Hard- and Software Security*[60] erbjuds en uppsättning åtgärder för att eliminera säkerhetsgap i hård- och mjukvara, upptäcka sårbarheter och mildra deras konsekvenser under produktens hela livscykel. Som åtgärder för ökad digital säkerhet och transpararens föreslår färdplanen bl.a. standardisering och certifiering. Man önskar harmonisera de olika standardiserings- och certifieringsinitiativen så mycket som möjligt och aktivt bidra till ett brett ömsesidigt erkännande av standarder

[58] *National Cyber Security Agenda – A cyber secure* Netherlands, se www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1. Strategin ska utvärderas årligen.

[59] 2017 utarbetade Nederländernas regering även en internationell cybersäkerhetsstrategi: *Building Digital Bridges. International Cyber Strategy: Towards an integrated international cyber policy*.

[60] Ministry of Economic Affairs and Climate Policy (2018). *Roadmap for Digitally Secure Hardware and Software. The Hague: Ministry of Economic Affairs and Climate Policy*.

och certifikat.[61] Vidare insisterar man på en aktiv utveckling av det europeiska ramverket för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt och ett snabbt antagande av obligatorisk certifiering för specifika IKT-produktgrupper, dvs. produkter som utgör den största risken. På lång sikt bör enligt landet obligatorisk certifiering eller efterlevnad av en CE-märkning för alla produkter med internetanslutning implementeras genom gradvis utvidgning.

Grundläggande informationssäkerhet i offentlig sektor

Baseline informatiebeveiliging Overheid (BIO) är ett grundläggande ramverk för informationssäkerhet som omfattar hela den offentliga sektorn. Det är Inrikesministeriet som svarar för regleringen. Ramverket syftar till att

- öka samordningen mellan statliga och privata aktörer och därigenom förbättra informationssäkerheten,
- minska den administrativ bördan för regeringen och industrin,
- möta internationella regleringar och standarder, och
- minska underhållskostnaderna.

Nationella it-säkerhetsordningar

När det gäller produktcertifiering har en nederländsk certifieringsordning på it-säkerhetsområdet, *NSCIB*, inrättats för att möjliggöra evaluering och certifiering i landet av it-säkerhetsprodukter och -system på ett sätt som överensstämmer med *Common Criteria*-metodiken (ISO-standard 15408). AIVD[62]/NLNCSA[63] är ägare av certifieringsordningen. Självbedömning tillåts inte.

Vidare finns en nationell ordning för grundläggande bedömning av säkerhetsprodukter, *BSPA* (Baseline Security Product Assessment), som är avsedd att bedöma lämpligheten av it-säkerhetsprodukter[64] i den ”känsliga men oklassificerade” domänen, på grundläggande evaluer-

[61] Nederländerna strävar efter att proaktivt skapa kopplingar till globala standardiserings- och certifieringsinitiativ via NEN-standardiseringsplattformen.
[62] *Algemene Inlichtingen- en Veiligheidsdienst* (den allmänna underrättelse- och säkerhetstjänsten).
[63] Nederländernas nationella byrå för kommunikationssäkerhet.
[64] Bl.a. IoT omfattas.

ingsnivå. Kraven uttrycks i det nederländska *Baseline Informatiebeveiliging Rijksdienst* (BIR).

Särskilda krav på IKT i säkerhetskänslig verksamhet

Informationssäkerhet i produkter och system

Som ovan berörts genomgår produkter som är av avgörande betydelse för säkerheten hos särskild offentlig information evaluering av den nationella byrån för kommunikationssäkerhet, NBV, innan dessa ska godkännas för skydd av informationen. Efter framgångsrik evaluering lämnar en arbetsgrupp för särskild informationssäkerhet, *WBI*, råd till Inrikesministeriet som har att besluta om godkännande för användning av systemet eller dess komponenter.[65] Några andra nationella krav på certifiering av nämnda system och produkter har dock inte kunnat noteras.

ABDO 2017 – försvarskontrakt

Det nederländska försvarsdepartementets dokument *ABDO 2017* innehåller cybersäkerhetskrav för försvarskontrakt där bl.a. leverantörer ska vidta vissa säkerhetsåtgärder. I dokumentet finns krav på att viss utrustning, såsom krypto eller specifik mjukvara för säker anslutning, endast får användas om den godkänts av ett s.k. säkerhetskontor (DISS/ISO). Godkännandet är automatiskt applicerbart också på utrustning som har godkänts av NBV. Sådan utrustning är föremål för en evaluering av NBV. Byråns godkännande gäller i princip för staten. Det automatiska godkännandet av säkerhetskontoret innebär att utrustningen också kan användas utanför staten med hänsyn till ett hemligt avtal av försvarsdepartementet. En lista över utrustning godkänd av NBV finns tillgänglig på nätet. Säkerhetskontors godkännande gäller också automatiskt för utrustning som har godkänts av försvarsdepartementets säkerhetsmyndighet. Säkerhetskontoret kan också godkänna utrustning själv.

[65] Detta följer av den nederländska förordningen nr 2350225/01 *om inrättandet av arbetsgruppen för särskild informationssäkerhe*t (*Instellingsregeling WBI*, 2005-06-27).

9.6 Tyskland

Aktörer inom informations- och cybersäkerhet

BSI – federal byrå för informationssäkerhet

I Tyskland har den federala byrån för informationssäkerhet, *Bundesamt für Sicherheit in der Informationstechnik* (BSI), till uppgift att på nationell nivå främja säkerhet inom it och försvara mot cybersäkerhetshot. BSI är även det nationella certifieringsorganet för federal it-säkerhet.[66] Byrån är underordnad det federala inrikesministeriet, *das Bundesministerium des Innern*, och ska informera ministeriet om sin verksamhet. Uppgifterna inbegriper bl.a.

– testning och evaluering av säkerheten i it-system,
– utfärdande av säkerhetscertifikat,
– drift av krypto- och säkerhetshanteringssystem för federala informationssäkerhetssystem som används inom statlig säkerhet (eller andra av myndigheten särskilt utpekade områden),
– rådgivning om och genomförande av tekniska tester för att skydda viss officiellt hemlig information mot obehörig åtkomst,
– utveckling av säkerhetskrav för federal it och lämplighetskrav på entreprenörer inom it-området med speciella skyddsbehov, och
– tillhandahållande av it-säkerhetsprodukter och stöd till federala myndigheter som ansvarar för it-säkerhet.

För att fullgöra sina uppgifter kan BSI bl.a. rekommendera säkerhetsåtgärder och användning av vissa säkerhetsprodukter. BSI kan vidare fastställa minimistandarder avseende säkerhetskrav för att säkra federal it.[67] BSI tillhandahåller även tekniska riktlinjer och specifikationer som används av de federala myndigheterna som en ram för utveckling av krav på entreprenörer och it-produkter vid upphandling.[68] I nationell rätt kan föreskrivas att federala myndigheter är skyldiga att införskaffa it-säkerhetsprodukter av BSI. Som certifieringsorgan har BSI även att erkänna, bedöma och utbilda evalueringsföretag.

[66] Vid BSI finns bl.a. funktionerna *CERT-Bund* och *Nationales IT-Lagezentrum*.
[67] Beträffande framtagandet av minimistandarder för it-säkerhet i vissa sektorer, se nedan.
[68] BSI bör involveras i ett tidigt skede i större federala digitaliseringsprojekt.

BSI får dock inte utfärda någon säkerhetscertifiering om det finns motstridande tvingande allmänna intressen, särskilt avseende nationella säkerhetsangelägenheter.[69]

Om it-säkerhetsbrister upptäcks kan BSI, i samråd med behöriga tillsynsmyndigheter[70], beordra utövare av kritisk verksamhet att åtgärda bristerna.[71]

Allians för cybersäkerhet

Allianz für Cyber-Sicherheit grundades 2012 och ger nationella myndigheter, företag och föreningar en samarbetsplattform genom vilken information om aktuella hot och praktiska cybersäkerhetsåtgärder kan utbytas. Deltagarna drar nytta av kunskapen och de många engagerade partnerna och kan därmed förbättra skyddet av sin egen it-infrastruktur. Som medlem kan man även få tillgång till BSI:s expertis på området.

ZITiS – centralkontor för it i säkerhetssektorn

I syfte att kontinuerligt utveckla säkerhetsmyndigheternas tekniska färdigheter och förhindra skada till följd av cyberaktivitet inrättades under det federala inrikesministeriet ett kontor för it i säkerhetssektorn, *Zentrale Stelle für Informationstechnik im Sicherheitsbereich* (ZITiS). ZITiS är en del av Tysklands cybersäkerhetsstrategi (se nedan). Kontoret tillhandahåller på detta område tjänster till säkerhetsmyndigheterna i Tyskland. ZITiS uppgifter utgår från de nationella säkerhetsmyndigheternas behov. Uppgifterna inbegriper bl.a. telekommunikationsövervakning, analys av krypto och stordata samt tekniska frågor om säkerhet. Också kvalitetssäkring av de produkter som används ingår i tjänsterna. Kontoret bidrar med rådgivning och support

[69] Se lagen om BSI: *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik* (BSI-Gesetz – BSIG).
[70] T.ex. utövar den federala myndigheten *Bundesnetzagentur* tillsyn över områdena elektricitet, gas, telekommunikation, post och järnväg.
[71] Enligt konstitutionell lag har den federala regeringen ingen behörighet att anta regler beträffande organisationen och funktionen av de offentliga tjänster eller funktioner som tillhandahålls av federala stater, utan den behöriga myndigheten på nationell nivå är BSI. Det är BSI som ansvarar för att förebygga och bedöma cyberhot samt utgör den primära tillsynsmyndigheten för IKT-system i kritisk infrastruktur.

men har inga befogenheter att ingripa och är inte någon upphandlingsorganisation.

Sektorsmyndigheter

I specifika sektorer, t.ex. banksektorn, kan den behöriga sektorsmyndigheten fastställa minimistandarder för it-säkerhet.

Övergripande reglering av informations- och cybersäkerhet

Nationell cybersäkerhetsstrategi

2016 antog Tyskland en uppdaterad nationell cybersäkerhetsstrategi[72] som tillhandahåller ett strategiskt ramverk för federal cybersäkerhetsverksamhet. Strategin uppmärksammar bl.a. behovet av att såväl statliga institutioner samarbetar för att säkerställa cybersäkerhet som att regeringen arbetar tillsammans med industrin.

Att staten har egna säkra informationssystem framhålls som särskilt angeläget. Inrättandet av ZITiS är en del av strategin. Att riskanalyser görs och säkra system används, genom tillämpning av lämpliga säkerhetsprodukter och standarder, är vägledande principer enligt strategin. Det ska ske återkommande utvärderingar av strategin som syftar till att hålla det rättsliga ramverket uppdaterat i förhållande till den snabba tekniska utvecklingen.

Reglering och certifiering av it-säkerhet

BSI:s övergripande uppgifter och befogenheter regleras i en särskild lag, den s.k. BSI-lagen.[73] It-säkerhet hos kritiska infrastrukturer behandlas särskilt. Verksamhetsutövare i samhällsviktiga sektorer åläggs vissa skyldigheter i lagen, såsom att vidta lämpliga och proportionella säkerhetsåtgärder för sina it-system, -komponenter eller -pro-

[72] Se www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-certifiering forgermany. Den föregående cybersäkerhetsstrategin var från 2011.
[73] Genom en lag för att öka säkerheten för it-system (*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*) från 2015 har införts diverse ändringar av it-säkerhetsregleringar i sektorslagar för kritisk infrastruktur samt befintlig lag om BSI så att byråns uppgifter och befogenheter utvidgats.

cesser samt att rapportera cybersäkerhetsincidenter till BSI. Certifiering är ett sätt som verksamhetsutövarna kan visa på överensstämmelse med säkerhetskraven. Ingen särskild certifieringsordning eller godkännandeförfarande krävs enligt lag. Överträdelser av skyldigheterna i fråga om it-säkerhet[74] och rapportering kan föranleda administrativa sanktioner.

Genom *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*, som är en lag om it-säkerhet, har den tyska lagstiftaren föreskrivit obligatoriska åtgärder för att uppnå en enhetlig nivå av säkerhet i nätverk och informationssystem inom vissa kritiska infrastrukturer. I lagen har införts bestämmelserna om kritisk infrastruktur i BSI-lagen som till stor del är i överensstämmelse med säkerhetskraven i NIS-direktivet.[75]

BSI får utfärda cybersäkerhetscertifikat efter att överensstämmelse med uppställda krav bedömts. När BSI gör sin granskning kan den använda sig av en kvalificerad oberoende tredje part.[76] Utfärdandet av certifikat förutsätter att det federala inrikesministeriet bestämt att certifikatutfärdande inte skulle strida mot tvingande allmänna intressen, i synnerhet nationella säkerhetsangelägenheter.

I enlighet med förordningen om utfärdande av säkerhetscertifikat och erkännanden av BSI, *BSI-Zertifizierungs- und -Anerkennungsverordnung – BSIZertV*, fastställer BSI förfaranden för certifiering av it-produkter, -komponenter, -system och skyddsprofiler vad gäller testkriterier, krav på utrustning och tillförlitlighet.[77] Regleringen ger även BSI i uppdrag att erkänna och kontrollera behöriga expertorgan.[78]

[74] Det är obligatoriskt att åtgärda it-säkerhetsbrister.
[75] I den utsträckning som kraven i NIS-direktivet inte redan fastställdes i it-säkerhetslagen ändrades BSI-lagen i enlighet med detta 2017. En andra version av it-säkerhetslagen håller på att utarbetas. Den nya lagen strävar efter att hålla jämna steg med den tekniska utvecklingen och stärka den rättliga ramen inom tre området: (1) skydd av kritisk infrastruktur i den privata sektorn inklusive kritiska komponenter och företag av särskilt allmänintresse, (2) konsumentskydd, och (3) skydd av federala it-system.
[76] BSI kan i sammanhanget definiera krav för hur säkerhetsgranskning och certifiering ska implementeras och vilka bevis som behöver tillhandahållas.
[77] BSI ska som utgångspunkt publicera listor över certifierade it-system, -produkter och -komponenter samt skyddsprofiler på internet. Sökande underkastar sig ett flertal skyldigheter att bistå och tillmötesgå BSI. BSI kan när som helst kontrollera om vissa krav för certifiering är uppfyllda.
[78] *Die Deutsche Akkreditierungsstelle GmbH* (DAkkS) är det nationella ackrediteringsorganet i Tyskland i enlighet med förordningen (EG) nr 765/2008 *om krav för ackreditering*.

Riktlinjer för federal cybersäkerhet

Regimen för cybersäkerhet inom den federala administrationen fastställs i *Umsetzungsplan Bund*-riktlinjerna. Dessa är endast bindande för den federala administrationen och föreskriver att ett informationssäkerhetshanteringssystem (ISMS) måste implementeras och underhållas i enlighet med *BSI IT-Grundschutz*.

Statliga myndigheter kan certifieras enligt ISO 27001 på grundval av *BSI IT-Grundschutz*. Certifikatet bekräftar då att it-säkerhetskonceptet uppfyller kraven i ISO 27001.

Särskilda krav på IKT i säkerhetskänslig verksamhet

Allmänt om it-system som behandlar klassificerad information

En förutsättning för användning av it-system för klassificerad information är ett informationssäkerhetskoncept i enlighet med standarderna för *BSI IT-Grundschutz*, som it-säkerhetsansvariga ansvarar för. Dessutom finns krav på sekretesskydd som går utöver det grundläggande it-skyddet och som ska definieras av säkerhetschefer enligt *VSA Bund*.

Certifiering enligt tekniska riktlinjer

Utöver certifieringen av it-produkter och -system med avseende på deras säkerhetsfunktioner tillhandahåller BSI även tjänsten att certifiera enligt tekniska riktlinjer avseende särskilda funktionskrav. En certifiering enligt tekniska riktlinjer krävs om implementeringen av särskilda funktionskrav är avgörande för driften av en it-produkt eller ett it-system. Detta gäller i synnerhet it-produkter eller -system som är avsedda att sättas in i säkerhetskänsliga domäner i Tyskland. Stor vikt läggs här vid krav som rör elektronisk manipulationsresistens, driftsäkerhet och interoperabilitet.[79]

Befintliga tekniska riktlinjer gäller för bl.a. smartkortläsare, lagring av kryptografiskt signerade dokument och kommunikations-

[79] Tekniska riktlinjer som specificerar dessa krav har utvecklats och släppts av BSI i nära samarbete med industrin.

processer[80] för officiella dokument. Nya tekniska riktlinjer utvecklas för att möta krav på nationell säkerhet eller för att tillgodose vissa behov av allmänt intresse.

Tillverkare och distributörer kan ansöka om certifiering enligt tekniska riktlinjer och få en bedömning av överensstämmelse av sina it-produkter eller -system utfärdad av BSI. Vid certifieringsförfarandet genomgår it-produkten eller -systemet en oberoende evaluering av överensstämmelse baserat på de testspecifikationer som definieras i den tekniska riktlinjen. Evalueringen av överensstämmelse sker under överinseende av BSI. Efter framgångsrik bedömning av överensstämmelse utfärdar BSI ett certifikat för it-produkten eller -systemet.

Allmänna administrativa instruktioner för skyddet av klassificerat material

2006 utfärdade det federala inrikesministeriet *Verschlusssachenanweisung – VSA Bund*[81] som är allmänna administrativa instruktioner för det fysiska och organisatoriska skyddet av klassificerat material[82]. Instruktionerna riktar sig till statliga organisationer som arbetar med klassificerat material[83] och därmed måste vidta försiktighetsåtgärder för att skydda det. Instruktionerna anger att vissa åtgärder för it-säkerhet ska vidtas. Enligt instruktionerna ska ”State-of-the-art”-åtgärder vidtas för att skydda klassificerat material mot risk för förlust av konfidentialitet, tillgänglighet eller integritet.[84] Klassificerat material får endast bearbetas på it-system som är begränsade till att an-

[80] Kommunikationsmodellen som beskrivs i *BSI-TR-03132* gäller för kommunikation mellan myndigheter och skapare av dokument. En del av kommunikationen kräver certifikat. Kryptering är också en säkerhetsåtgärd som måste vidtas för vissa meddelandetyper. Utöver denna tekniska riktlinje finns en tillhörande testspecifikation som definierar testkrav för att bestämma riktigheten av genomförandet av kraven som anges i den tekniska riktlinjen.

[81] *Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen*.

[82] Klassificerat material avser information, föremål eller fakta som i allmänhetens intresse måste hållas hemliga, i synnerhet för att skydda den federala regeringens eller en federal stats välfärd, oavsett i vilken form materialet presenteras. Affärs-, drifts-, uppfinnings-, skatte- eller andra privata hemligheter eller omständigheter i den personliga sfären kan också vara föremål för sekretess i allmänhetens intresse enligt *VSA Bund*.

[83] Med klassificerat material avses alla uppgifter och föremål som behöver hållas hemliga i allmänhetens intresse, oavsett form.

[84] Departement som använder it för att bearbeta klassificerat material ska tillsätta it-specialister med ansvar för informationssäkerheten. Bara personer med vederbörligt godkännande får arbeta med klassificerat material. Behovet av godkännande för militära säkerhetsändamål ska bestämmas av det federala försvarsministeriet. Se även lagen *Sicherheitsüberprüfung* om säkerhetskontroll och -godkännande av personer som ska utöva säkerhetskänslig verksamhet, där *Bundesamt für Verfassungsschutz* utför kontroll på uppdrag av anställande myndighet.

vända hård- och mjukvara som godkänts av chefer på myndigheten. Vidare kräver säkerhetsrelaterade ändringar av auktoriserade it-system förhandsgodkännande av berörda säkerhetsansvariga. Tekniska medel för att skydda klassificerat material måste inspekteras av BSI och bedömas lämpliga. It-system som ska behandla klassificerat material måste inspekteras av säkerhetsansvariga före användning. När det gäller undersökningen av om nödvändiga säkerhetsåtgärder vidtagits för komplexa it-system bör BSI konsulteras.

BSI ska hjälpa till med genomförandet av instruktionerna.[85] Bl.a. ska BSI bedöma lämpligheten av tekniska medel som ska skydda klassificerat material.

BSI ska vidare godkänna produkter med säkerhetsfunktioner för it, bl.a. produktion av nyckelmaterial, kryptering och nätseparation som ska användas till klassificerat material måste ha godkänts av.[86] Godkännandet måste också innehålla nödvändiga specifikationer angående användnings- och driftsvillkor. Produkter som har funktioner för kontroll av systemåtkomst, produktion av klassificerat material, loggning, förebyggande av manipulering av it-system, eller registrering – och som används för material som klassificeras som konfidentiellt – *bör* ha godkänts av BSI. Myndighetschefer kan tillåta användning av andra produkter, särskilt om inga lämpliga godkända produkter finns tillgängliga och det inte är möjligt att få några sådana i tid. Sådana andra produkter inkluderar särskilt produkter som certifierats av BSI i enlighet med *Common Criteria*, med användning av nationella skyddsprofiler. Tills nationella skyddsprofiler blir tillgängliga kan andra BSI-certifierade produkter också användas.[87]

Godkännanden ska rangordnas efter behovet av skydd för it-applikationer för klassificerat material, på grundval av allmänt vedertagna säkerhetskriterier och förfaranden, som ska kompletteras med särskilda attackskyddstester när det är nödvändigt. Ytterligare detaljer ska anges av BSI i en s.k. godkännandeplan som ska godkännas av federala inrikesministeriet.

Om it-system ska användas för hemligt material måste säkerhetsansvariga låta BSI utföra vissa tekniska tester av it-systemet för

[85] Hjälpen inkluderar teknisk testning och utbildning. BSI kan anlita tjänster från andra organ för stöd i detta arbete, men om privata organ ska vara inblandade krävs förhandsgodkännande av det federala inrikesministeriet. Inom försvarsministeriets område ska dessa uppgifter utföras av den militära underrättelsetjänsten *MAD* i samarbete med BSI.
[86] För begränsat hemligt material avser kraven bara kryptering.
[87] Vid valet av alternativa produkter ska BSI:s upphandlingsguide användas.

att se om nödvändiga it-säkerhetsfunktioner implementerats korrekt. När nätverksbaserade it-system används för klassificerat material kan även säkerhetsansvariga behöva genomföra ett penetrationstest.

9.7 Frankrike

Aktörer inom informations- och cybersäkerhet

ANSSI – nationell cybersäkerhetsmyndighet

Agence nationale de la sécurité des systèmes d'information (ANSSI) är den nationella myndigheten för cyberförsvar och nätverks- och informationssäkerhet. ANSSI är vidare behörig myndighet för skyddsvärda informationssystem. Myndigheten rapporterar till generalsekreteraren för försvar och nationell säkerhet (Secrétariat général de la défense et de la sécurité nationale, SGDSN).[88] ANSSI fastställer tekniska och organisatoriska cybersäkerhetsregler för samhällsviktiga sektorer och godkänner aktörer som ska utöva verksamhet i dessa sektorer. ANSSI:s godkännande är även nödvändigt när det gäller vissa produkter och system med säkerhetsfunktioner som ska användas i verksamhet som avser nationell säkerhet (se nedan).[89]

Vid ANSSI finns ett certifieringsorgan som utfärdar certifikat för it-produkter och föreskriver metoder och evalueringskriterier. Vidare behöver evalueringsföretag licensieras av ANSSI. ANSSI prövar sedan att evalueringsföretagen upprätthåller kompetensen i förhållande till dess licens.[90]

[88] På nationell nivå har generalsekreteraren för försvar och nationell säkerhet, SGDSN, å premiärministerns vägnar ansvaret för att styra den nationella politiken för säkerheten hos informationssystem, inbegripet definiering och koordinering av policy gällande skydd för klassificerad information. För att göra detta är SGDSN beroende av ANSSI.

[89] ANSSI ger vidare säkerhetsrekommendationer i fråga om tillhandahållare av kvalificerade betrodda tjänster. Kvalificering av en tjänsteleverantör intygar att denne uppfyller kraven från ANSSI på kompetens och i standarder. Det finns bl.a. kvalificerade granskare av säkerhet i informationssystem (PASSI).

[90] ANSSI har tagit fram en vägledning för certifieringsprocessen och en guide för utarbetandet av en säkerhetspolicy för informationssystem (PSSI Guide). Målet med PSSI-guiden är att ge support till informationssystemens säkerhetschefer för att utveckla en it-säkerhetspolicy inom sina organisationer. Den fokuserar på 16 domäner inom cybersäkerhet, särskilt informationssystem, säkerhetsriskhantering, assurans och certifiering, incidenthantering samt planering av företagskontinuitet. ANSSI anger även detaljerade regler för säkerheten hos informationssystem i små och medelstora företag i sin guide om god it-praxis, *Guide des bonnes pratiques de l'informatique*.

AQSSI – Kvalificerade myndigheter för säkerhet i informationssystem

På lokal nivå finns en organisation, *Autorité qualifiée pour la sécurité des systèmes* (AQSSI), med ansvar för informationssystemsäkerhet i förvaltning, offentliga anläggningar och decentraliserade tjänster. Chefen för organisationen ska definiera en säkerhetspolicy för informationssystem och säkerhetsställa genomförandet av gällande reglering. AQSSI ska också utse s.k. godkännandemyndigheter för berörda system (se nedan).

CESTI – evalueringscenter

Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI) utför oberoende och opartiska evalueringar vid certifieringsprocesser enligt *Common Criteria* och/eller den nationella ordningen för grundläggande säkerhetscertifiering av it-produkter (CSPN). Evalueringscentret är godkänt av ANSSI.

Övergripande reglering av informations- och cybersäkerhet

Nationell strategi och informationssystem

Frankrike har antagit en nationell cybersäkerhetsstrategi som gäller sedan 2015[91] – och i samband med det har man framhållit vikten av att prioritera införlivandet av cybersäkerhet i kritisk infrastruktur, s.k. skydd av kritisk informationsinfrastruktur (CIIP).

Alla informationssystem i statlig förvaltning omfattas av särskilda säkerhetskrav (se nedan). Behovet av att använda produkter och tjänster som är kvalificerade enligt ANSSI samt att skydda myndigheternas mest känsliga uppgifter på det nationella territoriet är framträdande i det nationella systemet.

ANSSI har länge rekommenderat en process för säkerhetsgodkännande av informationssystem för att bygga förtroende för systemen och deras framtida drift. Som utgångspunkt är det dock chefen för den berörda organisationen som ska fatta beslutet om godkännande.

[91] Se www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/information-systems-defence-and-security-frances-strategy.

Nationell certifieringsordning

Certification de Sécurité de Premier Niveau (CSPN) är en nationell certifieringsordning för säkerhetscertifiering av it-produkter på grundläggande nivå, som tagits fram, ägs och drivs av ANSSI, där evaluering ska utföras av en oberoende tredje part licensierad av ANSSI.[92] Certifieringsordningen avser att uppfylla kraven i artikel 54 i EU:s cybersäkerhetsakt (om minimikomponenter) och är redan delvis kompatibel med akten. Syftet med evaluering och certifiering enligt ordningen är att bedöma en produkts motståndskraft mot en måttlig nivå av angrepp. ANSSI är certifieringsorgan och utfärdar nationellt giltiga certifikat.

Riktlinjer för grundskydd av myndigheters it-system

Référentiel Général de Sécurité (RGS) är riktlinjer som tillhandahålls av ANSSI, avser ett grundskydd[93] som gäller för it-system som används av administrativa myndigheter. Myndigheterna är skyldiga att säkerställa säkerheten hos sitt elektroniska datautbyte och sin kommunikation. Här är dataskydd en viktig aspekt.

Industriella informations- och styrsystem

ANSSI har tagit fram ett dokument med rekommendationer och direktiv till stöd för ökad cybersäkerhet i industriella informations- och styrsystem där certifiering och godkännandeprocesser är återkommande inslag.[94] Bl.a. ska vissa tjänster[95], produkter[96], metoder och personer[97] vara certifierade.

[92] Även verksamhetsutövare omfattas av certifieringsordningen. Ordningen tillåter för övrigt inte självbedömning.
[93] Lägsta rekommenderade skyddsnivå för informationssystem och organisation.
[94] *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI), (2014): *Cybersecurity for Industrial Control Systems. Detailed measures*. Paris.
[95] T.ex. riskanalys av verksamheten, cybersäkerhetsträning och säkerhetsgranskning.
[96] T.ex. datadioder samt enheter som används i trådlösa nätverk.
[97] Fysisk tillgång till enheter på plats ska förbehållas certifierad personal.

IKT i säkerhetskänslig verksamhet

Skyddsvärd information i system

Alla informationssystem som hanterar säkerhetsklassificerad information ska godkännas så att systemet är kvalificerat att hantera sådana uppgifter i enlighet med eftersträvade säkerhetsmål och återstående säkerhetsrisker accepteras. Sådana informationssystem ska godkännas av en s.k. godkännandemyndighet. Om informationssystemet behandlar information som klassificerats som kvalificerat hemlig är SGDSN godkännandemyndighet.[98] Dessutom måste säkerhetsfunktionerna för dessa system godkännas av ANSSI.[99] Godkännandebeslut måste som utgångspunkt fattas innan informationssystemet tas i drift (”l’homologation du système”).[100] Det ovan anförda följer av *Instruction générale interministérielle n°1300* (IGI 1300) – en instruktion som bl.a. fastställer regler för skydd av information som rör nationella försvarshemligheter. Instruktionen anger villkor för att hantera känsliga och klassificerade uppgifter och säkerställa deras skydd. Instruktionen uppställer organisatoriska, tekniska och kontraktuella villkor för att säkerställa tillräcklig tillförlitlighet. T.ex. måste varje entitet som hanterar skyddsvärd information definiera roller och ansvar enligt instruktionen och berörda informationssystem ska ackrediteras på lämplig nivå av behörig myndighet före bearbetning av klassificerad information. ANSSI har deltagit i utarbetandet av instruktionen genom att definiera regler för att skydda informationen när den behandlas i informationssystem.[101]

---

[98] Godkännandeorgan för berörda system utses annars av berörd AQSSI i de fall systemet tillhör en organisation eller enhet under ledning av en minister. Det kan vara den kvalificerade myndigheten. När SGDSN ska godkänna systemet är ANSSI medlem i godkännandekommittén. När informationssystemet tillhör en privat organisation ligger godkännandeauktoritetens ansvar hos det eller de organ som berörs av systemet.

[99] Godkända säkerhetsanordningar i informationssystemen syftar till att skydda mot obehörig åtkomst. Godkännande begärs vanligtvis av den myndighet som ansvarar för utvecklingen eller användningen av systemet. Intyg om godkännande av förmågan att skydda relevant information utfärdas efter en säkerhetsevaluering av licensierade laboratorier. Ett tillstånd kan återkallas före giltighetstidens utgång beroende på utvecklingen av hot eller upptäckten av sårbarheter.

[100] Godkännandebeslutet gäller för en period om maximalt fem år för ett informationssystem på konfidentiell säkerhetsnivå respektive två år på hemlig eller kvalificerat hemlig nivå. Godkännandemyndigheten fastställer villkoren för att upprätthålla säkerhetsgodkännande för informationssystemet.

[101] Skyddsmärket ”Diffusion restreinte” kan användas när avslöjande av information sannolikt skulle påverka suveräna intressen. Används känsliga informationssystem, eller *Diffusion restreinte*-märkta system, måste använda betrodda säkerhetsprodukter. I det senare fallet ska använda säkerhetsprodukter vara godkända på rätt nivå, kvalificerade eller certifierade av ANSSI.

Ett säkerhetsgodkännande innebär ett formellt erkännande att den bedömda säkerhetsprodukten kan skydda information upp till angiven nivå eller att bedömt informationssystem kan bearbeta information på en viss klassificeringsnivå i enlighet med säkerhetsmålen och att återstående säkerhetsrisker accepteras. Den ansvarige organisationen intygar således, efter riskbedömning, att skyddet av informationen och systemet säkerställs till önskad nivå.

Kritiska informationssystem

Utöver vad som krävs av EU-lagstiftningen är operatörer av s.k. kritiska informationssystem skyldiga enligt en fransk lag om militär planering, *Les Lois de Programmation Militaire*, att skydda sina informationssystem genom cyberresiliens. Här har ANSSI en stor roll när det gäller att bidra med stöd till verksamhetsutövarna, förebygga cyberattacker och samla rapporter. Vidare kan certifiering vara av vikt för verksamhetsutövarna i de samhällsviktiga sektorerna.

La loi n°2018-607 relative à la programmation militaire pour les années 2019–2025 är en lag som rör militär programmering och innehåller bestämmelser om förstärkning av kapaciteten att detektera, karaktärisera och förhindra cyberattacker för att höja nationens säkerhet (se artikel 34). Samtidigt stärks mandatet för ANSSI att agera mot händelser som kan påverka nationell säkerhet och organisationers informationssystem. Om en attack rör kritisk infrastruktur kan ANSSI, tillsammans med den angripne, fastställa lämpliga skyddsåtgärder.

Systèmes d'information d'importance vitale är en särskild CIIP-lag som fastställer gemensamma minimikrav för cybersäkerhet hos kritiska verksamhetsutövare. Det rör sig om infrastrukturer som anses behöva särskilt skydd. Lagens säkerhetskrav gäller för såväl offentliga som privata verksamhetsutövares mest kritiska informationssystem.[102] Verksamhetsutövarna är bl.a. skyldiga att meddela ANSSI om incidenter som inträffar i deras kritiska informationssystem. En noggrann evalueringsprocess, framtagen av ANSSI, möjliggör kvalifi-

[102] ANSSI har upprättat tekniska och organisatoriska regler som är sektorsöverskridande och huvudsakligen består av grundläggande cybersäkerhetsåtgärder, inbegripet bl.a. nätverksmappning, nätverkssegmentering, implementering av tillförlitliga detekteringsfunktioner och ackreditering. Bortom säkerhetskraven bidrar ramverket till att bygga nationens motståndskraft.

cering av kandiderande cybersäkerhetsleverantörer[103] och produkter som uppfyller tillräckliga säkerhetskrav.[104]

Pågående reform av regelverket

Frankrike genomför för närvarande en reform av sina föreskrifter om skyddet av nationell säkerhet. Den nya regleringen ska träda i kraft den 1 juli 2021 och bygger huvudsakligen på dekret nr 2019-1271 om metoder för klassificering och skydd av nationella försvarshemligheter[105] samt IGI 1300.

Övriga kontroller av IKT

Frankrike tillämpar kontroller för export av programvara och hårdvara för informationssäkerhet, inklusive kryptering. Dessutom kontrollerar Frankrike leverans och import av kryptering till Frankrike.

Instruction interministérielle n°901 definierar särskilda regler för skydd av känsliga informationssystem, särskilt de som hanterar information märkt ”Restricted”, mot alla typer av hot. Målet med instruktionen är säkerställa kontinuitet hos verksamheter och förhindra att känslig information röjs.

En allmän bestämmelse i försvarskoden, *Code de la Défense*, tillåter franska myndigheter som står inför ett hot, mot t.ex. dess nationella intressen, att vidta alla tekniska åtgärder som anses nödvändiga för att tillskriva eller mildra en attack genom att få tillgång till information. Frankrike kräver också godkännande av utländska investeringar i känsliga sektorer som är avgörande för Frankrikes nationella intresse.

[103] Leverantörer kan t.ex. kvalificeras för tjänster inom säkerhetsgranskningar.
[104] Berörda organ ackrediteras av den franska ackrediteringskommittén COFRAC och licensieras av ANSSI.
[105] *Décret n° 2019-1271 du 2 décembre 2019 relatif aux modalités de classification et de protection du secret de la défense nationale*.

Sammanfattning av särskilda krav på IKT i säkerhetskänslig verksamhet

Av inhämtade uppgifter framgår att det finns centrala myndigheter i Frankrike med ansvar för nationell informations- och cybersäkerhet och IKT-evaluering och -godkännande av informationssystem och dess säkerhetsfunktioner där behandlad information är av betydelse för nationell säkerhet. När det gäller informationssystem som behandlar information som klassificerats som kvalificerat hemlig ska generalsekreteraren för försvar och nationell säkerhet (SGDSN) godkänna systemet. Några nationella krav på certifiering av sådana system har dock inte framkommit.

9.8 Storbritannien

Aktörer inom informations- och cybersäkerhet

GCHQ – underrättelse- och säkerhetstjänst

Government Communications Headquarters (GCHQ) är en underrättelse- och säkerhetstjänst som har till uppgift att skydda Storbritannien och dess medborgare från individer, grupper och länder som vill orsaka skada. Det finns bl.a. nationella krav på att GCHQ ska säkra (”assure”) kryptoutrustning som ska användas i säkerhetskänslig verksamhet. Vid GCHQ finns det nationella cybersäkerhetscentret (se nedan).

Nationellt cybersäkerhetscenter

Det nationella cybersäkerhetscentret, *National Cyber Security Centre* (NCSC), besitter expertkunskap om cybersäkerhet samt tillhandahåller råd för offentlig och privat sektor. NCSC är en del av GCHQ och svarar för informationssäkerheten.[106] Centret utgör landets tekniska myndighet för cyberhot.[107] Centrets uppgifter är bl.a. att motverka cyberbrott och svara på cybersäkerhetsincidenter och säkra nätverk för att minimera skador i samhället. Kritiska samhällssektorer

[106] Ytterst är det premiärministern och kabinettet som är ansvariga för regeringens säkerhet.
[107] I Storbritannien kategoriseras cyberhot som ett ”tier 1 threat”. Under 2011 uppskattade den brittiska regeringen, i sin rapport, Detica, Cabinet Office (2011): *The cost of cyber crime*, att nationen förlorade 27 miljarder pund årligen på grund av brist på cybersäkerhet.

är ett fokusområde. Centret erbjuder vidare certifiering som täcker en rad produkter, tjänster och organisationer – även på assuransnivån hög (främst kryptografiska produkter).[108] Som certifieringsorgan har centret också till uppgift att godkänna evalueringsföretag.

I fråga om utveckling av produkter som hanterar särskilt känslig information, t.ex. information som klassificeras som hemlig eller kvalificerat hemlig, rekommenderar emellertid centret att utvecklaren söker ytterligare specialistsråd om de särskilda hot som behöver beaktas i sammanhanget.

CERT-UK

Ansvaret för hantering av IKT-incidenter i Storbritannien har på nationell nivå tilldelats CERT-UK. CERT-UK grundades 2014 och var en viktig investering som en uppföljning av den nationella cybersäkerhetsstrategin (se nedan). CERT-UK fokuserar på att ha en uppdaterad lägesbild, incidenthantering på nationell nivå samt stödja verksamheter med samhällskritisk infrastruktur.

Reglering av informations- och cybersäkerhet

Nationell cybersäkerhetsstrategi

Storbritannien antog en nationell cybersäkerhetsstrategi 2016 som utvärderas kontinuerligt för att hålla det rättsliga ramverket uppdaterat i förhållande till den tekniska utvecklingen.[109] Ett mål med strategin är att fördjupa det internationella samarbetet på området. Strategin identifierar också ett behov av utvidgat nationellt samarbete mellan regeringen och privat respektive offentlig sektor för ökat säkerhetsmedvetande kring internet. Storbritannien lägger stort vikt vid att förbättra cybersäkerheten genom att upprätta informa-

[108] För vissa hotmodeller och teknologier genomför centret oberoende utvärderingar av produkter (främst kryptografiska produkter) som kräver ett certifikat från centret på nivå hög. Bedömningen görs i enlighet med en viss assuransordning innehållande detaljerade krav som härstammar från vissa principer avseende hög assurans: produkter ska komma från betrodda leverantörer med bevisad hög kunskap om hotdomänen, utvecklare som följer bästa praxis, produkter med specifika säkerhetsfunktioner med identifierade sårbarheter, oberoende bedömning av anspråkgjord säkerhetsfunktion, avsiktlig drift, och ett betrott läge.
[109] Se www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

tionsdelningsstrukturer och samarbete mellan offentlig och privat sektor.

Även i tidigare nationella strategier har klargjorts att myndigheternas inställning till cybersäkerhet är riskbaserad och att arbetet måste göras i partnerskap med privata aktörer. Man har följaktligen inlett ett gemensamt initiativ mellan myndigheterna och industrin om informationsdelning och samarbete för att möta de digitala hoten, kallat *Cyber-Security Information Sharing Partnership* (CiSP).

Cyberattacker mot kritisk infrastruktur bedöms kunna ha störst inverkan på den nationella säkerheten. Därför är det en strategisk prioritering att vidta åtgärder för att öka cybersäkerheten hos kritisk nationell infrastruktur.

Den nationella cybersäkerhetsstrategin framhåller att kryptografisk kapacitet är grundläggande för att skydda landets mest känsliga information och användningen av nationella säkerhetsfunktioner. För att upprätthålla tillräcklig förmåga kräver man kompetens och teknik från privat sektor som är garanterad av GCHQ.[110]

Storbritannien köper inte produkter eller tjänster ”från hyllan” när det gäller kvalificerat hemliga (”highly classified”) eller känsliga tekniker.[111]

Strategin framhåller att NCSC ska vara en auktoritet när det gäller nationella cybersäkerhetsangelägenheter. Därutöver syftar lanseringen av två nya cyberinnovationscenter till att driva utvecklingen av avancerade cyberprodukter och nya dynamiska cybersäkerhetsföretag.

Det kan konstateras att Storbritannien, i likhet med Tyskland, har organ med mandat vars syfte är att säkerställa kritisk infrastruktur och kritiska samhällsfunktioner, oavsett om detta är civilt eller militärt.

Ramverk för säkerhetspolicy

Den brittiska regeringen har antagit en säkerhetspolicy, *The security policy framework*,[112] som beskriver de standarder, riktlinjer för bästa praxis och metoder som krävs för att skydda nationella statliga till-

[110] Detta bedöms kräva att arbetet utförs i Storbritannien av brittiska medborgare med erforderligt säkerhetsgodkännande. Vidare förväntas berörda företag vara helt öppna med GCHQ när det gäller att diskutera design- och implementeringsdetaljer.
[111] HM Government (2015), *National Security Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom*. London: HM Government.
[112] Cabinet Office, *HMG Security Policy Framework*, version 1.1, maj 2018.

gångar (människor, information och infrastruktur). Policyn fokuserar på de resultat som krävs för att uppnå en proportionerlig och riskhanterad strategi för säkerhet som gör det möjligt för statliga organisationer att fungera effektivt och säkert. Den innehåller också beskrivningar av god förvaltning och stark säkerhetskultur på organisatorisk nivå.

Policyn anger riskhantering på styrelsenivå som en övergripande princip på säkerhetsområdet. Här ska bedömningar göras för att identifiera potentiella hot, sårbarheter och lämpliga kontroller för att minska riskerna till en acceptabel nivå.[113] Bl.a. ska det finnas utbildade specialister som kan analysera hot mot och potentiella skador på verksamheten. Vidare behövs assuransprocesser för att säkerställa att begränsningar är och förblir effektiva.

Informationssäkerhet är ett annat område som policyn behandlar. Personalen i statliga organisationer förutsätts vara utbildade att på ett ansvarsfullt sätt hantera informationen de kommer i kontakt med i sin verksamhet. Det ska också finnas mekanismer och processer som säkerställer att tillgångar är korrekt klassificerade och lämpligt skyddade. Man behöver ha ett förtroende för att säkerhetskontroller (se nedan) är effektiva och att system och tjänster kan skydda den information de har. För denna saks skull ska det ska finnas ett övergripande program för informationsassurans som drivs av styrelsen.

Vidare ska statliga organisationer identifiera om de har teknik och tjänster som avser kritisk nationell infrastruktur och i så fall hantera risker därefter.[114] Policyn föreskriver säkerhetskontroller som

- minskar potentiella hot,
- hanteras aktivt och hålls uppdaterade,
- skyddar mot och korrigerar skadligt beteende, och
- säkerställer att kritisk teknik och kritiska tjänster är motståndskraftiga mot cyberattacker och har möjlighet att återhämta sig från sådana.

[113] En årlig rapporteringsprocess behövs för att säkerställa lämplig riskhantering.
[114] Myndigheter i Storbritannien kräver också att leverantörer som ska behandla känslig information uppfyller givna informationssäkerhetsstandarder.

Cyber Essentials

Cyber Essentials är ett initiativ från NCSC som stöds av den brittiska regeringen och industrin för att ge organisationer en grundläggande nivå av cybersäkerhetskontroller som skydd mot de vanligaste cyberhoten.[115] Det är fråga om en certifieringsordning som täcker grunderna för cybersäkerhet i en organisations verksamhet eller ett företags itsystem och bedöms av regeringen passa alla typer av organisationer. Förutom att stimulera en utbredd användning av grundläggande säkerhetskontroller mot mindre avancerade IKT-incidenter syftar ordningen till att tillhandahålla klarhet när det gäller bästa cybersäkerhetspraxis. Tillsammans med *Cyber Essentials*-systemet har regeringen publicerat *Assurance Framework* som gör det möjligt för organisationer att få certifieringar för att försäkra kunder, investerare, försäkringsbolag och andra att de har vidtagit lämpliga säkerhetsåtgärder för cybersäkerhet. Systemet är som utgångspunkt frivilligt. Andra aktörer än NCSC kan vara certifieringsorgan (om de är ackrediterade). Innehållet i *Cyber Essentials* ska tillämpas av statliga myndigheter vid vissa upphandlingar (se nedan). Övrig offentlig och privat sektor kan välja att tillämpa de förebyggande åtgärderna, också vid affärer med privata tillhandahållare i leverantörskedjan. Även organisationer baserade utomlands kan använda sig av ordningen.

Den brittiska regeringen kräver att leverantörer som bjuder på centrala regeringskontrakt som involverar hantering av känslig och personlig information eller tillhandahållande av vissa IKT-produkter och -tjänster ska erhålla certifiering mot Cyber Essentials-ordningen. Det är därmed obligatoriskt för leverantörerna att visa att de möter de tekniska krav som certifieringsordningen föreskriver. Brandväggar, säker konfiguration, åtkomstkontroll, skydd mot skadlig programvara och patchhantering är tekniska områden som täcks. Kraven aktualiseras när kontrakt medför att

– personlig information om medborgare, statligt anställda eller ministrar hanteras av en leverantör, eller

[115] *Cyber Essentials*-ordningen fokuserar på att tillhandahålla råd och verktyg för att hjälpa företag att förstå och agera på cybersäkerhetshot samt att certifiera vissa typer av cybersäkerhetstjänster och utbildningar. *Cyber Essentials* utvecklades eftersom varken ISO 27001 eller andra tänkbara standarder var tillräckligt åläggande för att motverka vanliga internetbaserade hot.

– IKT-system och -tjänster tillhandahålls för att lagra eller bearbeta data på nivå ”Official” enligt regeringens ordning för skyddsmärkning (Government Protective Marking scheme).

Utöver ovanstående kan *Cyber Essentials* användas från fall till fall vid upphandlingar om den upphandlande myndigheten finner det lämpligt. En sådan användning kräver att en cybersäkerhetsrisk identifieras som inte skulle hanteras av något befintligt säkerhetskrav och där användningen av *Cyber Essentials* är ett relevant och proportionellt alternativ, t.ex. när data finns utanför landet. Avtal kan vara undantagna från kraven om det kan påvisas att användning av *Cyber Essentials* antingen är irrelevant eller klart oproportionerligt, t.ex. där en cybersäkerhetsrisk är bedöms vara mycket låg.

Leverantörer kan även visa på överensstämmelse med de tekniska kraven på andra sätt än genom ett certifikat, såtillvida den avtalsingående myndigheten är nöjd med uppfyllandet av Cyber Essentials-kraven. Normalt sett ska detta verifieras av en tekniskt kompetent och oberoende tredje part. Att skaffa certifikatet anses emellertid oftast vara det enklaste sättet att demonstrera att man uppfyller kraven, även om andra former av bevis är acceptabla.

Företag som ska leverera till försvarsmarknaden förutsätts ha en Cyber Essentials-certifiering. Sådan certifiering krävs för tilldelning av försvarskontrakt som inbegriper överföring av information rörande det brittiska försvarsdepartementet. Certifieringen tilldelas mot bakgrund av en validerad självbedömning som sökanden vidtar och gör att organisationen framstår som en pålitlig och cybersäker aktör inför leverans till försvarssektorn.[116]

Cyber Essentials Plus erbjuder en högre assuransnivå genom extern testning av organisationens cybersäkerhet, där bl.a. sårbarhetstester ska utföras. Vid några upphandlingar med högre risk är det troligt att inte heller *Cyber Essentials Plus* på egen hand kommer ge tillräcklig assurans, och ytterligare, bredare, säkerhetskrav kommer då att specificeras, t.ex. ISO 27000-serien.[117]

[116] Efter att organisationen gjort en självbedömning av sin implementering av kontrolltemana, som är godkänd av en ledande befattningshavare, ska ett oberoende certifieringsorgan utifrån självskattningen bedöma huruvida en lämplig standard nåtts. Därefter kan certifiering tilldelas. Detta alternativ erbjuder en grundläggande nivå av assurans. Åtgärderna är inte utformade för att adressera mer avancerade riktade attacker.

[117] Leverantörer som uppfyller ISO 27001-standarden där *Cyber Essentials* krav, antingen på grundnivå eller Plus-nivå (vid behov), inkluderats i tillämpningsområdet och verifierats som

Minimistandard för cybersäkerhet

Den tekniska standarden *Minimum Cyber Security Standard*[118] är ett dokument som definierar minimiåtgärder för säkerhet som departement och statliga myndigheter ska vidta för att skydda sina it-tjänster. Tillgång till känslig information och viktiga operativa tjänster ska endast ges till identifierade, autentiserade och auktoriserade användare eller system. System som hanterar känslig information ska skyddas från utnyttjande av kända sårbarheter.

Standarden kräver bl.a. att driften av operativsystem och mjukvarupaket ska patchas regelbundet. Vidare ska data krypteras när organisationen inte kan förvänta sig fysiskt skydd av berörd enhet. Det ska också säkerställas att angivna standarder uppfylls av tillhandahållare av tjänster från tredje part. Detta kan uppnås genom att leverantörer försäkrar (”assure”) sin cybersäkerhet mot regeringens cybersäkerhetsstandard, eller genom att kräva att de åtminstone har ett giltigt Cyber Essentials-certifikat.[119]

Standard och vägledning för cybersäkerhet på försvarsområdet

I Storbritannien ska en standard för cybersäkerhet, *Def Stan 05-138*, tillämpas vid upphandlingar av försvarsdepartementet och försvarsleverantörer. Denna standard specificerar de åtgärder som måste vidtas på respektive cyberrisknivå som ett avtal med försvarsdepartementet bedöms innebära.

Försvarsdepartementet uppställer krav beroende på hur cyberriskprofilen ser ut. Krav för en hög cyberriskprofil avser bl.a. upprätthållandet av en Cyber Essentials Plus-certifiering och att ha en policy för att kontrollera användningen av auktoriserad programvara.

sådant, skulle betraktas som innehavare av en motsvarande standard till *Cyber Essentials*. Sådana leverantörer behöver därför inte Cyber Essentials-certifiering, förutsatt att certifieringsorganet som utför denna verifiering är ackrediterat att utfärda ett *Cyber Essentials*-certifikat. Dock behöver de flesta företagen med ISO 27001 anta *Cyber Essentials* som komplement till ISO 27001.

[118] *Minimum Cyber Security Standard*, juni 2018, version 1.0. *The Cabinet Office Government Security Group* (GSG) har utfärdat minimistandarder för bl.a. cybersäkerhet och incidenthantering som definierar säkerhetsåtgärder som departementen måste implementera.

[119] Organisationen får, som en del av sin riskbedömning, själv avgöra om Cyber Essentials ger tillräcklig säkerhet.

CAPS – certifierade assisterade produkter

The National Cyber Security Centre (NCSC), tillsammans med partners, erbjuder certifiering av assisterade produkter, *Certified Assisted Products* (CAPS). CAPS kombinerar NCSC:s kryptografiska kunskap med den privata sektorns expertis och resurser för att påskynda utvecklingen av produkter av hög kvalitet. CAPS är en ordning för evaluering av högkvalitativa produkter som utvecklats av industrin för användning av den brittiska regeringen och andra lämpliga organisationer.

Kryptografiska produkter använder kryptering för att ge säkerhet. Exempel är skiv-, länk- och nätverkskrypterare, säkra radioapparater och åtkomstkontrollenheter. CAPS verifierar också produkter som styr dataflödet mellan domäner med olika klassificeringar. CAPS verifierar att produkter uppfyllt standarderna för den brittiska regeringens policy. Policyn anger godkända standarder som ska tillämpas när kryptering används för att skydda offentlig klassificerad data.

Utvecklare kan införliva lämpliga kryptografiska eller allmänna algoritmer i sina produkter och skicka in dem för evaluering av CAPS. När det väl accepterats, och efter inledande diskussioner mellan NCSC och utvecklaren, ger ett konsult- och rådgivningsavtal företag tillgång till NCSC:s kunskap, kompetens och erfarenhet inom informationsassurans, kompletterat med en rad vägledningsdokumentation innan produkterna går in i fullständig evaluering.

När produkterna slutligen godkänts utfärdas ett certifikat och/eller godkännandebrev som beskriver nivån på det kryptografiska skyddet som erbjuds. Bl.a. kan en förutsättning för tjänsten vara att utvecklaren ackrediterats enligt regeringens ”List X”-ordning[120] (se nedan).

List X – särskilda säkerhetskrav på företag i säkerhetskänslig verksamhet

Tillhandahållare av tjänster och tredjepartsleverantörer som hanterar hemliga tillgångar måste tillämpa lämpliga säkerhetskontroller, inbegripet List X-ackreditering. Omfattas företaget av List X är det skyldigt att vidta vissa säkerhetsåtgärder för övervakningen av lämpliga

[120] List X-entreprenörer är företag som är verksamma i Storbritannien och arbetar med brittiska statliga kontrakt som kräver att de hanterar sekretessbelagd information på nivå hemlig eller högre. Dessa entreprenörer måste uppfylla vissa säkerhetskrav som anges i *Cabinet Office's* dokument *Security Requirements for List X Contractors, april 2014, v. 10.0* (se nedan).

säkerhetsaspekter, bl.a. på organisatorisk nivå och beträffande säkerhetsgodkännande av personal. Vidare kräver t.ex. it-utrustningen lämplig ackreditering, och endast godkänd mjukvara får användas i it-utrustningen.

Sammanfattning av särskilda krav på IKT

Av inhämtade uppgifter framgår att det finns myndigheter i Storbritannien med ansvar för nationell informations- och cybersäkerhet och certifiering av IKT. I fråga om produkter som hanterar hemlig information krävs särskilt utvecklat skydd. På denna nivå används normalt inte vanligen förekommande kommersiella lösningar. Tillgång till känslig information ska endast ges till auktoriserade system.[121] Företag som tillhandahåller vissa IKT-produkter och -tjänster för hantering av känslig officiell information kan behöva certifiering eller motsvarande. Tillhandahållare av tjänster och tredjepartsleverantörer som hanterar hemlig offentlig information måste vidare erhålla ackreditering och använda lämpligt ackrediterad it-utrustning och godkänd mjukvara.

9.9 USA

Aktörer inom informations- och cybersäkerhet

Inledning

I USA är den nationella kapaciteten för IKT-säkerhet spridd över flera aktörer (se nedan), inklusive US-CERT, ett separat ICS CERT (CERT för SCADA-system), en nationell arbetsgrupp för utredning i det digitala rummet (NCIJTF) under FBI:s regi, *US Cyber Command under Department of Defense*, *Intelligence Community Incident Response Center* (IC-IRC), *National Security Agency/ Central Security Services Threat Operations Center* (NTOC), *DoD Defense Cyber Crime Center* (DC3) och det nyetablerade *Cyber Threat Intelligence Integration Center* (CTIIC). Samtidigt är ambitionen att *ICT incident management* ska vara en gemensam insats från dessa aktörer, samordnad genom *National Cyber Security and Communi-*

[121] Huruvida detta innebär att vissa IKT-system behöver godkännas av en utpekad myndighet framstår dock inte som helt klart.

cations Integration Center (NCCIC). NCCIC ska bl.a. ha en uppdaterad situationbild, genomföra IKT-incidenthantering och -kontroll och vara en nationell knutpunkt för de federala myndigheterna, underrättelsetjänsten och polismyndigheterna. US-CERT och ICS-CERT är en integrerad del av NCCIC. Department of Homeland Security (DHS) ansvarar för *National Cyber Incident Response Plan* (NCIRP).

De olika organen i den amerikanska satsningen på IKT-säkerhet illustrerar den mångfacetterade bilden i ett stort land med en komplex organisation. Medan DHS, genom *National Cyber Security and Communications Integration Center* (NCCIC), ska hantera digital risk proaktivt och tillhandahålla informationsdelning om digitala sårbarheter, har *National Cyber Investigative Joint Task Force* (NCIJTF), som består av 19 underrättelsetjänster och brottsbekämpande myndigheter, som mål att säkra internet genom att aktivt jaga hotfulla aktörer.

Inrikes säkerhet och cybersäkerhet

Department of Homeland Security (DHS) har i uppdrag att samordna arbetet med att förhindra katastrofer och hot mot nationen samt att agera till skydd för befolkningen vid sådana händelser. I personalen ingår bl.a. cybersäkerhetsanalytiker.

Cybersecurity and Infrastructure Security Agency (CISA) är en ledande cybersäkerhetsmyndighet på federal nivå. CISA ger råd om riskhantering och utgör kärnan i det kollektiva försvaret mot cyber- och fysiska hot mot landets kritiska infrastruktur. CISA erbjuder, utöver rådgivning, teknisk hjälp och utbildning på informationssäkerhetsområdet. Myndigheten är underställd DHS tillsyn.

National Risk Management Center (NRMC) är inrymt i CISA och arbetar för att identifiera, analysera, prioritera och hantera hot med potentiellt stora konsekvenser för kritisk infrastruktur. NRMC samarbetar med privat sektor och andra viktiga aktörer inom kritisk infrastruktur för att skapa ett informationsutbyte som gynnar säkerhet och resiliens i och mellan samhällsviktiga sektorer.

Övriga federala säkerhetsmyndigheter

Defence Counterintelligence and Security Agency (DCSA) är en federal säkerhetsmyndighet med uppdrag att skydda landets säkerhetskänsliga arbetsplatser och dess personal. Vid myndigheten finns *Center for Development of Security Excellence* (CDSE) som erbjuder säkerhetsprodukter och -tjänster till civil och militär personal inom såväl försvarsdepartementet (*U.S. Department of Defense*, DoD) som den federala regeringen i övrigt samt godkända entreprenörer enligt the *National Industrial Security Program* (NISP, se nedan). Centret utbildar, certifierar, validerar och främjar olika personalkategorier inom nationell säkerhetskänslig verksamhet.[122]

National Security Agency (NSA) är en federal myndighet i USA som lyder under DoD. NSA svarar för landets signalspaning och upprätthåller också säkra (krypterade) kommunikationer för högt uppsatta befattningshavare. NSA driver *National Information Assurance Partnership* (NIAP, se nedan) som är ett amerikanskt regeringsinitiativ för att möta utmaningar med säkerhetstestning bland it-tillverkare och -konsumenter.

Nationellt integrationscenter för cybersäkerhet och kommunikation

National Cybersecurity and Communications Integration Center (NCCIC) är en del av cybersäkerhetsdivisionen hos CISA. NCCIC har till uppgift att säkerställa att relevant information rörande riskbild, incidenter och analyser skyddas och delas. NCCIC delar information mellan offentliga och privata företag och är också ett dygnet runt-center som utgör en kontaktpunkt för federala myndigheter, underrättelsetjänster och polismyndigheterna.

Office of Management and Budget

Office of Management and Budget (OMB) är enligt lag ansvarigt för att övervaka federala myndigheters informationssäkerhets- och sekretesspraxis och för att utveckla och styra genomförandet av policyer och riktlinjer som stöder och upprätthåller dessa metoder. Inom

[122] Certifieringen av personal sker på olika nivåer och områden. Merparten av certifieringsprogrammen ackrediteras av *the National Commission for Certifying Agencies* (NCCA).

OMB delegeras dessa ansvarsområden till *Office of the Federal Chief Information Officer* (OFCIO) som samarbetar med partners inom regeringen för att utveckla cybersäkerhetspolicyer, genomföra data-driven tillsyn över byråns cybersäkerhetsprogram och samordna det federala svaret på cyberincidenter.

OMB arbetar kontinuerligt för att effektivt anpassa befintlig säkerhetspraxis till ett mer modernt teknologilandskap medan standardiseringen bland federala myndigheter ökar.

Nationellt säkerhetsråd

National Security Council (NSC) ansvarar för att koordinera policyinitiativ med presidentens seniora rådgivare samt befattningshavare inom militären och underrättelsetjänsten. Cybersäkerhetsdirektoratet vid NSC ger bl.a. presidenter råd i frågor om cybersäkerhet av betydelse för nationell säkerhet. NSC och OMB samarbetar med federala myndigheter för att implementera administrationens cybersäkerhetsprioriteringar.

Nationellt institut för tekniska standarder

National Institute of Standards and Technology (NIST) är USA:s nationella institut för standarder och teknologi. NIST drivs av USA:s handelsdepartement och dess kärnverksamhet avser utveckling av kritiska mätningslösningar och informationssäkerhetsstandarder. NIST ansvarar för att utveckla riktlinjer, inklusive minimikrav för federala informationssystem. För ackreditering av evalueringsföretag ställer NIST vissa krav på och bedömer personalens kompetens samt anger evalueringskrav för ackreditering. NIST tillhandahåller även verktyg och vägledning för att öka användningen av kryptering.

Kommitté för nationella säkerhetssystem

Committee on National Security Systems, CNSS, är en organisation som på nationell nivå fastställer cybersäkerhetspolicy, direktiv, instruktioner och vägledning för amerikanska departement och myndigheter när det gäller skydd av nationella säkerhetssystem (se nedan).

Tillsyn och ansvar på sektornivå

I USA utövas tillsyn på cybersäkerhetsområdet vanligen sektoriellt. Olika federala departement och myndigheter har ansvar att verka sektorsspecifikt i respektive samhällsviktig sektor. Sektorsmyndigheterna är ansvariga att samarbeta med DHS för att implementera NIPP-regleringen (National Infrastructure Protection Plan), utveckla skyddsprogram, resiliensstrategier och därmed sammanhängande krav, och ge vägledning om skydd av kritisk infrastruktur på sektornivå.[123]

Allmän reglering på cybersäkerhetsområdet

Inledning

De amerikanska myndigheterna har uppgett att cyberhotet är den största nationella säkerhetsutmaningen. USA ser ett tydligt behov av att inkludera alla relevanta aktörer i sitt cybersäkerhetsarbete. Detta återspeglas bl.a. i det faktum att myndigheterna i USA upprättat en s.k. ”whole of government”-strategi för cybersäkerhet (samma strategi som i kampen mot terrorism). I praktiken innebär detta att alla offentliga organ arbetar tillsammans över ansvarslinjer för att uppnå ett gemensamt mål att minska säkerhetsriskerna. Ett sådant tillvägagångssätt ställer höga krav på inrättandet av funktionella samarbetsstrukturer där alla relevanta aktörer deltar.[124] Det kan konstateras att USA lägger särskilt stort fokus på att förbättra cybersäkerheten genom att upprätta informationsdelningsstrukturer och samarbete mellan offentlig och privat sektor. Landet betonar behovet av ökad innovation relaterad till säkerhetslösningar till följd av allt strängare krav på effektivitet och mobilitet.

[123] För övrigt finns inga krav på att ge statliga tjänstemän fysisk tillgång till anläggningar, på att i en nödsituation avstå från kontroll av anläggningar eller på att tillhandahålla källkod eller andra dekrypteringsfunktioner.
[124] Flera länder erkänner att mandat och befogenheter hos myndigheter ofta överlappar varandra och att brist på samarbete och samarbete kan leda till framväxten av ”blinda fläckar”.

Nationell cybersäkerhetsstrategi

2018 antog USA, genom presidenten och försvarsdepartementet, en ny nationella cybersäkerhetsstrategi.[125] Strategin fokuserar på stärkt samarbete, skydd av kritisk infrastruktur och säkrande av offentliga och privata system och information som rör försvaret samt främjandet av en säker digital ekonomi. Strategins mål är att försvara nationen och främja amerikanskt välstånd.

Strategin bygger på och utvecklar arbetet som påbörjats under *Executive Order 13800*, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Den verkställande ordern identifierar betydelsen av uppdragsleverans, servicekvalitet och säkerställande av medborgarnas information även om skadliga cyberaktörer försöker störa dessa tjänster.

Verkställande order om cybersäkerhet

USA:s president undertecknade den 12 maj 2021 en verkställande order för att förbättra landets cybersäkerhet och skydda statliga nätverk mot bakgrund av att den senaste tidens eskalerande cybersäkerhetsincidenter i offentlig och privat sektor talar för att cybersäkerhetsförsvaret är otillräckligt.

Den verkställande ordern syftar till att

- förbättra delningen av cybersäkerhetsinformation mellan regeringen och privat sektor,
- stärka den nationella svarsförmågan,
- implementera starkare cybersäkerhetsstandarder i den federala regeringen,
- förbättra mjukvarusäkerheten i leveranskedjan,
- inrätta en styrelse för granskning av cybersäkerhet,
- inrätta en handbok för svar på cyberincidenter,
- förbättra detekteringen av cybersäkerhetsincidenter mot statliga nätverk, och
- förbättra utredande och avhjälpande förmågor.

[125] Se www.defense.gov/Explore/News/Article/Article/1641969/white-house-releases-first-national-cyber-strategy-in-15-years.

Ramverk för cybersäkerhet

The Cybersecurity Enhancement Act of 2014 är en lag på federal nivå som syftar till att tillhandahålla ett offentlig-privat partnerskap för att stärka cybersäkerheten och allmänhetens kunskap på området.

NIST har i samarbete med regeringen och privat sektor tagit fram ett ramverk för cybersäkerhet vilket ratificerats av kongressen som ett ansvarsområde inom *the Cybersecurity Enhancement Act of 2014*. Ramverket, som är frivilligt och används brett, syftar till att hjälpa organisationer att hantera sina cybersäkerhetsrisker och -incidenter med anpassade åtgärder.

Även om det inte är vanligt att ha en allmän lag för cybersäkerhet används allt fler standarder som grund för informationssäkerhetsarbetet. Många av dessa standarder överlappar varandra genom att de reglerar implementeringen av ett kontrollsystem för informationssäkerhet, med målet om ett mer strukturerat och systematiskt arbete för att förbättra kvaliteten på informationssäkerheten i allmänhet och genomförandet av riskreducerande åtgärder i synnerhet. Ett exempel på en sådan standard är *Framework for Improving Critical Infrastructure Cybersecurity*, publicerad av *National Institute of Standards and Technology* (NIST) i USA.

Program för evaluering av kommersiellt utvecklade it-produkter

NIAP tillhandahåller gemensamma kriterier för testning och validering av kommersiellt utvecklade it-produkter. NIAP ansvarar för den nationella, *Common Criteria*-baserade, certifieringsordningen *CCEVS*. *CCEVS* tillämpas för evalueringar av kommersiella it-produkter för användning i nationella säkerhetssystem. I samarbete med NIST godkänner NIAP också testningslaboratorier som ska utföra säkerhetsevalueringar i den privata sektorn enligt *Common Criteria*.

Federala myndigheters informationssäkerhet

I amerikansk lag föreskrivs att *the Director of the Office of Management*, i samråd med *the Secretary of Homeland Security*, ska bestämma vilka standarder för informationssäkerhet som ska användas för federala system, och bli kontrollerade emot.[126]

Federal Information Security Modenization Act 2014 (FISMA) är en lag som reglerar federal informationssäkerhet. FISMA identifierar myndighetens chef som ansvarig för sin respektive organisations förhållningssätt till cybersäkerhet. Myndigheterna är ansvariga för att allokera nödvändig personal, processer och teknologi för att skydda federal data.[127]

Office of Management and Budget (OMB) publicerar årliga rapporter i enlighet med FISMA vilka bl.a. innehåller analyser av intrångsdetekterings- och förebyggande kapacitet samt och uppgifter som rapporterats av federala myndigheter. Rapporten sammanfattar även cybersäkerhetsprestandan hos myndigheterna utifrån självbedömningar som respektive informationschef gjort. Självbedömningen är en skriftlig redogörelse som ger varje myndighet möjlighet att erbjuda inblick i framgångar eller utmaningar från det senaste året, och i vissa fall formulera myndighetens framtida prioriteringar.

NIST Risk Management Framework (RMF) är grunden för krav och kontroll av alla federala myndigheters informations- och it-säkerhet. I FISMA uppställs krav för myndigheterna avseende skydd av alla it-system som dessa hanterar. RMF behandlar även nationell säkerhet. Ramverket består av en enhetlig klassningsmodell med krav på åtgärder beroende på informationens och systemens klassifiering. Det innehåller möjlighet till lokala anpassningar, regler för kontroll av efterlevnad (certifiering) samt driftsgodkännande av verksamhetsansvarig (ackreditering).[128]

NIST Cybersecurity framework (CSF) är till skillnad från RMF ett frivilligt stöd till privata aktörer att välja ett adekvat skydd. I prin-

[126] Sektorsmyndigheter är skyldiga att arbeta med the *Department of Homeland Security* för att implementera det sektoriella NIPP-partnerskapsmodellen och ramverk för riskhantering, utveckla skyddande program, resiliensstrategier m.m. och på sektornivå tillhandahålla vägledning om skydd för kritisk infrastruktur.

[127] Varje myndighetschef är ansvarig för att delegera denna behörighet till informationssäkerhetschefen.

[128] Krav som ingår i RMF är ”mappade” mot ISO 27001 (och tvärtom, men noteras bör att vilka åtgärder som ska göras inte styrs av ISO 27000 eftersom i den senare överlåts riskbedömningen och val av åtgärder till verksamhetsutövaren, vilket är mycket mer centralt styrt i RMF).

cip delar CSF upp åtgärder i olika kategorier. Inom respektive kategori kan man välja en nivå. Man kan därmed skapa profiler för olika typer av verksamheter som anger vilka nivåer man bör sträva efter i varje nivå. Sådana profiler finns utarbetade inom flera sektorer. CSF är standardsoberoende, dvs. man kan använda CSF och dess metodik tillsammans med andra standarder, beroende på vad respektive organisation redan valt att använda. CSF kan därmed sägas vara ett slags ”metaspråk” för säkerhetsåtgärder.[129] CSF kan även användas av organisationers ledningar för att förstå nuläget samt besluta om vilken profil den egna organisationen ska ha och utgör samtidigt ett verktyg för ledningarna att mäta och styra arbetet.

NIST SP 800-171 är en särskild publikation som anger krav för skydd av konfidentialitet i s.k. kontrollerad oklassificerad information (CUI).[130] Dokumentet innehåller rekommendationer som riktar sig till federala myndigheter och behandlar säkerhetskontroller av komponenter tillverkade av kommersiella aktörer. Kraven används av federala myndigheter som ingått avtal med icke-federala organisationer. Riktlinjerna är tillämpliga på alla federala informationssystem med undantag för nationella säkerhetssystem (se nedan). Syftet är att de krav som ställs på organisationer och informationssystem ska överensstämma med och komplettera andra etablerade informationssäkerhetsstandarder.

NIST SP 800-53 tillhandahåller en katalog av säkerhetskontroller för federala informationssystem och organisationer samt en process för att välja anpassbara kontroller som ska skydda tillgångar, individer och nationen från en serie olika hot, däribland antagonistiska cyberattacker, som uppkommer i samband med driften av informationssystem. Säkerhetskontrollerna är utformade för att främja överensstämmelse med tillämplig författning och gällande standarder och

[129] Genom att organisationer som i sig valt olika standarder (t.ex. NIST RMF, ISO 27000, CMMC etc.) alla ganska lätt kan karaktärisera sig via CSF, så är CSF ett sätt att lätt skapa jämförelser mellan olika organisationers införda säkerhetsåtgärder.

[130] Publikationen utvecklades till följd av NIST:s ansvar enligt *Federal Information Security Modenization Act 2014* (FISMA). Vid framtagandet av standarder och riktlinjer med anledning av FISMA efterhör NIST med andra federala myndigheter och privat sektor för att förbättra informationssäkerhet och effektivitet samt tillse att publikationerna kompletterar standarderna och riktlinjerna som antagits för att skydda nationella säkerhetssystem. NIST arbetar också med diverse aktörer för att upprätta kartläggningar av och relationer till säkerhetsstandarder och riktlinjer som utvecklats av *International Organization for Standardization and International Electrotechnical Commission* (ISO/IEC). NIST innehåller ett flertal delmoment för anpassning till den egna verksamheten.

adresserar krav tvärs över den federala regeringen och kritisk infrastruktur.

NIST SP 800-53, 800-53A respektive 800-37 beskriver en riskhanteringsprocess som inbegriper kategorisering av informationssystem, val och bedömning[131] av säkerhetskontroller samt godkännande av informationssystemens drift.

FIPS Publication 200 är en obligatorisk federal standard utvecklad av NIST som uppställer minimikrav på säkerhet i federala informationssystem och kan kombineras med NIST SP 800-53. NIST SP 800-53 avser vidare att ge stöd åt federala myndigheter att möta kraven i FIPS 200. Sådana standarder och riktlinjer som NIST tar fram får dock inte tillämpas på nationella säkerhetssystem utan uttryckligt godkännande av behöriga federala tjänstemän som utövar politisk auktoritet över sådana system, om än riktlinjerna i NIST SP 800-53 utvecklats för att komplettera liknande vägledning för nationella säkerhetssystem (se nedan).

Kommersiella lösningar för hantering av klassificerad information

NSA:s program *Commercial Solutions for Classified* (CSfC) gör det möjligt för kommersiella produkter att användas i lagerlösningar som skyddar klassificerad NSS-information. NSA:s strategi för att skydda klassificerad information inbegriper både kommersiellt baserade och traditionella ”Government-off-the-Shelf Information Assurance” -lösningar. Informationsassuransdirektoratet (IAD) letar emellertid först efter kommersiell teknik för att formulera lösningar som hjälper kunder att skydda klassificerad information. En anledning är att detta tillvägagångssätt kan ge snabbare lösningar. Lösningarna enligt CSfC är designade eller godkända av NSA. Berörda komponenter ska vidare vara validerade enligt NIAP och uppfylla skyddsprofilkraven samt valideras mot *Common Criteria*. Slutligen ska de inbyggda assuransfunktionerna vara baserade på standarder, såsom NIST 800-30.

[131] Ansvaret för utförandet av säkerhetskontrollbedömningar ligger ofta hos informationssystemets ägare. Kontrollbedömningarna visar att de kontroller som organisationen valt implementeras korrekt och uppfyller kraven på säkerhet i författningar och standarder.

Upphandling av informationssäkerhetssystem

USA har haft regler som krävt att vissa myndigheter ska begära godkännande av tillsynsmyndigheter vid upphandling av informationssäkerhetssystem.[132] *Federal Acquisition Regulation* är en uppsättning regler om offentlig upphandling som omfattar alla upphandlingar och avtalsprocedurer associerade med den amerikanska regeringen. DoD är det administrativa organet bakom regelverket.

Enligt *Defence Federal Acquisition Regulation Supplement* (DFARS, paragraf 252.204-7012) måste leverantörer eller tillverkare på försvarsområdet implementera de av NIST rekommenderade kraven för att påvisa tillräcklig informationssäkerhet. För tillverkare som är del av en federal eller statlig myndighets leverantörskedja är säkerhetskraven obligatoriska. *The Manufacturing Extension Partnership National Network* vid NIST tillhandahåller en handbok om självbedömning, *NIST Handbook 162*, som är avsedd att hjälpa tillverkare som levererar produkter åt DoD att bedöma sin cybersäkerhet i förhållande till säkerhetskraven i NIST SP 800-171 och DFARS.[133] Även privata organisationer och andra aktörer uppmuntras att använda sig av vägledningen.

IKT i säkerhetskänslig verksamhet

Federala informationssystem och nationella säkerhetssystem

Nationella säkerhetssystem (NSS)[134], och även många andra informationssystem, är föremål för avancerade cyberhot.

NIAP (se ovan) samarbetar med användare av nationella säkerhetssystem för att säkerställa att skyddsprofiler tillhandahåller en strömlinjeformad certifieringsväg för kommersiella informationssäkerhetsprodukter som används i deras system. Som ovan nämnts kan CSfC möjliggöra användning av kommersiella produkter i lösningar som skyddar klassificerad NSS-information.

---

[132] I *Cybersecurity law overview – a report by Mannheimer Swartling*, april 2017, s. 4 (fotnot 10), anges att regleringen sedan 2016 verkar kräva en självbedömning.

[133] Råden kan lämna utrymme för alternativa metoder att bibehålla säkerhet så länge tillverkaren meddelar behörig myndighet om ändringarna och får dem godkända. I slutändan kan överensstämmelse med DFARS endast uppnås genom godkännande av DoD.

[134] Ett nationellt säkerhetssystem är ett informationssystem (inklusive alla telekommunikationssystem) som används eller drivs av en myndighet och har betydelse för nationell säkerhet.

Den riskhanteringsprocess som beskrivs i NIST SP 800-53, 800-53A respektive 800-37 har tidigare redogjorts för. *CNSS Instruction 1253* tillhandahåller motsvarande vägledning i fråga om nationella säkerhetssystem.[135] Tillstånd att driftsätta eller använda ett informationssystem ges av behöriga tjänstemän och baseras på att säkerhetsrisken för organisationen, individer och nationen är acceptabel. Den slutgiltiga åtgärden innan ett system tas i drift är alltså att den godkännande tjänstemannen uttryckligen accepterar risken. Varje steg i riskhanteringsramverket kan utföras av icke-federala externa leverantörer med undantag för auktoriseringssteget – dvs. acceptansen av risker är ett inneboende federalt ansvar för vilket ledande befattningshavare hålls ansvariga.[136]

CNSS Instruction 1253 tillhandahåller, med stöd av det nationella säkerhetsdirektivet (National Security Directive 42), federala organisationer en process för säkerhetskategorisering av nationella säkerhetssystem som hanterar nationell säkerhetsinformation.[137] Instruktionen hänvisar också till en omfattande uppsättning säkerhetskontroller och förbättringar förknippade med valet av den bestämda nivån av potentiell påverkan (eller förlust) på konfidentialitet, integritet och tillgänglighet som kan tillämpas på alla nationella säkerhetssystem som utvecklats och används av den nationella säkerhetsgemenskapen[138]. Följaktligen tillhandahåller instruktionen även skräddarsydda vägledningar, så att organisationer kan välja en robust uppsättning säkerhetskontroller för att säkra sina nationella säkerhetssystem, baserat på bedömd risk. Instruktionen är avsedd att användas som ett verktyg av ingenjörer för informationssäkerhetssystem, auktoriserade tjänstemän och informationssäkerhetsansvariga på myndigheter för att kunna välja och komma överens om lämpligt skydd för ett nationellt säkerhetssystem.

Alla federala organisationer som driver, använder eller förvaltar nationella säkerhetssystem måste etablera och implementera ett riskhanteringsprogram för informationsassurans (IARMP). Det finns vidare

[135] Den innehåller även riktlinjer om grundläggande säkerhetskontroller.
[136] Auktoriseringsbeslutet är direkt kopplat till hanteringen av risker relaterade till upphandling och användning av komponentprodukter, system och tjänster från externa leverantörer.
[137] Kunder med nationella säkerhetssystem (NSS) måste följa CNSSI 1253:s krav och kontroller. Dessas system testas mot instruktionens säkerhetskontroller.
[138] Dessa federala organisationer är ansvariga för att processa klassificerad säkerhetsinformation och har ett behov av att säkert kunna överföra sekretessbelagd information mellan säkerhetsdomäner utan att kompromissa säkerheten hos informationen eller respektive domän.

ett riskhanteringsramverk (RMF) som syftar till att underlätta organisationernas riskhantering.

CNSSI 1253 bygger på NIST SP 800-53 och är ämnad att fungera som ett kompletterande dokument till denna publikation. En skillnad är emellertid att CNSSI 1253-metoden uttryckligen definierar associeringar av konfidentialitet, integritet och tillgänglighet med säkerhetskontroller och förfinar användningen av säkerhetskontroller för den nationella säkerhetsgemenskapen. CNSS använder vidare flera separata kategoriseringar för respektive säkerhetsmål. Instruktionen tillhandahåller sedan lämpliga säkerhetsbaslinjer för varje möjlig systemkategorisering med hjälp av kontroller från NIST SP 800-53.[139] För nationella säkerhetssystem, där skillnad förekommer mellan CNSSI 1253 och NIST-dokumentation, äger instruktionen företräde.

Därefter görs en tredjepartsbedömning[140] genom att en organisation oberoende validerar en aktörs systems överensstämmelse med CNSSI 1253. Undersökande organisation intygar att en säkerhetsbedömningsrapport (SAR) enligt CNSSI 1253 från berörd aktör ger en fullständig bedömning av de tillämpliga säkerhetskontroller som anges i säkerhetsbedömningsplanen (SAP). SAR dokumenterar testningen för att validera systemet mot ett urval av CNSSI 1253-säkerhetskontroller för system som exempelvis kan kräva hög konfidentialitet, hög integritet och hög tillgänglighet.[141]

I många fall behövs ytterligare säkerhetskontroller eller förbättrade kontroller för att möta de specifika hoten mot eller sårbarheterna hos ett nationellt säkerhetssystem.

Ytterligare tekniska säkerhetsåtgärder för informationssystem

Den nationella säkerhetsgemenskapen har policyn att medlemsorganisationer ska tillämpa ömsesidighet med avseende på certifiering av system och systemkomponenter i möjligaste mån.[142] I CNSS 1253

[139] Det är chefen för organisationen som avgör vilken metod för val av säkerhetskontroller som ska användas för det egna nationella säkerhetssystemet. Ett nationellt säkerhetssystem – som tillhandahåller unika funktioner, fungerar i olika miljöer och är föremål för avancerade cyberhot – förutsätter att en riskbaserad metod antas på företagsnivå när de slutliga säkerhetskontrollerna ska implementeras.
[140] Denna ska vara godkänd av tillämplig standard.
[141] Testade säkerhetskontroller kan analyseras för att bestämma vilka säkerhetskontroller som ska testas för att säkerställa överensstämmelse med CNSSI 1253:s säkerhetsbaslinjer.
[142] För att stödja reciprocitet mellan nationella säkerhetsorganisationer kräver många parametrar i NIST SP 800-53-kontrollkatalogen specifik instansiering.

definieras värden[143] för tillämpliga kontroller som skapar en standard för att certifiera att en kontroll mildrar ett hot. I olika risktrösklar eller hotscenarier kan vissa ansvariga operatörer kräva att system avviker från denna standard. I dessa situationer kan ytterligare tekniker läggas till, eller arkitektoniska implementeringar modifieras för att på ett adekvat sätt minska risken. Genom att upprätta en standard för nyckelparametrar har organisationer en känd baslinje när de accepterar certifieringar av teknik eller system från andra organisationer inom den nationella säkerhetsgemenskapen och behöver inte duplicera den nivån av certifiering.[144]

Organisationstjänstemän, såsom informationssystemets ägare, uppdragsgivare, auktoriserare och informationssäkerhetschefer, bör bestämma de användningsbegränsningar som, med anledning av cyberhot, krävs för systemet. Exempel på användningsbegränsningar är begränsning av antingen informationen som ett informationssystem kan bearbeta, lagra eller överföra eller sättet på vilket ett uppdrag automatiseras, att förbjuda externa informationssystem åtkomst till kritisk organisationsinformation genom att ta bort utvalda systemkomponenter från nätverket (dvs. ”air gapping”), samt att förbjuda information med måttlig eller stor påverkan på ett informationssystem som allmänheten kan få tillgång till, såvida inte ett uttryckligt beslut fattas som tillåter sådan åtkomst.

Alla företag som ska leverera på uppdrag av DoD måste nå upp till en viss typ av krav och certifieringssystem som USA utvecklat. Det rör sig om fem nivåer av säkerhet enligt *Cybersecurity Maturity Model Certification* (CMMC) – ett obligatoriskt regelverk för leverantörer[145] som DoD nyligen tagit fram.[146] CMMC granskar och kombinerar olika cybersäkerhetsstandarder och bästa praxis och kart-

[143] T.ex. ytterligare precisering av hur och i vilken omfattning vissa kontroller ska ske när det gäller nationella säkerhetssystem.

[144] När ömsesidigt erkännande av certifiering ska utsträckas över auktoriserande tjänstemän, eller när ett system tillhandahåller säkerhet för ett annat system, förhandlas värdena för dessa parametrar mellan relevanta auktoriserare, och resultaten dokumenteras för båda systemen.

[145] Detta gäller bl.a. för svenska företag som Saab och Combitech.

[146] CMMC utvecklades av DoD i samarbete med *Carnegie Mellon University* och *Johns Hopkins University Applied Physics Laboratory*. Det primära målet med modellen är att skydda information från försvarsindustriella och tekniska basen (DIB). Informationen som omfattas av CMMC är klassificerad som antingen ”Federal Contract Information”, information från eller till regeringen enligt kontrakt som inte är avsett för offentliggörande, eller ”Controlled Unclassified Information”, information som kräver skydd eller spridningskontroll i enlighet med författningar och regeringsövergripande policy. CMMC mäter cybersäkerhetsmognad och tillhandahåller bästa praxis tillsammans med ett certifieringselement för att säkerställa implementeringen av metoder som är associerade med varje mognadsnivå. Den senaste versionen släpptes 2020.

lägger dessa kontroller och processer över flera mognadsnivåer som sträcker sig från grundläggande cyberhygien till avancerad. CMMC är endast tillämplig på DIB-entreprenörers oklassificerade nätverk som hanterar federal kontraktsinformation eller kontrollerad oklassificerad information. För en given CMMC-nivå kommer tillhörande kontroller och processer, när de implementeras, att minska risken mot en specifik uppsättning cyberhot. Självbedömning är inte tillåtet. Målet är att CMMC ska vara kostnadseffektivt och överkomligt för småföretag att implementera på lägre CMMC-nivåer. Auktoriserade och ackrediterade oberoende bedömningsorganisationer (C3PAO) kommer att genomföra bedömningar och utfärda CMMC-certifikat till *Defense Industrial Base*-företag (DIB) på lämplig nivå. Före denna process uppmuntras DIB-företag att genomföra en självbedömning enligt CMMC:s bedömningsguide.[147]

CMMC kan sägas bestå av en serie åtgärder inom olika kategorier av områden som företag har att genomföra. CMMC delas in i fem mognadsnivåer där organisationen behöver både införa egna konkreta åtgärder (som till stor del kommer från NIST RMF) inom respektive kategori samt egen förmåga att självständigt hantera säkerhetsarbetet. Ju högre mognadsnivå, desto större fokus sätts på organisationens egen personal, kompetens och förmåga att hänga med i teknikutvecklingen och täppa till säkerhetsproblem för egen maskin (utan att krav på varje enskild åtgärd ingår i listan av åtgärder från NIST). Varje organisation måste underkastas extern kontroll och bedömning (dvs. certifiering). DoD ställer sedan krav på vilken nivå organisationer måste ha nått för att få delta i mer eller mindre kritiska upphandlingar.

CMMC på lägsta nivån kräver inte utförligt pappersarbete och omfattande dokumentering utan inför ett antal obligatoriska säkerhetsåtgärder. På nivå 2 behöver man bygga bl.a. ledningssystem. På nivå 3 krävs ett fulländat certifieringssystem, och många krav enligt NIST-regelverket aktualiseras.[148] På övre nivåerna är de krav som ökar att myndigheten eller företaget ska visa att man har tillgång till experter som systematiskt arbetar inom it-säkerhet, har kompetens och följer med i utvecklingen på området – alltså krav på personal

[147] NSA utvecklar produktnivå-krav i statliga skyddsprofiler och möjliggör för kunder att välja komponenter från CSfC-listan.
[148] På nivå 3 inkluderar CMMC de 110 säkerhetskrav som specificeras i NIST SP 800-171. Därutöver inkorporerar modellen ytterligare processer från ett antal andra standarder och källor, bl.a. avseende kritiska säkerhetskontroller för effektiv cyberförsvarsförmåga.

som säkerhetsanalyseras på ett effektivt sätt. Härigenom tilldelar ledningen resurser åt cybersäkerhetsarbetet. Cyberskyddsansvariga måste ha viss kompetensnivå och ska även genomgå kurser för att få behövligt certifikat i sin arbetsroll.

Sammanfattning av särskilda krav på IKT i säkerhetskänslig verksamhet

Av inhämtade uppgifter framgår att det finns departement och centrala myndigheter i USA med ansvar för nationell informations- och cybersäkerhet. Det finns bl.a. krav på att driftsättningen av federala informationssystem ska godkännas av behöriga federala tjänstemän. Nationella säkerhetssystem som behandlar nationell säkerhetsinformation fordrar ytterligare säkerhetskrav som behöver godkännas. Vidare ska sådana system genomgå en oberoende tredjepartsbedömning där systemets överensstämmelse med särskilda instruktioner på området valideras. I USA kan kommersiella informationssäkerhetsprodukter i förhållandevis stor utsträckning användas för att skydda nationella säkerhetssystem och klassificerad information (om lösningarna är godkända av NSA och assuransfunktionerna validerade).[149]

9.10 Kanada

Aktörer inom informations- och cybersäkerhet

CSE – kommunikationssäkerhet

I Kanada har den statliga myndigheten *Communications Security Establishment Canada* (CSE) det främsta ansvaret för it-säkerhet och skyddet av federala institutioners elektroniska information och informationsinfrastruktur[150] av betydelse för den kanadensiska staten. CSE är ansvarig för landets signalspaning och utgör den tekniska myndigheten för cybersäkerhet. Myndigheten ska försvara statliga

[149] Det framstår som att utgångspunkten i USA är att ansvaret för godkännande av system ytterst ska ligga hos en enskild person/personal, snarare än på organisationen som sådan.
[150] Myndigheten får använda och avslöja infrastrukturinformation för att testa system eller genomföra cybersäkerhets- och informationssäkringsaktiviteter på den infrastruktur från vilken informationen förvärvades. Information om en kanadensare eller en person i Kanada kan anskaffas tillfälligtvis under utförandet av aktiviteter enligt ett lagligen grundat/utfärdat tillstånd.

nätverk och system samt skydda mot cybersäkerhetshot. Vidare ska myndigheten leda utvecklingen av betrodda leverantörer för staten och kritisk infrastruktur samt motverka risken för opålitlig utrustning. Ansvarsområdet omfattar också upphandling, distribution, kontroll och användning av kryptografiska enheter och krypteringsnyckelmaterial för nationella säkerhetssystem.

CSE:s verksamhet inbegriper bl.a. testning och evaluering av produkter, mjukvara och system.[151] Som certifieringsorgan utfärdar CSE nödvändiga certifikat om godkännande av evaluerare. CSE driver också det nationella cybersäkerhetscentret (se nedan).

Nationellt cybersäkerhetscenter

The Canadian Centre for Cyber Security är landets myndighet för cybersäkerhet. Centret samarbetar med både den offentliga och privata sektorn. Centret bedriver operativ cybersäkerhetsverksamhet och leder regeringens arbete med anledning av cybersäkerhetshändelser. Myndigheten inrymmer även den nationella CSIRT-funktionen (Computer Security Incident Response Team).

Centrets verksamhetsområden inbegriper därutöver bl.a. nationell expertrådgivning och praktisk support i fråga om cybersäkerhet, utveckling av cybersäkerhetsprodukter samt försvar av nationella cybersystem (inklusive statliga system).

Centret är även nationellt certifieringsorgan för *Common Criteria*-evalueringar som utförs i Kanada. Centret driver det kanadensiska *Common Criteria*-programmet för att certifiera it-produkter som testats av kanadensiska ackrediterade testningslaboratorier. Förutom att tillhandahålla vägledning åt både offentliga och privata organisationer publicerar centret direktiv om cybersäkerhet för projekt inom regeringen. Centret kan vidare föreskriva specifika cybersäkerhetsstandarder för statliga myndigheter. Centret har dessutom gett ut ett flertal direktiv om it-säkerhet som är obligatoriska att följa för såväl statliga myndigheter som privata företag.[152]

[151] CSE kan få ett cybersäkerhetsbemyndigande som, i cyber- och informationssäkerhetssyfte, tillåter myndigheten att få tillgång till en federal institutions informationsinfrastruktur eller information av betydelse för staten och förvärva all information som härrör från, riktas till, lagras på eller överförs på eller genom den infrastrukturen i syfte att hjälpa till att skydda den från ofog, obehörig användning eller störningar. Myndigheten kan även få ett bemyndigande att utföra angivna aktiviteter för att främja defensiva eller aktiva cyberoperationer samt andra aktiviteter som är rimliga och nödvändiga för verksamheten.

[152] Direktiven avser bl.a. it-säkerhet för hantering av kommunikationssäkerhet och kryptografi.

Public Safety Canada

Public Safety Canada (PSC) är ett departement som skapades 2003 för att säkerställa samordning mellan alla federala departement och myndigheter som ansvarar för nationell säkerhet. Uppdraget är att skydda landet från olika risker som naturkatastrofer, brott och terrorism genom ökad nationell säkerhet och motståndskraft. Departementet stödjer och rapporterar till ministern för allmän säkerhet och beredskap i frågor som rör allmän säkerhet och nödhantering som inte tilldelats någon annan federal organisation. Departementet arbetar också med andra statliga organisationer, gemenskaper, privat sektor och internationella partners på säkerhetsområdet, bl.a. i syfte att skydda kritisk infrastruktur och kritisk information.

PSC ansvarar också för *Cyber Incident Management Framework for Canada* (CIMF) som är ett vägledande dokument för guvernörer, ägare och operatörer av kritiska infrastrukturer samt andra sektorpartners (se nedan).

Inom PSC finns *Canadian Cyber Incident Response Center* (CCIRC) som ansvarar för att övervaka och tillhandahålla råd om cyberhot och samordna det nationella svaret på eventuella cybersäkerhetsincidenter. CCIRC:s fokus är att skydda nationell kritisk infrastruktur mot cyberattacker.

Reglering av informations- och cybersäkerhet

Nationell cybersäkerhetsstrategi

Kanada har antagit en nationell cyberstrategi från 2018 som bl.a. betonar behovet av samarbete mellan regeringen och privat sektor för att öka cybersäkerheten i landet.[153] Skyddet av kritisk infrastruktur[154] är ett prioriterat område.

[153] Se cyberhttps://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx#s1.

[154] Att förbättra motståndskraften hos kritisk infrastruktur genom en lämplig kombination av säkerhetsåtgärder för att hantera avsiktliga och oavsiktliga incidenter och störningar är ett verksamhetsområde för *Public Safety Canada* (se nedan).

Ramverk för hantering av cyberincidenter

Cyber Incident Management Framework (CIMF) publicerades 2013 av PSC och är utformat för att komplettera och knyta samman befintliga ramar och planer för federala, provinsiella och territoriella nödhanteringsramverk och -planer samt nödplaner från ägare och operatörer av kritiska infrastrukturer. Syftet med CIMF är att tillhandahålla en strategi för hela nationen för hantering av och samordning vid cyberhot eller -incidenter. Ramverket anger roller och ansvarsområden för samtliga styrningsnivåer och aktörer i kritisk infrastruktur när det gäller samordnat förebyggande av, svar på och återhämtning från it-incidenter. CIMF är således tänkt att göra det möjligt för varje organisation att fullt ut och effektivt delta i en samordnat nationell cyberincidentrespons.

Nationella certifieringssystem

Som ovan nämnts finns det en nationell ordning för certifiering av it-produkter enligt *Common Criteria*. Bl.a. små och medelstora företag kan ansöka om att bli certifierade under grundläggande cybersäkerhetskriterier uppställda av det kanadensiska cybersäkerhetscentret.

CyberSecure Canada Certification är ett annat certifieringsprogram som hjälper små och mellanstora företag att implementera certifieringskrav för ökat skydd mot cyberattacker. Programmet inbegriper ett antal säkerhetskontroller som utvecklats i samarbete med det nationella cybersäkerhetscentret. Organisationerna måste implementera säkerhetskontrollområdena för att kunna erhålla certifiering enligt programmet.

The Baseline Cyber Security Controls for Small and Medium Organizations är ett dokument ämnat för små och medelstora organisationer som vill ha rekommendationer för att förbättra sin cybersäkerhet. Dokumentet presenterar det nationella cybersäkerhetscentrets grundläggande cybersäkerhetskontroller för de nationella företagen.

MITS – minimikrav på it-säkerhet för federala myndigheter

Operational Security Standard: Management of Information Technology Security (MITS) definierar grundläggande säkerhetskrav som federala departement och myndigheter måste uppfylla för att säkerställa säkerheten för informations- och it-tillgångar under deras kontroll. Standarden tillhandahåller riktlinjer på organisationsnivå och för hanteringen av it-säkerhetsprogram samt ett antal skyddsåtgärder. Standarden kräver bl.a. att departementen har sina system eller tjänster certifierade och ackrediterade innan de godkänns för drift. Utförandet av certifieringen beror på kvantiteten av och kvaliteten på de certifieringsbevis[155] som krävs av ackrediteringsmyndigheten.

Departementen och myndigheterna måste regelbundet granska ackrediteringen av systemen eller tjänsterna om dessa förändrats avsevärt eller om det är motiverat på grund av förändringar i riskmiljön.

För vanliga system eller tjänster är *the Government of Canada Chief Information Officer* ackrediteringsmyndighet. För system eller tjänster som är specifika för ett departement ansvarar program- eller tjänsteleverantören för ackreditering. För system eller tjänster som delas av två eller flera organisationer är chefen för programmet eller tjänsten ackrediteringsmyndighet.

Departementet ska genomföra en årlig självbedömning av sina it-säkerhetsprogram för att se om de överensstämmer med statliga säkerhetspolicys och standarder. Åtkomstkontroll genom krav på säkerhetsgodkännande av personal, användning av krypto samt nätverkssegregering är exempel på förebyggande åtgärder.

Den statliga säkerhetspolicyn kräver att departementen tillämpar sanktioner i förhållande till it-säkerhetsincidenter när det förekommit försumlighet.

[155] Sådana bevis kan innehålla resultaten av alla tillämpliga hot- och riskbedömningar, en bedömning av affärseffekter, en integritetsbedömning, en sårbarhetsbedömning, säkerhetstester och produktevaluering, självbedömningar, revisioner och säkerhetsgranskningar och relaterade juridiska eller politiska bedömningar som visar överensstämmelse med relevant lagstiftning eller policy.

It-säkerhetskrav vid hantering av säkerhetsklassificerad statlig information

När aktörer ingår kontrakt med den kanadensiska regeringen blir vissa krav på it-säkerhet tillämpliga när organisationen ska hantera skyddad eller säkerhetsklassificerad information elektroniskt. Säkerhetskraven är dock specifika för varje kontrakt och säkerhetsnivån beror på hur känslig den berörda informationen är.

För att få behörighet att processa känslig information elektroniskt måste den berörda organisationen först ha genomgått en säkerhetsprövning eller ha ett säkerhetsgodkännande för anläggningen. Dessa åtgärder ska säkerställa att endast betrodda individer och organisationer med ett giltigt behov av kunskap får tillgång till känslig myndighetsinformation (om t.ex. militära planer). Vidare krävs en förmåga att skydda dokument. Dessutom kan det behövas s.k. organisationsgodkännanden när det gäller informationssäkerheten. Organisationerna måste även underkasta sig it-säkerhetsinspektioner[156] och rapportera it-säkerhetsincidenter. Organisationen behöver också säkerställa att dess säkerhetschef förstår it-kraven. Dessutom kan krävas att organisationen erhåller ett skriftligt godkännande från *Public Services and Procurement Canada* (PSPC) innan skyddad eller sekretessbelagd statlig information nås elektroniskt.

I federala kontrakt mellan regeringen och privata organisationer ingår klausuler med säkerhetskrav[157]. När organisationer tilldelas kontrakt med regeringen som kräver att de använder sina egna it-system för att lagra, bearbeta och/eller skapa skyddad eller säkerhetsklassificerad information måste de ha tillstånd enligt PSPC:s *Contract Security Program* (CSP) före det att arbetet kan påbörjas. Organisationen får inte använda sitt it-system för att hantera informationen förrän it-säkerhetsinspektionsprocessen är klar och formaliserad i ett skriftligt it-godkännandebrev från PSPC:s CSP. Att börja använda ett sådant it-system utan tillstånd utgör ett brott mot villkoren i avtalet. It-godkännanden är kontraktsspecifika och gäller under hela kontraktets löptid.[158]

[156] Efter it-säkerhetsinspektionen ger it-inspektören rekommendationer som ska valideras.
[157] Säkerhetskrav anger de säkerhetsnivåer som krävs för att skydda känslig information, tillgångar och arbetsplatser.
[158] Ytterligare it-säkerhetsåtgärder för organisationer kan avse auktorisering av organisationer att sända och ta emot känslig information med s.k. COMSEC-material, dvs. objekt som är utformade för att säkra eller verifiera telekommunikationsinformation, t.ex. en kryptografisk nyckel.

En precisering av säkerhetskraven för ett kontrakt kan återfinnas i en begäran om förslag respektive checklistan för säkerhetskrav, *Security Requirements Check List* (TBS/SCT 350-103), ifylld av det avtalsslutande departementet. I checklistan kan kryssas i huruvida leverantören kommer att behöva använda sina it-system för att elektroniskt bearbeta, producera eller lagra skyddad (protected)[159] och/eller klassificerad information och/eller data. Den senare typen gäller information eller tillgångar som, om de äventyras, kan förväntas skada det nationella intresset, försvaret och upprätthållandet av Kanadas sociala, politiska och ekonomiska stabilitet. Klassificerad information finns på nivåerna konfidentiell, hemlig och kvalificerat hemlig.[160] Om svaret är ja behöver it-säkerhetskraven för upphandlingen specificeras i ett tekniskt dokument. Leverantören måste också beakta dokumentet *Treasury Board of Canada Secretariat – Operational Security Standard: Management of Information Treasury Board of Canada Secretariat – Operational Security Standard: Management of Information Technology Security* (MITS, se ovan). Om det kommer att finnas en elektronisk länk mellan leverantörens it-system och den statliga myndigheten måste leverantören få sina it-system godkända.[161] Berört departement måste också tillhandahålla anslutningskriterier som beskriver villkoren och åtkomstnivån för den elektroniska länken.[162]

The Contract Security Manual (CSM) beskriver de krav som organisationer inom den privata sektorn måste följa för att skydda statlig information och tillgångar som tillhandahålls eller produceras av organisationer som tilldelats ett statligt kontrakt med säkerhetskrav. Det gäller organisationer som är registrerade i PSPC:s CSP och alla kontrakt – kanadensiska eller utländska – som PSPC ansvarar för. Denna handbok avhandlar bl.a. ovan nämnda checklista för säkerhetskrav, säkerhetskontroller och elektronisk informationssäkerhet.

[159] Gäller information eller tillgångar som, om de äventyras, kan förväntas orsaka skada på ett icke-nationellt intresse – dvs. ett enskilt intresse som en person eller en organisation.
[160] Vidare krävs behörighet för tillgång till Nato-klassificerad information för ett specifikt kontrakt. Vissa internationella avtal kräver Nato-godkännanden krävs för personal och organisationer.
[161] Den avtalsslutande säkerhetsmyndigheten är ansvarig för att säkerställa att leverantörerna uppfyller säkerhetskraven i checklistan.
[162] Ingen information som rör ett skyddat eller klassificerat statligt kontrakt får släppas av leverantörer utan föregående skriftligt godkännande.

Sammanfattning av särskilda krav på IKT i säkerhetskänslig verksamhet

Av inhämtade uppgifter framgår att det finns centrala myndigheter i Kanada med ansvar för nationell informations- och cybersäkerhet och certifiering av IKT. Vidare måste federala departement och myndigheter ha sina it-system och tjänster certifierade och ackrediterade innan de godkänns för drift.

Organisationer som ingår kontrakt med regeringen och har it-system som ska behandla säkerhetsklassificerad information (mellan leverantören och en statlig myndighet) måste få sitt system godkänt av en myndighet (PSPC) före det att arbetet kan påbörjas och systemet används. Säkerhetskraven är emellertid specifika för varje kontrakt och beror på hur känslig den berörda informationen är.

9.11 Nya Zeeland

Aktörer inom informations- och cybersäkerhet

Byrån för kommunikationssäkerhet

Government Communications Security Bureau (GCSB) är ett departement med uppdrag att bidra till Nya Zeelands nationella säkerhet genom att tillhandahålla informations- och cybersäkerhet till landets regering och kritiska infrastrukturorganisationer.[163] GCSB samlar in och analyserar underrättelser samt samarbetar med och ger stöd åt andra nationella myndigheter. Myndigheten har två kommunikationsavlyssningsstationer samt kommunikations- och kryptografispecialister i sin personal.

Nationellt cybersäkerhetscenter

Inom GCSB finns *National Cyber Security Centre* (NCSC) som har i uppdrag att samordna landets cybersäkerhetsaktiviteter. Centret tillhandahåller avancerade funktioner och tjänster för detektering av cyberhot och störningar till statliga myndigheter och organisationer av nationell betydelse (såsom tillhandahållare av kritisk infrastruk-

[163] På ett mer övergripande plan ansvarar premiärministerns och kabinettets departement för rådgivning om nationell säkerhet till regeringen.

tur). Centret svarar vidare på kraftfulla cyberincidenter på nationell nivå och genomför cyberhotsanalyser. Man främjar en säkerhetskultur baserad på standarder som anges i regeringens skyddskrav, *Protective Security Requirements* (PSR) och *New Zealand Information Security Manual* (NZISM).

Säkerhets- och underrättelsetjänst

New Zealand Security Intelligence Service (NZSIS) är en statlig myndighet som har till uppdrag att skydda Nya Zeeland genom att utreda hot mot den nationella säkerheten och analysera underrättelser för att kunna ge nationella beslutsfattare god säkerhetsrådgivning. NZSIS tillhandahåller också ett antal tjänster till andra myndigheter, bl.a. råd om personal- och fysisk säkerhet. Man ansvarar även för att underhålla landets statliga säkerhetsklassificeringssystem (*New Zealand Government Security Classification System*).

DIA – departementet för inrikes frågor

Office of the Government Chief Information Officer (GCIO) vid *The Department of Internal Affairs* (DIA) tillhandahåller rådgivning och förvaltning åt sektor- och statliga system och IKT-processer, inklusive IKT-assurans och -säkerhet. DIA har ansvar för ett assuransramverk för statlig IKT-drift, *All-of-Government ICT Operations Assurance Framework*. Systemet syftar till att ge hög nivå av tillförlitlighet i digitala offentliga tjänster.

IKT-säkerhetsexperter

The Security and Related Services Panel är en grupp branschexperter som är har i uppdrag av regeringen att förse myndigheter med IKT-säkerhetstjänster och råd om säkerhets- och sekretessfrågor.

NCPO – nationellt cyberpolicykontor

National Cyber Policy Office (NCPO) leder utvecklingen av landets cybersäkerhetspolicy och ger politiska råd till regeringen om investeringar i cybersäkerhetsaktiviteter. NCPO driver landets nationella CERT, CERT NZ. CERT NZ har till uppgift att identifiera hot och sårbarheter samt tillhandahålla tjänster för incidentrapportering och samordning av gensvar. CERT NZ arbetar med flera olika organisationer på cybersäkerhetsområdet.

Reglering av informations- och cybersäkerhet

Nationell cybersäkerhetsstrategi

Nya Zeelands senaste nationella cybersäkerhetsstrategi är från 2019.[164] Strategin betonar behovet av samarbete mellan offentlig och privat sektor samt internationellt för att öka cybersäkerheten i landet. Vidare framhålls vikten av utbildningsåtgärder för att öka medborgarnas cybersäkerhetsmedvetande. Att skydda samhällsviktig informationsinfrastruktur i landet är ett annat område som prioriteras. Slutligen vill man även fokusera på att investera mer i individer och resurser med särskild kompetens på cybersäkerhetsområdet.[165]

AISEP – program för evaluering av informationssäkerhet

Australasian Information Security Evaluation Program (AISEP) syftar till att säkerställa att evaluerade säkerhetsprodukter är tillgängliga för att tillgodose behoven hos australiensiska och nyzeeländska myndigheter. AISEP möjliggör evaluering och certifiering av produkter enligt *Common Criteria* (CC) och fortsatt underhåll av assuransen hos evaluerade produkter. En annan av programmets funktioner avser erkännande av produkter evaluerade enligt en utländsk ordning med vilken AISEP har ett avtal om ömsesidigt erkännande (vanligtvis CCRA).

The AISEP Evaluated Products List (EPL) underhålls av *Australian Signals Directorate* (ASD) och innehåller en lista över godkända pro-

[164] Se https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019.
[165] Det kan tilläggas att tillsyn på cybersäkerhetsområdet utövas på sektoriell basis.

dukter för skyddet av klassificerad information, bl.a. godkända skyddsprofiler.

Innan myndigheter väljer en produkt som inte utvärderats av AISEP rekommenderas man att kontakta GCSB för att efterhöra om produkten kommer att erkännas i Nya Zeeland när den har fullständig evaluering i en utländsk ordning. Evalueringar som genomförs enligt CC i andra nationer kan erkännas av GCSB under AISEP. Att en produkt genomgått CC-evaluering innebär dock inte nödvändigtvis att den är lämplig för det avsedda ändamålet. Vanligtvis kommer sådana produkter att ha kryptografisk funktionalitet som inte täcks i tillräcklig grad under CC.[166]

Närmare om krav på informationssäkerhet

NCSC rekommenderar att myndigheter i sina nätverk och system använder produkter som regeringen godkänt då dessa ger högre nivåer av assurans i förhållande till säkerhetsöverväganden. Centret ser vidare certifiering av organisationers informationssystem som en väsentlig komponent av styrnings- och assuransprocessen.

PSR – säkerhetsskyddskrav

Protective Security Requirements (PSR) ges ut av NZSIS och anger regeringens krav på informationssäkerhet. Säkerhetskraven anger bl.a. vad statliga myndigheter ska beakta för att säkerställa att de hanterar säkerheten ändamålsenligt och effektivt. PSR innehåller grundläggande säkerhetskrav och riktlinjer för styrning och säkerhet samt support för bästa praxis, och inkorporerar även *New Zealand Information Security Manual* (NZISM, se nedan). Ett av de obligatoriska kraven enligt PSR är att berörda organisationer årligen ska använda en evidensbaserad bedömningsprocess för att ge assurans om att organisationens säkerhetsförmåga är ändamålsenlig (GOV8). På begäran ska en försäkringsrapport tillhandahållas regeringen.[167] PSR innehåller också en process för årlig självbedömning av säkerhet och

[166] Se www.nzism.gcsb.govt.nz/xml/index/3212.
[167] I ett PSR-hanteringsprotokoll beskrivs vikten av certifiering och ackreditering av informationssäkerhet för att skydda organisationers information.

assurans. Alla statliga organisationer är skyldiga att hålla information om regeringen och statens resurser säker.[168]

Vidare behöver IKT-systemen genomgå en certifierings- och ackrediteringsprocess i enlighet med NZISM, för att vara godkända att tas i drift sedan informationssäkerhetsåtgärder vidtagits. Säkerhetsåtgärderna måste valideras för att säkerställa att de fungerar som förväntat. Processen bygger på en riskbedömning, tillämpningen av kontroller som beskrivs i NZISM och bestämning av eventuell kvarvarande risk.

PSR rekommenderar även att andra organisationer än statliga betraktar angivna krav som bästa praxis.

NZISM – handbok om informationssäkerhet

NZISM är en omfattande och detaljerad handbok utgiven av GCSB som beskriver processer och IKT-säkerhetskontroller som är väsentliga för skyddet av statlig information och system.[169] Handboken är avsedd att användas av statliga organisationer, men även privata organisationer uppmuntras att använda den. Handboken gäller också för organisationer som ingått ett formellt avtal med Nya Zeelands regering för att få tillgång till klassificerad information. Den används framför allt för att styra myndigheters arbete med informations- och cybersäkerhet. Även om de övergripande kraven är obligatoriska för departement och myndigheter när de bygger sin it-infrastruktur krävs inte överensstämmelse med handboken enligt lag. Vidare kontrolleras inte de åtgärder som organisationerna bör eller ska vidta.[170] Vilken bindande roll PSR har förtydligas däremot genom ett kabinettdirektiv (CAB MIN (14) 39/38).

Enligt NZISM ska respektive myndighetschef ansvara för informationssäkerheten inom sin organisation. Handboken, som används av såväl myndigheters informationssäkerhetschefer som leverantörer, entreprenörer och konsulter som tillhandahåller tjänster till myndigheter, innehåller ett ramverk för certifiering och ackreditering samt tekniska minimisäkerhetsstandarder (i linje med bl.a. ISO/IEC). Information klassificerad som konfidentiell, hemlig eller kvali-

[168] Säkerhetsåtgärderna måste även uppfylla kraven i *New Zealand Government Security Classification System*.
[169] Handboken har sitt ursprung i Australiens ISM (se nedan), men är i dag helt omskriven.
[170] Är det fråga om nationell säkerhet kan dock undantag aktualiseras.

ficerat hemlig är föremål för fler kontroller än övrig information. I den process som handboken föreskriver för IKT-system måste certifiering slutföras innan nödvändig ackreditering kan äga rum. Resultatet av en ackreditering är ett godkännande för driftsättning, från ackrediteringsorganet till systemägaren. Syftet är att bekräfta huruvida resultaten av en lämplig systemgranskning är av acceptabel standard. Processen i sin helhet bygger på en riskbedömning och tillämpning av vissa kontroller samt bestämning av eventuellt kvarvarande risk.[171] För samtliga myndigheters informationssystem är informationssäkerhetschefen certifikatutfärdare.[172] Ackrediteringen tilldelas när systemet överensstämmer med handboken och ackrediteringsorganet accepterar kvarvarande säkerhetsrisk. Ackrediteringen innebär ett formellt godkännande att ta systemet i drift. Myndigheter får inte tillåta att deras system hanterar sekretessbelagd information över den klassificeringsnivå som systemet fått ackreditering för.

Det är systemägaren som är ansvarig för den övergripande driften av informationssystemet. Systemägaren måste därmed även se till att systemet är ackrediterat för att uppfylla organisationens operativa krav och att ackrediteringen underhålls.[173] Myndigheterna får inte använda ett system utan giltig ackreditering såvida inte ackrediteringsorganet beviljat dispens.

För myndigheter med system som hanterar information som rör nationell säkerhet är GCSB:s generaldirektör behörig ackrediteringsmyndighet oavsett informationens klassificeringsnivå. Också användning av högassurans-kryptoutrustning samt system med kompartmentaliserad eller förbehållen (”caveated”) information klassificerad som konfidentiell och högre kräver kontroll i form av ackreditering av GCSB (eller formell delegat).[174] När det gäller information och system klassificerade som begränsat hemliga (restricted) och lägre, svarar generellt respektive myndighetschef för ackrediteringen.

[171] Certifiering förutsätter att valda kontroller är lämpliga och överensstämmer med PSR och särskilt de relevanta NCISM-komponenterna samt fungerar ändamålsenligt.
[172] Uppdraget att utarbeta certifiering ligger hos värdmyndigheten eller den ledande organisationen.
[173] Ledningen eller systemägaren ska vidare avge formella påståenden om vissa aktiviteter för informationssystemet.
[174] Det kan tilläggas att s.k. fack upprättas för att ge ytterligare skydd åt information av betydelse för nationell säkerhet. I övriga fall då informationen är begränsat hemlig eller systemet klassificerats som konfidentiellt och högre har respektive organisations vd eller det ledande organet att acceptera kvarvarande säkerhetsrisk med driften av informationssystemet (vilket ackrediteringen förutsätter).

När myndigheters system hanterar känslig information ämnad endast för nationellt bruk (”New Zealand Eyes Only”) måste myndigheterna säkerställa att en nyzeeländsk medborgare, som arbetar för regeringen, alltid har kontroll över systemet och informationen. Sådana system är särskilt känsliga och kräver ytterligare säkerhetsåtgärder vid anslutning till andra system.[175]

Produkter som tillhandahåller säkerhetsfunktioner för att skydda klassificerad information evalueras av assuransskäl. Myndigheter som väljer högassuransprodukter måste kontakta GCSB och uppfylla alla produktspecifika krav innan något köp görs.[176]

För att säkerställa nätverkssäkerhet och funktionalitet behöver varje ändring av ett nätverk godkännas och kontrolleras genom lämpliga ledningsprocesser. När det gäller system klassificerade konfidentiella, hemliga eller kvalificerat hemliga måste myndigheterna implementera nätverksåtkomstkontroller i alla nätverk. Alla myndigheter som överväger att distribuera ett trådlöst kvalificerat hemligt nätverk behöver ansöka om godkännande från GCSB innan de initierar några nätverksprojekt. Myndigheter får inte använda sådana trådlösa nätverk såvida inte säkerheten för myndighetens trådlösa distribution godkänts av GCSB.[177]

Sammanfattning av särskilda krav på IKT i säkerhetskänslig verksamhet

Av inhämtade uppgifter framgår att det finns departement i Nya Zeeland med ansvar för informations- och cybersäkerhet, bl.a. när det gäller nationell säkerhet. Statliga myndigheter som hanterar hemlig information om nationen är skyldiga att ständigt ha kontroll över sina system och hålla informationen säker. IKT-systemen kan vidare behöva genomgå en särskild certifierings- och ackrediteringsprocess för att få tas i drift. Detta förfarande regleras i en nationell handbok vars användning rekommenderas brett i samhället. Rör hanterad in-

[175] Myndigheter som har åtkomst till ett system som innehåller hemlig information om nationella intressen och ett system med samma klassificering som inte är ackrediterat för att behandla sådan information måste använda en evaluerad produkt med assuransnivå EAL2 (eller högre) eller motsvarande skyddsprofil.
[176] Myndigheter måste vidare bekräfta integriteten hos programvara som de installerar innan de distribueras i ett system för att säkerställa att ingen oavsiktlig programvara installeras samtidigt.
[177] Alla trådlösa åtkomstpunkter som används för statliga trådlösa nätverk måste vara ”Wi-Fi Alliance”-certifierade.

formation nationell säkerhet måste myndighetens system ackrediteras av den nationella byrån för kommunikationssäkerhet (GCSB) innan ett resulterande formellt godkännande av systemets driftsättning kan ske. Vidare kräver system och tjänster med kompartmentaliserad eller förbehållen (”caveated”) information klassificerad som konfidentiell och högre ackreditering av generaldirektören på GCSB (eller formell delegat). Också användning av högassurans-kryptoutrustning kräver kontroll i form av ackreditering av GCSB. Generellt i fall där information och system är klassificerade begränsat hemliga (restricted) eller lägre ligger uppgiften att godkänna systemet internt hos organisationens chef.

9.12 Australien

Aktörer inom informations- och cybersäkerhet

ASD – Australienska signaldirektoratet

Australian Signals Directorate (ASD) är en statlig myndighet med uppdraget att försvara Australien från globala hot och att främja Australiens nationella intressen. Ytterst ansvarig för ASD är Försvarsministern. ASD arbetar med underrättelse- och säkerhetstjänst samt cybersäkerhet för att stödja regeringen, försvarsmakten och samhället i stort. ASD har funktioner inom kryptografi och IKT. ASD utför bl.a. produktevalueringar av programvara och IKT-utrustning som används för att skydda hemlig och kvalificerat hemlig information.

Nationellt cybersäkerhetscenter

Australian Cyber Security Center (ACSC) är en del av ASD. ACSC leder och samordnar den australiensiska regeringens insatser för ökad nationell cybersäkerhet. Centret utgör ett nav för samarbete mellan offentlig och privat sektor samt inom informationsdelning avseende cybersäkerhet. Centret bistår med cybersäkerhetsrådgivning och stöd i hela det australienska samhället. Inom centret finns den nationella CERT-funktionen som svarar på cybersäkerhetshot och incidenter.

ACSC certifierar produktevalueringar vilka utförs av licensierade kommersiella evalueringsföretag (AISEF, se nedan) i enlighet med

Common Criteria som en del av det australiensiska programmet för evaluering av informationssäkerhet, AISEP.

AISEF och ACA – evalueringar

Australian Information Security Evaluation Facility (AISEF) är ett privat företag licensierat av ASD och ackrediterat av *National Association of Testing Authority, Australia* (NATA), för att genomföra evalueringar i enlighet med Australasian *Information Security Evaluation Program*, AISEP (se nedan). Utvärderingsaktiviteterna är certifierade av *Australian Certification Authority* (ACA). Samtliga evalueraringsföretag måste godkännas av ACA. AISEF och ACA genomför evaluerings- och certifieringsaktiviteterna genom samarbete.

NATA-ackreditering

National Association of Testing Authority, Australia (NATA) är Australiens nationella ackrediteringsorgan för ackreditering av organ för bedömning av överensstämmelse. NATA är också Australiens s.k. övervakningsmyndighet inom *Organisation for Economic Co-operation and Development* (OECD).

NATA har ingått ett samförståndsavtal (Memorandum of Understanding) med den australienska regeringen som erkänner dess nyckelroll i Australiens tekniska infrastruktur. Regeringen rekommenderar användning av NATA-ackrediterade företag när detta är ett alternativ och uppmuntrar organisationer att göra detsamma.[178]

NATA tillhandahåller oberoende assurans om teknisk kompetens och integritet hos organ för bedömning av överenstämmelse. Detta görs för kunder som behöver förtroende för leveransen av sina produkter och tjänster. Förutom ackreditering tillhandahåller NATA bedömningar och utbildningstjänster till laboratorier och tekniska anläggningar.

[178] Avtalet anger vidare att NATA är skyldig att vidta alla ackrediteringsaktiviteter opartiskt i enlighet med kraven i ISO/IEC 17011 och tillhandahålla nationellt ledarskap genom att ge ut ackrediteringsprogram som medför att ackrediterade organ möter nationella intressen. I tillämpliga fall ska NATA:s procedurer överensstämma med internationella standarder. Dokumentet innehåller även ett antal ytterligare åtaganden som syftar till att involvera andra viktiga aktörer i aktiviteterna och skapa transparens. Regeringen å sin sida åtar sig att assistera NATA finansiellt och informera organisationer om NATA:s roll som nationellt ackrediteringsorgan. Vidare kräver regeringen att just NATA utför ackreditering i vissa situationer.

NATA har också undertecknat internationella ackrediteringsavtal som föranleder ömsesidigt erkännande.

IRAP

The Information Security Registered Assessors Program (IRAP) är ASD-certifierade IKT-experter som har särskild kunskap om ISM-säkerhetskrav (se nedan). IRAP syftar till att säkerställa att aktörer inom regeringen och industrin kan få tillgång till högkvalitativa bedömningar av IKT. Bedömarna kan tillhandahålla bedömningar av bl.a. informationssystem upp till ”top secret”-nivån. De ackrediterar eller certifierar dock inte system å ASD:s vägnar.

Reglering av informations- och cybersäkerhet

Allmänt

Lagtext om det nationella cybersäkerhetsarbetet är begränsad i Australien. Landet lägger visserligen stora ansträngningar på cybersäkerhet, men gör det utan lagstiftning och förlitar sig mer på ”mjuk lag” (soft law).[179]

Nationell cybersäkerhetsstrategi

2020 antog Australien en ny cybersäkerhetstrategi.[180] I strategin anges att regeringen kommer att stödja företagens cybermotstånd bl.a. genom att dela hotinformation, ställa tydliga förväntningar på roller och stärka partnerskap. Regeringen avser vidare att arbeta med industrin för att skydda landets mest kritiska system från mer allvarliga hot. Dessutom ges brottsbekämpande myndigheter större befogenhet att skydda medborgarna online.

Strategin framhåller även att berörda företag bör producera säkra produkter och tjänster samt att en frivillig uppförandekod kommer att beskriva regeringens säkerhetsförväntningar för internetanslutna konsumentenheter som medborgarna använder dagligen. Regeringen bedömer att lagstiftningsreformer och ett samarbete med industrin

[179] Se *Cybersecurity law overview – a report by Mannheimer Swartling*, april 2017, s. 8.
[180] Se www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy.

behövs för att tydliggöra industrins skyldigheter angående cybersäkerhet i framtiden.

Slutligen kommer den australienska regeringen att lägga mer resurser på att öka allmänhetens medvetenhet om cybersäkerhetshot.

AISEP – program för evaluering av it-säkerhetsprodukter

Australasian Information Security Evaluation Program, AISEP, hanterar evaluering och certifiering av it-säkerhetsprodukter enligt *Common Criteria*-standarden för att skydda system och information mot cyberhot. Det är främst australienska och nyzeeländska statliga myndigheter som förvärvar och använder de certifierade it-säkerhetsprodukterna. Genom AISEP är Australien och Nya Zeeland signatärer inom CCRA.[181]

ISM – nationell handbok för informationssäkerhet

Som en del av sin rådgivning tillhandahåller ACSC *Australian Government Information Security Manual* (ISM) innehållande ett ramverk för cybersäkerhet som organisationer kan tillämpa för att skydda sina system och information från cyberhot.[182]

Organisationer är som utgångspunkt inte skyldiga enligt lag att följa ISM. ISM är vidare subsidiär i förhållande till avvikande lagstiftning. Syftet med cybersäkerhetsprinciperna i ISM är att ge praktisk vägledning om cybersäkerhet, inbegripet IKT-säkerhet. Handboken använder ett ramverk för riskhantering som är baserat på NIST 800-37 (se ovan under USA), enligt vilket systemet ska definieras och anpassade säkerhetskontroller införs. ISM används framför allt för att styra myndigheters arbete med informations- och cybersäkerhet.

När det gäller informationstillgångar som ägs av eller anförtrotts den australiensiska regeringen finns ett antal grundläggande krav på informationssäkerhet som aktörer tillämpar. Bl.a. måste varje enhet säkerställa en säker drift av sina IKT-system för att skydda informa-

[181] Certifikat på evalueringsnivåerna EAL 1–4 är därmed ömsesidigt erkända.
[182] ISM är avsedd att användas av informationssäkerhets- och it-chefer.

tion om statliga angelägenheter genom att tillämpa ISM:s cybersäkerhetsprinciper under alla stadier av varje systems livscykel.[183]

För kvalificerat hemliga (”top secret”) system kan bedömningar av säkerhetskontroller genomföras av ASD-bedömare (eller deras delegater). På nivån hemlig och lägre kan säkerhetsbedömningen av systemen göras av en organisations egna bedömare eller IRAP-bedömare (Information Security Registered Assessors Program). I alla fall ska bedömarna ha ett lämpligt säkerhetsgodkännande och tillräcklig kompetens i förhållande till berörd systemtyp.[184]

Innan ett system får tas i drift behöver beslut fattas i fråga om åtföljande säkerhetsrisk kan accepteras. Om riskerna med systemets drift accepteras kan driftsättningen godkännas, annars kan den nekas. Den som har till uppgift att godkänna systemet (authorising officer) kan dessutom, i avvaktan på att en acceptabel standard nås, kräva ytterligare information av systemägaren eller tillåta driftsättning av systemet med vissa användningsbegränsningar. För kvalificerat hemliga system och system som bearbetar, lagrar eller kommunicerar kvalificerat hemlig eller känslig kompartmentaliserad information är ASD:s generaldirektör godkännandeorgan. På nivån hemlig och lägre ligger uppgiften att godkänna systemet hos en organisations informationssäkerhetschef eller motsvarande. I alla fall bör godkännaren ha en lämplig nivå av kompetens och förståelse för säkerhetsrisker.

Som tidigare berörts utför ASD produktevalueringar i syfte att tillhandahålla en högre nivå av assurans hos produkters säkerhetsfunktionalitet. Som vägledning vid anskaffning (”acquisition”) hänvisar ISM till dessa evalueringar som sker genom dels programmet *ASD Cryptographic Evaluation* (ACE) för produkter som används för att skydda klassificerad (”classified”) information, dels *High Assurance Evaluation*-programmet för produkter som används för mycket känslig (”highly classified”) information. Vid upphandling av specifik IKT-utrustning med assuransnivån hög kontaktas ACSC.

ISM har många likheter med NIST RMF (se ovan), fast är något förenklad.

[183] Se den australienska regeringens *Protective Security Policy Framework*, Policy 11 om robusta IKT-system (www.protectivesecurity.gov.au/information/Pages/default.aspx).
[184] Ibid.

Policyramverk för säkerhetsskydd

Attorney-General's Department inom den australienska regeringen har tagit fram ett policyramverk för säkerhetsskydd, där robusta IKT-system är en del av policyn. Huvudkravet i denna del är att aktörerna måste säkerställa en säker drift av sina IKT-system för att skydda information om statliga angelägenheter genom att tillämpa ISM:s cybersäkerhetsprinciper under alla stadier av varje systems livscykel. Enheter får endast hantera information om IKT-systemets drift auktoriserats av behörig auktoritet. När man skapar nya IKT-system eller implementerar förbättringar av befintliga system måste beslutet att godkänna att ett IKT-system tas i drift baseras på den riskbaserade cybersäkerhetsstrategin i ISM. Det krävs att alla IKT-system erhåller godkännande inför driftsättningen för att säkerställa att en lämplig säkerhetsnivå tillämpas på systemet och att återstående säkerhetsrisker accepterats av den berörda myndigheten. IKT-systemen måste vara godkända för åtminstone den känslighet eller klassificering av information som det kommer att behandla.

Bemyndigande att driva ett IKT-system är inte permanent. Under ett IKT-systems livscykel kan det kräva att godkännande återkallas för att kunna drivas eller så småningom tas ur drift. T.ex. kan förändringar av systemet eller upptäckten av nya cyberhot motivera en omprövning.

Kvalificerat hemliga system ska säkerhetsbedömas, och i tillämpliga fall godkännas, av ASD.

Sammanfattning av särskilda krav på IKT i säkerhetskänslig verksamhet

Av inhämtade uppgifter framgår att det finns myndigheter i Australien med ansvar för nationell informations- och cybersäkerhet samt uppgifter att evaluera respektive certifiera IKT. När det gäller information om statliga angelägenheter som tillhör regeringen behöver berörda IKT-system godkännas innan de får tas i drift. För kvalificerat hemliga system och system som hanterar kvalificerat hemlig eller känslig kompartmentaliserad information är en underrättelse- och säkerhetstjänst (ASD:s generaldirektör) godkännandeorgan. I övriga fall brukar uppgiften att godkänna systemen ligga hos respektive

organisations säkerhetschef. Några motsvarande nationella krav på certifiering av sådana system har dock inte framkommit.

9.13 Gränsöverskridande system

Inledning

Så som uppdraget får förstås har utredningen i denna del endast till uppgift att göra en jämförelse med nationell lagstiftning i andra intressanta länder. För att utröna behovet av ytterligare nationella krav på certifiering och godkännande är det emellertid relevant att även göra en kartläggning av gränsöverskridande system och förfaranden som kan aktualiseras på internationell nivå. I kapitel 13 lämnar utredningen en sammanfattning av de gränsöverskridande systemen på området.

Nationella säkerhetsmyndigheter (NSA)

Det ska finnas säkerhetsmyndigheter i EU:s medlemsstater med uppdrag att så långt det är möjligt enligt nationell rätt säkerställa att aktörer på deras territorium vidtar alla lämpliga åtgärder för att skydda säkerhetsskyddsklassificerade EU-uppgifter under förhandlingar som förs innan ett kontrakt ingås och när ett kontrakt som kräver säkerhetsskyddsavtal genomförs. Vidare ska medlemsstaterna säkerställa att entreprenörerna innehar ett säkerhetsskyddsgodkännande av verksamhetsställe på relevant säkerhetsskyddsklassificeringsnivå (se artikel 11 p. 4 och 5 i *Rådets beslut om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter* [2013/488/EU]). Medlemsstaterna ska således utse en nationell säkerhetsmyndighet (NSA) med ansvar för säkerhetsarrangemangen för skydd av uppgifterna så att Rådets beslut (2013/488/EU, se nedan) respekteras av berörda aktörer.

Organisationen av säkerhetsmyndigheter varierar i medlemsstaterna. I t.ex. Frankrike har man en dedikerad myndighet som har det samlade ansvaret för säkerheten nationellt (ANSSI). I Sverige finns i stället flera myndigheter som har olika mandat; Försvarsmakten och Säkerhetspolisen. Härutöver finns internationella överenskommelser.

Enligt säkerhetsskyddsförordningen (2018:658) 6 kap. 1 § ska Regeringskansliet vara nationell säkerhetsmyndighet för internationella säkerhetsskyddsåtaganden gentemot Europeiska unionen och dess medlemsländer inom ramen för EU-arbetet, Nato och Europeiska rymdorganet (ESA) och fullgöra de uppgifter som en sådan myndighet har enligt dessa internationella säkerhetsskyddsåtaganden. I 20 § 8 p. förordningen med instruktion för Regeringskansliet (2009:923) anges att Regeringskansliet ska vara den nationella säkerhetsmyndighet som ansvarar för att upprätthålla säkerheten för sekretessbelagda uppgifter enligt Europeiska rådets säkerhetsföreskrifter samt enligt Sveriges åtaganden om detta i överenskommelser med Västeuropeiska unionen och Nato inom ramen för samarbetet *Partnerskap för fred*.

NSA-funktionen i Sverige är placerad på UD.[185] Säkerhetspolisen är enligt säkerhetsskyddsförordningen 7 kap. 1 § s.k. kompetent säkerhetsmyndighet (med föreskrifts- och tillsynsrätt) civilt medan den militära underrättelse- och säkerhetstjänsten (Must) vid Försvarsmakten är det militärt. FMV är nationell industrisäkerhetsmyndighet enligt förordningens 6 kap. 1 §.

NSA ansvarar för att upprätthålla säkerheten för de säkerhetsskyddsklassificerade uppgifter som Sverige tar emot från EU, ESA och NATO – oavsett var den förvaras (inrikes/utrikes, myndighet/organ respektive offentliga/privata). NSA ska vidare periodiskt inspektera att säkerheten är tillfredställande, vilket sköts av Försvarsmakten och Säkerhetspolisen. NSA ansvarar för att personal som hanterar EU-/Nato-konfidentiell information säkerhetsgodkänns (3 kap. säkerhetsskyddslagen). NSA:s uppdrag inbegriper även att säkerhetsplaner för informationen upprättas.

NSA-funktionen vid Regeringskansliet står även som garant för de säkerhetsgodkännanden som görs mot EU, ESA och NATO vad gäller ackrediteringar av it-system och anläggningar. Funktionen hanterar och koordinerar vidare EU-, ESA- och Nato-förfrågningar, där godkännande av krypton respektive delgivning av EU-/ESA-/Nato-interna dokument är en del.

[185] Regeringskanslets föreskrifter med arbetsordning för Utrikesdepartementet (UF 2019:3, 37 §) anger att Säkerhetsenheten ansvarar för frågor rörande säkerheten för sekretessbelagda uppgifter enligt säkerhetsskyddsavtal med Europeiska unionens medlemsländer och Europeiska rådet samt enligt åtaganden om detta i överenskommelser med Nato och Europeiska rymdorganet (ESA).

Rådets beslut om skydd av säkerhetsskyddsklassificerade EU-uppgifter och AQVA

Den 23 september 2013 antog Europeiska unionens råd ett beslut om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (2013/488/EU). Beslutet fastställer grundläggande principer och miniminormer för säkerhet för att skydda säkerhetsskyddsklassificerade EU-uppgifter[186] som ska gälla för rådet och rådets generalsekretariat. Reglerna ska iakttas av medlemsstaterna i enlighet med deras nationella författningar, så att de alla kan vara förvissade om att säkerhetsskyddsklassificerade EU-uppgifter ges en motsvarande skyddsnivå.

Rådets beslut innehåller bl.a. bestämmelser om hur säkerhetsskyddsklassificerade EU-uppgifter i kommunikations- och informationssystem ska skyddas. Dessa system ska till en början genomgå en ackrediteringsprocess, där godkännandet från säkerhetssynpunkt syftar till att skapa förvissning om att alla lämpliga säkerhetsåtgärder vidtagits och att tillräckligt hög skyddsnivå för uppgifterna och systemen uppnåtts i enlighet med beslutet. Vidare ska säkerhetsåtgärder genomföras för att skydda system som hanterar uppgifter på säkerhetsskyddsklassificeringsnivån *EU CONFIDENTIAL* och högre mot vissa risker för oavsiktlig spridning. Om de säkerhetsskyddsklassificerade EU-uppgifterna skyddas med hjälp av kryptoprodukter, ska sådana produkter godkännas på föreskrivet sätt. Rådet är kryptogodkännande myndighet för uppgifter på säkerhetsskyddsklassificeringsnivån *EU SECRET*. Konfidentialiteten för uppgifter på säkerhetsskyddsklassificeringsnivån *EU CONFIDENTIAL* eller *EU RESTRICTED* ska skyddas genom kryptoprodukter som har godkänts av rådets generalsekreterare. Uppgifter på denna nivå inom medlemsstaternas nationella system får även skyddas genom kryptoprodukter som godkänts av en medlemsstats kryptogodkännande myndighet.

Endast godkänd utrustning eller godkända anordningar ska användas för att skydda säkerhetsskyddsklassificerade EU-uppgifter på nivån *EU CONFIDENTIAL* eller högre. Om angivna produkter inte används ska uppgifterna antingen överföras på elektroniska medier som

[186] Säkerhetsskyddsklassificerade EU-uppgifter är uppgifter vars obehöriga röjande skulle kunna åsamka Europeiska unionens eller en eller flera av dess medlemsstaters väsentliga intressen olika grader av skada.

skyddas med godkända kryptoprodukter eller som föreskrivet av den behöriga säkerhetsmyndigheten om säkerhetsåtgärder.

När säkerhetsskyddsklassificerade EU-uppgifter överförs på elektronisk väg ska godkända kryptoprodukter användas (artikel 10.7). Trots detta krav får specifika förfaranden i krissituationer eller specifika tekniska konfigurationer enligt bilaga IV till beslutet tillämpas. I bilagan beskrivs bl.a. ett förfarande för utvärdering och godkännande av produkter för it-säkerhet. Säkerhetsnivån, som avser den grad av förtroende som krävs i säkerhetsåtgärderna, ska kontrolleras genom att internationellt erkända eller nationellt godkända processer och metoder används. Detta inbegriper i första hand evaluering, skyddsåtgärder och revision. Kryptoprodukter för skydd av säkerhetsskyddsklassificerade EU-uppgifter ska evalueras och godkännas av en medlemsstats nationella kryptogodkännande myndighet. Innan sådana kryptoprodukter rekommenderas för godkännande av rådet eller generalsekreteraren ska de ha genomgått och klarat en andrapartsevaluering av en medlemsstats kvalificerade utvärderingsmyndighet, *Appropriately Qualified Authority* (AQUA) som inte deltagit i utformningen eller tillverkningen av utrustningen. Hur detaljerad andrapartsevalueringen ska vara beror på den planerade högsta säkerhetsskyddsklassificeringsnivån för de säkerhetsskyddsklassificerade EU-uppgifter som ska skyddas genom dessa produkter. En kvalificerad utvärderingsmyndighet (AQUA) ska vara en kryptogodkännande myndighet i en medlemsstat, vilken har ackrediterats på grundval av kriterier som rådet har fastställt för att genomföra andrapartsevalueringen av kryptoprodukter för skydd av säkerhetsskyddsklassificerade EU-uppgifter.[187]

AQUA, dvs. godkänd andrapartsevaluerare av krypto inom EU, finns i fem medlemsstater, däribland Sverige[188]. Frankrike, Italien, Nederländerna och Tyskland är de övriga kryptogodkända länderna.[189]

Även om säkerhetskraven i det nu nämnda beslutet formellt endast riktar sig till rådet och den egna organisationen har angivna krav inkorporerats även i multilaterala avtal (se nedan) som en form av standard och bästa praxis i ett vidare sammanhang. I denna del blir det

[187] Det kan emellertid även förhålla sig på det sättet att EU accepterar att en medlemsstat under viss tid använder s.k. Nato-godkänt krypto.
[188] Det är Swedish NCSA (National Communications Security Authority) som är AQUA i Sverige, och vidare är Must Swe NCSA (utpekade av NSA på UD).
[189] Alla länder skapar sina egna krypton för nationellt bruk, men vissa kryptoprodukter som blir evaluerade kan fritt användas för EU-klassificerade uppgifter och motsvarande, med fördelen att produkterna är föremål för ömsesidigt erkännande.

därmed fråga om en gemensam regeluppsättning för säkerhet och en samverkan mellan medlemsstaterna om hur säkerhetsskyddsklassificerade EU-uppgifter ska hanteras.

Multilateralt säkerhetsskyddsavtal

Vid hantering av gemensamt hemliga uppgifter ingår EU:s medlemsstater bl.a. multilaterala säkerhetsskyddsavtal för att skydda uppgifterna. I dessa avtal hänvisas till rådets beslut (se ovan) i fråga om gällande säkerhetskrav och -åtgärder, vilket innebär att godkända kryptoprodukter/gemensamhetsprodukter ska användas. Avtalet anger att rådets beslut ska respekteras och att det nationella skyddet minst ska motsvara det som föreskrivs vad gäller hanteringen av säkerhetsskyddsklassificerade EU-uppgifter.

EU:s medlemsstater har ingått ett multilateralt avtal om skydd av säkerhetsskyddsklassificerade uppgifter som utbyts i EU:s intresse (2011/C 202/05). Syftet med avtalet är att skydda säkerhetsskyddsklassificerade uppgifter som härrör från unionen eller parterna.

Genom det multilaterala avtalet förbinder sig parterna att vidta alla lämpliga åtgärder enigt nationell rätt för att säkerställa att den säkerhetsnivå som ges säkerhetsskyddsklassificerade uppgifter som omfattas av avtalet är likvärdig med den som ges enligt säkerhetsbestämmelserna inom unionens råd för säkerhetsskyddsklassificerade EU-uppgifter som har motsvarande säkerhetsskyddsklassificeringsnivå (artikel 3). Parterna ska vidare säkerställa att de uppgifter som omfattas av avtalet har vederbörligt skydd (artikel 6). Varje part ska också säkerställa att lämpliga åtgärder[190] vidtas för skydd av de säkerhetsskyddsklassificerade uppgifter som hanteras i kommunikations- och informationssystem (artikel 7).

[190] Sådana åtgärder ska åtminstone säkerställa uppgifternas konfidentialitet, integritet och tillgänglighet.

NATO:s regler för säkerhet

Liksom vid utbyte på EU-nivå (se ovan) aktualiseras gemensamma hemliga uppgifter också vid Nato-samarbetet.

För att skydda Nato-information och informationssystem som behandlar Nato-information eller Nato-utrustning kan krav i nationell rätt gälla när inget annat följer av Nato:s säkerhetsregler.

Förutom nationella klassificeringar av hemlig information beaktas att det även finns kategorier som avser Nato: *Nato Restricted*, *Nato Confidential*, *Nato Secret* och *Cosmic Top Secret*.

Behörighet krävs för tillgång till Nato-klassificerad information för ett specifikt kontrakt. Vissa internationella avtal kräver Natogodkännanden för personal och organisationer.

Ett kryptosystem avsett att skydda information klassificerad *Nato Secret* och uppåt ska vara godkänt av *Nato Military Committee*, (NAMILCOM) vilket innefattar en andrapartsevaluering av *Nato's Information Security and Evaluation Agency* (SECAN). För att nationellt skydda *Nato Restricted* och *Nato Confidential* ska systemet vara godkänt av lämplig myndighet i landet. För länder som inte tillhör Nato krävs det dock ett särskilt godkännande för detta, och ett sådant har Sverige och Swe NCSA (dvs. Must).

9.14 Sammanfattande slutsatser

En allt viktigare aspekt för IKT-system är att dessa alltmer behöver säkerställa informations konfidentialitet men även bibehålla dess integritet och tillgänglighet. Utmaningarna med samhällets ökande grad av digitalisering är gränsöverskridande och många. Nationella myndigheter i de flesta jämförbara länder tillstår att den digitala utvecklingen medför oerhörda positiva möjligheter samtidigt som ett stort antal säkerhetsutmaningar måste hanteras.

I syfte att öka cybersäkerheten i IKT-system har många stater utvecklat sina egna nationella ordningar för cybersäkerhetscertifiering med olika cybersäkerhetskrav och assuransnivåer, vilka återspeglar deras rättsliga och ekonomiska kontexter. Särskilda krav på evaluering och certifiering av IKT förekommer i varierande säkerhetskänsliga domäner. Flertalet länder har också infört krav på godkännande av informationssystem i säkerhetskänslig verksamhet. Det

finns även gränsöverskridande processer för evaluering och ackreditering av IKT, inbegripet användning av kryptoutrustning.

Merparten av de undersökta länderna lägger stor vikt vid en helhetssyn, även om de organisatoriska lösningarna för att skapa skydd skiljer sig något åt.[191] Alla länder har också en eller flera nationella svarsmiljöer för hantering av IKT-händelser. Överlag lägger länderna tonvikt på att organisera sitt cybersäkerhetsarbete på ett sätt som säkerställer att förebyggande säkerhetsarbete ses i ett sammanhang av brottsförebyggande, beredskap och incidenthantering.[192] Samtidigt ökar medvetenheten om vikten av att inkludera alla relevanta aktörer i cybersäkerhetsarbetet.[193] Flera av länderna prioriterar att inkludera offentliga och privata företag, säkerhetsindustrin, den akademiska världen och andra organisationer både i utvecklingen av nationella cybersäkerhetsstrategier och genomförandet av anslutande åtgärder.[194] Under de senaste åren har myndigheterna i flera av länderna varit mycket tydliga med att cybersäkerhet är ett högt prioriterat område på den politiska agendan. I linje med detta har de offentliga budgeterna för organ som ansvarar för cybersäkerhet ökat betydligt de senaste åren. Detta återspeglar en växande oro över IKT-riskbilden och en större vilja att stoppa denna utveckling.

Länderna investerar i att bygga både offensiva och defensiva kapaciteter relaterade till cybersäkerhet. Dock finns för närvarande inga länder som har övergripande nationella indikatorer för att mäta IKT-säkerhet. Ett genomgående drag är att justitie-/inrikes- och försvarsdepartement har centrala roller i länderna. Flera länder utvecklar också sin egen ”cyberdiplomati” som en del av utrikestjänsten.

Av utredningens internationella jämförelse av ett tiotal utländska system framgår att nästintill alla länder har krav på att informations-

[191] Skydd av personliga uppgifter är visserligen en viktig faktor i samband med informationssäkerhet, men denna aspekt behandlas inte närmare i detta betänkande med hänsyn till uppdragets snävare utformning. Av samma anledning har också brottsbekämpande myndigheter lämnats därhän. Inte heller personal- eller fysisk säkerhet tillägnas närmare studier i kapitlet, om än dessa utgör delar av informationssäkerheten.

[192] Mekanismer och plattformar för informationsutbyte är ofta nära integrerade med incidenthanteringsmiljöer.

[193] I vissa länder med särskilt stort fokus på samarbete mellan offentlig och privat sektor har marknadsincitament skapats för innovation och utveckling av säkerhetslösningar, samt en grund för implementering av övergripande standarder för cybersäkerhet. Dessa länder inkluderar många relevanta aktörer i utvecklingen av sina cybersäkerhetsstrategier och genomförandet av åtgärder.

[194] Sedan 2010 har samtliga av de undersökta länderna utvecklat egna nationella strategier för informations-, it- och/eller cybersäkerhet. Flertalet länder har en nationell säkerhetsstrategi som cybersäkerhetsstrategin är förankrad i.

system som kan komma att hantera hemlig och/eller kvalificerat hemlig information ska godkännas av en utpekad nationell myndighet, eller ett departement, innan systemet får driftsättas i säkerhetskänslig verksamhet. Nationella krav på evaluering och/eller certifiering av motsvarande IKT framstår som emellertid inte som lika vanliga, om än det förekommer i ett par jämförbara länder. Utredningen kan samtidigt notera att det på området finns betydande organisatoriska skillnader mellan merparten av de undersökta länderna och Sverige.

10 Allmänna överväganden

10.1 Inledning

Utredningen bedömer att det finns skäl att som utgångspunkt för överväganden i de frågor som tas upp i direktiven till utredningen behandla några mer grundläggande frågor om digitaliseringens konsekvenser för informations- och cybersäkerhet mer allmänt, utvecklingen av hot, risker och sårbarheter som följer av den pågående digitaliseringen samt förekomsten av brister i informations- och cybersäkerheten inom säkerhetskänsliga och samhällsviktiga verksamhetsområden.

Vidare behandlas även betydelsen av styrning och samordning av arbetet med informations och – cybersäkerhet samt behovet av kompetens på detta område. Förekomsten av brister inom dessa områden kan allvarligt påverka förutsättningarna att kunna åstadkomma stärkt informations- och cybersäkerhet inom olika viktiga samhällsverksamheter, bl.a. vad gäller säkerhet i nätverks- och informationssystem som används i säkerhetskänslig verksamhet.

10.2 Digitaliseringen av samhällsverksamheter

Bedömning: Den pågående digitala utvecklingen i Sverige och i världen går på många plan mycket fort. Digitaliseringen påverkar hela samhället och området kan beskrivas som horisontellt, bland annat för att det omfattar alla samhällssektorer. På samma sätt som utvecklingen av digitaliseringen kan föra med sig fördelar kan den också föra med sig nya eller förändrade hot, sårbarheter och risker som påverkar informations- och cybersäkerheten i bl.a. nätverks- och informationssystem hos olika verksamhetsutövare.

Utredningen kan konstatera – och som också Digitaliseringskommissionen framhåller – att digitaliseringen utgör en katalysator och motor i samhällsutvecklingen sedan ett par decennier tillbaka och att utvecklingen nu går mycket fort. Samhällsutvecklingen har genom historien varit nära sammanlänkad med den tekniska utvecklingen. Det som är särskilt kännetecknande för den av digitaliseringen drivna samhällsutvecklingen är hastigheten i utvecklingen. Det har sin grund i att informations- och kommunikationstekniken (IKT) kontinuerligt och snabbt utvecklar nya användningsområden och funktioner, högre prestanda samt att användarnas intresse för och kompetens att använda tekniken ständigt växer och driver utvecklingen. Det medför en omvälvande förändring och en transformering inom flera viktiga samhällsområden. Det medför nya förutsättningar för samhället i stort och påverkar alla samhällsaktörer, t.ex. påverkar det sättet att arbeta med olika utmaningar inom de flesta samhällsområden. Digitaliseringen och användningen av ny teknik förändrar förutsättningar och villkor för både offentlig och enskild verksamhet.

Som framgår av kapitel 4 har Sverige tagit fram en rad olika strategier för att tillvarata digitaliseringens möjligheter. I det övergripande målet i den nuvarande digitaliseringsstrategin anges att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter samtidigt som ett antal olika delmål satts upp, bl.a. ska det finnas de bästa förutsättningarna för alla att på ett säkert sätt ta del av, ta ansvar för och ha tillit till det digitala samhället (D-trygghet).

Betydelsen av att Sverige stärks inom digital infrastruktur och datahantering har pekats på i både regeringsuppdrag och internationella mätningar. Olika initiativ sker för att i större utsträckning kunna strukturera, tillgängliggöra och vidareutnyttja centrala datamängder, skapa en gemensam digital infrastruktur för informationsutbyte samt utveckla och effektivisera verksamheter genom datadriven innovation och automatisering med stöd av AI-tillämpningar. Därutöver är användandet av molntjänster och outsourcad it-drift redan en realitet för många myndigheter.

Myndigheten för digital förvaltning (DIGG) bedömer också att det på senare tid har det skett en tydlig ambitionshöjning vad gäller den digitala förvaltningen i Sverige. Sedan 2018 har flera större projekt initierats, bl.a. etablerandet av en förvaltningsgemensam digital infrastruktur för informationsutbyte, etableringen av flera nationella grunddatadomäner och ett intensifierat arbete med öppna data. Vidare

har styrningen av den offentliga sektorns digitalisering, som tidigare präglades av fragmentering och ett stort självbestämmande, ändrat fokus och handlar i dag mycket om att öka helhetssynen och konsolidera och standardisera de komponenter och lösningar som behövs i hela eller stora delar av förvaltningen. Denna utveckling bedöms kunna ha stor positiv inverkan på den svenska förvaltningens förutsättningar att tillvarata digitaliseringens möjligheter.

Statliga myndigheter bedriver sedan många år olika digitaliseringsarbeten. Digitaliseringen har använts och används fortsatt som ett verktyg för att uppnå kostnadsbesparingar, effektivisera och utveckla myndigheters förmåga att lösa sina uppdrag. Från att tidigare ha datoriserat informationshantering är svenska myndigheter nu inne i en fas som karaktäriseras av effektivisering och kapacitetsförbättring av sin verksamhet och tillgängliggörande av data, som är ett viktigt steg mot att Sverige ska kunna tillvarata digitaliseringens möjligheter.

DIGG leder även ett arbete med att etablera en hållbar digital infrastruktur som ska möjliggöra ett effektivt och säkert utbyte av information inom och med det offentliga. Utvecklingen av infrastrukturen ska främja nya förvaltningsgemensamma tjänster och lösningar för framtiden. Arbetet med den digitala infrastrukturen möjliggör även att nya datadrivna tekniker, t.ex. AI, kan användas för att öka innovationsförmågan och ge bättre service. En fullt utvecklad digital infrastruktur ska underlätta för medborgare och företagare i deras myndighetskontakter både nationellt och inom EU, där en uppgift till exempel bara ska behöva lämnas en gång.

Utredningen anser att man dock inte kan bortse för att digitaliseringen även medför nya eller förändrade hot, sårbarheter och risker. I takt med ett större beroende till och sammankoppling av olika digitala system, t.ex. nätverks- och informationssystem, skapas situationer där cyberangrepp och enskilda it-incidenter kan få stora och svårutredda konsekvenser som även kan påverka andra aktörer. På motsvarande sätt kan cyberangrepp och it-incidenter utanför den egna verksamheten, även utanför det egna landet, medföra stora nationella konsekvenser och för offentliga och enskilda aktörer. Digitaliseringsrådet framhåller vikten av funktionell säkerhet i digitala system, dvs. att nätverks- och informationssystem är tillförlitliga, tillgängliga och robusta. Över tid kan man förvänta sig att en hög informations- och cybersäkerhet också bidrar till ökad tillit för information och för nätverks- och informationssystem. Ökad tillit stödjer ökad använd-

ning av de digitala systemen vilket i sin tur driver på transformeringen i samhället.

10.3 Hot, sårbarheter och risker

Bedömning: Digitaliseringen av samhällets olika verksamheter medför att hot, sårbarheter och risker kontinuerligt ökar. Det innebär att risken för cyberangrepp ökar mot olika samhällsverksamheter, särskilt vad gäller säkerhetskänsliga och andra samhällsviktiga verksamheter, som många har höga skyddsvärden.

Hoten kommer främst från statliga aktörer som genomför cyberangrepp i olika syften, bl.a. som förberedelser för cyberangrepp och som industrispionage. Hoten kommer även från kriminella aktörer och ideellt motiverade aktörer, som har förmåga till cyberangrepp för olika syften.

Att kunna skydda sig mot cyberangrepp från kvalificerade hotaktörer är en nationell angelägenhet. Metoder och verktyg för cyberangrepp utvecklas ständigt och hotaktörernas spelplan förändras i takt med teknikutvecklingen. Bland de svenska mål som utsätts för cyberangrepp finns verksamheter som är väsentliga för samhällets grundläggande funktioner.

Som framgår av den myndighetsgemensamma rapporten som Säkerhetspolisen, Försvarsmakten, Försvarets radioanstalt (FRA) och Myndigheten för samhällsskydd och beredskap (MSB) offentliggjort 2020 ökar den aktuella hotbilden (se kapitel 5). Ett stort antal stater bedöms i dagsläget ha förmåga att genomföra cyberangrepp och använder cyberangrepp för att uppfylla olika nationella intressen. Vissa statliga aktörer är dessutom mycket kvalificerade och genomför cyberangrepp på ett sätt som är storskaligt, systematiskt, uthålligt och globalt. Cyberangrepp ger även angriparen möjligheter till anonymitet, förnekbarhet och vilseledning jämfört med mer traditionella metoder, vilket öppnar upp för nya möjligheter att agera utan att hamna i öppna konflikter med andra länder. Cyberangrepp från statliga aktörer pågår ständigt mot svenska mål i syfte att inhämta underrättelser. De angriper bland annat verksamheter som hanterar känslig eller skyddsvärd information som rör Sveriges säkerhet, men även öppen information kan vara av intresse.

I rapporten påpekas också att många länder utvecklar förmåga att genomföra avancerade cyberoperationer, bl.a. i form av offensiva cyberangrepp, t.ex. angrepp som stör eller avbryter försvarsrelaterade eller samhällsviktiga funktioner i syfte att minska ett lands förmåga att stå emot ett kommande militärt angrepp eller försvaga ett lands motståndskraft mot påtryckningar. Statliga aktörer bedriver även underrättelseinhämtning mot svenska myndigheter och försvarsindustri i form av cyberangrepp i syfte att kartlägga Sveriges förmåga och sårbarheter med koppling till den nationella försvarsförmågan. Statliga aktörer studerar – som förberedelse för att använda cyberangrepp i konflikter – sårbarheter som kan utnyttjas och utvecklar därefter verktyg som behövs för att genomföra cyberoperationer. Sårbarheterna utnyttjas för att ta sig in i system och infektera dessa för att kunna slå ut systemet i det fall en konflikt uppstår. Attackerna förbereds således i fredstid och kan sedan koordineras med konventionella stridsmedel om det gynnar operationen. Takten i den tekniska utvecklingen är hög och det upptäcks kontinuerligt nya sårbarheter och det pågår en ständig kapplöpning mellan medel och motmedel och det krävs därför ett fortlöpande utvecklingsarbete för att upprätthålla en förmåga till och skydd mot avancerade cyberoperationer.

Cyberangrepp genomförs även av stater som bedriver omfattande program som syftar till att genom industrispionage stjäla företagshemligheter från andra länder för att påskynda sin egen teknikutveckling. Cyberangrepp i syfte att genomföra industrispionage mot svenska mål är vanligt förekommande och innebär att svenska företag som utvecklar ny teknik kan komma att konkurreras ut av sina egna lösningar som stulits av statliga aktörer.

Cyberangrepp genomförs även av kriminella aktörer som bedriver cyberkriminalitet där det finns möjligheter till ekonomisk vinning. Ransomware, bedrägerier, stölder och liknande kriminella aktiviteter drabbar såväl myndigheter som företag och deras leverantörer, som ofta bedriver verksamheter med höga skyddsvärden. Cyberangrepp genomförs också av ideologiskt motiverade aktörer, som betraktar angrepp mot svenska mål som legitima, även om förmågan inte motsvarar vilja och ambition att genomföra sådana angrepp. Försök till cyberangrepp med enklare metoder och tekniska medel bedöms dock fortsätta, t.ex. genom distribuerade överbelastningsattacker och kapade hemsidor.

Sammanfattningsvis kan utredningen konstatera att hotbilden är sammansatt, komplex och fortlöpande ökar. Cyberangreppen både ökar i omfattning och blir alltmer tekniskt avancerade i takt med den globala teknikutvecklingen på cyberområdet. Den nationella ambitionen med den pågående digitaliseringen i samhället och av säkerhetskänsliga och andra samhällsviktiga verksamheter öppnar upp för nya sårbarheter och risker, bl.a. i de nätverks- och informationssystem som används i dessa verksamheter.

Som utredningen tidigare beskrivit följs takten i digitaliseringen inte av motsvarande utveckling när det gäller informations- och cybersäkerhet i stort i samhället och inom många viktiga samhällsverksamheter kapitel 4).

10.4 Brister i informations- och cybersäkerhet

Bedömning: Av offentliga utredningar och myndighetsrapporter framkommer att det finns allvarliga brister i informations- och cybersäkerheten inom en rad olika samhällsverksamheter. Detta gäller såväl statliga myndigheter som regioner och kommuner men även organisationer och näringslivet. Bristerna innebär uppenbara risker för angrepp mot nätverveks- och informationssystem som kan medföra allvarliga konsekvenser för samhället och aktörer inom olika verksamhetsområden.

Utredningen har – som framgår ovan – strävat efter att skaffa sig en överblicksbild över nivån på informations- och cybersäkerhet i säkerhetskänslig verksamhet. Utredningen har tagit del av offentliga utredningar och myndighetsrapporter som offentliggjorts under den senast femårsperioden, några har offentliggjorts så sent som under 2020 och 2021. Ett fåtal av dessa utredningar har behandlat frågor med anknytning till nivån på informations- och cybersäkerhet i säkerhetskänsliga verksamheter. De övriga utredningar som förekommer i detta avseende omfattas naturligen av sekretess eller i något fall även av kvalificerad sekretess, vilket innebär att utredningen inte haft tillgång till allt underlag som kan belysa om det föreligger anledning att föreslå att det införs en nationellt anpassad certifieringsordning för IKT-produkter, -tjänster och -processer i nätverks- och

informationssystem i säkerhetskänslig verksamhet. Utredningen anser att detta påverkat förutsättningarna för utredningsarbetet.

Även om det av offentliggjorda utredningar och myndighetsrapporter som utredningen tagit del av, och som redogjorts för i kapitel 8, kan dras slutsatsen att det förekommer allvarliga brister i informations- och cybersäkerheten i verksamheten hos många offentliga aktörer och i viss mån även i företag så kan inte dras en tillräckligt säker slutsats om nivån när det gäller den säkerhetskänsliga verksamheten.

Utredningen bedömer dessutom att när det gäller aktörer och verksamheter som avser säkerhetskänslig verksamhet finns anledning att göra viss åtskillnad vid analyser av verksamhet som bedrivs inom Säkerhetspolisens respektive Försvarsmaktens ansvarsområde. Inom den senare myndighetens ansvarsområde återfinns i huvudsak myndigheter under Försvarsdepartementet, dvs. i första hand inom den militära försvarssektorn. Inom Säkerhetspolisens tillsynsområde återfinns i praktiken övriga aktörer som bedriver säkerhetskänslig verksamhet. Försvarsmakten har en sedan lång tid tillbaka meddelat föreskrifter om informations- och cybersäkerhet som gäller för de övriga s.k. försvarsmyndigheterna och har dessutom genom den militära säkerhets- och underrättelsetjänstens (MUST) arbete en välutvecklad ordning för att bedriva tillsynsverksamhet inom tilldelat ansvarsområde. Utredningen har i samtal med experter med anknytning till Försvarsmaktens tillsynsområde inte erhållit sådan information att det finns befogad anledning anta att det på det området skulle förekomma motsvarande allvarliga brister i informations- och cybersäkerheten som kan återfinnas hos övriga civila aktörer som – i större eller mindre omfattning – bedriver verksamhet som omfattas av regleringen om säkerhetsskydd.

Det innebär också att när utredningen analyserar behov av åtgärder för att stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet blir utgångspunkten i denna del den överblicksbild på brister i informations- och cybersäkerhet som kan observeras i första hand hos statliga myndigheter samt kommuner och regioner inom Säkerhetspolisens tillsynsområde. Av några rapporter och studier kan även dras vissa slutsatser när det gäller brister i informations- och cybersäkerhet hos företag i näringslivet.

Av sammanställningen av offentliga utredningar och myndighetsrapporter framkommer en mycket bekymmersam bild av nivån på och omfattningen av informations- och cybersäkerheten i främst

offentlig verksamhet men även till viss del hos enskilda verksamhetsutövare. Sammantaget måste bristerna bedömas som allvarliga och utredningen anser att omfattande och samordnade åtgärder behöver vidtas i syfte att stärka informations- och cybersäkerheten i samhället i stort och särskilt inom säkerhetskänsliga och andra samhällsviktiga verksamheter. Frågor som berör förslag på mer övergripande åtgärder för att öka informations- och cybersäkerheten inom angivna verksamheter, såväl vad avser styrning som organisering och resursbehov, kräver omfattande utredningsresurser. Även om frågorna berör förutsättningarna för de åtgärder som utredningen har att överväga ligger dessa frågor utanför utredningsuppdraget och utredningen har avgränsat arbetet främst till frågorna om behov av certifiering respektive godkännande av myndighet av IKT-produkter, – tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet.

10.5 Behovet av ökad informations- och cybersäkerhet

Bedömning: Den digitala utvecklingen i samhället visar att det blir allt mer nödvändigt för alla typer av myndigheter, kommuner och regioner, organisationer och företag att arbeta systematiskt med informationssäkerhet. Det finns en grupp av myndigheter som fokuserar på digitaliseringens möjligheter, t.ex. ur ett effektiviseringsperspektiv, och en annan grupp som fokuserar på olika typer av hot, sårbarheter och risker. I takt med ökad digitalisering kommer en ökad samverkan och samordning mellan dessa grupper att få betydelse för utvecklingen i sin helhet.

Vidare krävs att informations- och cybersäkerhet går från att vara en teknikfråga till en strategisk verksamhetsfråga hos verksamhetsutövare. Ledningsfunktioner i olika former av verksamheter behöver ta ett större ansvar för det systematiska arbetet med informations- och cybersäkerhet. För det krävs kunskap och kompetens samt att dessa frågor i högre grad integreras i verksamhetsutövarnas ordinarie styrningsprocesser, t.ex. i system för ledning- och ekonomistyrning.

Digitaliseringen är något som ofta drivs genom att visa på nytta, t.ex. genom att förenkla processer och arbetssätt. Digitaliseringen medför att myndigheter och andra aktörer måste ha tillgång till och kunna behandla digital information. Detta ställer krav på ett strukturerat arbetssätt för att säkerställa att den information som behandlas hanteras på ett säkert sätt. Med säker hantering avses både att säkra tillgång till öppen information och att information som inte är öppen ska skyddas. Det kräver även att nätverks- och informationssystem som används för styrning och kontroll av verksamhet på samhällsviktiga områden är säkra. När det uppstår brister i informations- och cybersäkerheten kan följden bli omfattande konsekvenser både för samhället i stort och för individers integritet.

Utredningen kan emellertid konstatera att det många gånger är en betydande utmaning att kunna motivera investeringar i informations- och cybersäkerhet eftersom det inte omedelbart ger synbar eller upplevd nytta direkt vid investeringstillfället. Åtgärder som syftar till en stärkt informations- och cybersäkerhet i verksamheten kan i många fall betraktas som något som endast riskerar att försvåra, försena och fördyra ett projekt eller den löpande verksamheten. Många aktörer ser även utmaningar med att sätta sig in i vilka värden en säker hantering av information och säkra nätverks- och informationssystem har på längre sikt.

Utredningen kan även konstatera att inte sällan betraktas också informations- och cybersäkerhetsfrågor som enbart it-säkerhetsfrågor vilket medför att säkerhetsåtgärder av administrativ och organisatorisk art riskerar att förbises, t.ex. när det gäller utformning och följsamhet av rutiner och arbetssätt. Krav på personella och ekonomiska resurser i syfte att stärka informations- och cybersäkerheten tenderar dessutom ofta att ingå ordinarie budgetarbete för verksamheten och riskerar därmed också att inte tas upp eller beaktas som en strategisk lednings- och resursfråga.

Ett aktivt arbete med informations- och cybersäkerhet är en förutsättning för en fortsatt säker digitalisering. Det bör ses som ett grundkrav i alla verksamhetsutövares hantering av information samt nätverks- och informationssystem. Målbilden för styrning inom informations- och cybersäkerhetsområdet bör vara att få motsvarande effekt av styrningen som på t.ex. arbetsmiljö och miljöområdet. Det innebär att höja medvetenheten om behovet av strategisk styrning och ett systematiskt informationssäkerhetsarbete och att tydliggöra

detta inte bara hos statliga myndigheter utan även hos andra offentliga och enskilda verksamhetsutövare. Alla statliga myndigheter och andra offentliga aktörer, dvs. regioner och kommuner, måste bedriva ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. Vikten av att medvetenheten om informations- och cybersäkerhet ökar och att dessa frågor ingår i alla digitaliseringsprocesser har också tidigare framhållits i olika offentliga utredningar och rapporter (kapitel 4 och 8).

10.6 Ökat behov av styrning och samordning av informations- och cybersäkerhet

Bedömning: Bristen på reglering, styrning och samordning i det samlade arbetet med att stärka informations- och cybersäkerheten i samhället i stort medför betydande utmaningar för både offentliga och enskilda verksamhetsutövare. Åtgärder krävs som ger offentliga och enskilda aktörer förutsättningar att kunna uppnå en tillräcklig grad av informations- och cybersäkerhet i verksamheten. Det närmare behovet av ytterligare reglering samt tydligare styrning och samordning av arbetet med samhällets informations- och cybersäkerhet bör därför utredas i särskild ordning.

Utredningen kan konstatera att arbetet med informations- och cybersäkerhet i dag är – i enligt med den nationella regleringen och modellen för arbetet med informations- och cybersäkerhet – i allt väsentligt varje verksamhetsutövares eget ansvar. I och med att verksamhetsutövare i dag är blir allt mer beroende av andra aktörer för sin informationshantering, bl.a. i förvaltningsgemensamma digitala systemlösningar och funktioner, är det nödvändigt med samordnade åtgärder för att öka informations- och cybersäkerheten, dvs säkerhetsnivån och samtidigt reducera sårbarheter och risker i informations- och nätverkssystemen.

Utredningen kan även notera att det nationella informations- och cybersäkerhetsarbetet alltjämt är uppdelat i olika, delvis överlappande, ansvarsområden, både på departements- och på myndighetsnivå. Detta medför att det i dag också saknas ett enhetligt regelverk och ett enhetligt arbetssätt för samhällets informations- och cybersäkerhetsarbete samtidigt som det är få gemensamma krav på informations-

och cybersäkerhet, utom när det gäller tillsynsmyndigheternas krav på säkerhet i nätverks- och informationssystem i säkerhetskänslig verksamhet och verksamhet som avser samhällsviktiga och digitala tjänster. Expert- och sektorsmyndigheter har, utifrån sitt specifika ansvarsområde eller expertområde, gett ut föreskrifter som i olika grad ställer krav på säkerhet i dessa system.

Utredningen bedömer att det finns en stor risk att fragmenteringen av bl.a. kravställningen på området ökar när flera aktörer – om inte samordning sker när det är möjligt – utfärdar föreskrifter och allmänna råd om informations- och cybersäkerhet för olika verksamheter på området Detta riskerar även att få till följd att kunskap och erfarenheter som finns hos olika aktörer inte nyttjas ändamålsenligt och effektivt, dvs. att tillgängliga resurser inte riktas mot och används inom de områden där bristerna i informations- och cybersäkerheten är som störst. Det riskerar även att information om och krav på åtgärder för att möta hot och reducera sårbarheter och risker fördröjs eller aldrig blir utförda på grund av oklara ansvarsförhållanden.

Utredningen bedömer att det fragmenterade arbetet även leder till att det i allt väsentligt inom den samlade offentliga sektorn saknas gemensamma riktlinjer för vilket skydd olika typer av nätverks- och informationssystem bör ha. Detta riskerar att leda till att samma typ av information och nätverks- och informationssystem kan erhålla olika skyddsåtgärder beroende på vilken verksamhetsutövare som hanterar informationen och var i dennes system som informationen och nätverks- och informationssystemen finns. Detta riskerar att medföra effektivitetsbrister och ökade kostnader, då systemen kan få olika utformning som medför minskad interoperabilitet.

Utredningen behandlar i delbetänkande vissa frågor med anknytning till tillsyn, bl.a. att det är viktigt att regleringens olika delar samspelar så att det inte uppstår en obalans mellan dem. Om t.ex. vissa delar av tillsynsverksamheten är reglerad med avseende på vilka prestationer en tillsynsmyndighet ska åstadkomma medan andra delar har mer övergripande målformuleringar finns en risk att den detaljerade regleringen får en styrande inverkan på tillsynen, med den konsekvensen att annan mer strategiskt inriktad tillsyn får stå tillbaka. Det finns också en stor risk att verksamhetsutövare som är utsatta för tillsyn fokuserar arbetet på de delar som granskas mer specifikt och att arbetet med det övergripande arbetet med informationssäkerhet får stå tillbaka.

Mot bakgrund av detta anser utredningen att bristen på gemensam reglering, styrning och samordning av arbetet med informations- och cybersäkerhet medför betydande utmaningar i arbetet för såväl offentliga som enskilda verksamhetsutövare, t.ex. när det gäller arbete uppnå tillräcklig säkerhet i nätverks- och informationssystem i verksamheten.

Utredningen bedömer dock att förlag på åtgärder som ger offentliga och enskilda aktörer bättre förutsättningar med att genomföra och förvalta digitaliseringsarbetet och samtidigt uppnå en tillräcklig grad av informations- och cybersäkerhet kräver en fördjupad analys som ligger utanför utredningens uppdrag. Utredningen anser dock att frågan om gemensamma regler och tydligare styrning och samordning av arbetet med samhällets informations- och cybersäkerhet bör utredas och analyseras ytterligare i särskild ordning.

10.7 Tillgången på personal med kompetens inom informations- och cybersäkerhet måste öka

Bedömning: Det finns i dag ett omfattande behov av personal med kompetens i informations- och cybersäkerhet på olika nivåer hos många verksamhetsutövare, såväl inom den offentliga verksamheten som i näringslivet. Tillgången på personal med kompetens inom informations- och cybersäkerhet behöver därför öka.

En förutsättning för att kunna hantera frågor om informations- och cybersäkerhet i offentlig och privat sektor är att det finns tillgång till kvalificerad kompetens på området. Det råder emellertid en stor brist på kompetens inom informations- och cybersäkerhetsområdet.

Enligt IT & Telekomföretagens rapport *IT-kompetensbristen – en rapport om den svenska digitala sektorns behov av spetskompetens*[1] är bristen på kompetens så stor att den fortsatta utvecklingen och tillväxtkraften inom hotas. I rapporten bedöms underskottet ligga på ungefär 70 000 personer i Sverige år 2022.

[1] *IT-kompetensbristen – en rapport om den svenska digitala sektorns behov av spetskompetens*, IT & Telekomföretagens, 2020.

Brister som kan ha sin orsak i kompetensbrist på området är:

- En betydande andel myndigheter arbetar inte systematiskt med att identifiera sina skyddsvärden eller att säkerhetsskyddsklassificera sina uppgifter.
- Säkerhetsincidenter med misstänkt eller konstaterad informationsförlust av hemliga uppgifter till följd av bristfälligt implementerad och underhållen it-säkerhetsarkitektur.
- It-system som hanterar skyddsvärd information är uppkopplat mot ett öppet nätverk.
- Bristfälliga kravställningar på cybersäkerhet vid upphandlingar.

I Digitaliseringsrådets lägesbild för digital kompetens beskrivs behovet av digital kompetensförsörjning där informationssäkerhet är en del. En av rekommendationerna i lägesbilden är att utöka antalet utbildningsplatser för digitala specialister hos lärosätena genom riktade insatser. För informationssäkerhet är det dock inte bara antalet utbildningsplatser som är ett problem utan avsaknaden av utbildningar hos universitet och högskolor.

I ett digitalt samhälle behöver alla grundläggande digital kompetens för att kunna vara delaktiga. Kompetensen handlar om att förstå såväl möjligheter som risker. Internetstiftelsen anger att den generella internetkunskapen behöver öka i Sverige för att fler ska förstå riskerna med användandet av digitala tjänster och vad man själv kan göra för att förebygga riskerna. Digitaliseringsrådet framhåller behovet att växla upp arbetet med att nå alla invånare för att öka kunskapen om bland annat informationssäkerhetsfrågor. Digitaliseringsrådet föreslår att även att t.ex. Myndigheten för samhällsskydd och beredskap (MSB) kartlägger vilken typ av ytterligare stöd som efterfrågas hos myndigheter och kommuner och regioner och i vilken omfattning det befintliga metodstödet används och är känt.

Utredningen kan konstatera att bristen på informations- och cybersäkerhetskompetens i olika verksamheter är något som utmanar säkerheten hos många verksamhetsutövare. Även om tekniska risker många gånger kan hanteras riskerar ett mer strukturerat arbete med informations- och cybersäkerhet och som ser till olika aspekter och risker i verksamheten att falla bort eller bli underutvecklat. Rätt kompetens

är också en förutsättning för att kunna driva systematiskt arbetet med informations- och cybersäkerhet.

10.8 Sammanfattning

Av vad som framkommer av offentliga utredningar och myndighetsrapporter under den senaste femårsperioden kan slutsatsen dras att det pågår en omfattande digitalisering av det svenska samhället och av verksamheter inom flera viktiga samhällsområden. Digitaliseringen medför stora utvecklingsmöjligheter men medför också ökade hot, sårbarheter och risker. Informations- och cybersäkerheten har inte utvecklats på motsvarande sätt vilket medför att gapet mellan digitaliseringen och informations- och cybersäkerheten ökat och fortsätter att öka om inte kraftfulla åtgärder vidtas på området. Orsaken till att gapet ökar har sin förklaring bl.a. i form av brister i reglering, styrning och samordning av arbetet med informations- och cybersäkerhet samt brist på kompetent personal. Åtgärder som behöver vidtas innefattar bl.a. bättre styrning och samordning av arbetet med att stärka informations- och cybersäkerheten mer allmänt i samhället och särskilt inom säkerhetskänsliga och samhällsviktiga verksamheter. Vidare behöver utbildning och tillgång till personal med kompetens inom informations- och cybersäkerhet öka. Många verksamhetsutövare behöver också förbättra arbetet med ett systematiskt informationssäkerhetsarbete.

Utredningen har genom kartläggningen och sammanställningen av offentliga utredningar och myndighetsrapporter i ett tidigt skede av utredningsarbetet dragit slutsatsen att det föreligger flera olika mer eller mindre allvarliga brister i informations- och cybersäkerheten mer allmänt inom många samhällssektorer och viktiga samhällsverksamheter, bl.a. i säkerhetskänsliga verksamheter på främst Säkerhetspolisens tillsynsområde. Utredningen bedömer att flera åtgärder krävs för att stärka säkerheten i dessa verksamheter. Arbetet med att överväga sådana mer generella åtgärder för att stärka informations- och cybersäkerheten i viktiga samhällsverksamheter kräver en fördjupad och omfattande analys och ligger dessutom utanför utredningens uppdrag som är avgränsad till den säkerhetskänsliga verksamheten. Utredningen vill samtidigt framhålla att frågan med att stärka informations- och cybersäkerheten i samhället i stort och inom olika säkerhetskänsliga

och samhällsviktiga verksamheter präglas av gemensamma grunder och samberoenden, bl.a. påverkar brister i det grundläggande systematiska arbetet med informations- och cybersäkerhet i verksamheten även förutsättningarna för att kunna uppnå säkerhet i nätverks- och informationssystem i säkerhetskänslig verksamhet hos samma verksamhetsutövare. Vidare kan cyberangrepp mot en enskild verksamhetsutövare innebära följdskador hos en eller flera andra verksamhetsutövare, vid mer allvarliga angrepp kan i vissa fall kan hela samhällssektorer slås ut. I nästa kapitel (kapitel 11) redovisas utredningens allmänna överväganden om behovet av att stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet.

11 Åtgärder för stärkt säkerhet i nätverks- och informationssystem

11.1 Inledning

Utredningen har i föregående kapitel behandlat några av de mer grundläggande frågor som är av betydelse för möjligheterna att kunna stärka informations- och cybersäkerhet mer allmänt men som även utgör förutsättningar för att kunna stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet. För nätverks- och informationssystem som används i eller har betydelse för säkerhetskänslig verksamhet finns i dag särskilda krav i säkerhetsskyddsförordningen (2018:658). Det rör sig bl.a. om förberedande åtgärder inför driftsättning av informationssystem och om säkerhetskrav som kontinuerligt ställs på informationssystemen. Bestämmelserna innehåller även krav på samråd med Säkerhetspolisen eller Försvarsmakten i vissa fall. Detta gäller för informationssystem som kan komma att behandla säkerhetsskyddsklassificerade uppgifter av visst slag och informationssystem där obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är obetydlig. Bestämmelserna innebär att det är verksamhetsutövaren som ansvarar för att se till att informationssystemen upprätthåller kraven på informationssäkerhet.

11.2 Begreppet informationssystem

Bedömning: Begreppet informationssystem används i säkerhetsskyddslagen respektive säkerhetsskyddsförordningen, medan begreppet nätverks- och informationssystem är det begrepp som används i första hand inom bl.a. det europeiska ramverket för cybersäkerhetscertifiering och området för samhällsviktiga och digitala tjänster (dvs. NIS-direktivets tillämpningsområde). Båda begreppen används i nationell författningsreglering och tillämpas för i allt väsentligt samma typer av nätverks- och informationssystem. Efter införandet av föreslagna ändringar i säkerhetsskyddsregleringen (se bl.a. prop. 2020/21:194) bör vid en ny författningsöversyn på området frågan om samstämmighet av nu nämnda begrepp övervägas närmare.

Som utredningen tidigare anger förekommer, såväl nationellt som internationellt, olika begrepp och definitioner på informations- och cybersäkerhetsområdet. Mångfalden av begrepp väcker frågan vad som avses med begreppet i det sammanhang som det används. Ett exempel på en sådan fråga är om det föreligger någon skillnad mellan begreppet informationssystem, som är det begrepp som används i den nationella regleringen av säkerhetsskydd och begreppet nätverks- och informationssystem, som är det begrepp som används inom bl.a. det europeiska ramverket för cybersäkerhetscertifiering och inom tillämpningsområdet för samhällsviktiga och digitala tjänster, dvs. NIS-direktivets tillämpningsområde. Det senare begreppet används i den nationella författningsreglering som införts i anslutning till EU:s författningsreglering på angivna områden. Det medför att såväl begreppen informationssystem som nätverks- och informationssystem används i den nationella författningsregleringen och tillämpas för i allt väsentligt samma typer av nätverks- och informationssystem. Företeelsen är i och för sig förståelig mot bakgrund av områdets i vissa fall mycket komplexa karaktär och att utvecklingen på nätverks- och informationsområdet sker över tid med många olika aktörer involverade, såväl nationellt som internationellt. Man kan samtidigt notera att i den nationella regleringen på säkerhetsskyddsområdet används begreppet informationssystem genomgående, såväl i gällande författningsreglering som i offentliga utredningar och rapporter från myndigheter, vilket medför en utmaning när det gäller vilka

begrepp som utredningen lämpligen bör använda i detta utredningsarbete.

Utredningen anser att det finns starka skäl för att samma begrepp och definition bör användas för nätverks- och informationssystem om det inte finns anledning till annat förhållningssätt. Utredningen kan emellertid konstatera att den nationella författningsregleringen för skydd av säkerhetskänslig verksamhet tidigare och även nu är föremål för revidering och att någon ändring av begreppet informationssystem i denna författningsreglering inte aktualiserats.

Uppdraget innefattar frågor – som det uttrycks i direktiven – om behovet av att stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet. Utredningen anser att begreppet informationssystem som det används i den nu gällande författningsregleringen och i det förslag till förförfattningsförändring som tas upp i propositionen *Ett starkare skydd för Sveriges säkerhet* (prop. 2020/21:194) bör kvarstå i avvaktan på revidering av lagstiftningen. Vid en ny översyn av författningsregleringen av skydd för säkerhetskänslig verksamhet bör dock frågan om samstämmighet av begreppen på området övervägas närmare. Utredningen använder därför begreppet informationssystem i efterföljande kapitel när frågan om certifiering respektive godkännande av informationssystem övervägs, utom i de fall då begreppet informationssystem relaterar till begreppet nätverks- och informationssystem i annan författning, då det senare begreppet används. I sak avses emellertid inte någon skillnad.

11.3 Nuvarande brister i säkerheten i informationssystem

Bedömning: Av offentliga utredningar och myndighetsrapporter kan slutsatsen dras att det finns allvarliga brister mer allmänt i informations- och cybersäkerhet hos offentliga och enskilda verksamhetsutövare. Om motsvarande brister även finns hos verksamhetsutövare som bedriver säkerhetskänslig verksamhet är svårare att överblicka och redovisa då dessa uppgifter naturligen omfattas av sekretess med stöd av offentlighet- och sekretesslagen. Av vad som anges i ett begränsat antal offentliga utredningar och myndighetsrapporter kan ändå – med viss grad av säkerhet – slutsatsen dras att framför allt offentliga verksamhetsutövare, dvs. statliga

myndigheter, regioner och kommuner, som bedriver säkerhetskänslig verksamhet på Säkerhetspolisens tillsynsområde uppvisar allvarliga brister i informations- och cybersäkerhet i verksamheten och att det även gäller brister i säkerheten i informationssystem som används i sådan verksamhet. I vad mån motsvarande brister finns hos enskilda verksamhetsutövare, dvs. företag i näringslivet, är mer osäkert men utredningen bedömer att utgångspunkten här bör vara att även hos dessa behöver säkerheten öka i informationssystem.

Angivna brister innebär uppenbara risker för angrepp mot informationssystem i säkerhetskänslig verksamhet och som kan medföra allvarliga konsekvenser för samhället som helhet och för olika aktörer inom samhällsviktiga områden.

Som utredningen tidigare framhåller förutsätter förslag på åtgärder som syftar till att stärka säkerheten i informationssystem i säkerhetskänslig verksamhet att det föreligger brister i denna säkerhet alternativt att det kan klarläggas att även om några egentliga brister inte kan observeras så finns det skäl att ytterligare förstärka säkerheten för att motverka eventuella framtida hot, sårbarheter och risker. Genom sammanställningen av de olika offentliga utredningar och rapporter som redogörs för i kapitel 8 framkommer en bekymmersam bild över nivån på informations- och cybersäkerheten i många samhällsviktiga verksamheter, detta gäller såväl säkerhetskänsliga verksamheter som verksamheter som avser samhällsviktiga och digitala tjänster. Denna bild har också bekräftats av utredningens sakkunniga och experter under utredningsarbetet. Som utredningen konstaterar i kapitel 8 respektive 10 berör bristerna många olika delar av informations- och cybersäkerheten, bl.a. vad gäller brister i styrning och samordning av arbetet med informations- och cybersäkerhet men även i det systematiska informationssäkerhetsarbetet och i it-säkerheten hos både offentliga och enskilda verksamhetsutövare.

11.4 Flera olika åtgärder krävs för att öka säkerheten i informationssystem i säkerhetskänslig verksamhet

Bedömning: Det saknas en enhetlig styrning och samordning av arbetet med att stärka informations- och cybersäkerheten i säkerhetskänslig verksamhet. Vidare behöver det systematiska informationssäkerhetsarbetet och säkerheten i nätverks- och informationssystem hos verksamhetsutövare i sådan verksamhet öka. Det krävs därför åtgärder som ger offentliga och enskilda aktörer bättre förutsättningar att kunna uppnå informations- och cybersäkerhet i den säkerhetskänsliga verksamheten. Frågan om behov av ytterligare åtgärder – utöver vad som anges i direktiven – bedöms dock ligga utanför utredningens uppdrag och behandlas inte vidare i betänkandet.

Som ovan framkommer anser utredningen att det finns ett stort behov av att stärka säkerheten i nät- och informationssystem i säkerhetskänslig verksamhet, särskilt vad gäller verksamheten på Säkerhetspolisens tillsynsområde. Behoven som framträder genom sammanställningen av offentliga utredningar och myndighetsrapporter framstår – mot redovisade aktuella hot, sårbarheter och risker – som akuta och omfattande inom flera olika områden på informations- och cybersäkerhetsområdet. Behoven av stärkt säkerhet i nätverks- och informationssystem i säkerhetskänslig verksamhet finns hos många aktörer som bedriver sådan verksamhet, bl.a. statliga myndigheter, regioner och kommuner. Det krävs åtgärder inom såväl arbetet med systematisk informationssäkerhet som mer it-tekniska åtgärder för att stärka denna säkerhet. Vidare behöver kompetensen och kunskapen om informations- och cybersäkerhet öka hos myndigheter och verksamhetsutövare, hos vilka även frågor om strategisk styrning och ökade resurser på området behöver uppmärksammas mer. Informations- och cybersäkerhet kan endast uppnås när alla väsentliga förutsättningar för en sådan säkerhet är uppfyllda.

Utredningen kan konstatera att arbetet med informations- och cybersäkerhet i dag är i allt väsentligt varje verksamhetsutövares eget ansvar, även när det gäller den säkerhetskänsliga verksamheten. Detta gäller även om Säkerhetspolisen och Försvarsmakten inom respektive tillsynsområde har både en stödjande roll och uppgiften att –

tillsammans med övriga tillsynsmyndigheter – kontrollera att regelsystemet efterlevs.

I och med att hot, sårbarheter och risker förändras och ökar ställs ökade krav på gemensam och samordnad hantering av åtgärder för att stärka informations- och cybersäkerheten inom det säkerhetskänsliga området och särskilt vad avser de informationssystem som hanterar skyddsvärd eller mycket skyddsvärd information. Motsvarande krav på gemensamma och samordnade åtgärder gäller också för att stärka nätverks- och informationssystem som används för styrning och kontroll av säkerhetskänsliga funktioner och verksamheter inom bl.a. elektroniska kommunikationer och, energiförsörjning, och som är av betydelse för Sveriges säkerhet. Verksamhetsutövare inom säkerhetskänslig verksamhet blir allt mer beroende av andra aktörer för sin informationshantering, bl.a. i förvaltningsgemensamma digitala funktioner och systemlösningar och det blir alltmer nödvändigt med samordnade åtgärder för att öka informations- och cybersäkerheten, dvs. säkerhetsnivån och samtidigt reducera sårbarheter och risker i informations- och nätverkssystemen.

Utredningen kan konstatera att det finns en rad olika statliga aktörer som har olika uppdrag och roller för det nationella arbetet med informations- och cybersäkerhet i säkerhetskänslig verksamhet. Säkerhetspolisen och Försvarsmakten är samrådsmyndigheter och har även tillsynsansvar. Vidare har Försvarets radioanstalt (FRA), Försvarets materielverk (FMV) och övriga tillsynsmyndigheter uppdrag och roller på området. Myndigheternas arbete samordnas sedan 2020 genom det nationella cybersäkerhetscentret. Myndigheterna har på regeringens uppdrag tagit fram en samlad handlingsplan med förslag på olika åtgärder som kan stärka Sveriges arbete med informations- och cybersäkerhet (se kapitel 3). Dessa förslag och åtgärder ska konkretisera behov och rekommendationer som identifierats på en mer övergripande nivå i den nationella informations- och cybersäkerhetsstrategin. Den centrala handlingsplanen som myndigheterna i cybersäkerhetscentret lagt fram stödjer i och för sig till del genom föreslagna åtgärder en ökad ambition med att stärka informations- och cybersäkerheten i säkerhetskänslig verksamhet.

Utredningen kan samtidigt notera att regeringen anger att uppgifterna i det nationella cybersäkerhetscentret är mer av samverkanskaraktär och att varje myndighet i enlighet med ansvarsprincipen har ansvar för respektive myndighets eget ansvars- och tillsynsområde.

Utredningen kan även konstatera att förändrad hotbild med åtföljande ökning av sårbarheter och risker i förening med den snabba tekniska utvecklingen ställer ökade krav på enhetlig styrning samt gemensamma och samordnade åtgärder när det gäller framtagande av bl.a. en nationell hotbild och sårbarhets- och riskbedömningar som kan tillämpas av verksamhetsutövare inom det säkerhetskänsliga området (se även kapitel 12).

Vidare behöver arbetet med systematisk informationssäkerhet öka mer generellt hos verksamhetsutövare och vikten av detta gör sig särskilt påmind inom det säkerhetskänsliga området, bl.a. vad gäller strategisk styrning, ökning av kompetens och tilldelning av såväl ekonomiska som personella resurser hos ansvariga verksamhetsutövare. Det är ett rimligt antagande att många verksamhetsutövare, inom olika samhällsområden med olika förutsättningar och krav, kan komma att behöva stöd från en central myndighet i arbetet med informations- och cybersäkerhet, särskilt vad gäller anskaffning och utveckling av nätverks- och informationssystem i säkerhetskänslig verksamhet, men även hot-, sårbarhets- och riskbedömning i anslutning till anskaffning och utveckling av sådana system. Utredningen anser därför att omfattande åtgärder bör skyndsamt vidtas för att höja informations- och cybersäkerheten mer allmänt och särskilt vad gäller nivån på säkerheten i nätverks- och informationssystem. Utöver åtgärder som omhändertar de allvarliga brister som framkommit bör även åtgärder genomföras som bidrar till att öka användningen av certifierade IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i samhället generellt, men särskilt i säkerhetskänsliga verksamheter och i verksamheter som avser samhällsviktiga digitala tjänster. Åtgärder som generellt bidrar till ökad användning av certifierade IKT-produkter, -tjänster och -processer i statliga myndigheters verksamhet bör därför eftersträvas (se kapitel 12).

Som utredningen tidigare anger förutsätter flera av dessa frågeställningar fördjupad analys innan förslag på närmare åtgärder kan lämnas och som kan bidra till att öka informations- och cybersäkerheten mer allmänt, men särskilt vad gäller säkerheten i informationssystem i säkerhetskänslig verksamhet och övrig samhällsviktig verksamhet. Frågorna berörs inte heller i direktiven och utredningen har därför – som tidigare framgår – avgränsat utredningsarbetet till frågorna om det finns anledning att införa en nationell särskilt anpassad

certifieringsordning för IKT-produkter, -tjänster och processer som används i informationssystem i säkerhetskänslig verksamhet och/eller kräva godkännande av en myndighet innan ett sådant system får driftsättas samt vissa därtill anslutande frågor. Den första frågeställningen gällande certifiering behandlas i kapitel 12 och den senare frågan om krav på godkännande övervägs i kapitel 13.

12 Certifiering av nätverks- och informationssystem

Förslag: Regeringen ska ge Försvarets materielverk (FMV) i uppdrag att i samråd med övriga myndigheter som ingår i det nationella cybersäkerhetscentret och övriga tillsynsmyndigheter inom säkerhetsskyddsområdet

- analysera och lämna förslag på formerna för framtagande av ordning för nationell kravställning som utgör grund för evaluering och/eller certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet,
- analysera och lämna förslag på vilka resurser som behövs för att inrätta en sådan ordning, vilka myndigheter som bör ges i uppgift att bidra till kravställningsarbetet samt hur näringsliv och företag kan beredas möjlighet att delta i arbetet,
- analysera och lämna förslag på formerna för hur myndigheter och andra verksamhetsutövare kan få stöd vid upphandling och användning av certifierade IKT-produkter, -tjänster och -processer i syfte att främja ökad användning av certifierade IKT-produkter, -tjänster och -processer i säkerhetskänslig verksamhet, och
- analysera behov av och formerna för framtagande av en nationell sammanställning över certifierade och rekommenderade IKT-produkter, -tjänster och -processer för användning i nätverks- och informationssystem i säkerhetskänslig verksamhet.

Bedömning: Eftersom det bl.a. saknas en nationell fastställd hot-, sårbarhets- och riskbedömning som kan ligga till grund för kravställning och framtagande av skyddsprofiler vid certifiering av IKT-produkter, -tjänster och -processer och då oklarheter råder kring övriga förutsättningar föreligger för närvarande inte skäl att föreslå att den aktuella certifieringsordningen införs.

Tillsynsmyndigheterna kan redan i dag ställa krav på att certifierade IKT-produkter, -tjänster och -processer ska användas med stöd av gällande författningar som reglerar krav på säkerhetsskyddsåtgärder i säkerhetskänslig verksamhet.

En nationell gemensamt framtagen och fastställd hot-, sårbarhets- och riskbedömning utgör en av flera förutsättningar för införande av en nationell särskilt anpassad ordning för certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet. Att ställa krav på certifierade IKT-produkter, -tjänster och -processer vid upphandling och driftsättning förutsätter kunskap och teknisk kompetens på området. För att stödja användning av certifierade IKT-produkter, -tjänster och -produkter behöver det finnas stöd i form av råd och anvisningar om hur certifiering kan användas som kravställning vid upphandling, vilka eventuellt ytterligare säkerhetsrelevanta krav som kan behöva ställas vid upphandlingen och hur certifierade IKT-produkter, -tjänster och -processer i nätverks- och informationssystem kan driftsättas på ett sätt som höjer säkerheten i systemen. Stöd kan t.ex. lämnas av central funktion som även tillhandahåller en nationell sammanställning över certifierade och rekommenderade IKT-produkter, -tjänster och -processer för användning i nätverks- och informationssystem i säkerhetskänslig verksamhet.

Vidare föreligger oklarhet hur det europeiska ramverket för cybersäkerhetscertifiering utvecklas och i vilken utsträckning som IKT-produkter, -tjänster och -processer på nivå hög kommer att finnas tillgängliga och som – vid behov efter nationell anpassning kan användas i säkerhetskänslig verksamhet.

Det råder även osäkerhet om den nationella marknaden är tillräckligt omfattande för att medge förutsättningar för införande av en nationell certifieringsordning för säkerhetskänslig verksamhet.

12.1 Inledning

Som framgår av föregående kapitel (kapitel 10 och 11) gör utredningen bedömningen att det föreligger allvarliga brister i informations- och cybersäkerheten inom många samhällsverksamheter och då även inom verksamheter som är att bedöma som säkerhetskänsliga. Det finns brister vad avser såväl det systematiska informationssäkerhetsarbetet och som i it-säkerheten. Det finns enligt utredningens uppfattning därför ett stort behov av att skyndsamt vidta många olika åtgärder inom ramen för det systematiska informationssäkerhetsarbetet och i it-säkerheten hos många aktörer inom såväl offentlig som enskild verksamhet för att öka säkerheten i närverks- och informationssystem. Detta berör frågor om organisering, styrning- och ledning av verksamheter, kompetens inom cybersäkerhet, kunskapsuppbyggnad, m.m. Flertalet av dessa frågeställningar och åtgärder är av komplex och långsiktig karaktär och kan varken behandlas närmare av utredningen eller bedöms ens ligga i utredningens uppdrag som det formulerats i direktiven.

Utredningen ska dock enligt direktivet överväga om ytterligare krav bör införas för att säkerställa att nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet uppfyller de krav som behövs för att upprätthålla skyddet av sådana verksamheter. En möjlighet kan – enligt direktivet – vara att införa krav på att IKT-produkter, -tjänster och -processer i nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet ska vara certifierade enligt en nationell särskild certifieringsordning som ställer krav anpassade för användning i säkerhetskänslig verksamhet. Vidare anges att en kompletterande eller alternativ möjlighet är att införa krav på godkännande från en utpekad myndighet innan en sådan IKT-produkt, -tjänst eller -process tas i drift i säkerhetskänslig verksamhet.

I detta kapitel redogörs för utredningens analys och överväganden när det gäller frågan om det bör införas krav på att IKT-produkter, -tjänster och -processer i nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet ska vara certifierade enligt en särskild certifieringsordning som ställer krav anpassade för användning i säkerhetskänslig verksamhet. Frågan om godkännande av myndighet innan driftsättning av sådana system behandlas i nästa kapitel.

12.2 Utgångspunkter

Det systematiska informations- och cybersäkerhetsarbetet inkluderar bl.a. uppgifter att identifiera informationsmängder i verksamheten, klassa dessa och göra val avseende säkerhetsåtgärder för att skydda informationen. Ett systematiskt informations- och cybersäkerhetsarbete innefattar administrativa, fysiska och tekniska åtgärder, och där analys och behov av t.ex. evaluerade och certifierade IKT-produkter, -tjänster och -processer i nätverks- och informationssystem utgör en delmängd av alla åtgärder som kan behövas för att uppnå tillräcklig säkerhet i systemen.

Innebörden av evaluering och certifiering av IKT-produkter, -tjänster och -processer

Frågan i vilken utsträckning som *certifiering* av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem kan anses bidra till ökad säkerhet i sådana system har tidigare behandlats i utredningens delbetänkande (kapitel 3 och 5). Utredningen behandlar i delbetänkandet bl.a. betydelsen av och formerna för certifiering av IKT-produkter, -tjänster och -processer jämte behovet och betydelsen av att använda vedertagna standarder i evaluerings- och certifieringsarbetet (s. 75 ff.).

Utgångspunkten för utredningens analys och överväganden i den delen var emellertid behovet av att komplettera det europeiska ramverket för cybersäkerhetscertifiering med bl.a. kompletterande nationell författningsreglering och att lämna förslag på nationell myndighet för cybersäkerhetscertifiering i enlighet med EU:s cybersäkerhetsakt. Utredningens uppdrag var sålunda inte att behandla och överväga frågan om behov av *krav på certifiering* av IKT-produkter, -tjänster och -processer för att öka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet. Redogörelsen i delbetänkandet är avgränsat mot det behov som förelåg i den första delen av uppdraget och som redovisas i delbetänkandet.

Utredningen har dock i delbetänkandet framhållit att certifiering av IKT-produkter, -tjänster och -processer anses allmänt bidra till ökat säkerhet i dessa och därigenom även ökat tillit till funktionalitet och säkerhet. Certifieringsprocessen består av en formell och oberoende utvärdering (evaluering) av IKT-produkter, -tjänster och -processer

utifrån fastställda kriterier. Certifiering är ett formellt fastställande av resultatet från utvärderingen (evaluering). I det ingår granskning att evalueringsarbetet genomförts med erforderlig noggrannhet och med utnyttjande av godkänd metodik samt att resultatet påvisat att evalueringsobjektet svarar mot någon viss *kravnivå* enligt givna *evalueringskriterier*. Ett utfärdat certifikat och tillhörande rapporter informerar användaren om säkerhetsegenskaperna hos IKT-produkten, -tjänsten och -processen. Certifiering utgör dessutom ofta ett väsentligt underlag vid ackreditering av system.[1] En certifieringsprocess under ackreditering innebär att en organisation, produkt eller person – av ett ackrediterat certifieringsorgan – bedöms uppfylla krav som ställs i standarder eller andra styrdokument.

Det finns särskilda organ med uppgiften att fatta beslut om utfärdande av certifikat rörande it-säkerhet. Behovet av certifieringsorgan för it-säkerhet grundar sig på att man med internationellt accepterade standarder kan bidra med tillit och förtroende (s.k. assurans) såväl inom som mellan organisationer, nationellt och internationellt.[2] I Sverige är det för närvarande endast det offentliga organet CSEC vid Försvarets materielverk (FMV) som är erkänt inom CCRA och SOG-IS MRA och som certifierar enligt *Common Criteria* på it-säkerhetsområdet (se nedan).[3]

I många länder finns inom cybersäkerhetsområdet myndigheter som utgör nationella certifieringsorgan för it-säkerhet, ofta med nära koppling till myndigheter med ansvar för nationell säkerhet (se kapitel 9).

Det europeiska ramverket för cybersäkerhetscertifiering

Ökad digitalisering, samman- och uppkoppling av bl.a. ”smarta” digitala produkter (IoT) och den allt snabbare tekniska utvecklingen (t.ex. kvantdatorer) leder till ökade cyberhot, sårbarheter och risker i bl.a. nätverks- och informationssystem. För att minska dessa sårbarheter och risker måste nödvändiga åtgärder vidtas för att stärka

[1] Certifiering utgör ofta ett väsentligt underlag vid ackreditering (driftsgodkännande) av system. En certifiering under ackreditering (kompetensprövning) innebär att en organisation, produkt eller person – av ett ackrediterat certifieringsorgan – bedöms uppfylla kompetenskrav som ställs i standarder eller andra styrdokument.
[2] Bl.a. CCRA och svensk standard EN ISO/IEC 17065:2012 innehåller krav på certifieringsorgans opartiskhet och oberoende.
[3] Se bl.a. kapitel 5 i utredningens delbetänkande.

cybersäkerheten i IKT-produkter, -tjänster och -processer i nätverks- och informationssystem, elektroniska kommunikationsnät samt styr- och kontrollsystem för kritisk infrastruktur, m.m.

Det europeiska ramverket för cybersäkerhetscertifiering, dvs. EU:s cybersäkerhetsakt och anslutande genomförandeordningar, innebär att det införs ett omfattande och komplext system på europeisk nivås om ska bidra till att öka informations- och cybersäkerheten i samhället, bl.a. i ovan angivna system. I ramverket behandlas och regleras frågor om bl.a. certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i syfte att öka säkerheten i dessa system. Det europeiska ramverket för cybersäkerhetscertifiering beskrivs närmare i utredningens delbetänkande *EU:s cybersäkerhetsakt – kompletterande bestämmelser om cybersäkerhetscertifiering* (SOU 2020:58).

Den nuvarande nationella ordningen för certifiering av it-säkerhet i produkter och system

I 5 § förordningen med instruktion för Försvarets materielverk (FMV) anges att det vid myndigheten ska finnas ett nationellt certifieringsorgan för it-säkerhet i produkter och system. FMV/certifieringsorganet ska verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat. Certifieringsorganet utgörs av myndighetens enhet Sveriges Certifieringsorgan för it-säkerhet (CSEC), som har en oberoende ställning inom myndigheten.

CSEC har till uppgift att utveckla den nationella certifieringsordningen för it-säkerhet med regler och metoder för oberoende granskning och se till att ordningen följs. CSEC:s verksamhet styrs bl.a. av standarden ISO/IEC 17065 och lagen om ackreditering och teknisk kontroll som bygger på EG-förordningen 765/2008[4]. CSEC verkar också som Sveriges nationella certifieringsorgan för it-säkerhet i produkter och system enligt den internationella standarden *Common Criteria* (CC). CSEC:s huvuduppgifter är att skriva certifieringsrapporter, utfärda certifikat och publicera en lista på certifierade produkter samt granska evalueringsrapporter och utöva tillsyn över evalueringar.

[4] Europaparlamentets och Rådets förordning (EG) nr 765/2008 av den 9 juli 2008 *om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93*.

CSEC ska även licensiera evalueringsföretag och utöva tillsyn över deras verksamhet samt bidra med stöd och råd vid utnyttjandet av CC för kravspecifikation.

CSEC deltar även i internationellt samarbete för tolkningar av CC och utveckling av standarder samt marknadsför CC. CSEC representerar Sverige i arbetet inom ramen för *Common Criteria Recognition Arrangement* (CCRA) i rollerna som nationellt certifieringsorgan och signatär, där samverkan för närvarande sker mellan 31 länder, varav 17 är ackrediterade att utfärda certifikat upp till och med evalueringsnivå EAL2 och upp till EAL4 för skyddsprofiler med tillhörande stöddokument.

CSEC representerar även Sverige inom den europeiska organisationen SOGIS-MRA.

Medlemmarna i CCRA- och SOGIS-MRA-grupperna utövar även vis tillsyn över CSEC och dess certifieringsordning i enlighet med respektive arrangemang.

CSEC representerar även FMV i det nationella cybersäkerhetscentret, som är under etablering (se kapitel 3).

CSEC verkar i nära samarbete med Militära underrättelse- och säkerhetstjänsten (MUST) i nationella frågor om krypto. MUST granskar och godkänner också it-säkerhetsprodukter för användning i säkerhetskänslig verksamhet.

Den svenska myndigheten Swedac är nationellt ackrediteringsorgan. Det innebär att myndigheten bl.a. ackrediterar evalueringslaboratorier, certifieringsorgan och kontrollorgan enligt internationella standarder och regelverk. Myndigheten ger även råd i frågor om teknisk kontroll och i frågor om s.k. bedömning av överensstämmelse. Swedac ackrediterade CSEC som nationellt certifieringsorgan 2008. Swedac utövar även regelbunden tillsyn över CSEC för att säkerställa att certifieringsorganet håller den standard som ligger till grund för ackrediteringen.

12.3 Finns krav på evaluering/testning av IKT-produkter, -tjänster och -processer i olika verksamheter?

Som redovisas i kapitel 3 finns i dag *ingen allmän reglering* med krav på säkerhet i nätverks- och informationssystem i samhället. Som utredningen redovisar i kapitel 6 och 7 finns i dag en detaljerad reglering för skydd av säkerhetskänslig verksamhet i form av säkerhetsskyddslagen, säkerhetsskyddsförordningen och tillsynsmyndigheternas föreskrifter med krav på olika säkerhetsskyddsåtgärder, bl.a. i form av informationssäkerhetsåtgärder i säkerhetsskyddad verksamhet. Dessa senare författningar innehåller dock *inga formella krav på certifiering* av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem.

Frågan som då uppkommer är om – i de fall det finns en reglering av informationssäkerhet på andra samhällsviktiga områden – det förekommer krav på att IKT-produkter, -tjänster och -processer i nätverks- och informationssystem ska certifieras eller i övrigt bli föremål för evaluering/testning för att uppnå ökad säkerhet.

Det blir då närmast fråga om författningsreglering som gäller för

- statliga myndigheters verksamhet allmänt,
- samhällsviktiga och digitala tjänster i anslutning till NIS-direktivet och
- övriga samhällssektorer.

Krav på informationssäkerhet i statliga myndigheters verksamhet

Myndigheten för samhällsskydd och beredskap (MSB) har med stöd av 21 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap utfärdat föreskrifter som ansluter till bestämmelserna om statliga myndigheters informationssäkerhet i 19 § i förordningen. Av 19 § i förordningen följer att varje myndighet har ansvar för säker informationshantering. Ansvaret gäller även när myndighetens information hanteras av en extern aktör eller när myndigheten tillhandahåller andra aktörer tjänster för informationshantering inom e-förvaltning eller motsvarande.

I 1 § i myndighetens föreskrifter om informationssäkerhet för statliga myndigheter[5] anges att dessa avser sådana säkerhetskrav som avses i 19 § i den angivna förordningen. Av 2 § följer att om en annan författning innehåller en bestämmelse som ställer högre krav än vad som anges i dessa föreskrifter tillämpas den bestämmelsen.

Av 4 § följer att en myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav och SS-EN ISO/IEC 27002:2017 Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder eller motsvarande. Om en myndighet väljer att använda en annan standard bör myndigheten analysera och dokumentera de likheter och skillnader som finns mellan ISO-standarden och vald standard för att säkerställa att vald standard ger tillräckligt stöd i det systematiska och riskbaserade informationssäkerhetsarbetet.

I 5 § anges att informationssäkerhetsarbetet ska utformas utifrån de risker och behov myndigheten identifierar. Det ska omfatta all behandling av information som myndigheten ansvarar för och integreras med myndighetens befintliga sätt att leda och styra sin organisation

Av 6 § följer att myndigheten ska säkerställa att informationssäkerhetsarbetet är systematiskt och riskbaserat genom att

- klassa sin information avseende konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få (informationsklassning),
- identifiera, analysera och värdera risker för sin information (riskbedömning),
- utifrån genomförd informationsklassning och riskbedömning identifiera behov av och införa ändamålsenliga och proportionella säkerhetsåtgärder, och
- utvärdera säkerhetsåtgärderna och vid behov anpassa skyddet av informationen. I arbetet ingår att genomföra en gapanalys.

[5] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

MSB har även med stöd av 21 § förordningen (2015:1052)1 om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap utfärdat föreskrifter och allmänna råd om säkerhetsåtgärder i informationssystem för statliga myndigheter.[6] Dessa föreskrifter innehåller bestämmelser om sådana säkerhetskrav som avses i 19 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Om en annan författning innehåller en bestämmelse som ställer högre krav än kraven i dessa föreskrifter tillämpas den bestämmelsen.

Med begreppet informationssystem i föreskrifterna avses applikationer, tjänster eller andra komponenter som hanterar information samt nätverk och infrastruktur. Av 3 kap 1 § i föreskrifterna följer att en myndighet ska vid anskaffning, utveckling eller utkontraktering av informationssystem identifiera krav på säkerhet i systemet. I myndighetens allmänna råd till den angivna bestämmelsen anges att ”vid anskaffning av informationssystem bör myndigheten överväga att välja produkter som är certifierade genom tredjepartsgranskning mot etablerad standard.” Några formella krav på att använda certifierade IKT-produkter, -tjänster eller -processer finns sålunda inte i föreskrifterna.

Krav på informationssäkerhet för samhällsviktiga och digitala tjänster

Till grund för den nationella författningsregleringen om informationssäkerhet för samhällsviktiga och digitala tjänster ligger Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i *nätverks- och informationssystem* i hela unionen (NIS-direktivet).

I NIS-direktivet samt anslutande nationell författningsreglering på området finns bestämmelser som bl.a. reglerar krav på säkerhet i närverks- och informationssystem i verksamheter som rör samhällsviktiga tjänster. Säkerhet i system och anläggningar enligt artikel 16.1 a i direktiv (EU) 2016/1148 avser säkerheten för nät- och informationssystem och deras fysiska miljö och innefattar följande aspekter:

[6] Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).

a) Systematisk förvaltning av nät- och informationssystem, vilket avser mappning av informationssystem och fastställande av ett antal ändamålsenliga policyer för hantering av informationssäkerheten, inklusive riskanalys, mänskliga resurser, driftssäkerhet, säkerhetsarkitektur, säker livscykelhantering av data och system och, i förekommande fall, kryptering och hantering av sådan kryptering.

b) Fysisk säkerhet och miljösäkerhet, vilket avser tillgången till ett antal åtgärder för att skydda säkerheten för nät- och informationssystem hos leverantörer av digitala tjänster från skador med användning av en riskbaserad strategi som omfattar alla faror och som t.ex. omfattar systemfel, den mänskliga faktorn, avsiktligt skadliga handlingar eller naturfenomen.

c) Försörjningstrygghet, vilket avser införande och upprätthållande av lämpliga policyer för att säkerställa tillgängligheten och i förekommande fall spårbarheten för kritiska insatsprodukter som används för tillhandahållandet av tjänsten.

d) Åtkomstkontroll för nät- och informationssystem, vilket avser tillgången till en uppsättning åtgärder för att säkerställa att den fysiska och logiska åtkomsten till nät- och informationssystem, inklusive administrativ säkerhet för nät och informationssystem, tillåts och begränsas baserat på verksamhetskrav och säkerhetskrav.

I *Kommissionens genomförandeförordning (EU) 2018/151 av den 30 januari 2018 om tillämpningsföreskrifter för Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen* finns närmare specificering av de aspekter som ska beaktas av leverantörer av digitala tjänster när de hanterar risker som hotar säkerheten i deras nät- och informationssystem samt parametrarna för fastställande av om en incident har avsevärd inverkan.[7]

[7] Kommissionens genomförandeförordning (EU) 2018/151 av den 30 januari 2018 om tillämpningsföreskrifter för Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen vad gäller närmare specificering av de aspekter som ska beaktas av leverantörer av digitala tjänster när de hanterar risker som hotar säkerheten i deras nät- och informationssystem samt parametrarna för fastställande av om en incident har avsevärd inverkan. I förordningen framhålls att enligt direktiv (EU) 2016/1148 bör (1) leverantörer av digitala tjänster fritt kunna vidta de tekniska och organisatoriska åtgärder som de anser lämpliga för att hantera risker för

I lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster finns bestämmelser om informationssäkerhet för sådana tjänster. Lagen gäller för (1) leverantörer av det slag som anges i bilaga 2 till NIS-direktivet och som tillhandahåller en samhällsviktig tjänst, under förutsättning att leverantören är etablerad i Sverige, att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten (leverantörer av samhällsviktiga tjänster), och (2) juridiska personer som tillhandahåller en digital tjänst och som har sitt huvudsakliga etableringsställe i Sverige eller har utsett en företrädare som är etablerad här (leverantörer av digitala tjänster). Av 8 § framgår att lagen dock inte gäller för verksamhet som omfattas av säkerhetsskyddslagen (2018:585). Vidare anges i 9 § att när det gäller leverantörer som omfattas av krav på informationssäkerhet i andra författningar ska – om det i lag eller annan författning finns bestämmelser som innehåller krav på säkerhetsåtgärder och incidentrapportering – de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enlig lagen, varvid bestämmelsernas omfattning ska beaktas samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.

I 5 § i förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster anges att leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster ska när det gäller organisatoriska och tekniska åtgärder beakta europeiska och

säkerheten i deras nät- och informationssystem, om dessa åtgärder säkerställer en lämplig säkerhetsnivå och tar hänsyn till de aspekter som föreskrivs i direktivet. (2) När leverantörer av digitala tjänster fastställer vilka tekniska och organisatoriska åtgärder som är ändamålsenliga och proportionella bör de ta ett systematiskt grepp på informationssäkerheten och tillämpa ett riskbaserat tillvägagångssätt. (3) För att garantera säkerheten för system och anläggningar bör leverantörer av digitala tjänster genomföra bedömnings- och analysförfaranden. Förfarandena bör omfatta en systematisk förvaltning av nät- och informationssystem, fysisk säkerhet och miljösäkerhet, försörjningstrygghet och åtkomstkontroll. (4) När leverantörer av digitala tjänster utför en riskanalys inom ramen för en systematisk förvaltning av nät- och informationssystem bör de uppmuntras att identifiera särskilda risker och kvantifiera deras betydelse, t.ex. genom att identifiera hot mot kritiska tillgångar och hur dessa hot påverkar driften och fastställa hur de bäst kan begränsas baserat på befintlig kapacitet och befintliga resurskrav. (5) Policyn för mänskliga resurser kan avse förvaltningen av kompetens, inklusive aspekter förbundna med utvecklingen av säkerhetsrelaterad kompetens och åtgärder för att öka medvetenheten. Vid fastställandet av ett antal ändamålsenliga policyer för driftssäkerhet bör leverantören av digitala tjänster uppmuntras att ta hänsyn till aspekter rörande förändringshantering, sårbarhetshantering, formaliserade drifts- och förvaltningsmetoder och systemmappning. (6) Policyerna för säkerhetsarkitektur kan i synnerhet omfatta segregering av nätverk och system liksom specifika säkerhetsåtgärder för kritisk drift såsom förvaltningsdrift. Segregeringen av nätverk och system kan göra det möjligt för en leverantör av digitala tjänster att skilja mellan element som dataflöden och datorresurser som hör till en kund, en grupp av kunder, leverantören av digitala tjänster eller tredje part.

internationellt accepterade standarder och specifikationer vid utformningen av säkerhetsåtgärder.

Av 6 § följer att vid bedömningen av om säkerhetsåtgärder enligt 15 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster säkerställer en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till risken, ska bl.a. beaktas säkerheten i system och anläggningar (punkten 1), hantering av driftskontinuitet, övervakning (punkten 3), revision och testning (punkten 4), och efterlevnad av internationella standarder (punkten 5). I förordningen anges vidare att i artikel 2 i kommissionens genomförandeförordning om leverantörer av digitala tjänster finns bestämmelser som närmare anger vad som avses med bl.a. punkterna 1 och 3–5.

I förordningen anges vidare att Myndigheten för samhällsskydd och beredskap får, efter att ha gett tillsynsmyndigheterna och Socialstyrelsen tillfälle att yttra sig, meddela föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete enligt 11 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Statens energimyndighet, Transportstyrelsen, Finansinspektionen, Livsmedelsverket och Post- och telestyrelsen får meddela föreskrifter om säkerhetsåtgärder enligt 12–14 §§ lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster för sina respektive tillsynsområden. Socialstyrelsen får meddela sådana föreskrifter för Inspektionen för vård och omsorgs tillsynsområde. Innan föreskrifterna meddelas ska Myndigheten för samhällsskydd och beredskap ges tillfälle att yttra sig. Vidare anges att Myndigheten för samhällsskydd och beredskap ska lämna råd och stöd till tillsynsmyndigheterna och Socialstyrelsen när de tar fram föreskrifterna.

Myndigheten för samhällsskydd och beredskap har med stöd av den angivna lagen och förordningen meddelat föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster med krav på att aktörer med verksamhet inom samhällsviktiga tjänster ska bedriva ett systematiskt arbete med informationssäkerhet och vidta åtgärder som stärker it-säkerheten i verksamheten. I 8 § angivna föreskrifter anges att leverantör ska ha ett dokumenterat arbetssätt för sitt informationssäkerhetsarbete som stöd för att klassa information med utgångspunkt i vilka konsekvenser som kan uppkomma vid brister i konfidentialitet, riktighet och tillgänglighet (punkten 1), identifiera, analysera och värdera risker för organisationens information,

nätverk och informationssystem (punkten 2), utifrån genomförd informationsklassning och riskbedömning införa ändamålsenliga och proportionella säkerhetsåtgärder (punkten 3) samt följa upp och utvärdera säkerhetsåtgärder i syfte att vid behov anpassa skyddet av informationen (punkten 4). Av 10 § följer att en leverantör ska ha interna regler och arbetssätt som säkerställer att samtliga nätverk och informationssystem för samhällsviktiga tjänster uppfyller identifierade behov av informationssäkerhet. Drift och förvaltning över tid, arkitektur samt sammankoppling mot andra nätverk och informationssystem ska särskilt beaktas.

De angivna sektorsmyndigheterna/tillsynsmyndigheterna inom respektive sektor har rätt att meddela föreskrifter på respektive område.[8]

Post och telestyrelsen har utfärdat myndighetsföreskrifter och allmänna råd om säkerhetsåtgärder för samhällsviktiga tjänster inom sektorn digital infrastruktur (TSFS 2021:3)[9] I föreskrifterna finns bestämmelser om säkerhetsåtgärder för nätverk och informationssystem enligt 12–14 §§ lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Föreskrifterna och allmänna råd gäller för leverantörer av samhällsviktiga tjänster inom sektorn digital infrastruktur. Av 6 § följer att leverantören ska bedöma om risker ska elimineras, reduceras eller accepteras utifrån genomförd riskbedömning enligt 4 §. Om leverantören behöver eliminera eller reducera identifierade risker ska leverantören vidta åtgärder för att hantera riskerna i enlighet med vad som föreskrivs i 8–16 §§ nedan. Leverantören ska därutöver vidta de ytterligare åtgärder som är nödvändiga för att hantera de risker som framkommit utifrån genomförd riskbedömning enligt 4 §. Samtliga åtgärder ska vidtas på en nivå som är proportionerlig i förhållande till den föreliggande risken. Redogörelser för skälen för bedömning av om riskerna ska elimineras, reduceras eller accepteras ska dokumenteras och bevaras i fem år. I till 6 § anslutna allmänna råd anges att leverantören bör beakta den senaste tekniska utvecklingen för att säkerställa en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till den föreliggande risken. Leverantören bör endast acceptera risker

[8] Statens energimyndighet, Transportstyrelsen, Finansinspektionen, Livsmedelsverket och Post- och telestyrelsen. Socialstyrelsen får meddela sådana föreskrifter för Inspektionen för vård- och omsorgs tillsynsområde.

[9] Post- och telestyrelsen har utfärdat föreskrifterna och allmänna råd med stöd av stöd av 8 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

om riskbedömningen i det aktuella fallet påvisar att säkerheten i den samhällsviktiga tjänsten kan upprätthållas. Av 7 § följer att eventuella åtgärder ska dokumenteras. Några formella krav på certifiering av IKT-produkter, -tjänster och -processer i *nätverks- och informationssystem* uppställs inte.

I *Statens energimyndighets* föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn (STEMFS 2021:3)[10] föreskrivs i 2 § att leverantören ska upprätta en systemförteckning över sin IT och OT genom att kartlägga och analysera de IT- och OT-tjänster samt nätverk och informationssystem som används vid leverantörens tillhandahållande av samhällsviktiga tjänster samt hur dessa kommunicerar med och är beroende av varandra (punkten 1), inventera vilka hårdvaror som används i leverantörens IT och OT (punkten 2), inventera vilka mjukvaror som används i leverantörens IT och OT (punkten 3), identifiera vilka interna och externa nätverk och informationssystem liksom vilka hårdvaror och mjukvaror som är mest kritiska för leverantörens tillhandahållande av samhällsviktiga tjänster (punkten 4), samt upprätta en nätverkskarta avseende leverantörens IT och OT (punkten 5).

Inga av de övriga angivna sektorsmyndigheterna/tillsynsmyndigheterna har på motsvarande sätt som PTS eller Statens energimyndighet utfärdat några föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem hos leverantörer av samhällsviktiga tjänster.

Utredningen kan notera att varken i MSB:s föreskrifter eller i någon av sektorsmyndigheternas förskrifter ställs sålunda några formella krav på att IKT-produkter, -tjänster eller -processer i *nätverks- och informationssystem* som används i verksamhet som innefattar samhällsviktiga och digitala tjänster ska vara *certifierade* enligt en av Sverige erkänd certifieringsordning. I föreskrifterna finns i och för sig bestämmelser om att en leverantör ska ha interna regler och arbetssätt som säkerställer att samtliga nätverk- och informationssystem för samhällsviktiga tjänster uppfyller identifierade behov av informationssäkerhet, dock saknas bestämmelser om evaluering eller certifiering av sådana.

[10] Statens energimyndighets föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn (STEMFS 2021:3).

Informationssystem i verksamhet hos kommuner och regioner

Det finns i dag inte någon formell författningsreglering med krav på att använda certifierade IKT-produkter, -tjänster och -processer i *nätverks- och informationssystem* som används i verksamheter som bedrivs av kommuner och regioner, annat än om verksamheten i ett eller flera avseenden träffas av kraven på informationssäkerhet i regleringen av säkerhetsskydd eller om samhällsviktiga och digitala tjänster.

Näringslivet och företag

På motsvarande sätt som gäller för kommuner och regioner finns det för enskilda företag eller enskilda organisationer i dag inte någon formell författningsreglering med krav på att använda certifierade IKT-produkter, -tjänster och -processer i *nätverks- och informationssystem* som används i olika verksamheter. Detta gäller dock inte om verksamheten i ett eller flera avseenden träffas av kraven på informationssäkerhet i regleringen av säkerhetsskydd eller om samhällsviktiga och digitala tjänster.

12.4 Finns krav på certifiering i andra länder?

Utredningen har genomfört en översiktlig kartläggning av om det i andra jämförbara länder finns reglering som innefattar krav på certifiering av IKT-produkter, -tjänster och -processer i verksamhet som motsvarar den svenska definitionen av säkerhetskänslig verksamhet eller i övrigt definitionen på verksamhet som kan anses beröra nationell säkerhet. En sammanfattning av vad som framkommit vid kartläggningen finns i kapitel 9.

Utredningen kan konstatera att det framkommer en splittrad bild av förekomsten av reglering med krav på certifiering av IKT-produkter, -tjänster och -processer i verksamhet som kan anses motsvara det svenska begreppet säkerhetskänslig verksamhet eller i övrigt nationell säkerhet.

I *Norge* ställs i nationell författning krav på att verksamheter vid valet av säkerhetsåtgärder använder *evaluerade* produkter och tjänster om dessas funktion är avgörande för att personer inte obefogat ska få tillgång till hemlig eller kvalificerat hemlig information och

inte heller påverkar driften av kritisk infrastruktur. Evalueringen ska utföras av den nationella säkerhetsmyndigheten (NSM) eller ett ackrediterat laboratorium som utsetts av NSM. *Kraven på själva evalueringen* kan uppfyllas genom en *certifiering* utfärdat av NSM eller ett ackrediterat certifieringsorgan som utsetts av NSM.[11]

Av inhämtade uppgifter framgår att det finns myndigheter i *Finland* med ansvar för nationell informations- och cybersäkerhet samt uppgiften att godkänna vissa informationssystem. Några nationella krav på *certifiering* av sådana system har dock inte framkommit. Det kan i vissa fall vara obligatoriskt att inhämta intyg om godkännande från behörig myndighet för informationssystem som behandlar säkerhetsklassificerad information.

I *Danmark* finns krav på cybersäkerhetscertifiering i fråga om säkerheten i nätverks- och informationssystem, främst i vissa sektorer (bl.a. inom transport och sjöfart). För statliga myndigheter finns också krav på att ackreditering av informationssystem som används för klassificerad information. Sådana system kan vara föremål för certifiering och/eller godkännande.

I *Nederländerna* finns centrala myndigheter med ansvar för nationell cybersäkerhet, evaluering respektive godkännande av informationssäkerhetsprodukter och system för att skydda särskild information av betydelse för staten. Några nationella krav på formell *certifiering* av nedan angivna system och produkter har inte kunnat noteras. Produkter för information som kan medföra negativa konsekvenser för staten ska dock evalueras av den nationella byrån för kommunikationssäkerhet (NBV). Arbetsgruppen för särskild informationssäkerhet, WBI, lämnar sedan råd till Inrikesministeriet som har att godkänna användningen av informationssäkerhetssystem och dess komponenter. Vidare kan användning av viss mjukvaruutrustning som omfattas av försvarskontrakt förutsätta godkännande av s.k. säkerhetskontor.

I *Tyskland* finns myndigheter med ansvar för informationssäkerhet och certifiering respektive godkännande av it-produkter och -system i säkerhetskänslig verksamhet i landet. Vissa komponenter och ändringar av it-system som ska behandla klassificerat material ska godkännas av chefer på berörda myndigheter. En förutsättning för användning av it-system för klassificerad information är ett in-

[11] Det rör sig här inte om ett absolut krav på certifiering, utan överensstämmelse kan visas även på andra sätt.

formationssäkerhetskoncept i enlighet med angivna standarder. Dessutom finns krav på sekretesskydd som går utöver det grundläggande it-skyddet och som ska definieras av säkerhetschefer enligt administrativa instruktioner för skyddet av klassificerat material. Utöver certifiering av it-produkter och -system med avseende på deras säkerhetsfunktioner finns även tillgång till tjänsten att certifiera enligt tekniska riktlinjer avseende särskilda funktionskrav. En certifiering enligt tekniska riktlinjer krävs om implementeringen av särskilda funktionskrav är avgörande för driften av en it-produkt eller ett it-system. Detta gäller i synnerhet it-produkter eller -system som är avsedda att sättas in i säkerhetskänsliga domäner i Tyskland. BSI bedömer tillverkares och distributörers it-produkter och -system varvid oberoende evaluering av överensstämmelse med de tekniska riktlinjerna görs.[12]

I *Frankrike* finns centrala myndigheter med ansvar för nationell informations- och cybersäkerhet. Myndigheterna ansvarar för *evaluering* och -godkännande av informationssystem och dess säkerhetsfunktioner där behandlad information är av betydelse för nationell säkerhet. Några nationella krav på *certifiering* av sådana system har dock inte framkommit När det gäller informationssystem som behandlar information som klassificerats som kvalificerat hemlig ska generalsekreteraren för försvar och nationell säkerhet (SGDSN) godkänna systemet.

I *Storbritannien* finns myndigheter med ansvar för nationell informations- och cybersäkerhet samt *certifiering* av IKT. I fråga om produkter som hanterar hemlig information krävs särskilt utvecklat skydd. På denna nivå används normalt inte vanligen förekommande kommersiella lösningar. Tillgång till känslig information ska endast ges till auktoriserade system. Företag som tillhandahåller vissa IKT-produkter och -tjänster för hantering av känslig och officiell information kan behöva *certifiering* eller motsvarande. Tillhandahållare av tjänster och tredjepartsleverantörer som hanterar hemlig offentlig information måste vidare erhålla ackreditering och använda lämpligt ackrediterad it-utrustning och godkänd mjukvara.

I *USA* finns flera departement och federala myndigheter med ansvar för nationell informations- och cybersäkerhet. Det finns krav

[12] Om it-system ska användas för hemligt material måste säkerhetsansvariga låta BSI utföra vissa tekniska tester av it-systemet för att se om nödvändiga it-säkerhetsfunktioner implementerats korrekt. När nätverksbaserade it-system används för klassificerat material kan även säkerhetsansvariga behöva genomföra ett penetrationstest.

på att driftsättningen av federala informationssystem ska godkännas av behöriga federala tjänstemän. Nationella säkerhetssystem som behandlar nationell säkerhetsinformation fordrar ytterligare säkerhetskrav som behöver godkännas. Vidare ska sådana system genomgå en oberoende tredjepartsbedömning där systemets överensstämmelse med särskilda instruktioner på området valideras. I USA kan kommersiella informationssäkerhetsprodukter i förhållandevis stor utsträckning användas för att skydda nationella säkerhetssystem och klassificerad information (om lösningarna är godkända av NSA och assuransfunktionerna validerade).

I *Kanada* finns myndigheter med ansvar för informations- och cybersäkerhet samt *certifiering* av IKT. Federala departement och myndigheter måste ha sina it-system och tjänster *certifierade* och ackrediterade innan de godkänns för drift. Organisationer som ingår kontrakt med regeringen och har it-system som ska behandla säkerhetsklassificerad information (mellan leverantören och en statlig myndighet) måste få sitt system godkänt av en myndighet (PSPC) före det att arbetet kan påbörjas och systemet används. Säkerhetskraven är emellertid specifika för varje kontrakt och beror på hur känslig den berörda informationen är.

I *Nya Zeeland* finns departement med ansvar för informations- och cybersäkerhet, bl.a. när det gäller nationell säkerhet. Statliga nationella myndigheter som hanterar hemlig information om nationen är skyldiga att ha kontroll över sina system och hålla informationen säker. IKT-systemen kan vidare behöva genomgå en särskild *certifierings*- och ackrediteringsprocess för att få tas i drift. Detta förfarande regleras i en nationell handbok vars användning rekommenderas brett i samhället. Rör hanterad information nationell säkerhet måste myndighetens system ackrediteras av den nationella byrån för kommunikationssäkerhet (GCSB) innan ett resulterande formellt godkännande av systemets driftsättning kan ske. Vidare kräver system och tjänster med kompartmentaliserad eller förbehållen (”caveated”) information klassificerad som konfidentiell och högre ackreditering av generaldirektören på GCSB (eller formell delegat). Också användning av högassurans-kryptoutrustning kräver kontroll i form av ackreditering av GCSB. Generellt i fall där information och system är klassificerade begränsat hemliga (restricted) eller lägre ligger uppgiften att godkänna systemet internt hos organisationens chef.

I *Australien* finns myndigheter med ansvar för informations- och cybersäkerhet samt uppgifterna att *evaluera* respektive *certifiera* IKT. När det gäller information om statliga angelägenheter som tillhör regeringen behöver berörda IKT-system godkännas innan de får tas i drift. För kvalificerat hemliga system och system som hanterar kvalificerat hemlig eller känslig kompartmentaliserad information är en underrättelse- och säkerhetstjänst (ASD:s generaldirektör) godkännandeorgan. I övriga fall brukar uppgiften att godkänna systemen ligga hos respektive organisations säkerhetschef. Några motsvarande nationella krav på certifiering av sådana system har dock inte framkommit.

12.5 Överväganden

12.5.1 Behov av att stärka säkerheten i nätverks- och informationssystem

Utredningen ska – enligt direktiven - överväga om det finns behov av att stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet, t.ex. genom att det införs en nationell särskild anpassad ordning med krav på certifiering av IKT-produkter, -tjänster och -processer som ska användas i informationssystem i säkerhetskänslig verksamhet.

Utgångpunkten för utredningens överväganden när det gäller frågan om det finns anledning att införa en nationell särskilt anpassad ordning för certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet är att det finns konstaterade brister i säkerheten i systemen som ett krav på certifiering av produkter, tjänster och -processer kan bidra till att åtgärda.

Utredningens experter på informations- och cybersäkerhet, bl.a. på området för evaluering och certifiering, har framhållit att IKT-produkter, -tjänster och -processer som genomgår evaluering och certifiering bidrar till att öka säkerheten i nätverks- och informationssystem, men att det inte genom ett sådant förfarande går att uppnå någon fullständig säkerhet. Även andra nödvändiga säkerhetsskyddsåtgärder måste vidtas och finnas på plats. En ökad användning av certifierade IKT-produkter, -tjänster och -processer utgör således endast en delmängd av många andra angelägna åtgärder som behöver

vidtas inom ramen för ett systematiskt informationssäkerhetsarbete och i arbetet med att stärka it-säkerheten i säkerhetskänslig verksamhet (se kapitel 10 och 11).

Utredningen tolkar vidare uppdraget när det gäller frågan om det finns anledning att införa en nationell särskilt anpassad ordning för certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet som att utgångspunkten är att utreda behovet av en särskild certifieringsordning som till struktur, regelsystem och arbetsformer motsvarar den nu befintliga nationella certifieringsordningen vid FMV/CSEC, men som är anpassad för den säkerhetskänsliga verksamheten. Utredningens överväganden om det finns anledning att införa en nationell särskilt anpassad ordning för certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet ska därför göras mot den ovan angivna bakgrunden. Det kan samtidigt konstateras att det därutöver måste föreligga ett antal förutsättningar för att möjliggöra ett införande och tillämpning av en sådan ordning och att i detta sammanhang även att ett antal andra bedömningar behöver göras, bl.a. vilken påverkan som certifieringar som sker med stöd av det europeiska ramverket kan ha för behovet av nationella certifieringar av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i för säkerhetskänslig verksamhet. Dessa förutsättningar och andra grundläggande frågeställningar behandlas mer utförligt i efterföljande avsnitt.

12.5.2 Förutsättningar för en nationell certifieringsordning för säkerhetskänslig verksamhet

Befintligt regelsystem

Frågan om krav på certifiering av IKT-produkter, -tjänster och -processer i säkerhetskänslig verksamhet berör även frågor av rättslig karaktär, dvs. hur detta i sådana fall ska regleras. Oavsett om regleringen sker i lag, förordning eller förskrifter ställer det rättsliga krav på dels att eventuella krav är förutsebara, dels att de begrepp och definitioner som används i regleringen är tydligt definierade, vilket får en särskild betydelse om det finns administrativa åtgärder och sanktioner kopplade till krav på en aktör att använda certifierade IKT-produkter, -tjänster och -processer i en viss typ av verksamhet.

Den fråga som inledningsvis uppkommer är om nu gällande regelsystem för informationssäkerhet i säkerhetskänslig verksamhet ger stöd för att närmare reglera och ställa krav på användning av evaluerade och certifierade IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i sådan verksamhet.

Av 4 § första stycket i säkerhetsskyddsförordningen framgår – när det gäller säkerhetskrav för informationssystem som används i säkerhetskänslig verksamhet – att en verksamhetsutövare som ansvarar för ett informationssystem som ska användas i sådan verksamhet ska vidta *lämpliga skyddsåtgärder* för att kunna upptäcka, försvåra och hantera skadlig inverkan på informationssystemet samt obehörig avlyssning av, åtkomst till och nyttjande av informationssystemet. Av 6 § följer att Säkerhetspolisen och Försvarsmakten får inom respektive myndighets tillsynsområde meddela föreskrifter om undantag från kraven i 4 §.

Utredningen noterar att av Säkerhetspolisen förskrifter om *granskning* vid utveckling och anskaffning av informationssystem i säkerhetskänslig verksamhet framgår att verksamhetsutövaren ska se till att *egenutvecklad programvara* i informationssystem som har betydelse för säkerhetskänslig verksamhet *granskas* för att upptäcka och åtgärda säkerhetsbrister och sårbarheter (4 §). Vidare anges att verksamhetsutövaren ska se till att *tredjepartsprogramvara* i informationssystem som har betydelse för säkerhetskänslig verksamhet *granskas* för att upptäcka och åtgärda säkerhetsbrister och sårbarheter, eller att programvaran på annat sätt *bedöms vara tillförlitlig* från säkerhetsskyddssynpunkt (5 §).

Utredningens experter från Säkerhetspolisen respektive Försvarsmakten har under utredningsarbetet gjort bedömningen att nu gällande författningsreglering av säkerhetsskydd i och för sig ger stöd för att meddela föreskrifter som anger att en verksamhetsutövare i vissa fall *ska* använda IKT-produkter, -tjänster och -processer som ska vara *evaluerade* och *certifierade* enligt en viss ordning men att några sådana föreskrifter inte utfärdats.

Utredningen gör därför bedömningen att nuvarande författningsreglering ger tillräckligt utrymme för tillsynsmyndigheterna att – vid behov – kunna meddela närmare föreskrifter om *krav* på användning av evaluerade och certifierade IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet.

Den nationella ordningen för certifiering av it-säkerhet i produkter och system

I detta sammanhang kan noteras att det finns en nationell ordning för certifiering av it-säkerhet i produkter och system, även om den ordningen inte närmare reglerar vad som ska gälla för certifiering av IKT-produkter, -tjänster och -processer på det säkerhetsskyddade området. Den fråga som då uppkommer är om denna certifieringsordning kan anses ge samma möjligheter att uppnå tillräcklig säkerhet i nätverks- och informationssystem som en särskilt anpassad certifieringsordning med certifieringskrav på området kan medföra.

Här uppkommer även frågan vilken uppgift och roll som det nationella certifieringsorganet CSEC bör och kan ha när det kommer till frågan om evaluering och certifiering av IKT-produkter, -tjänster och -processer i säkerhetskänslig verksamhet. Här ska noteras att den nu gällande nationella certifieringsordningen kan komma att upphöra om/när en motsvarande certifieringsordning inom ramen för det europeiska ramverket för cybersäkerhetscertifiering införs, som då blir den gällande certifieringsordningen på det aktuella området. Vidare kan noteras att regeringen har givit FMV i uppdrag att vara nationell cybersäkerhetsmyndighet enligt EU:s cybersäkerhetsakt med uppgifter som följer av denna förordning, vilket bl.a. innebär att det nationella certifieringsorganet CSEC, som är en fristående enhet i vid myndigheten, har ansvar för certifieringar på nivå hög enligt det europeiska ramverket för cybersäkerhetscertifiering.

Frågan om vilken betydelse den befintliga nationella ordningen för certifiering av it-säkerhet i produkter och system kan få när det gäller att överväga eventuellt behov av att införa en särskild motsvarande ordning för det säkerhetskänsliga området behandlas mer i efterföljande avsnitt.

Det europeiska ramverket för cybersäkerhet

För nationellt vidkommande uppkommer även frågan vilken betydelse och påverkan som certifieringsordningar inom ramen för det europeiska ramverket för cybersäkerhetscertifiering – utöver vad som följer direkt av tillämpningsområdet för dessa ordningar – kan få för arbetet med att stärka den nationella informations- och cybersäker-

heten, och särskilt vad gäller nätverks- och informationssystem i säkerhetskänslig verksamhet.

Utredningen noterar att de olika certifieringsordningar som kommer att etableras inom ramen för det europeiska ramverket för cybersäkerhetscertifiering kan förväntas användas för certifiering av allt från programvaror, IoT, molntjänster till olika styr- och kontrollsystem, dvs. många olika former och typer av informations- och kommunikationsteknologi (IKT) och som berör nätverks- och informationssystem.

Utredningens experter har under utredningsarbetet framhållit behovet av att fler certifierade IKT-produkter, -tjänster och -processer för nivån hög tas fram inom ramen för det europeiska ramverket för cybersäkerhetscertifiering och att dessa ska kunna användas – vid behov efter anpassning till nationella krav – i såväl säkerhetskänslig som annan samhällsviktig verksamhet.

Målbilden bör vara att certifierade IKT-produkter, -tjänster och -processer på nivån hög och som tas fram inom det angivna ramverket, eller på annat sätt, ska kunna användas också nationellt på motsvarande sätt som sker inom ramen för samarbetet inom CCRA och där Sverige aktivt deltagit.

Frågan uppkommer om det finns behov av att, utöver den redan befintliga nationella certifieringsordningen för it-säkerhet i produkter och system[13] och vad som följer genom införandet av det europeiska ramverket för cybersäkerhetscertifiering, även införa en särskild anpassad nationell certifieringsordning för IKT-produkter, -tjänster och -processer som ska användas i nätverks- och informationssystem i säkerhetskänslig verksamhet.

I anslutning till denna frågeställning uppkommer även frågan om certifiering enligt de ordningar som skapas inom ramen för det europeiska ramverket för cybersäkerhet kan/bör användas på detta område och om det eventuellt föreligger behov av en kombination av sådana certifieringsordningar.

[13] Denna nationella certifieringsordning kan delvis eller helt komma att upphöra när motsvarande europeiska certifieringsordningar antas inom ramen för EU:s cybersäkerhetsakt.

Utkast till reviderat NIS-direktiv

Det kan i detta sammanhang noteras att det för närvarande pågår ett arbete med att utveckla NIS-ramverket inom ramen för det så kallade NIS2-direktivet och som föremål för en pågående förhandling inom EU. Enligt det utkast till NIS2-direktiv som offentliggjorts kommer det att ställas betydande krav på säkerhet i nätverks- och informationssystem i berörda verksamheter inom hela unionen.

En fråga som då uppkommer i detta sammanhang är om det finns skäl att överväga krav på certifieringar av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet och inte samtidigt analysera behovet av motsvarande krav på certifiering i verksamhet som rör samhällsviktiga och digitala tjänster (NIS2) eller kritisk infrastruktur (se nedan).

Vidare uppkommer frågan om den praktiska tillämpningen av krav på säkerhet i nätverks- och informationssystem enligt NIS-lagen och säkerhetsskyddslagen. Detta kan vid en första anblick förefalla okomplicerat men det kan observeras att hos många verksamhetsutövare finns moderna nätverks- och informationssystem som är både omfattande och komplexa, eller i vissa fall mycket komplexa, samtidigt som olika delar av nätverks- och informationssystemen kan beröras av bl.a. olika rättsliga och tekniska krav. Det gäller t.ex. krav enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och/eller säkerhetsskyddslagen (2018:585).

Det kan därför ifrågasättas om inte säkerhetskraven på IKT-produkter, -tjänster och -processer som tas fram inom ramen för bl.a. det europeiska ramverket för cybersäkerhetscertifiering för att användas i nätverks- och informationssystem på nivån hög bör kunna användas – vid behov efter anpassning till nationella säkerhetskrav – även i säkerhetskänslig verksamhet.

Utredningen vill i detta sammanhang betona vikten att det skapas förutsättningar för att det utvecklas fler certifierade IKT-produkter, -tjänster och -processer som kan användas inom ramen för alla ovan nämnda regelverk. Frågan om krav på nationell certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet kan därför inte behandlas eller bedömas avskilt från frågan om den mer allmänna nivån på informations- och cybersäkerhet i samhället generellt och särskilt vad gäller nivån

på och behovet av ökad säkerhet i verksamheter som rör samhällsviktiga och digitala tjänster.

Förslag till EU-direktiv om kritiska entiteters motståndskraft

EU-kommissionen har den 16 december 2020 presenterat ett förslag till *Europaparlamentets och Rådets direktiv om kritiska entiteters motståndskraft* (COM[2020] 829 final). Syftet med förslaget är att förbättra tillhandahållandet på den inre marknaden av tjänster som är nödvändiga för att upprätthålla centrala samhällsfunktioner eller central ekonomisk verksamhet genom att öka kritiska entiteters motståndskraft som tillhandahåller sådana tjänster. Det avspeglar de uppmaningar om åtgärder som nyligen har utfärdats av rådet[14] och Europaparlamentet,[15] som båda har uppmuntrat kommissionen att se över den nuvarande strategin för att bättre avspegla de ökade utmaningarna för kritiska entiteter och säkerställa en närmare överensstämmelse med direktivet om säkerhet i nätverks- och informationssystem (NIS-direktivet). Förslaget är förenligt och skapar nära synergier med det föreslagna NIS2-direktivet i syfte att ta itu med den ökade sammankopplingen mellan den fysiska och digitala världen genom en lagstiftningsram med kraftfulla åtgärder för motståndskraft för såväl cyberrelaterade som fysiska aspekter, i enlighet med strategin för EU:s säkerhetsunion.

Ett syfte med det föreslagna direktivet är att införa harmoniserade minimiregler för att säkerställa tillhandahållandet av samhällsviktiga tjänster på den inre marknaden och öka kritiska entiteters motståndskraft. För att uppnå det målet bör medlemsstaterna identifiera kritiska entiteter som bör omfattas av särskilda krav och tillsyn, men också särskilt stöd och vägledning för att uppnå en hög motståndskraft mot alla relevanta risker. Därmed ska medlemsstaterna enligt förslaget säkerställa att kritiska entiteter vidtar lämpliga och proportionella tekniska och organisatoriska åtgärder för att säkerställa sin motståndskraft samt kan genomföra säkerhetskontroller av personal. Några uttryckliga krav på certifiering anger direktivet emellertid inte.

[14] Europaparlamentets och rådets direktiv 2019/944 av den 5 juni 2019 om gemensamma regler för den inre marknaden för el.
[15] Europaparlamentets och rådets förordning (EU) 2019/943 om den inre marknaden för el.

Behovet av nationell kravställning

Utredningens experter har vidare betonat behovet och vikten av att det finns en gemensamt framtagen och fastställt nationell kravställning som kan ligga till grund för evaluering och certifiering av IKT-produkter, -tjänster och -processer, särskilt på det säkerhetsskyddade området, men även som nationellt instrument inom ramen för det med EU-institutioner och andra medlemsstater gemensamma arbetet med att utveckla det europeiska ramverket för cybersäkerhetscertifiering. I dag saknas en sådan kravställning som grundas på en gemensamt framtagen hotbild, sårbarhets- och riskbedömningar och som möjliggör framtagande av adekvata skyddsprofiler i arbetet med evaluering och certifiering av IKT-produkter, -tjänster och -processer.

Frågan som också uppkommer är hur arbetet med att styra, organisera och resurssätta arbetet med framtagande av en kravställning ska ske, bl.a. vilken eller vilka myndigheter som ska delta och vilka andra berörda aktörer som är involveras i arbetet. Utredningen bedömer att utgångspunkten här bör vara att det är en statlig myndighet som får ansvaret för att utveckla och fastställa kravbilden och säkerhetskrav när det gäller säkerhetskänslig verksamhet och i övrigt på nivån hög inom ramen för det europeiska ramverket för cybersäkerhetscertifiering.

Behovet av nationell sammanställning över certifierade och rekommenderade IKT-produkter, -tjänster och -processer

Utredningens experter har även påpekat att en grundläggande förutsättning för att kunna ställa krav – vid behov med stöd av författning – på att certifierade IKT-produkter, -tjänster och -processer ska användas i nätverks- och informationssystem i säkerhetskänslig verksamhet är att det kan ske först när en utvecklad *sammanställning* över certifierade IKT-produkter, -tjänster och -processer är tillgänglig.

Marknadsfrågor

Flera av utredningens experter på detta område har under utredningsarbetet även ifrågasatt om det kan anses föreligga tillräckliga förutsättningar för att införa en nationell särskilt anpassad ordning

med krav på certifiering av IKT-produkter, -tjänster och -processer enbart för att täcka det nationella behovet på området för säkerhetskänslig verksamhet. Bl.a. har ifrågasatts möjligheterna att nationellt ställa enskilda certifieringskrav för det begränsade användningsområde som det nationella området i detta sammanhang utgör. Från experthåll framhålls vidare att dessa IKT-produkter, -tjänster och -processer som eventuellt tas fram för nationella behov även måste ha en internationell räckvidd eftersom den nationella marknaden inte bedöms som tillräcklig. Det innebär att det föreligger en risk för att det kommer att saknas marknadsmässiga förutsättningar för att ta fram särlösningar för enbart nationella behov. På motsvarande sätt behöver svenska företag som tar fram olika IKT-produkter, -tjänster och -processer verka på den globala marknaden och därför även ha en internationell räckvidd.

Förekomsten av certifieringsordningar i andra jämförbara länder

Utredningen har genom den internationella utblicken eftersträvat att få en översiktlig bild över förekomsten av certifieringsordningar för nätverks- och informationssystem som används inom området för nationell säkerhet i andra länder. Det ska noteras att den internationella utblicken och kartläggningen i allt väsentligt grundas på tillgänglig offentlig information som kunnat återfinnas på berörda myndigheters hemsidor. I syfte att kvalitetssäkra information har även skriftliga frågor ställts till myndigheterna. Mot bakgrund av att frågeställningarna rör frågor med beröring till nationell säkerhet och försvar har myndigheternas svar av naturliga skäl varit av skiftande slag och digitala möten har inte kunnat avhjälpa bristen av att på plats i olika länder kunna diskutera och inhämta information i frågor av känslig natur. Detta har medfört en begränsning av utredningens möjligheter att få ett fullgott underlag i denna del och informationen i den internationella utblicken ska bedömas mot denna bakgrund.

Den internationella utblicken – med ovan angivna begränsningar – ger vid handen att det i några med Sverige jämförbara länder finns regleringar som behandlar certifiering av IKT-produkter, -tjänster och -processer i nätverk- och informationssystem som används i verksamhet som motsvarar det svenska begreppet säkerhetskänslig verksamhet eller annars rör nationell säkerhet (se kapitel 9.).

I bl.a. Norge är föreskrivet i författning att IKT-produkter, -tjänster och -processer i nätverks- och informationssystem som behandlar hemlig eller kvalificerat hemlig information eller som används i kritisk och mycket kritisk infrastruktur ska evalueras, och att evalueringen *kan* godtas om den bl.a. certifieras av certifieringsorganet vid den norska säkerhetsmyndigheten, och godkänns) av utpekad myndighet.[16] I andra länder saknas helt reglering om formella krav på *certifiering* enligt en nationell certifieringsordning för nationell säkerhet även om det i flertalet fall finns krav på att sådana nätverks- och informationssystem ska godkännas av en myndighet.

12.5.3 Inhämtade synpunkter från Säkerhetspolisen och Försvarsmakten

Utredningen har begärt att *Säkerhetspolisen*, i egenskap av tillsynsmyndighet för den civila delen av tillämpningsområdet för säkerhetsskyddsregleringen och där behovet av ytterligare säkerhetsskyddsåtgärder för nätverks- och informationssystem framstår som mest akut, ska lämna myndighetens bedömning över ett eventuellt behov av att införa en nationell särskilt anpassad certifieringsordning för den säkerhetskänsliga verksamheten.

Säkerhetspolisen, som samrått med *Försvarsmakten* i denna fråga, bedömer att det kan finnas både för- och nackdelar med särskilda certifieringsordningar för nätverk- och informationssystem i säkerhetskänslig verksamhet, men anser att det för närvarande är oklart om fördelarna överväger, bl.a. om säkerheten skulle öka i de nätverks- och informationssystem som certifieras. Myndigheten anser att det inte är klarlagt om certifiering är den åtgärd som skulle lösa de brister i säkerhetsskyddet som har konstaterats. Effekterna av ytterligare krav på certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem som används i säkerhetskänslig verksamhet behöver därför utredas närmare innan en sådan reglering införs.

Säkerhetspolisen pekar vidare på att det för närvarande är osäkert vilken påverkan som framtida certifieringar inom ramen för det

[16] I exempelvis Tyskland ska vissa it-system och -produkter, som är avsedda att användas i säkerhetskänslig verksamhet, certifieras enligt tekniska riktlinjer avseende särskilda funktionskrav. En oberoende evaluering av överensstämmelse görs baserat på de testspecifikationer som definieras i den tekniska riktlinjen.

europeiska ramverket för cybersäkerhetscertifiering kan få för möjligheten att stärka säkerheten i nätverks- och informationssystem. Myndigheten kommer att behöva förhålla sig till de certifieringar som kommer att utfärdas med stöd av olika certifieringsordningar enligt EU:s cybersäkerhetsakt. Detta förhållningssätt kan med fördel förtydligas genom att behöriga myndigheter inom säkerhetsskyddet i föreskrifter och genom vägledning anger hur verksamhetsutövare ska förhålla sig till och tillämpa sådana certifieringar.

Säkerhetspolisen anser sammanfattningsvis att en nationell särskild anpassad certifieringsordning för säkerhetskänslig verksamhet inte bör tas fram i nuläget och dessutom behöver frågan om effekterna av sådan certifieringsordning på säkerheten i nätverks- och informationssystem utredas närmare.

12.5.4 Behovet av gemensam och fastställd kravbild

Flera av utredningens experter har samstämmigt framhållit att en grundläggande förutsättning för att överväga införande av en nationell särskilt anpassad ordning för certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet är att det finns en nationell, gemensam och fastställd hot-, sårbarhets- och riskbedömning. En certifiering av IKT-produkter, -tjänster och -processer behöver utgå från en gemensam bedömning som grund för det efterföljande arbetet med att ta fram gemensamma säkerhetskrav och nivåer för att kunna ta fram adekvata skyddsprofiler och granskningsscheman. Detta behov föreligger såväl för arbetet med informations- och cybersäkerhet i stort i samhället och som för arbetet med att stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet. För närvarande saknas dock en sådan nationell gemensam struktur för framtagning av hot-, sårbarhets och riskbedömning och en reglerad kravbild på säkerhetsnivåer och skyddsprofiler. Eftersom säkerhetshöjande effekter kommer ur den kravställning som ligger bakom certifieringen blir en central frågeställning i detta sammanhang hur formerna för att ta fram kravställning i samband med certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem ska se ut.

Utredningen anser att det är av betydande nationellt intresse att en formell struktur etableras för arbetet med att ta fram en gemen-

sam hot-, sårbarhets- och riskbedömning som kan ligga till grund för nationell kravställning och verksamhet, och som också kan användas för nationella syften inom det EU-gemensamma arbetet med framställning av skyddsprofiler inom ramen för bl.a. det europeiska ramverket för cybersäkerhetscertifiering (se nedan).

Formerna för arbetet med kravställning

Utgångspunkten för all certifiering är att det finns krav på det som ska certifieras och en ordning för hur detta ska ske, hur granskningen och evalueringen ska gå till. Detta gäller oaktat vilken typ av IKT-produkt, -tjänster eller -process det rör sig om. Hur dessa krav uttrycks kan också variera utifrån vilken typ av verksamhet det rör sig om.

En vanlig utgångspunkt är en internationell standard som tagits fram för ändamålet, t.ex. en ISO-standard som tagits fram inom ramen för *International Organization for Standardization*. Det finns i dagsläget över 22 000 globala standarder som ISO tagit fram, bl.a. standarden ISO-27001 avseende informationssäkerhet.

När det gäller höga krav på it-säkerhet så har arbetet internationellt skett inom ramen för *Common Criteria Recognition Arrangement* (CCRA), och motsvarande överenskommelse inom Europa, *Senior Officials Group Information Systems Security – Mutual Recognition Arrangement* (SOG-IS MRA).[17]

Som beskrivs i utredningens delbetänkande (SOU 2020:58) tillåts privata certifieringsorgan endast att utfärda certifikat på nivån ”grundläggande” eller ”betydande”. För nivån ”hög”, som kan anses motsvara säkerhetskraven i säkerhetskänslig verksamhet, är det den nationella myndigheten för cybersäkerhetscertifiering som är behörig.[18] Med den utgångspunkten uppkommer frågan *hur* formerna för arbetet med att ta fram en nationell kravbild ska se ut och *vilken* eller *vilka* myndigheter som bör ansvara för detta arbete.

[17] Denna ordning beskrivs i utredningens delbetänkande *EU:s cybersäkerhetsakt – kompletterande bestämmelser om cybersäkerhetscertifiering* (SOU 2020:58). Där beskrivs certifiering och betydelsen av standarder i evaluerings- och certifieringsarbetet (s. 75 ff.).
[18] Se avsnitt 3.5 i delbetänkandet.

Tidigare och pågående arbete med kravställning

Utredningen kan notera att berörda myndigheter har inom ramen för samverkan i SAMFI bedrivit olika arbeten för att ta fram gemensamma skyddsprofiler för IKT-produkter, -tjänster och -processer.

I den *Nationella handlingsplanen för samhällets informationssäkerhet* från 2012 redogörs för arbetet och där bl.a. målet för detta anges som:

> Att svenska myndigheter, och andra verksamheter, ska få stöd vid upphandling av it-säkerhetsprodukter, genom att myndigheterna i SAMFI utvecklar en serie skyddsprofiler. Skyddsprofilerna utgör grund för minimikrav på säkerhetsfunktioner och granskning av sådana produkter som har stor betydelse för verksamheters informationssäkerhet.[19]

Den föreslagna åtgärden innebar att bl.a.:

– utveckla och certifiera skyddsprofiler,

– ta fram föreskrifter (MSB) med krav på it-produkternas säkerhetsegenskaper, baserade på kraven i certifierade skyddsprofiler, och

– ta fram råd och anvisningar för hur verksamheter kan använda produkter som certifieras för att uppnå god informationssäkerhet.

Genomförandet av arbetet med föreslagna åtgärder skulle ske enligt följande:

– Arbetet med skyddsprofiler skulle genomföras av MSB med stöd av FMV/CSEC och experter från övriga myndigheter i SAMFI.

– Arbetet med föreskrifter med krav på it-produkternas säkerhetsegenskaper skulle genomföras av MSB i samverkan med FMV/CSEC och Försvarsmakten samt andra berörda aktörer.

I *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022,* från de myndigheter som tidigare har ingått i SAMFI och numera ingår i det nationella cybersäkerhetscentret, finns följande målsättningar och förslag på åtgärder:

– etablera och förvalta en referenslista för it-säkerhetsprodukter där MSB i samverkan med FMV anges som ansvariga,[20]

[19] Kapitel 5.2 – *Ökad användning av CC-evaluerade produkter.*
[20] Kapitel 1.1.13.

– utveckla säkerhetskrav för specifika it-produkter med FMV i samverkan med MSB som ansvariga,[21]
– utveckling och anskaffning av it-säkerhetsprodukter med Försvarsmakten och FMV som ansvariga myndigheter.

Utredningen kan notera att det historiska nationella arbetet kring säkerhetskrav på IKT-produkter, -tjänster och -processer har skett mer systematiskt inom ramen för Försvarsmaktens arbete och då med fokus på det egna behovet och inte primärt generella behov i övriga samhällsviktiga verksamheter. Det arbete som bedrivit utifrån samhällets mer allmänna behov har skett inom ramen för SAMFI och primärt i samarbete mellan MSB och FMV och med stöd av i första hand Försvarsmakten och FRA, vilket framkommer av de handlingsplaner för informations- och cybersäkerhet som redogörs för ovan.

Utredningen kan också notera att frågan om kravställning på IKT-produkter, -tjänster och -processer för samhällsviktig verksamhet är en fråga som angivna ansvariga myndigheter för informations- och cybersäkerhet arbetat med under en längre tid. Det arbete som bedrivits har dock varit av begränsad omfattning vad avser det faktiska framtagandet av IKT-produkter, -tjänster och -processer för samhället i stort. En del av förklaringen till detta står sannolikt att finna i att arbetet tidigare bedrivits splittrat hos flera olika myndigheter med olika ansvar för denna typ av kravställning. Därtill kommer att ingen myndighet haft det uttalade direkta ansvaret från regeringen att bedriva detta arbete samlat.

Närmare om arbetet med att ta fram skyddsprofiler

Det kan noteras att det arbete som bedrivits nationellt har från början utgått från CCRA och inom ramen för detta alltmer utifrån arbetet med så kallade *Collaborative protection profiles* (CPP). Arbete med CPP har internationellt bedrivits inom ramen för CCRA och där inom olika arbetsgrupper, s.k. *International Technical Communities* (iTC). De iTC som skapas inom ramen för arbetet i CCRA i syfte att ta fram en CPP utgörs främst av olika experter från natio-

[21] Kapitel 1.3.5.

nella myndigheter, produktleverantörer, laboratorier, och andra intressenter med.

I Sverige har arbeten med flera olika CPP genomförts, dels har svenska aktörer deltagit i det internationella arbetet inom ramen för iTC för olika internationella CPP, därtill har ett nationellt arbete bedrivits för *Virtual Private Network* (VPN), brandväggar, VoIP klienter till mobila enheter, m.m. Utgångspunkten för arbetet har varit att dessa IKT-produkter, -tjänster och -processer även ska kunna tillhandhållas på den internationella marknaden. De centrala myndigheterna i detta arbete har främst varit FMV och MSB med stöd av Försvarsmakten, och FRA. Även Säkerhetspolisen har i viss utsträckning deltagit i arbetet.

Utredningen bedömer att det sedan tidigare finns förutsättningar och en god grund för att etablera en mer strukturerad nationell process för kravställning i samband med certifiering av IKT-produkter, -tjänster och -processer, bl.a. i syfte att skapa förutsättningar att kunna utveckla och få tillgång till certifierade IKT-produkter, -tjänster och -processer på nivå ”hög” inom ramen för det europeiska ramverket för cybersäkerhetscertifiering. Efterhand som IKT-produkter, -tjänster och -processer utvecklas av olika aktörer i näringslivet, kommer allt fler sådana certifierade IKT-produkter, -tjänster och -processer att finnas tillgängliga och som kan användas inom ramen för såväl säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) och som lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster men även inom övrig verksamhet.

Sammanfattningsvis gör utredningen bedömningen att denna typ av arbete och reglering av säkerhetsnivåer och krav måste ske i form av sammanhållet ansvar för samhällets informations- och cybersäkerhet och utgå från en central instans (myndighet) med sådant ansvar.

Utredningen bedömer vidare att eftersom säkerhetsmässiga samberoenden är utbredda inom informations- och cybersäkerhetsområdet pekar detta mot att gemensamma certifieringsordningar inom ramen för det europeiska ramverket för cybersäkerhetscertifiering i framtiden kan komma att användas i stor utsträckning. Det medför även ett nationellt behov av att gemensamt med andra länder påverka och ta fram relevanta skyddsprofiler till grund för evaluering och certifiering av IKT-produkter, -tjänster och -processer som sker med stöd av det europeiska ramverket för cybersäkerhetscertifiering. Det

utbredda säkerhetsberoendet innebär att nationell säkerhet kan tillvaratas genom ett aktivt nationellt deltagande i utarbetandet av gemensamma skyddsprofiler och ett sådant samarbete innebär inte avsteg från den egna rådigheten över nationell säkerhet och försvar.

För att kunna bevaka och tillvarata nationella intressen i detta sammanhang måste det finnas en nationell struktur som skapar förutsättningar för att nationella krav kan bevakas vid hot-, sårbarhets- och riskbedömningar och vid framtagande av skyddsprofiler inom ramen för det europeiska ramverket för cybersäkerhetscertifiering.

En annan förutsättning för att ställa krav på att verksamhetsutövare i första hand ska använda certifierade IKT-produkter, -tjänster och-processer är att detupprättas en *nationell sammanställning* över certifierade IKT-produkter, -tjänster och -processer som bör alternativt inte bör användas i nätverks- och informationssystem i säkerhetskänslig respektive samhällsviktig verksamhet och som underhålls av en kompetent myndighet (se nedan).

12.5.5 Behov av nationell sammanställning över certifierade och rekommenderade IKT-produkter, -tjänster och -processer

Utredningen bedömer att en grundläggande förutsättning för att kunna ställa krav – vid behov med stöd av författning – på att certifierade IKT-produkter, -tjänster och -processer ska användas i nätverks- och informationssystem i säkerhetskänslig verksamhet är att det kan ske först när en utvecklad *sammanställning* över certifierade IKT-produkter, -tjänster och -processer är tillgänglig. Detta kan t.ex. åstadkommas genom att en utsedd myndighet ges i uppdrag att administrera en katalog med certifierade och rekommenderade IKT-produkter, -tjänster och -processer och som underlättar för en verksamhetsutövare att planera för och införa säkra nätverks- och informationssystem (se nedan).

Statliga myndigheter bör – om det inte finns skäl att frångå rekommendationerna – utgå från denna sammanställning vid val av tekniska komponenter och lösningar för säkerhet i nätverks- och informationssystem i sin verksamhet. Finns certifierade produkter som möter verksamhetens krav så ska de i första hand användas. Finns det inga certifierade IKT-produkter, -tjänster och -processer som möter verk-

samhetens krav bör det rapporteras till myndigheten för att kunna återföras till framtida kravställning.

Aktörer som nyttjar IKT-produkter, -tjänster och -processer från den nationella sammanställningen bidrar även till att skapa en bild över behövliga säkerhetsfunktioner. I den praktiska tillämpningen identifieras brister, risker, nya behov av säkerhetsfunktioner, m.m. och som genererar information som återförs in i systemet för att utgöra grund för att kravställa nästa generation eller version av it-säkerhetsprodukter. Information erhålls direkt från tillverkarna om nya sårbarheter som upptäcks hos aktörerna, vilket kan återföras in i systemet för kommande arbete med kravställning av säkerhet. Vidare kan incidentrapportering och tillsynsverksamhet identifiera risker, sårbarheter eller behov av åtgärder som föds in i systemet. Den föreslagna ordningen bidrar även till en uppdaterad lägesbild över hur, vilka och i vilken omfattning vissa produktkategorier används inom offentlig sektor, dvs. i första hand statliga myndigheter, vilken sedan kan användas för att prioritera vilka fokusområden Sverige bör ha i det kravställande och normerande arbetet på central nivå gentemot kommissionen och Enisa.

Det nu redovisade nationella systemet (ordningen) ger enligt utredningens bedömning betydande möjligheter att dra nytta av det europeiska ramverket för cybersäkerhetscertifiering för nationella ändamål när det gäller att stärka informations- och cybersäkerheten generellt i samhället, men särskilt i säkerhetskänslig verksamhet och samhällsviktig verksamhet. Detta förutsätter samtidigt att följande beaktas i den fortsatt utvecklingen av den föreslagna ordningen:

- Ska Sverige i större omfattning nyttja certifierade IKT-produkter, -tjänster och -processer är det nödvändigt att det på nationell nivå sker ett aktivt arbete med kravställning och utveckling på området samt samverkan mellan berörda aktörer i dessa frågor.
- Vidare förutsätter det föreslagna ordningen att det finns ett tydligt nationellt engagemang i arbetet med kommissionen och i Enisa:s arbete med det europeiska ramverket för cybersäkerhetscertifiering, dvs. arbetet med de framtida certifieringsordningarna. Om så inte sker finns – enligt utredningens bedömning – en uppenbar risk för att det uppstår ett läge där Sverige nationellt ställer krav på nyttjande men inte deltar och påverkar utformningen och därmed inte heller utvecklar och tillgodoser säkerheten utifrån

nationella behov och krav. Det innebär att stora delar av de resurser som tillförs det nationella arbetet med det europeiska ramverket med cybersäkerhetscertifiering inte kommer det nationella arbetet med att stärka informations- och cybersäkerheten tillgodo.

- För att åstadkomma ett ändamålsenligt och effektivt arbete med att stärka informations- och cybersäkerheten måste centrala myndigheter ges tydliga roller och uppgifter samtidigt som ett aktivt deltagande av svensk industri i arbetet säkerställs. Det innebär att myndigheter med ansvar inom informations- och cybersäkerhet ska få ett tydligt uppdrag att delta i det nationella arbetet inom ramen för respektive ansvarsområde. De författningar som i dag primärt berörs är NIS-lagen och säkerhetsskyddslagen, vilket innebär att MSB, Försvarsmakten, Säkerhetspolisen och berörda sektorsmyndigheter utgör centrala aktörer i detta arbete. Vidare måste näringslivet delta i arbetet, bl.a. stora företag som Ericsson, Saab, m.fl. Vidare behöver intresseorganisationer i form av t.ex. Teknikföretagen och Säkerhets- och försvarsföretagen (SOFF) delta, detta för att kunna samla och ge innovationsföretag som kommer beröras av den föreslagna ordningen ökade möjligheter att delta.

Sammanfattningsvis anser utredningen att en nationell ordning med framtagande av den kravställning som utredningen föreslår ska tas fram och upprättandet av den ovan angivna sammanställningen behöver utvecklas omgående och som bidrar till att möta ökade krav på säkerhet i nätverks- och informationssystem i säkerhetskänsliga respektive samhällsviktiga verksamheter. En sådan ordning bedöms också i betydande omfattning bidra till att resultaten av det europeiska ramverket för cybersäkerhetscertifiering kan återföras till det nationella arbetet med att stärka säkerheten i nätverks- och informationssystem mer allmänt i samhället men särskilt vad gäller säkerhetskänslig respektive samhällsviktig verksamhet. En sådan ordning kommer därigenom även att i betydande omfattning bidra till att stärka utvecklingen av informations- och cybersäkerheten i totalförsvaret, såväl det civila som det militära försvaret.

Utredningen vill samtidigt betona att användningen av certifierade IKT-produkter, -tjänster och -processer inte i sig självt skapar ett fullgod skydd och tillräckliga mekanismer för en korrekt och säker informationshantering. Den föreslagna ordningen ska ses som ett kom-

plement och en åtgärd i det systematiska informations- och cybersäkerhetsarbetet som också understödjer säkerhetsskyddskänslig verksamhet. Övriga säkerhetsskyddsåtgärder i form av rekommendationer/vägledningar kring designval/it-arkitektur är en nödvändighet och utgör kompletterade åtgärder för att kunna åtgärda många av de allvarliga brister som för närvarande finns i informations- och cybersäkerheten i många verksamheter, vilket tidigare redovisats i 8 kapitlet.

12.5.6 Det föreligger f.n. inte behov av en nationell särskild ordning för certifiering i säkerhetskänslig verksamhet

Utgångspunkten är enligt direktiven att överväga om det finns skäl att införa en nationell särskilt anpassad certifieringsordning för IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet. Under utredningens gång har därför förutsättningarna för att införa en nationell certifieringsordning för IKT-produkter, -tjänster eller -processer enbart för säkerhetskänslig verksamhet diskuterats.

Som ovan anges måste ett antal grundläggande förutsättningar föreligga och andra faktorer beaktas för att överväga införande av en nationell anpassad ordning för (krav) certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet. Dessa är bl.a.:

- nuvarande *regelsystem för säkerhetskänslig verksamhet*,
- tillgång till en *gemensam och fastställd nationell kravbild* som bygger på en gemensam hot-, sårbarhets- och riskbedömning till stöd för arbetet med skyddsprofiler,
- en *nationell sammanställning* över certifierade och rekommenderade IKT-produkter, -tjänster och -produkter,
- den fortsatta *utvecklingen* av det *europeiska ramverket för cybersäkerhetscertifiering*, och
- tillgång till en tillräckligt omfattande *nationell marknad*, dvs. tillräcklig utbud och efterfrågan på certifierade IKT-produkter, -tjänster och -produkter som skapar ekonomiska incitament för företag tillhandhålla sådana produkter, tjänster och -processer för säkerhetskänslig verksamhet.

Nuvarande regelsystem

Frågan om behovet av och eventuella krav på användning av certifierade IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i verksamhetsutövares säkerhetskänsliga verksamhet bör i första hand – enligt utredningen bedömning – regleras i föreskrifter som utfärdas av berörda tillsynsmyndigheter och som meddelas med stöd av säkerhetsskyddslagen och säkerhetsskyddsförordningen. Vidare bör frågan om eventuella behov och krav dessutom utgöra en central del av det samråd om bl.a. säkerheten i informationssystemet som en verksamhetsutövare ska ha med tillsynsmyndigheten vid framtagande, utveckling och driftsättning av informationssystem i säkerhetskänslig verksamhet. En sådan utvecklad samrådsprocess kan dessutom bidra till att utveckla generella krav och rekommendationer när det gäller ökat utnyttjande av certifierade IKT-produkter, -tjänster och -processer.

I detta sammanhang bör uppmärksammas de svårigheter som uppkommer för en verksamhetsutövare i frågan vem som ska fastställa certifieringskrav, säkerhetsprofiler och andra eventuella krav på säkerhetsnivåer, m.m. och som bör ligga till grund för samrådet. Samrådsförfarandet, bl.a. vad avser rådgivning, rekommendationer, säkerhetsbeslut, m.m. i dessa frågor, försvåras redan i dag genom avsaknad av närmare reglering inom detta område.

Som framgår ovan bedömer utredningen att gällande regelsystem för säkerhetskänslig verksamhet medger tillsynsmyndigheterna redan i dag att inom ramen för föreskriftsrätten närmare reglera och ställa krav på att en verksamhetsutövare ska använda evaluerade och certifierade IKT-produkter, -tjänster och -processer i nätverks- och informationssystem när säkerheten i systemet kräver en sådan åtgärd. Tillsynsmyndighetens roll vid samrådet bör inledas redan då sådant system planeras eftersom säkerhet behöver utgöra en central del av nätverks- och informationssystemet funktion och design och där adekvat kravställning och frågan om användande av certifierade IKT-produkter, -tjänster och -processer utgör en viktig del av samrådet.

Utredningen anser att denna möjlighet bör prövas i syfte att stärka säkerheten i nätverk- och informationssystem i säkerhetskänslig verksamhet. Det kan t.ex. avse IKT-produkter, -tjänster och -processer som kommer att bli framtagna med stöd av det europeiska ramverket för cybersäkerhetscertifiering, företrädesvis på assuransnivån hög,

Det kan dock uppstå behov av ytterligare evaluering av sådana produkter, tjänster och produkter med anledning av de nationella säkerhetskrav som finns i säkerhetskänslig verksamhet.

Den nuvarande nationella ordningen för certifiering av it-säkerhet i produkter och system

Som ovan framgår finns det i dag redan en nationell ordning för certifiering av it-säkerhet i produkter och system, även om den ordningen inte närmare reglerar vad som ska gälla för certifiering av IKT-produkter, -tjänster och -processer på det säkerhetsskyddade området. Osäkerhet råder dock kring giltigheten av denna certifieringsordning när en motsvarande certifieringsordning fastställs inom ramen för det europeiska ramverket för cybersäkerhetscertifiering. Vidare kan noteras att regeringen har givit FMV i uppdrag att vara nationell cybersäkerhetsmyndighet enligt EU:s cybersäkerhetsakt med uppgifter som följer av denna förordning, vilket bl.a. innebär att det nationella certifieringsorganet CSEC, som är en fristående enhet i vid myndigheten, har ansvar för certifieringar på nivå hög enligt det europeiska ramverket för cybersäkerhetscertifiering. Det råder dock osäkerhet om vilken uppgift och roll som det nationella certifieringsorganet CSEC bör och kan ha, utöver vad som följer av det europeiska ramverket för cybersäkerhetscertifiering, bl.a. när det kommer till frågan om evaluering och certifiering av IKT-produkter, -tjänster och -processer i säkerhetskänslig verksamhet. Denna fråga behöver utredas ytterligare i belysning av utvecklingen av det europeiska ramverket för cybersäkerhetscertifiering.

En gemensam och fastställd nationell kravbild

Som ovan framgår är en grundläggande förutsättning i sig för en nationell särskild anpassad ordning för certifiering tillgången på en av berörda myndigheter gemensam och fastställd nationell kravbild som i sin tur grundas på gemensam hot-, sårbarhets- och riskbedömning, och som kan ligga till grund för framtagande av säkerhetskrav och skyddsprofiler.

Utredningen kan konstatera att frågan om kravställning på IKT-produkter, -tjänster och -processer är en fråga som ansvariga myn-

digheter för informations- och cybersäkerhet arbetat med under en längre tid. *I Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022,* från de myndigheter som tidigare har ingått i SAMFI och numera ingår i det nationella cybersäkerhetscentret framkommer att det dock finns målsättningar och förslag på åtgärder, dock har – enligt uppgift – inte något mer konkret arbete ännu påbörjats.

Utredningen bedömer att behovet av ta fram en sådan kravställning är angeläget och att detta arbete bör omgående påbörjas, eftersom det är av betydelse inte bara för möjligheten att åstadkomma ökad säkerhet i nätverks- och informationssystem i säkerhetskänslig verksamhet utan även har stor betydelse för möjligheterna att nationellt kunna påverka arbetet med att ta fram och certifiera säkra IKT-produkter, -tjänster och -processer inom ramen för det europeiska ramverket för cybersäkerhetscertifiering.

Nationell sammanställning över certifierade och rekommenderade IKT-produkter, -tjänster och -produkter

Som tidigare framgår finns ett stort behov av en nationell sammanställning över evaluerade och certifierade samt rekommenderade IKT-produkter, -tjänster och -produkter som kan användas i såväl säkerhetskänslig verksamhet som verksamhet som rör samhällsviktiga och digitala tjänster. Någon sådan sammanställning finns ännu inte och utredningen anser att även arbetet med en sådan sammanställning bör omgående påbörjas.

Utvecklingen och effekter av det europeiska ramverket för cybersäkerhetscertifiering

Utvecklingen av olika certifieringsordningar inom ramen för det europeiska ramverket för cybersäkerhetscertifiering har betydelse för bedömningen av behov av ytterligare ordningar för certifiering på nationell nivå av IKT-produkter, -tjänster och -produkter i nätverks- och informationssystem i säkerhetskänslig verksamhet. Oklarheter om den framtida utvecklingen av och tillämpningsområdet för olika certifieringsordningar medför dock svårigheter att bedöma behov av och utformningen av en nationell särskild ordning för evaluering och certifiering av IKT-produkter, -tjänster och -produkter i nätverks- och

informationssystem i säkerhetskänslig verksamhet. Vidare bör effekterna – som också Säkerhetspolisen och Försvarsmakten anför – av utvecklingen av det europeiska ramverket för cybersäkerhetscertifiering beaktas och utvärderas innan en nationell särskilt anpassat ordning för certifiering införs, även om det inte finns några formella hinder i sig mot en sådan ordning eftersom det gäller frågor som rör bl.a. försvar och säkerhet.

Nationell marknad

Frågan om ett eventuellt införande av en nationell särskilt anpassad ordning för certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet väcker även – som ovan framgår – marknads- och handelsrelaterade frågor. En mer svårbedömd frågeställning är om det finns förutsättningar för försörjning av den svenska marknaden, dvs. tillgång till certifierade och lämpliga IKT-produkter, -tjänster och -processer för användning i nätverks- och informationssystem i säkerhetskänslig verksamhet. Certifiering av IKT-produkter, -tjänster och -processer utförs på initiativ av producerande företag i syfte att vinna konkurrens- eller marknadsfördelar. En evaluering och certifiering innebär kostnader som behöver kalkyleras och göras till en del av beslutsunderlag. Det råder stor osäkerhet om den svenska marknaden är tillräckligt omfattande för att skapa förutsättningar och ekonomiska incitament för aktuella företag att låta evaluera och certifiera IKT-produkter, -tjänster och -processer i enlighet med nationella krav på säkerhet. Det förefaller inte självklart att företag med en global marknad för IKT-produkter, -tjänster och -processer kommer att få eller ha incitament att lägga resurser och i detta sammanhang inte obetydliga kostnader för certifiering som ger tillgång till en i sammanhanget – globalt sett – mycket begränsad marknad.

Vidare riskerar nationella certifieringskrav som t.ex. inte ansluter till gemensamma standarder att i betydande mån begränsa utbudet av tillgängliga IKT-produkter, -tjänster och -processer och därigenom också negativt påverka samhällets cybersäkerhet och förmåga till att upprätthålla och utveckla säkerhetsskydd. Om en sådan ordning omfattar IKT-produkter, -tjänster och -processer som också omfattas av krav på nationella godkännanden medför detta att Sverige kan

komma att ställa krav som går utöver de som gemensamt beslutats inom t.ex. det europeiska kryptosamarbetet. Detta skulle innebära att svenska företag på området skulle få konkurrensnackdelar gentemot övrig europeisk industri på området. Det väcker även frågan om det finns risk för uppkomsten av handelshinder gentemot andra medlemsstater som godkänt IKT-produkter, -tjänster och -processer inom ramen för t.ex. det europeiska kryptosamarbetet.

Utredningen bedömer att även ovan angivna marknads- och handelsrelaterade frågor behöver analyseras ytterligare innan det kan bli aktuellt att införa en nationell ordning av det aktuella slaget.

Slutsatser i frågan om behovet av en nationell särskilt anpassad ordning för certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet

För att en nationell särskilt anpassad ordning för certifiering ska ha förutsättningar att fungera ställs krav på strukturer, funktioner och processer som i dag i viss mån saknas. Det har inte varit möjligt för utredningen att inom ramen för uppdraget, främst på grund av tillgänglig tid och resurser, att i tillräcklig omfattning utreda alla dessa frågor och det väcker även frågan om angivna frågor kan anses rymmas i uppdraget som det formulerats i direktiven. Att utreda, överväga och föreslå om, och i sådana fall, hur angivna strukturer, funktioner och processer kan skapas och hur de bör och kan fungera, kräver i flera av frågorna långtgående analyser och klargöranden. Det har inte bedömts möjligt att inom ramen för utredningen – och som uppdraget formulerats – att genomföra denna typ av djupgående analyser och utredningar.

Flera av de ovan behandlade frågeställningarna är av sådan grundläggande karaktär och behöver bli föremål för en djupare och samlad analys varför ett förslag att införa en nationell särskilt anpassad ordning för certifiering av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet för närvarande inte är lämplig och skulle sannolikt inte heller framgångsrikt kunna omsättas i praktik. Flera av de ovan angivna frågeställningarna indikerar dessutom på behov av omfattande undantag från obligatoriskt användande av certifierade IKT-produkter, -tjänster

och -processer i aktuell verksamhet.[22] Sådana behov av undantag kommer troligen också främst att uppkomma hos de myndigheter som i störst omfattning redan hanterar skyddsvärd information och skyddsvärda system.

Sammanfattningsvis bedömer utredningen att det för närvarande inte finns tillräckliga skäl att införa en nationell särskilt anpassad ordning med krav på certifiering av IKT-produkter, -tjänster och -processer som används i säkerhetskänslig verksamhet

Det är viktigt att åtgärder som planeras införs fullt ut först när nationell kravställning och en sammanställning med certifierade och rekommenderade IKT-produkter. -tjänster och -processer finns tillgänglig. Samtidigt kommer verksamheter som omfattas av nationella godkännanden, t.ex. kryptoprodukter och specifika verksamheter med särskilda krav och förutsättningar, att eventuellt behöva undantas från en nationell certifieringsordning på området.

Utredningen kan samtidigt notera att frågan om krav på och användning av certifierade IKT-produkter, -tjänster och -processer i nätverks- och informationssystem bör kunna utgöra del i det förstärkta samråd som är under införande och där även Säkerhetspolisen och Försvarsmakten föreslås få möjlighet att besluta åtgärdsföreläggande och förbjuda driftsättning i de fall systemen inte bedöms som säkra (se vidare kapitel 13.).

Behov av att öka användningen av certifierade IKT-produkter, -tjänster och -processer i statlig verksamhet

Utredningen vill i detta sammanhang samtidigt framhålla att det finns behov av att öka användningen av certifierade IKT-produkter, -tjänster och -processer i statlig verksamhet. Det är i dag upp till en statlig myndighet, dvs. verksamhetsutövare, att själv avgöra om en IKT-produkt, -tjänst eller -process är tillräckligt säker, att eventuella kryptofunktioner är korrekt implementerade och att det finns säkerhetsfunktioner som är granskade av någon annan än tillverkaren själv. Det är således upp till varje myndighet, dvs. verksamhetsutövare, att

[22] Till detta kommer att det kan finnas behov av att en nationell certifieringsordning anpassad för säkerhetskänslig verksamhet skapar synergier med eventuella krav, till följd av NIS2-direktivet, att väsentliga och viktiga entiteter certifierar viss IKT enligt särskilda europeiska ordningar för cybersäkerhetscertifiering.

på eget ansvar avgöra behovet av att använda certifierade IKT-produkter, -tjänster och -processer.

Myndigheten för samhällsskydd och beredskap (MSB) anger i och för sig i myndighetens allmänna råd att en statlig myndighet bör *överväga* – vid anskaffning av informationssystem – att välja produkter som är certifierade genom tredjepartsgranskning mot etablerad standard, med det är endast en rekommendation. En sådan åtgärd är därför frivillig för statliga myndigheter och det är oklart för utredningen i vilken utsträckning som myndigheterna följer detta råd.

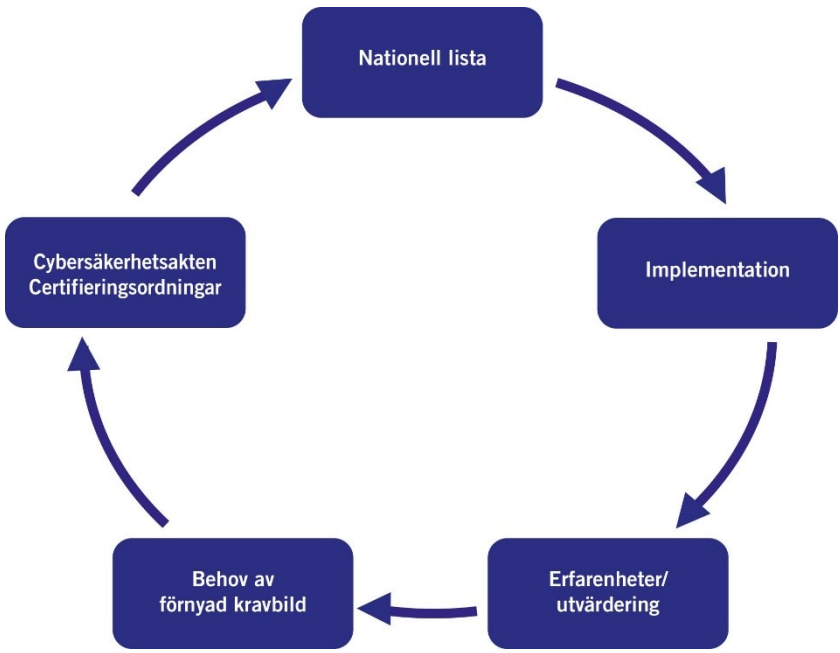
Utredningen bedömer – som tidigare anges – att informations- och cyberssäkerheten i statliga myndigheters verksamhet behöver stärkas och en åtgärd är att myndigheterna i större utsträckning använder certifierade kommersiella IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i verksamheten om inte detta framstår som olämpligt eller omöjligt att genomföra. Även om utredningen bedömer att det för närvarande inte finns förutsättningar för att införa en nationell särskilt anpassad ordning med krav på certifiering av IKT-produkter, -tjänster och -produkter i nätverks- och informationssystem i säkerhetskänslig verksamhet bedömer utredningen att det bör vidtas åtgärder som kan öka användningen av sådana produkter, tjänster och processer generellt i statliga myndigheters verksamhet. Det kan t.ex. övervägas om det bör ställas krav på att certifierade, även kommersiella, IKT-produkter, -tjänster och -processer ska användas i nätverks- och informationssystem i övrig verksamhet om det inte finns skäl för undantag från en sådan skyldighet. En sådan ordning saknas för närvarande, eftersom det är upp till varje statlig verksamhetsutövare att i enlighet med ansvarsprincipen själv bedöma och besluta om vilka åtgärder som är nödvändiga för att stärka informations- och cybersäkerheten i den egna verksamheten.

Genom att ställa krav på att statliga myndigheter att de bör använda certifierade IKT-produkter, -tjänster och -processer så skapas en ordning som förutom att bidra till att stärka säkerheten i nätverks- och informationssystem även kan bidra till att generera nödvändig eller behövlig information och som bidrar till att utveckla kravställningen och grundnivån på säkerheten i IKT-produkter, -tjänster och -processer i nätverks- och informationssystem.

En ordning som innebär att i första hand bör certifierade, även kommersiella, IKT-produkter, -tjänster och -processer användas skulle

ge statliga myndigheter, men även andra aktörer, ett stöd i val av it-säkerhetsprodukter. Det skulle också medföra att det skapas ett grundläggande fundament som kan utvecklas vidare för att stärka säkerheten i nätverks- och informationssystem i olika verksamheter och därigenom även bidra till att möta krav i den säkerhetskänsliga verksamheten. Ett sådant grundläggande fundament saknas dock för närvarande eftersom det är upp till varje statlig verksamhetsutövare att i enlighet med ansvarsprincipen själv bedöma och besluta om vilka åtgärder som är nödvändiga för att stärka informations- och cybersäkerheten i den egna verksamheten.

Figur 12.1 Effekter av ökad användning av certifierade IKT-produkter, -tjänster och -processer



Ökade krav på användning och en ökad tillgång på certifierade IKT-produkter, -tjänster och -processer bidrar till att generera kunskap och erfarenheter som kan återföras in i den nationella ordningen utan att behöva röja att produkten, tjänsten och processen används i säkerhetskänslig verksamhet. Granskning (evaluering) av de tillkommande funktions- och säkerhetskrav på IKT-produkter, -tjänster

och -processer i nätverks- och informationssystem som används i säkerhetskänslig verksamhet, och som det europeiska ramverket för cybersäkerhetscertifiering inte omhändertar, kan ske genom den kompletterande nationella granskning (evaluering) som redan i dag sker, bl.a. med stöd av Säkerhetspolisens och Försvarsmaktens samråds- och tillsynsverksamhet samt föreskrifter på område. Vidare kan genom tillsynsverksamheten av säkerhetsskydd kunskap och erfarenheter vinnas när det gäller omfattning av nyttjandegraden av olika IKT-produkter, -tjänster och -processer, vilket kan bidra till att kraftsamla nationella resurser i kravställningen för olika framtida produktkategorier inom bl.a. det europeiska ramverket för cybersäkerhetscertifiering. Även implementeringsval och design i säkerhetskänslig verksamhet kan påverka kravbilden när det gäller utformning och funktionalitet på produkter och tjänster som används i sådan verksamhet.

Detta medför också att den befintliga verksamheten i det nationella certifieringsorganet CSEC vid Försvarets materielverk (FMV) bör kunna utnyttjas på ett mer ändamålsenligt och kostnadseffektivt sätt i verksamhet som gäller evaluering och certifiering av IKT-produkter, -tjänster och -processer, även sådana som används i nätverks- och informationssystem i säkerhetskänslig verksamhet. FMV och dess certifieringsorgan bör därigenom även kunna utvecklas till att – utöver att vara nationell cybersäkerhetsmyndighet enligt det europeiska ramverket för cybersäkerhetscertifiering – utgöra en nationell resurs för kompletterande nationella granskningar av IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i bl.a. säkerhetskänslig verksamhet. I detta samarbete bedöms också Försvarsmakten och Försvarets radioanstalt behöva bidra, framför allt med kompetens inom kryptologi och frågor som rör kryptolösningar. Samverkan bör även ske med Myndigheten för samhällsskydd och säkerhet, även om myndigheten i dag inte har några formella uppgifter inom ramen för säkerhetskyddsregleringen. Myndigheten har dock i uppdrag och en central roll med att stärka informations- och cybersäkerheten i samhället mer allmänt och även en central roll när det gäller informations- och cybersäkerhet i nätverks- och informationssystem i samhällsviktiga och digitala tjänster.

Sammantaget gör utredningen bedömningen att alla åtgärder som tar sikte på att stärka säkerheten i nätverks- och informationssystem som inte omfattas av reglering av säkerhetsskyddskänslig verksam-

het bidrar till att mer allmänt höja nivån på informations- och cybersäkerhet hos statliga myndigheter och därigenom även inom det säkerhetskänsliga området.

Utredningen kan samtidigt konstatera att frågan om eventuell ytterligare reglering av och krav på åtgärder mer allmänt för att stärka informations-och cybersäkerheten i statliga myndigheter inte omfattas av utredningens uppdrag, som är begränsat till den säkerhetskänsliga verksamheten, och frågeställningen behandlas utöver vad som ovan framhållits därför inte ytterligare i detta betänkande.

12.6 Uppdrag till berörda myndigheter

Utredningen bedömer att arbetet med att ta fram en nationell kravställning, dvs. en gemensamt framtagen och fastställd kravställning som grundas på en gemensam hot-, sårbarhets- och riskbedömning, och som kan ligga till grund för arbetet med att ta fram säkerhetskrav och skyddsprofiler för att evaluera och certifiera IKT-produkter, -tjänster och -processer i bl.a. nätverks- och informationssystem bör påbörjas omgående. En sådan kravställning är också av stor nationell betydelse för att kunna påverka arbetet inom ramen för det europeiska ramverket för cybersäkerhetscertifiering. Vidare bör även arbetet med att ta fram en nationell sammanställning över certifierade och rekommenderade IKT-produkter, -tjänster och -processer för användning inom främst säkerhetskänslig och samhällsviktig verksamhet påbörjas.

Vilken myndighet som bör ansvara för detta arbete?

När det gäller frågan vilken eller vilka myndigheter som bör ges uppgiften och ansvaret för att leda och genomföra detta arbete kan ett antal myndigheter övervägas.

Försvarsmakten har etablerade strukturer för denna typ av kravställning. Myndighetens huvudsakliga uppgift finns dock i första hand på det militära försvarsområdet till stöd för Sveriges säkerhet varför en sådan uppgift framstår som mindre lämplig för den myndigheten. Däremot bör myndigheten kunna delta i och stödja arbetet med att ta fram säkerhetskrav för IKT-produkter, -tjänster och -processer inom andra samhällsviktiga verksamheter.

När det gäller Säkerhetspolisen så kan även den myndigheten övervägas då myndigheten har en helhetsbild över de hot som finns mot det civila samhällets säkerhetskänsliga verksamheter och kan därför vara den myndighet som har detta ansvar för kravställningen. Myndigheten har dock – på motsvarande sätt som Försvarsmakten – i första hand ett ansvar för Sveriges säkerhet (förutom militärt försvar) och inte ansvar för generell säkerhet för IKT för all samhällsviktig verksamhet.

FRA har en mycket djup och omfattande teknisk kompetens inom informations- och cybersäkerhetsområdet. Myndigheten har också i uppdrag att stödja Försvarsmakten i verksamhet som avser utveckling och vidmakthållande av Försvarsmaktens cyberförsvarsförmåga. Verksamheten inom FRA är dock mer av teknisk karaktär där den förmåga myndigheten besitter är kritisk för Sveriges säkerhet och där fokus är att nyttja denna unika förmåga till att stödja andra verksamheter. Med det som utgångspunkt är myndighetens roll mer att stödja i arbetet med att ta fram de mer tekniska kraven i en ordning som nu övervägs.

Utredningen bedömer att alla dessa tre myndigheter dock är centrala – var och en utifrån sina förutsättningar – för det kvalificerade arbetet som behöver ske i samband med att det tas fram en nationell kravställning för IKT-produkter, -tjänster och -processer.

MSB har i dag ett brett uppdrag och mandat på området för samhällets informations – och cybersäkerhet och har som ovan framgår en roll och uppgift på området inom ramen för SAMFI-arbetet. MSB har även ett övergripande ansvar för att utfärda föreskrifter och allmänna råd för statliga myndigheters informationssäkerhet och för verksamheter som avser samhällsviktiga och digitala tjänster (NIS-lagen). Inom ramen för NIS-arbetet sker också sedan flera år tillbaka ett strukturerat arbete mellan MSB och de myndigheter som har tillsynsansvar för de samhällsviktiga sektorer som NIS omfattar. Detta samarbete ger framöver också en möjlighet för MSB att strukturerat få del av de utmaningar som dessa samhällskritiska sektorer har vad avser IKT. Denna kunskap kan vägas samman med den unika kunskap avseende kvalificerade hot- och riskbedömningar som Försvarsmakten, Säkerhetspolisen och FRA besitter.

MSB har teknisk kompetens på området genom det arbete som myndigheten bedriver i sitt systematiska informationssäkerhetsarbete men myndigheten skulle behöva att i viss omfattning stärka den

djupa tekniska kompetensen som krävs för det samlade arbetet med kravställning för IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i säkerhetskänslig verksamhet. Härtill kommer att myndighetens ansvarsområde formellt inte omfattar verksamhet inom den säkerhetskänsliga verksamheten, som primärt är Säkerhetspolisens och Försvarsmaktens ansvarsområden inom respektive tillsynsområde.

FMV är den myndighet som nu har den högsta kompetensen när det kommer till frågor som rör evaluering och certifiering av IKT-produkter, -tjänster och -produkter. Myndigheten har vidare – i linje med de bedömningar och förslag som lämnats i utredningens delbetänkande (SOU 2020:58), och som delas av regeringen, – fått delvis nya uppgifter på området, bl.a. som nationell myndighet för cybersäkerhetscertifiering.

FMV framstår mot den bakgrunden som lämplig myndighet att få i uppgift och ansvar att leda och organisera arbetet med att ta fram struktur för en nationell kravställning, dvs. en gemensamt framtagen och fastställd kravställning som grundas på en gemensam hot-, sårbarhets- och riskbedömning, och som kan ligga till grund för arbetet med att ta fram säkerhetskrav och skyddsprofiler för att evaluera och certifiera IKT-produkter, -tjänster och -processer i bl.a. nätverks- och informationssystem. En sådan kravställning är också av stor nationell betydelse för att kunna påverka arbetet inom ramen för det europeiska ramverket för cybersäkerhetscertifiering, där myndigheten också har en viktig uppgift som nationell myndighet för cybersäkerhetscertifiering. I uppgiften bör även ingå att överväga hur arbetet med att ta fram en nationell sammanställning över certifierade och rekommenderade IKT-produkter, -tjänster och -processer för användning inom främst säkerhetskänslig och annan samhällsviktig verksamhet kan utföras.

Ett första steg i att etablera en ordning som denna bör vara ett regeringsuppdrag till FMV att i samråd med Försvarsmakten, Säkerhetspolisen, FRA och MSB, ta fram ett närmare förslag till hur en ordning som den nu föreslagna kan etableras till den 1 januari 2023.

Detta myndighetsgemensamma arbete bedrivs lämpligen inom ramen för det cybersäkerhetscentrum som nu etablerats av Försvarsmakten, MSB, FRA och Säkerhetspolisen och där även flera andra myndigheter av vikt för en ordning som denna redan ingår.

I uppdraget bör också ingå att samråda och samverka med de myndigheter som har tillsynsansvar inom NIS-området.

13 Krav på godkännande och utvidgat samrådsförfarande för informationssystem

Förslag: Säkerhetsskyddsförordningens bestämmelser om förberedande åtgärder inför driftsättning av informationssystem ska överföras till säkerhetsskyddslagen.

Dessutom införs krav på verksamhetsutövaren att pröva om en driftsättning av ett informationssystem i säkerhetskänslig verksamhet, eller en väsentlig förändring av informationssystemet, är lämplig ur säkerhetsskyddssynpunkt. Lämplighetsprövningen ska, liksom den särskilda säkerhetsskyddsbedömningen, dokumenteras. Om lämplighetsprövningen leder till bedömningen att det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt får det inte inledas. Om lämplighetsprövningen leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt ska verksamhetsutövaren i vissa fall samråda med samrådsmyndigheten (Säkerhetspolisen eller Försvarsmakten). Eventuella samråd med Säkerhetspolisen eller Försvarsmakten ska emellertid inte begränsas till en skriftlig process.

Även samrådsmyndigheten ska ha rätt att initiera samråd. Samrådsmyndigheten ska inom ramen för ett samråd kunna besluta åtgärdsföreläggande mot verksamhetsutövaren. Om ett sådant föreläggande inte följs eller om det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt även om ytterligare åtgärder vidtas, ska samrådsmyndigheten få besluta att driftsättningen eller förändringen av informationssystemet inte får genomföras (förbud).

Befintligt krav på att verksamhetsutövaren ska godkänna driftsättningen av ett informationssystem som ska användas i säkerhetskänslig verksamhet ska uppfyllas efter samrådet.

Bedömning: Även med beaktande av de ändringar i säkerhetsskyddslagen (2018:585) som regeringen nyligen föreslagit finns behov av att ytterligare stärka säkerheten i nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet. Ett krav på att informationssystem som behandlar vissa säkerhetsklassificerade uppgifter, eller andra informationssystem där obehörig åtkomst kan medföra en skada för Sveriges säkerhet, ska godkännas av en utpekad central myndighet före driftsättning torde i sammanhanget kunna bidra till ökad säkerhet. För närvarande finns emellertid övervägande skäl att i stället först utvärdera vilka effekter de kompletterande säkerhetsskyddsbestämmelserna, i förening med en stärkt samrådsroll, har.

13.1 Inledning och utgångspunkter

I utredningsdirektiven anges att särskilda krav på säkerhet måste kunna ställas på nätverks- och informationssystem för att skydda nationell säkerhet. Utredningen ska enligt direktiven överväga om det finns anledning att införa krav på godkännande från en utpekad myndighet av IKT-produkter, -tjänster och -processer inom nätverks- och informationssystem som ska tas i drift i viss eller all säkerhetskänslig verksamhet. I detta kapitel redogörs för utredningens analys, överväganden och förslag i frågan om det bör införas ett sådant krav. Frågan om behovet av krav på certifiering av nätverks- och informationssystem i säkerhetskänslig verksamhet har behandlats i föregående kapitel.

Utredningen är enligt utredningsdirektiven också fri att lämna sådana författningsförslag som i övrigt behövs och är lämpliga. Vid bedömningen av om det finns behov av ett nytt krav på formellt förhandsgodkännande behöver en jämförelse göras med det befintliga systemet och de av regeringen föreslagna ändringarna i säkerhetsskyddslagen som avses träda i kraft den 1 december 2021 (se propositionen *Ett starkare skydd för Sverige säkerhet* [prop. 2020/21:194]). I sammanhanget är effekterna av en utvidgad samrådsskyldighet och utökade tillsynsbefogenheter av särskilt intresse. En stärkt samrådsroll för Säkerhetspolisen och Försvarsmakten är ett tänkbart alternativ till godkännandeförfarandet som övervägs närmare.

Som berörts i det föregående är begreppsanvändningen på informationssäkerhetsområdet inte helt konsekvent. Flera EU-dokument, såsom NIS-direktivet, EU:s cybersäkerhetsakt m.fl., omfattar *nätverks- och informationssystem* medan begreppet *informationssystem* företrädesvis används på säkerhetsskyddsområdet. Enligt vissa nationella definitioner kan nätverk ingå i begreppet informationssystem (se t.ex. MSBFS 2020:7). Med informationssystem avses enligt säkerhetsskyddsförordningen (2018:658) ett system av sammansatt mjuk- och hårdvara som behandlar information (5 §). Med hänsyn till den begreppsanvändning som är dominerande i Sverige vad beträffar säkerhetsskydd använder utredningen i detta kapitel främst begreppet informationssystem när författning relaterar till det. I avsnitt 11.2 redogörs närmare för övervägandena kring begreppen.

13.2 Allvarliga brister i informationssäkerheten

13.2.1 Utredningar och kartläggningar[1]

Som framgår av kapitel 8 har *Utredningen om vissa säkerhetsskyddsfrågor* (SOU 2018:82) identifierat ett antal allvarliga problem och brister i säkerhetsskyddsarbetet i Sverige. Enligt denna utredning gäller vissa av bristerna säkerhetsskyddet generellt, t.ex. att verksamhetsutövaren inte tillämpar säkerhetsskyddsreglerna eller har bristande kunskap om sina skyddsvärden. Det konstateras att det finns verksamheter av stor betydelse för Sveriges säkerhet som inte alls tillämpar säkerhetsskyddslagens bestämmelser. Utöver att medvetenheten om säkerhetsskyddsregleringen är för dålig hos vissa verksamhetsutövare kopplas problemen till att säkerhetsskyddsarbetet inte har en tillräckligt framskjuten roll inom verksamheten. Andra brister handlar specifikt om olika förfaranden där utomstående involveras i den säkerhetskänsliga verksamheten. Bristerna handlar om att man inte alltid prövar om förfarandet är lämpligt eller att det är svårt att pröva lämpligheten, att säkerhetsskyddsavtal kan vara bristfälliga, att man inte följer upp förfarandet medan det pågår och att det saknas tillräckliga möjligheter för samhället att ingripa mot förfaranden

[1] Se kap. 8 för en utförligare redogörelse av bristerna i informationssäkerheten.

som är olämpliga från säkerhetsskyddssynpunkt.[2] Denna uppfattning delas av regeringen.[3]

Av kapitel 8 framgår vidare att det genomförts ett stort antal utredningar om och kartläggningar av informationssäkerheten i Sverige det senaste decenniet. Som utredningen anfört i kapitel 3 görs bedömningen att detta underlag får anses ge en tillräckligt säker bild av förekommande brister i nationell informationssäkerhet.

Nedan redogörs för vad som i huvudsak framkommit om bristerna i syfte att belysa om det finns ytterligare behov av åtgärder för att öka säkerheten i nätverk och informationssystem.

När det gäller informationssäkerhet inom ramen för säkerhetsskyddet har det identifierats behov av att förtydliga och utvidga säkerhetsskyddschefens roll i arbetet med att ta fram och bibehålla ett väl anpassat skydd. Behovet har bl.a. framkommit genom flera uppmärksammade händelser de senaste åren där det visat sig att centrala verksamhetsutövare haft ett eftersatt säkerhetsskydd. Ett exempel är den upphandling om förändrad it-drift hos Transportstyrelsen som medförde att säkerhetsskyddsklassificerade och av andra skäl sekretessbelagda uppgifter hanterades på ett sätt som stred mot svensk lag. Under 2017 genomfördes därför en granskning av upphandlingen som redovisas i promemorian *Granskning av Transportstyrelsens upphandling av it-drift* (Ds 2018:6). Av granskningen framgår att det förekommit allvarliga brister i Transportstyrelsens hantering av hemliga uppgifter och andra skyddsvärda uppgifter, bl.a. känsliga personuppgifter, för att man i allt för hög grad saknade relevant kunskap om vilken information myndigheten hade och hur denna information skulle hanteras. Skäl till detta var bl.a. att arbetet med informationssäkerhet vid myndigheten var eftersatt under lång tid samt avsaknaden av tillräcklig kunskap om relevanta regler. Utredaren identifierade att säkerhetsfunktionerna på myndigheten var utspridda och saknade tillräcklig samordning. Enligt utredaren uppfattade säkerhetsskyddschefen att det var svårt att få genomslag för säkerhetsskyddsfrågor både på ledningsnivå och i verksamheten samt att säkerhetsfrågorna kom in alldeles för sent i processen.[4]

Myndigheten för samhällsskydd och beredskap (MSB) fick 296 rapporter år 2019 om allvarliga it-incidenter från 101 myndigheter, vil-

[2] *Kompletteringar till den nya säkerhetsskyddslagen* (SOU 2018:82), s. 24 och 196.
[3] Prop. 2020/21:194, *Ett starkare skydd för Sverige säkerhet*, s. 75.
[4] Ds 2018:6 s. 98 och 220.

ket motsvarar 40 procent av det totala antalet rapporteringsskyldiga myndigheter. Motsvarande siffror för 2018 var 297 rapporter från 34 procent av myndigheterna. Den vanligaste typen av incident under 2019 var handhavandefel, följd av rapporterade angrepp och oönskad eller oplanerad störning i kritisk infrastruktur.

MSB har de senaste åren gjort flera kartläggningar av informationssäkerhetsarbetet i länsstyrelserna och kommunerna samt små och medelstora företag (se kapitel 8). Resultaten visar att det på i princip samtliga nivåer behövs ytterligare resurser och kompetens på informationssäkerhetsområdet samt tydligare ansvarsroller. MSB drar även slutsatserna att få myndigheter följer myndighetens föreskrifter i sin helhet samt att arbetet med informations- och cybersäkerhet och säkerhetsskydd inte är tillräckligt integrerat. Man konstaterar vidare att företagens informationssäkerhet inte ökar i samma takt som den digitala utvecklingen i samhället. Också för kommunernas del återstår arbete i införandet av ett systematiskt och riskbaserat informationssäkerhetsarbete, inom samtliga undersökta områden. Många gånger förefaller det saknas tillräcklig kunskap om den egna organisationens behov av informationssäkerhet. Särskilt informationssäkerhetsarbete relaterat till säkerhetsskydd eller samhällsviktig verksamhet uppfattas ofta som en utmaning. MSB anser att en förbättring av informationssäkerhetsarbetet är påkallad men bedömer att såväl deltagande av offentlig förvaltning som resurstillsättning behövs.

Det finns ytterligare studier om läget för informationssäkerheten i regioner och kommuner som visar att det föreligger stora utmaningar för huvuddelen av aktörerna i arbetet med att skapa en säker digitalisering. En av de största utmaningarna för en enskild offentlig aktör är att ha tillräckliga resurser för att informationssäkra sina it-miljöer.[5]

Vidare framgår av Riksrevisionens rapport *Föråldrade it-system – hinder för en effektiv digitalisering* (RiR 2019:28) att det finns ett stort antal större myndigheter som har föråldrade it-system, varav ett flertal av verksamhetskritisk karaktär, och att många myndigheter inte gör tillräckligt för att hantera de problem som systemen innebär. Riksrevisionen fann också att regeringen hade bristande kunskap om

[5] *Övergripande studie av offentlig it-drift (informationssäkerhet) i Västra Götaland*, Knowit, 2020.

förekomsten och konsekvenserna av problemen med föråldrade it-system.

Genom *It-driftsutredningens* (SOU 2021:1)[6] kartläggning av 200 statliga myndigheter framkommer att hälften av myndigheterna inte arbetar systematiskt med informationssäkerhet i sin verksamhet. Enligt insamlade enkätsvar hanterar 40 procent säkerhetsskyddsklassificerade uppgifter, medan 4 procent inte vet om de hanterar sådana uppgifter.[7] It-driftsutredningen bedömer att två av de största hindren för säker it-drift är bristande informationsklassificering och avsaknad av kompetens inom it och säkerhet.

Därutöver har Säkerhetspolisen rapporterat att de myndigheter som bedriver de mest skyddsvärda verksamheterna i många fall har svårt att bedöma vad som är skyddsvärt med hänsyn till Sveriges säkerhet. Enligt Säkerhetspolisen har myndigheter också vanligtvis svårt att bedöma hotbilden mot den egna verksamheten. I stor utsträckning saknar även myndigheter förmågan att bedöma den egna verksamhetens sårbarheter. Som följd av dessa brister har många myndigheter svårt att vidta ändamålsenliga och kostnadseffektiva säkerhetsskyddsåtgärder. Säkerhetspolisen finner det därför angeläget att alla myndigheter genomför säkerhetsanalyser och bedömer vilken information och verksamhet som är skyddsvärd. Dessutom framhålls att säkerhetsarbetet bör prioriteras högre.[8]

Sverige anses ha en hög nivå av digitalisering. Dock bedöms cybersårbarheten vara besvärande hög.[9] Enligt OECD behöver regeringen vidta olika åtgärder för en bättre hantering av data. Bl.a. förespråkas ökade befogenheter för och användning av DIGG.[10]

Även flera av utredningens experter har påtalat att informationssäkerhetsarbetet i Sverige är undermåligt. Utredningen har också varit i kontakt med andra aktörer på den svenska IKT-marknaden – både offentliga och privata – som påpekat att det brådskar med att göra IKT-systemen säkrare.

---

[6] Delbetänkandet *Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering* (SOU 2021:1).
[7] Utredningen skickade en enkät till 200 statliga myndigheter. 22 myndigheter svarade inte på frågorna.
[8] Säkerhetspolisens offentliga redovisning *Säkerhetsskydd hos myndigheter med mest skyddsvärd verksamhet*, 2018-02-13.
[9] ITU: *Global Cybersecurity Index (GCI)*, 2018, och OECD: *Digital Government Index*, resultat för 2019.
[10] OECD: *Digital Government Review of Sweden – Towards a Data-driven Public Sector*, 2019.

13.2.2 Slutsatser om säkerhetsbrister och -behov

Som utredningen anfört i föregående kapitel kan konstateras att det under det senaste decenniet framkommit av olika offentliga kartläggningar och utredningar att det finns betydande brister i såväl det systematiska informationssäkerhetsarbetet som i själva it-säkerheten. Kompetensbrist, utebliven eller inkorrekt informationsklassificering och undermåliga it-system är en del av problembilden. Bristerna förekommer brett i samhället, både hos offentliga och privata aktörer. Underlaget ger vid handen att mycket information samlas i informationssystemen, varav en betydande del är skyddsvärd. Fråga uppkommer då om motsvarande brister föreligger i även säkerhetskänslig verksamhet. För denna slutsats talar förarbetena till kompletteringarna till den nya säkerhetsskyddslagen (SOU 2018:82 och prop. 2020/21:194), *It-driftsutredningens* kartläggning samt utlåtanden av utredningens experter. Det kan således antas att nu nämnda problem med informationssäkerhet även gör sig påtagligt gällande i säkerhetskänslig verksamhet.

Utredningen gör mot bakgrund av vad som ovan redovisats bedömningen att det finns ett betydande behov av att om möjligt vidta åtgärder för att stärka säkerheten i nätverk och informationssystem. Behovet framstår som skyndsamt. Som framgår av kapitel 4, 5 och 8 förekommer allvarliga angrepp mot it-systemen i dag. Om säkerheten inte höjs i nätverken och informationssystemen finns en uppenbar risk att det uppstår allvarliga följder och skador i samhället och för Sveriges säkerhet. I utredningsdirektiven anges att en möjlig skyddsåtgärd i sammanhanget skulle kunna vara att ställa krav på godkännande från utpekad myndighet innan driftsättning av systemen. Utredningen kan konstatera att något sådant krav inte finns i befintlig reglering men att säkerhetsskyddslagstiftningen är föremål för kompletteringar. Så sent som i maj 2021 föreslog regeringen i sin proposition *Ett starkare skydd för Sverige säkerhet* (prop. 2020/21:194) betydande kompletteringar bl.a. vad gäller organisation och tillsyn av säkerhetskänslig verksamhet, inbegripet informationssäkerhet.

De konstaterade allvarliga bristerna i arbetet med informationssäkerheten ligger till grund för utredningens överväganden om den nuvarande och föreslagna ordningen bör kompletteras med ett formellt krav på godkännande innan driftsättning sker av IKT-systemen i säkerhetskänslig verksamhet. Ett sådant krav kan avse alla system i

säkerhetskänslig verksamhet, vissa delar av sådan verksamhet eller endast system som hanterar information som delas in i viss säkerhetsskyddsklass.

13.3 Nuvarande system

Som utredningen konstaterat i föregående avsnitt föreligger betydande brister brett inom flera olika samhällsområden och hos alla typer av aktörer. Fråga uppkommer då om den nuvarande regleringen i förening med föreslagna lagstiftningsåtgärder på säkerhetsskyddsområdet kan anses tillräckliga för att säkerställa fullgod säkerhet i nätverks- och informationssystem i säkerhetskänslig verksamhet.

13.3.1 Granskning och godkännande

Begrepp och nationella system

Såsom redogjorts för i kapitel 3 och 11 föreligger viss osäkerhet i fråga om innebörden av begreppen granskning, godkännande och ackreditering och deras inbördes förhållanden. Att granskning i sammanhanget certifieringsgranskning av produkt eller tjänst inte sker innebär inte att produkten eller systemet på säkerhetsskyddsnivå inte är granskade eller godkända. Militära underrättelse- och säkerhetstjänsten (Must) som tillsynsutövare inom Försvarsmakten och som nationell kryptomyndighet har, liksom Säkerhetspolisen, nyckelroller i detta.

Kryptomekanismer som föreskrivs i säkerhetsskyddsförordningen granskas av Must som också utfärdar nationella godkännanden. Sådana granskningar och godkännanden finns också avseende produkter utanför det omedelbara kryptoområdet. Must är också tillsynsmyndighet inom Försvarsmakten och granskar system, dvs. sammansatta system av ibland hundratals produkter, liksom ”system av system”.[11] Verksamhetschefen godkänner efter att systemet befunnits uppfylla aktuella krav. Säkerhetspolisen har en liknande roll gentemot andra myndigheter och privat sektor. Det är verksamhetsutövaren som har uppgiften att godkänna driftsättningen av informationssystem i säker-

[11] Försvarsmakten har tillsynsansvar för säkerhetsskyddet inom försvarssektorn, dvs. de myndigheter som ligger under Försvarsdepartementet samt Försvarshögskolan och Fortifikationsverket. Dessa myndigheter är i vissa fall skyldiga att samråda med Försvarsmakten.

hetskänslig verksamhet (se nedan) efter Säkerhetspolisens eller Försvarsmaktens granskning och utlåtande om uppfyllandet av säkerhets- och författningskrav. Nu nämnda granskningar och godkännanden ska inte förväxlas med motsvarande termer avseende certifieringsverksamheten.

Av utredningens internationella jämförelse (se kapitel 9 och avsnitt 13.5) framgår att ackreditering respektive godkännande av skyddsvärda informationssystem ofta hänger ihop och mer eller mindre används synonymt (jfr t.ex. Australiens system med Nya Zeelands krav). I detta sammanhang inbegriper ackreditering (”accreditation”) och godkännande eller tillåtelse (”authorisation”) att en behörig person dels formellt accepterar återstående säkerhetsrisker med drift av informationssystemet, dels godkänner/tillåter dess driftsättning. När fråga är om det för nationen mest skyddsvärda brukar uppgiften att ackreditera/godkänna ligga hos ett departement eller en myndighet. Vidare kan noteras att kraven på godkännande i säkerhetskänslig verksamhet vanligtvis gäller informationssystemen och den information som systemen behandlar. Kravet på formellt godkännande syftar här till att bidra till ökad säkerhet i informationssystem. Det förekommer också att vissa it- och informationssäkerhetsprodukter, inte minst kryptoutrustning, omfattas av godkännandeförfarandena.

Ett godkännande kan även innebära att en process tillåts fortskrida, utan att närmare ställningstagande till eller dokumentation av befintliga brister görs. Detta förfarande framstår emellertid, enligt föreliggande system, inte som dominerande på området. Om inte annat anges avses fortsättningsvis med godkännande ett behörigen fattat beslut att acceptera kvarvarande säkerhetsrisker med driftsättning av ett informationssystem.

Vid utredningen har framkommit att kraven på godkännande primärt tar sikte på tre parametrar: antingen nationell säkerhet, säkerhetsklassificerad information på viss nivå, eller assuransnivå (hög). Värt att framhålla är emellertid att assuransnivån hög inte automatiskt innebär att berörd produkt, tjänst eller process även ska vara säkerhetsskyddsklassificerad, om än dessa i praktiken inte sällan torde vara skyddsvärda.[12] Krav på godkännande i förhållande till assuransnivå och produkttyp förefaller vara vanligast förekommande i fråga

[12] Vidare hänger själva assuransnivån snarare ihop med evaluerings- och certifieringsprocesser än godkännandeförfaranden. Assurans avser tilltro till en produkt och har inget att göra med om produkten är säkerhetsskyddsklassificerad – vanligen är den inte det.

om s.k. högassurans-kryptoutrustning (se t.ex. systemen i Australien och Nya Zeeland).

Gränsöverskridande krypto- och säkerhetssamarbete

Godkännande av kryptoprodukter och vissa närliggande produkter sker inte enbart mot nationella krav och föreskrifter utan också inom ramen för ett internationellt kryptosamarbete (se kapitel 9). Detta kryptosamarbete utgör en gemensam bottenplatta för tekniska krav och processer som medverkar till att göra såväl produkter som processer föremål för ömsesidiga granskningar, värderingar och godkännanden. Detta medför interoperabilitet mellan nationer och organisationer och skapar också en internationell marknad för denna typ av produkter. Inte minst genom det europeiska kryptosamarbetet som genom gemensamma krav och möjligheter till ömsesidiga godkännanden skapas en inre marknad för krypto- och andra säkerhetsprodukter.[13] I sammanhanget bidrar AQUA-förfarandet till ett ökat förtroende (se kapitel 9).[14]

Rådets beslut om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (2013/488/EU) innehåller bestämmelser om hur säkerhetsskyddsklassificerade EU-uppgifter i kommunikations- och informationssystem ska skyddas. Dessa system ska genomgå en ackrediteringsprocess och vissa säkerhetsåtgärder ska vidtas.

Överföring av klassificerad EU-information ska enligt Rådets beslut ske med godkänd krypteringsmetod. För överföring av säkerhetsskyddsklassificerade EU-uppgifter på nivåerna *EU RESTRICTED* och *EU CONFIDENTIAL* ställs krav på metod som omfattas av nationellt godkännande. För överföring av EU-uppgifter säkerhetsskyddsklassificerade som *EU SECRET* eller högre ställs krav på an-

[13] Det bör observeras att ordningen och processen för kryptogodkännande kan brytas upp, vilket i sin tur har inverkan på de internationella krypto- och säkerhetssamarbetena, inbegripet möjligheterna till ömsesidiga godkännanden.

[14] Den s.k. AQUA-evalueringen är ett system för EU-samarbete på kryptoområdet. Vid elektronisk överföring av säkerhetsskyddsklassificerade EU-uppgifter ska som utgångspunkt godkända kryptoprodukter användas. Kryptoprodukterna som ska skydda dessa uppgifter ska evalueras och godkännas av en medlemsstats nationella kryptogodkännande myndighet. En del av godkännandeprocessen avser andrapartsevaluering av en medlemsstats kvalificerade utvärderingsmyndighet (AQUA) – i antingen Frankrike, Italien, Nederländerna, Sverige eller Tyskland – som inte deltagit i utformningen eller tillverkningen av utrustningen. Det kan emellertid även förhålla sig på det sättet att EU accepterar att en medlemsstat under viss tid använder s.k. Nato-godkänt krypto.

vändning av produkter som omfattas av specifikt EU-godkännande som innefattar andrapartsevaluering utförd av annan medlemsstat.[15]

Vidare finns inom såväl det europeiska säkerhetssamarbetet som inom Nato en pågående diskussion om huruvida man bör närma sig användandet av s.k. ”kommersiellt tillgängliga produkter” för skyddet av begränsat hemlig information.

13.3.2 Allmänna krav på informationssäkerhet i statliga myndigheters verksamhet

Som framgår av kapitel 3 och 12 har Myndigheten för samhällsskydd och beredskap (MSB) uppdaterat sina föreskrifter om informationssäkerhet för statliga myndigheter.[16] Föreskrifterna ställer krav på att myndigheterna ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. MSB har även utfärdat nya föreskrifter om säkerhetsåtgärder i informationssystem (it-säkerhet) för statliga myndigheter.[17] Dessa föreskrifter är tvingande och ligger till grund för myndigheternas arbete med säkerhet i nätverk och informationssystem[18].

MSB:s reviderade föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6) anger att myndigheterna ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av vissa internationellt erkända standarderna (ISO/IEC 27001-serien) eller motsvarande (4 §). Systematiskt informationssäkerhetsarbete ska vidare utformas utifrån de risker och behov som myndigheten identifierar (5 och 6 §§). Ändringarna innebär att det nu ställs tydligare krav på myndighetsledningens uppgift att inrikta, säkerställa resurser och följa upp informationssäkerhetsarbetet.[19] Kraven är tämligen allmänt hållna och även om de anger att informa-

[15] Även om säkerhetskraven i nu nämnda beslut utformats för Rådet och den egna organisationen har angivna krav inkorporerats även i multilaterala säkerhetsskyddsavtal som en form av säkerhetsstandard vid utbyte av säkerhetsskyddsklassificerade uppgifter. Hänvisningen i dessa avtal till Rådets beslut i fråga om gällande säkerhetskrav innebär således bl.a. att godkända kryptoprodukter/gemensamhetsprodukter ska användas.

[16] MSBFS 2020:6, *Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter*.

[17] MSBFS 2020:7, *Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter*.

[18] Det bör noteras att MSB i föreskrifterna enbart använder begreppet informationssystem.

[19] Ändringarna innebär att det nu ställs tydligare krav på myndighetsledningens uppgift att inrikta, säkerställa resurser och följa upp informationssäkerhetsarbetet. Det har även tillkommit nya krav på säkerhetsåtgärder rörande lokaler och personal.

tion ska behandlas utifrån informationsklassning och riskbedömning, finns inte några uttryckliga krav på godkännande av nätverk och informationssystemen. De omfattar inte heller andra aktörer än statliga myndigheter.

MSB:s föreskrifter om it-säkerhet (MSBFS 2020:7) inriktar myndigheternas arbete genom att tydliggöra vilka säkerhetsåtgärder som en statlig myndighet minst ska ha på plats i den tekniska it-miljön. Föreskrifterna är subsidiära till författningar som ställer högre krav (1 kap. 2 §). Enligt 3 kap. 2 § ska statliga myndigheter, innan driftsättning och inför förändring som kan påverka säkerheten i informationssystemen,

– genom säkerhetstester och granskning kontrollera att valda säkerhetsåtgärder är tillräckliga för att möta identifierade krav på säkerhet, och
– verifiera att det finns nödvändig dokumentation för drift och förvaltning.

I de fall brister identifieras ska myndigheten riskbedöma och hantera dessa brister innan driftsättning eller inför förändring som kan påverka säkerheten i informationssystemen. Myndigheterna ska vidare ha interna regler för dels kryptering med krav på godkännande av krypteringslösningar (4 kap. 9 § 2 p.), dels ärendehantering med krav på vilka kriterier som ska användas för att godkänna hård- och mjukvara innan installation eller användning (4 kap. 12 § 1 p.). MSB bedömer att majoriteten av de säkerhetsåtgärder som nämns i föreskrifterna om it-säkerhet redan är införda.[20] Utredningen noterar dock att det här inte finns någon tillsyn eller något sanktionssystem.

Till följd av NIS-direktivet har MSB meddelat föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2018:7) samt rapportering av it-incidenter för statliga myndigheter (2020:8). På området har MSB också tagit fram föreskrifter om informationssäkerhet och metodstöd för leverantörer av samhällsviktiga tjänster. Sådana leverantörer ska enligt regleringen bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete

[20] Det kan tilläggas att *Utredningen om civilt försvar* (SOU 2021:25) föreslagit en ny beredskapsförordning men att dess bestämmelse om informationssäkerhet (14 §) motsvarar den nu gällande (19 §): ”Varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt”.

med stöd av ISO 27000-standarden (5 §).[21] Särskilda krav på att IKT ska godkännas av en utpekad myndighet anges inte.

Det kan i detta sammanhang noteras att NIS-direktivet är föremål för upphävande genom ett nytt direktiv (NIS2) som bl.a. medför ändrade definitioner av och krav på samhällsviktiga verksamheter i EU. Förslaget till NIS2-direktivet innehåller inte krav på formellt godkännande. Dock ska noteras att medlemsstaterna enligt den föreslagna artikeln 21.1, för kontroll av att vissa krav är uppfyllda, ges möjlighet att kräva att väsentliga och viktiga entiteter certifierar viss IKT enligt särskilda europeiska certifieringsordningar. Frågan om krav på certifiering behandlas i kapitel 12.

Som redogjorts för i föregående kapitel har sektorsmyndigheterna till följd av bl.a. NIS-regleringen föreskriftsrätt avseende informationssäkerhet inom sina respektive ansvarsområden. Dessa författningar är emellertid begränsade och i förekommande fall huvudsakligen av mer allmän karaktär. *Statens energimyndighet* har förvisso föreskrivit flera specifika krav på riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn. Vidare har PTS nyligen meddelat föreskrifter relaterade till NIS som bl.a. kräver att leverantörer av samhällsviktiga tjänster inom digital infrastruktur ska vidta säkerhetsåtgärder avseende nätverk och informationssystem för att hantera vissa risker. Nu nämnda föreskrifter innehåller emellertid inga formella krav på att produkter, tjänster eller processer inom nätverks- och informationssystem som används i samhällsviktig verksamhet ska vara godkända.

Sammanfattningsvis kan konstateras att varken i MSB:s generella förskrifter för statliga myndigheter eller föreskrifter utfärdade av MSB och sektorsmyndigheter på NIS-området förekommer det några krav på godkännande från en utpekad myndighet av nätverks- och informationssystem.

[21] Även leverantörer av digitala tjänster ska vidta säkerhetsåtgärder för att hantera risker och säkerställa kontinuiteten.

13.3.3 Krav på informationssäkerhet i säkerhetsskyddsregleringen[22]

Inledning

Att ansvaret för identifiering och bedömning av behovet av säkerhetsskydd är knutet till verksamhetsutövaren har ansetts vara grundläggande för säkerhetsskyddslagstiftningen.[23]

Som framgår av kapitel 6 och 7 uppställer säkerhetsskyddsregleringen särskilda krav för informationssystem som används i eller har betydelse för säkerhetskänslig verksamhet. Verksamhetsutövare ska dels vidta förberedande åtgärder inför driftsättning av sådana informationssystem, dels tillgodose de säkerhetskrav som kontinuerligt ställs på informationssystemen.[24] Vidare finns det krav på samråd med Säkerhetspolisen eller Försvarsmakten i vissa fall.

Säkerhetsskyddsavtal och samråd vid vissa anskaffningar

Verksamhetsutövare har enligt säkerhetsskyddslagen en skyldighet att ingå säkerhetsskyddsavtal inför vissa upphandlingar och andra anskaffningar, om den leverantör som anlitas kan få tillgång till verksamhetsutövarens säkerhetskänsliga verksamhet. Säkerhetsskyddsavtalet ska klargöra för leverantören vilka säkerhetsskyddsåtgärder som denne ska vidta under samarbetets gång för att säkerhetsskyddet ska kunna tillgodoses.

Skyldigheten att ingå säkerhetsskyddsavtal kompletteras för statliga myndigheter med ett krav på att göra en särskild säkerhetsskyddsbedömning och samråda med tillsynsmyndigheten inför vissa särskilt känsliga upphandlingar.

Tillsynsmyndigheten får under samrådet förelägga myndigheten att vidta åtgärder enligt säkerhetsskyddslagen och de föreskrifter som har meddelats i anslutning till den lagen. Om ett föreläggande inte följs eller om tillsynsmyndigheten bedömer att säkerhetsskyddslagens krav inte kan tillgodoses trots att ytterligare åtgärder vidtas,

[22] Hittills gällande säkerhetsskyddsreglering har redogjorts för mer ingående i kapitel 6 och 7.
[23] Bedömningen av om en verksamhetsutövare omfattas av säkerhetsskyddslagen är beroende av att denne gjort en korrekt analys av verksamhetens skyddsvärden.
[24] Verksamhetsutövaren är skyldig att se till att informationssystemet upprätthåller kraven på informationssäkerhet.

får tillsynsmyndigheten besluta att myndigheten inte får genomföra upphandlingen.

Inför driftsättning av skyddsvärda informationssystem

En verksamhetsutövare som avser att driftsätta ett informationssystem som har betydelse för säkerhetskänslig verksamhet är ansvarig för att säkerhetsskyddet kring ett sådant informationssystem utformas så att författningarna avseende säkerhetsskydd efterlevs.[25] Innan ett sådant informationssystem tas i drift ska verksamhetsutövaren enligt Säkerhetspolisens föreskrifter om säkerhetsskydd (4 kap. 7 § PMFS 2019:2) genomföra tester av sina säkerhetsskyddsåtgärder.[26]

Innan ett informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *konfidentiell* eller *högre* tas i drift, eller i väsentliga avseenden förändras, ska verksamhetsutövaren skriftligen samråda med Säkerhetspolisen (3 kap. 2 § säkerhetsskyddsförordningen [2018:658]). Om verksamhetsutövaren hör till Försvarsmaktens tillsynsområde enligt 7 kap. 1 § första stycket 1 säkerhetsskyddsförordningen, ska denne i stället samråda med Försvarsmakten. Samrådsskyldigheten gäller även i fråga om andra informationssystem, om obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är obetydlig.[27]

Vidare följer av 3 kap. 3 § säkerhetsskyddsförordningen att ett informationssystem som ska användas i säkerhetskänslig verksamhet

[25] Detta gäller såväl vid utveckling som anskaffning av ett system.

[26] Verksamhetsutövaren ska vidare årligen granska säkerheten i informationssystem som är avsett för att behandla uppgifter i säkerhetsskyddsklassen *hemlig* eller *kvalificerat hemlig* eller i informationssystem där en incident kan medföra allvarlig eller synnerligen allvarlig skada för Sveriges säkerhet (4 kap. 11 § Säkerhetspolisens föreskrifter om säkerhetsskydd [PMFS 2019:2]). Försvarsmaktens förskrifter (FFS 2019:2, 9 kap. 2 §) anger att berörd verksamhetsutövare (dvs. en myndighet som hör till Försvarsdepartementet) ska kontrollera att en leverantör följer säkerhetsskyddsavtalet samt att kontrollen ska genomföras varje år om säkerhetsskyddsavtalet avser kvalificerat hemliga uppgifter eller säkerhetskänslig verksamhet som är av synnerlig betydelse för Sverige säkerhet.

[27] Vid ett sådant samråd lämnar Säkerhetspolisen ett yttrande kring de säkerhetsskyddsåtgärder verksamhetsutövaren vidtagit, eller har för avsikt att vidta, samt hur dessa förhåller sig till bestämmelserna om säkerhetsskydd i författningarna. För att Säkerhetspolisen ska kunna lämna ett kvalitativt yttrande förutsätts att verksamhetsutövaren genomfört tester och verifierat att de säkerhetsskyddsåtgärder (säkerhetskrav) som identifierats i den särskilda säkerhetsskyddsbedömningen har implementerats och att de ger avsedd effekt, säkerställt att samtliga identifierade sårbarheter och säkerhetsbrister i informationssystemet som kan medföra negativ påverkan för den säkerhetskänsliga verksamheten har omhändertagits. samt säkerställt att eventuella undantag och kompenserande åtgärder som vidtagits i förhållande till säkerhetskraven i den särskilda säkerhetsskyddsbedömningen är dokumenterade.

inte får tas i drift förrän det har godkänts ur säkerhetsskyddssynpunkt av verksamhetsutövaren.

Överlåtelse av säkerhetskänslig verksamhet

En verksamhetsutövare som avser att överlåta säkerhetskänslig verksamhet är skyldig att göra en särskild säkerhetsskyddsbedömning och en lämplighetsprövning samt samråda med en samrådsmyndighet. Samrådsmyndigheten har möjlighet att förelägga verksamhetsutövare att vidta åtgärder för att uppfylla sina skyldigheter enligt lagen och ytterst besluta att en överlåtelse inte får genomföras (förbud).

Övrig reglering

Försvarsmakten och Säkerhetspolisen utfärdar föreskrifter kring hur system som hanterar Sveriges säkerhet konstrueras och vägledningar som styr andra myndigheter och privata aktörer inom säkerhetsskyddet. Försvarsmakten har tagit fram både föreskrifter och detaljerade interna kravställningsdokument (s.k. KSF:er)[28] för att underlätta att rätt säkerhet uppnås i it-systemen. T.ex. har Försvarsmakten utförliga krav på it-säkerhetsförmågor hos it-system.

13.3.4 Cybersäkerhetscertifiering i enlighet med EU:s cybersäkerhetsakt

På cybersäkerhetsområdet har även den nationella myndigheten för cybersäkerhetscertifiering, FMV, sedan den 28 juni 2021 långtgående tillsynsbefogenheter och sanktionsmöjligheter (se EU:s cybersäkerhetsakt och lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt). Systemet avser cybersäkerhetscertifiering av IKT och syftar till att generellt höja nivån på cybersäkerhet, men inbegriper inget sådant godkännandeförfarande som utredningsdirektiven beskriver.

[28] KSF står för ”Krav på säkerhetsförmågor”.

13.3.5 Slutsatser om samrådsförfarandet och skyldigheter i säkerhetskänslig verksamhet

Som framgår av det ovan anförda ska verksamhetsutövaren vidta ett antal åtgärder innan informationssystem får användas i säkerhetskänslig verksamhet. När informationssystem kan komma att behandla uppgifter i säkerhetsskyddsklassen *konfidentiell* eller *högre*, eller i fråga om andra informationssystem där obehörig åtkomst kan medföra en *inte obetydlig skada för Sveriges säkerhet*, ska verksamhetsutövaren vidare samråda med Säkerhetspolisen eller Försvarsmakten innan driftsättning eller vid väsentliga förändringar av systemet. Innebörden av ett sådant samråd är dock inte helt klar. Det är inte heller klart vilka verktyg som står till buds om en verksamhetsutövare beslutar att driftsätta ett informationssystem trots ett negativt samrådsyttrande från Säkerhetspolisen eller Försvarsmakten.[29] I vilket fall som helst innehåller säkerhetsskyddsregleringen inga uttryckliga krav på att tillsynsmyndigheten, eller någon annan utpekad myndighet, ska godkänna driftsättningen av informationssystem i säkerhetskänslig verksamhet.[30] Det finns visserligen redan förfaranden där vissa IKT-produkter i säkerhetskänslig verksamhet behöver godkännas av en utpekad myndighet, men dessa krav avser i huvudsak krypto som i sammanhanget utgör en begränsad del av området.

Enligt utredningen är det samrådsförfarande som följer av säkerhetsskyddsregleringen – till skillnad från ett förfarande med formellt godkännande – inte ett uttryck för tillåtelse (se utförligare resonemang nedan). Ansvaret för informationssystems säkerhetsskydd och samråd ligger vidare ytterst hos verksamhetsutövaren och inte hos någon tillsyns- eller samordningsmyndighet. Det innebär dock inte att tillsynsmyndigheten inte ska eller kan överpröva verksamhetsutövarens bedömningar. Utredningen noterar också att det i dag endast finns begränsade befogenheter att ingripa mot den som inte sköter sitt säkerhetsskydd. Tillsynen på säkerhetsskyddsområdet är i huvudsak av rådgivande och stödjande karaktär. Möjligheten för tillsyns- eller samordningsmyndigheten att förbjuda ett förfarande gäller endast vid vissa upphandlingar av statliga myndigheter och överlåtelser av

[29] Sannolikt hindrar inte ett negativt samrådsyttrande en driftsättning.
[30] Vid kommunikation av säkerhetsskyddsklassificerade uppgifter till ett informationssystem utanför verksamhetsutövarens kontroll ska däremot uppgifterna skyddas med hjälp av kryptografiska funktioner som godkänts av Försvarsmakten.

säkerhetskänslig verksamhet.[31] Tillsynsmyndigheterna har inga särskilda undersökningsbefogenheter och kan inte besluta sanktioner. Avsaknaden av sedvanliga tillsynsbefogenheter och möjligheter att ingripa gör att det finns en risk att verksamhetsutövare är mindre benägna att följa tillsynsmyndigheternas anvisningar och säkerhetsskyddslagstiftningens krav. Som regeringen konstaterat i propositionen *Ett starkare skydd för Sverige säkerhet* (se prop. 2020/21:194, s. 21 f.) finns därför behov av att ytterligare skärpa säkerhetsskyddslagstiftningen.

Den nuvarande ordningen innebär brister och medför att det finns en uppenbar risk för att aktörer inom informationssäkerhetsområdet kan agera skadligt för Sveriges säkerhet. Sammantaget kan regleringen inte anses tillräcklig för att nå fullgod informationssäkerhet i nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet.

Utredningen noterar att regeringen i nyss nämnda proposition föreslagit att tillsynsmyndigheten ska få sedvanliga tillsynsbefogenheter och kunna besluta sanktionsavgift, i syfte att möta behovet av skärpningar för att skydda Sveriges säkerhet. Delar av regeringens lagförslag behandlas nedan.

13.4 Pågående åtgärder för ökad informationssäkerhet

För att stärka skyddet för Sveriges säkerhet har regeringen föreslagit vissa ändringar i säkerhetsskyddslagen (prop. 2020/21:194) som är avsedda att träda i kraft den 1 december 2021. Fråga uppkommer om dessa är tillräckliga för att omhänderta problemen med informationssäkerhet. Enligt utredningen kan lagskärpningarna i sig tjäna som belysning för de fortsatta övervägandena i fråga om behovet av ytterligare krav på godkännande.

[31] Fr.o.m. den 1 december 2021 kommer tillsynsmyndigheten i stort även ha motsvarande befogenheter i samband med vissa förfaranden som kräver säkerhetsskyddsavtal (se nedan).

13.4.1 Anmälningsplikt

I dag finns på säkerhetsskyddsområdet ingen skyldighet för en verksamhetsutövare att anmäla sin verksamhet. Som tidigare berörts har regeringen dock föreslagit att den som till någon del bedriver säkerhetskänslig verksamhet ska anmäla detta till en tillsynsmyndighet.

13.4.2 Utvidgad samrådsskyldighet och befogenheter vid överlåtelse och utkontraktering av säkerhetskänslig verksamhet

Regeringen har nu föreslagit en utvidgad skyldighet för verksamhetsutövaren att i vissa fall samråda med tillsynsmyndigheten[32]. Enligt lagförslaget ska en verksamhetsutövare som avser att genomföra en upphandling, ingå ett avtal eller inleda en samverkan eller ett samarbete med en annan aktör, först ingå ett säkerhetsskyddsavtal med aktören, om aktören genom förfarandet kan få tillgång till säkerhetskänslig verksamhet av viss betydelse för Sveriges säkerhet. Innan ett sådant förfarande ska verksamhetsutövaren även göra en särskild säkerhetsskyddsbedömning och lämplighetsprövning. Om lämplighetsprövningen leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt, ska verksamhetsutövaren samråda med tillsynsmyndigheten innan den inleder förfarandet, om det planerade förfarandet innebär att den andra aktören kan få tillgång till

– säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller högre, eller
– annan säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Motsvarande krav föreslås gälla inför överlåtelse av säkerhetskänslig verksamhet. De föreslagna ändringarna i säkerhetsskyddslagen innebär vidare att tillsynsmyndigheten inom ramen för ett samråd får förelägga verksamhetsutövaren att vidta åtgärder enligt säkerhetsskydds-

[32] Tillsynsmyndigheten är en sektorsmyndighet som ska kontrollera att verksamhetsutövaren följer lagen. Tillsyn i detta syfte ska även få utövas hos de aktörer som verksamhetsutövare ingått säkerhetsskyddsavtal med. Liksom tidigare ska tillsynen bedrivas sektorsvis. Försvarsmakten och Säkerhetspolisen har emellertid en särställning inom tillsynen och samordningen avseende säkerhetsskyddet (jfr kapitel 6 och 8).

lagen och föreskrifter som meddelats i anslutning till den lagen. Samrådsansvaret fördelas mellan tillsynsmyndigheterna utifrån deras respektive ansvarsområde. Om verksamhetsutövaren inte samråder med tillsynsmyndigheten trots att det finns en skyldighet att göra det, ska tillsynsmyndigheten få inleda samrådet. Om ett beslut om föreläggande inte följs eller om tillsynsmyndigheten bedömer att det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt även om ytterligare åtgärder vidtas, ska tillsynsmyndigheten få besluta att verksamhetsutövaren inte får genomföra det planerade förfarandet (förbud). Utöver att tillsynsmyndigheten ska få förbjuda ett olämpligt förfarande kan den även ingripa i ett pågående förfarande (se nedan).

I sammanhanget bör framhållas att regeringen i sitt fortsatta författningsarbete utreder om det i säkerhetsskyddsförordningen ska införas en skyldighet för tillsynsmyndigheterna att i vissa fall ge Säkerhetspolisen respektive Försvarsmakten tillfälle att yttra sig under ett samråd, eller i övrigt innan samrådet avslutas, så att deras unika kunskaper om bl.a. hotbilder vid behov kan tillföras ärendet.[33]

Tillsynsmyndighetens åtgärdsföreläggande inom ramen för ett samråd kan exempelvis gälla vad en verksamhetsutövare behöver förbättra i fråga om säkerhetsskyddsåtgärderna som anges i 2 kap. 2–4 §§ säkerhetsskyddslagen, dvs. informationssäkerhet, personalsäkerhet och fysisk säkerhet. Föreläggandet bör också enligt regeringen kunna innebära att verksamhetsutövaren vid en senare tidpunkt under samrådsförfarandet ska återrapportera till tillsynsmyndigheten hur olika åtgärder har genomförts. I samrådet fyller alltså föreläggandet funktionen att beskriva vad som behöver göras för att det planerade förfarandet ska vara godtagbart från säkerhetsskyddssynpunkt. Dessa förelägganden behöver enligt regeringen inte kunna förenas med vite. Huvudskälet till detta är att följden av att inte följa ett föreläggande är att det planerade förfarandet inte får genomföras, och att något ytterligare incitament för verksamhetsutövaren att följa föreläggandet inte behövs. Föreläggande under samråd överlappar till viss del med befogenheten att besluta om åtgärdsföreläggande vid tillsyn (se nedan).[34]

[33] Prop. 2020/21:194 s. 59.
[34] Prop. 2020/21:194, s. 61.

13.4.3 Närmare om tillsynsbefogenheter och ingripande möjligheter

Genom den föreslagna säkerhetsskyddslagstiftningen ges tillsynsmyndigheterna även vissa undersökningsbefogenheter och möjligheter att besluta vitesföreläggande och sanktionsavgift mot den som inte följer säkerhetsskyddslagstiftningens krav.

Den som står under tillsyn ska på begäran ge tillsynsmyndigheten den information som behövs för tillsynen. Tillsynsmyndigheten har rätt att i den omfattning det behövs för tillsynen få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamhet som omfattas av tillsyn.[35] Tillsynsmyndigheten får vidare förelägga den som står under tillsyn att tillhandahålla information och att ge tillträde till lokaler och liknande, vid äventyr av vite. Tillsynsmyndigheten får även begära handräckning av Kronofogdemyndigheten för att genomföra tillsynsåtgärder.

Regleringen av sanktionsavgift föreslås bygga på strikt ansvar. Det kommer emellertid inte vara obligatoriskt att ta ut sanktionsavgift för överträdelser, utan det ligger hos tillsynsmyndigheten att bedöma om en överträdelse ska leda till sanktionsavgift i det enskilda fallet. En sanktionsavgift ska enligt regeringen bestämmas till lägst 25 000 kronor och högst 50 miljoner kronor. För en statlig myndighet, kommun eller region är det högsta sanktionsbeloppet dock 10 miljoner kronor. Vissa överträdelser av säkerhetsskyddslagstiftningen är dessutom straffsanktionerade.[36]

[35] Utredningen noterar att undersökningsbefogenheterna inte innefattar en uttrycklig rätt till tillgång till tillsynsobjekts informationssystem. Denna fråga behandlas i kapitel 14.

[36] Den som röjer säkerhetsskyddsklassificerade uppgifter för någon obehörig på ett sätt som kan medföra men för Sveriges säkerhet kan, under vissa förutsättningar, ha gjort sig skyldig till obehörig befattning med hemlig uppgift, grov obehörig befattning med hemlig uppgift eller vårdslöshet med hemlig uppgift enligt 19 kap. 7, 8 eller 9 § brottsbalken (BrB). Vidtas gärningen för att gå främmande makt tillhanda kan det i stället vara fråga om spionieri eller grovt spionieri enligt 19 kap. 5 eller 6 § BrB. Åsidosättanden av åligganden enligt säkerhetsskyddslagen kan även utgöra tjänstefel enligt 20 kap. 1 § BrB, om det sker vid myndighetsutövning, t.ex. i samband med en säkerhetsprövning av personal. Dessutom kan någon som olovligen röjer en hemlig (säkerhetsskyddsklassificerad) uppgift i vissa fall göra sig skyldig till brott mot tystnadsplikt enligt 20 kap. 3 § BrB. Detta gäller även om uppgiften hanterats av en enskild verksamhetsutövare (5 kap. 2 § första stycket säkerhetsskyddslagen).

13.4.4 Slutsatser om föreslagna ändringar i säkerhetsskyddslagen

Utredningen kan konstatera att den föreslagna lagstiftningen på säkerhetsskyddsområdet innebär införandet av en anmälningsplikt och utvidgad samrådsskyldighet för verksamhetsutövaren samt utökade befogenheter och ingripandemöjligheter för tillsynsmyndigheter. Samrådet som aktualiseras i ett förhållandevis tidigt skede möjliggör för berörda att lämna synpunkter på verksamhetsutövarens planerade förfarande (som innebär eventuell hantering av säkerhetsskyddsklassificerade uppgifter). Åtgärdsförelägganden, i vissa fall vid äventyr av vite, och sanktionsavgifter torde i detta sammanhang kunna vara effektiva verktyg för att få aktörer i säkerhetskänslig verksamhet att följa uppställda säkerhetskrav, vilket i förlängningen kan bidra till ökad informationssäkerhet.

Den föreslagna samrådsskyldigheten – med tillsynsmyndighetens befogenheter att inleda samråd och vid samrådet besluta åtgärdsföreläggande och förbjuda ett ur säkerhetsskyddssynpunkt olämpligt förfarande – uppvisar visserligen vissa likheter med ett godkännandeförfarande, men utgör inte ett formellt krav på tillstånd. Vidare gäller dessa skyldigheter och befogenheter endast när en annan aktör än verksamhetsutövaren kan få tillgång till säkerhetskänslig verksamhet (och säkerhetsskyddsavtal eventuellt ska ingås) genom upphandling, samverkan, samarbete eller överlåtelse. Dessa förfaranden skiljer sig således från driftsättning av informationssystem som är en operativ åtgärd av verksamhetsutövaren utan att säkerhetskänslig verksamhet behöver exponeras för utomstående.

Frågan är då om den av regeringen föreslagna regleringen ändå medför effekter för säkerheten i nätverks- och informationssystem som är ändamålsenliga och likvärdiga med ett krav på förhandsgodkännande från en utpekad myndighet. I det följande behandlar utredningen argument för och emot införandet av ett kompletterande formellt godkännandeförfarande.

13.4.5 Åtgärder enligt den samlade informations- och cybersäkerhetshandlingsplanen

Utredningen noterar att FMV, FRA, Försvarsmakten, MSB, Polisen, PTS och Säkerhetspolisen enligt den samlade informations- och cybersäkerhetshandlingsplanen[37] vidtar ett antal åtgärder inom sina respektive ansvarsområden för att stärka informations- och cybersäkerheten i det svenska samhället. Dock avser de pågående och planerade åtgärderna inte ytterligare krav på godkännande och/eller certifiering av IKT i säkerhetskänslig verksamhet. Den åtgärd som ligger närmast de frågor som utredningen arbetar med avser övervägandet av en nationell modell för cybersäkerhet där arbetet ska drivas av det nationella cybersäkerhetscentret. Den nationella handlingsplanen har även målsättningen att öka tillgången till säkra kryptosystem för it- och kommunikationslösningar, bl.a. genom att FMV med stöd av FRA, Försvarsmakten och MSB utarbetar en åtgärdsplan för säkra kryptografiska funktioner i samhället. Åtgärder har emellertid ännu inte vidtagits i denna del.

13.5 Krav i andra länder

Utredningen har i kapitel 9 gjort en kartläggning av ett tiotal utländska system på området, med fokus på särskilda krav på IKT i säkerhetskänslig verksamhet. Nästintill alla länder har någon form av godkännandeförfarande. Vanligt förekommande är en modell där en utpekad nationell myndighet, eller ett departement, har det yttersta ansvaret att inom sin jurisdiktion godkänna informationssystem som hanterar uppgifter som rör nationell säkerhet samt hemlig och/eller kvalificerat hemlig information.[38] Motsvarande krav på godkännande gäller i flera av de undersökta länderna också för vissa informationssäkerhetsprodukter i säkerhetskänslig verksamhet, inte minst kryptoutrustning. Samrådsförfarande i linje med den svenska modellen förekommer däremot inte i nämnvärd utsträckning i utlandet.

Med tanke på de likheter som finns mellan Sverige och de övriga länderna i Norden är det naturligt att i första hand göra en jämförelse

[37] MSB, FRA, FMV, Försvarsmakten, PTS, Polisen, Säkerhetspolisen: *Samlad informations- och cybersäkerhetshandlingsplan 2019–2022*, Redovisning mars 2021.
[38] I övriga fall brukar uppgiften att godkänna IKT-systemen ligga hos respektive organisations informationssäkerhetschef eller motsvarande.

med dessa. I Norge ska s.k. skyddsvärda informationssystem godkännas av en nationell säkerhetsmyndighet (NSM), och även informationssystem som ska behandla kvalificerat hemlig eller hemlig information måste godkännas av NSM innan de tas i bruk.[39] I Finland har det nationella cybersäkerhetscentret vid Transport- och kommunikationsverket (*Traficom)* behörigheten att godkänna informationssystem i säkerhetskänslig verksamhet. Statsrådet har rätt att föreskriva att en myndighet är skyldig att skaffa ett intyg om godkännande från *Traficom* i fråga om informationssystem som behandlar handlingar som hör till de två högsta säkerhetsklasserna (av fyra) där störst skada för nationell säkerhet riskeras. Denna föreskriftsrätt har emellertid inte utnyttjats, varför godkännande för informationssystem för närvarande inte är obligatoriskt i Finland. I Danmark uppställs krav på informationssäkerhet inom statliga myndigheter som innefattar ackreditering av informationssystem som används för klassificerad information. Sådana system kan vara föremål för certifiering och/eller godkännande.

Om myndigheter i exempelvis Nya Zeeland har informationssystem som behandlar information som rör nationell säkerhet måste systemet enligt nationell reglering ackrediteras av en central myndighet för kommunikationssäkerhet (GCSB) innan ett resulterande formellt godkännande av systemets driftsättning kan ske. Detta gäller oavsett informationens klassificeringsnivå. Ackreditering av generaldirektören på GCSB (eller formell delegat) krävs vidare för användning av högassurans-kryptoutrustning samt system och tjänster med kompartmentaliserad eller förbehållen (”caveated”) information klassificerad som *konfidentiell* och *högre*.

I Australien måste just kvalificerat hemliga (”top secret”) system och system som bearbetar, lagrar eller kommunicerar kvalificerat hemlig eller känslig kompartmentaliserad information godkännas av en underrättelsetjänst (ASD) innan systemet får tas i drift.

Av den internationella jämförelsen kan slutsatsen dras att författningar och förvaltningssystem på säkerhetsskyddsområdet inte sällan påtagligt skiljer sig åt mellan olika länder. Av inhämtad tillgänglig information framgår emellertid inte närmare hur den faktiska tillämpligheten ser ut i respektive land och i vilken utsträckning det i praktiken förekommer undantag eller speciallösningar (jfr avsnitt 9.9).

[39] Även kryptosystem som ska användas för att skydda säkerhetsklassificerad information måste godkännas av den nationella säkerhetsmyndigheten.

13.6 Behov av samordnat samråd och nationellt godkännande för säkerhetskänslig verksamhet

Säkerhetspolisen expert har under utredningen tagit upp frågan om behov av ett nationellt godkännande för säkerhetskänslig verksamhet där ett informationssystem används av flera verksamhetsutövare. I samband med det har – efter samverkan med Försvarsmakten – följande synpunkter lämnats.

> Säkerhetspolisen ser att det finns ett behov av att lämna ett samordnat samråd och godkännande inför driftsättning av informationssystem. Detta har kommit till uttryck genom att flera verksamhetsutövare inkommit med förfrågan till Säkerhetspolisen om samråd om driftsättning av informationssystem som är lika i sin natur, t.ex. fristående dator för hemlig information. Det finns också ett behov av gemensamma nätverkskopplade informationssystem där flera verksamhetsutövare tillsammans kan utbyta information. För sådana informationssystem skulle ett nationellt godkännande enligt Säkerhetspolisen innebära att säkerhetsskyddet på ett mer enhetligt sätt omhändertas.[40]
>
> I dagsläget har Säkerhetspolisen kännedom om i vart fall en verksamhetsutövare som har samordnat samrådsprocessen inför driftsättning av ett informationssystem som ska användas av andra verksamhetsutövare. Förhållandet har genomgått en samrådsprocess och har inte resulterat i ett negativt yttrande från Säkerhetspolisen. Ett sådant godkännande kan dock innebära svårigheter vid tillsyn då det kan vara svårt att avgöra vilken verksamhetsutövare som ska bära ansvaret för en brist i säkerhetsskyddet i ett sådant informationssystem.
>
> Att informationssystem godkänns för användning för alla eller flera verksamhetsutövare skulle dock i sig kunna vara positivt och i förlängningen möjliggöra för dessa att få tillgång till säkra informationssystem.
>
> Frågan blir då vem som ska godkänna driftsättningen i ett sådant fall. Att en verksamhetsutövare själv godkänner ett informationssystem innebär vissa problem om hur ansvaret ska fördelas mellan de olika verksamheterna. Ett nationellt godkännande bör därför i dessa fall lämnas av en central myndighet och kompletteras med att vissa säkerhetsskyddsfrågor ska hanteras med ett lokalt godkännande hos respektive verksamhetsutövare. Exempel på sådana frågor som bör hanteras i ett lokalt godkännande kan vara säkerställande av att utrustningen har ett tillräckligt fysiskt skydd och att endast behörig personal har tillgång till systemet.
>
> En möjlig lösning är att informationssystem som är avsedda att stödja flera eller alla säkerhetskänsliga verksamheter ska nationellt godkännas av Säkerhetspolisen. Även övriga tillsynsmyndigheter bör kunna nationellt godkänna informationssystem inom egen sektor efter samråd med

[40] Med godkännande avses här primärt ett beslut av utpekad myndighet genom vilket kvarvarande säkerhetsrisker med verksamhetsutövares driftsättning av ett informationssystem accepteras.

Säkerhetspolisen. En sådan reglering bör avgränsas till informationssystem som avser att hantera säkerhetsskyddsklassificerade uppgifter.

En reglering med nationellt godkännande bör kompletteras med att en eller flera myndigheter får i uppdrag att till andra myndigheter tillhandahålla informationssystem för behandling av säkerhetsskyddsklassificerade uppgifter.

Sammanfattningsvis kan det konstateras att det finns ett behov av att kunna godkänna driftsättning av informationssystem för flera eller alla verksamhetsutövare samtidigt. En sådan lösning har både för- och nackdelar och skulle behöva hantera de andra frågor som nämnts ovan för att på ett ändamålsenligt sätt passa in i den säkerhetsskyddsrättsliga regleringen. Frågan om ett sådant nationellt godkännande behöver därför utredas närmare.

13.7 Kompletteringarna till säkerhetsskyddslagen kontra godkännandeförfarande

Nästa fråga som utredningen har att ta ställning till är om de föreslagna ändringarna i säkerhetsskyddslagen är tillräckliga för att jämställa med ett krav på formellt godkännande från en utpekad myndighet.

Enligt förslaget till ändring av säkerhetsskyddslagen ska verksamhetsutövare som avser att anskaffa, utkontraktera eller överlåta säkerhetskänslig verksamhet i vissa fall samråda med sin tillsynmyndighet. Om förfarandet är olämpligt ur säkerhetsskyddssynpunkt kan tillsynsmyndigheten besluta att det inte får genomföras och även ingripa i ett pågående förfarande. Om tillsynsmyndigheten inom ramen för ett samråd inte förbjuder ett förfarande som verksamhetsutövaren planerar kan det möjligen uppfattas som ett informellt tyst godkännande.[41] Därmed kan verksamhetsutövare inleda vissa förfaranden som innebär hantering av hemliga uppgifter. Den föreslagna förbudsmöjligheten avser emellertid inte själva driftsättningen av informationssystem. Även om tillsynsmyndigheten också ges en generell befogenhet att besluta åtgärdsföreläggande vid tillsyn saknas i nu nämnda del motsvarande förebyggande åtgärder. Inte heller står det klart huruvida ett negativt samrådsyttrande från berörd myndighet hindrar verk-

[41] Huruvida den föreslagna säkerhetsskyddsordningen kommer att innebära ett de facto- godkännande är i dag oklart då myndigheterna har olika synpunkter om detta.

samhetsutövares beslut att driftsätta informationssystem.[42] En skillnad mellan processerna är att samrådet inte resulterar i en tydlig stämpel på att förfarandet är lämpligt utan bara inbegriper att det inte bedömts olämpligt. Inte desto mindre torde den föreslagna ordningen – inbegripet anmälningsplikten och möjligheten att vid samråd besluta åtgärdsföreläggande och förbud – i likhet med angivna krav på formellt förhandsgodkännande bidra till ökad informationssäkerhet i informationssystemen. Kraven bör medföra dels ökad identifiering av ansvar för säkerhetsskydd,[43] dels minskad risk för förfaranden som är olämpliga från säkerhetsskyddssynpunkt. Det tillkommer incitament för noggrannare kontroll av säkerheten i verksamheterna. Den föreslagna regleringen säkerställer emellertid inte en utomstående myndighets ställningstagande i varje tillämpligt fall. Å andra sidan förutsätter även ett effektivt förfarande för myndighetsgodkännande att verksamhetsutövaren anmäler sitt informationssystem för godkännande.

Ett krav på godkännande från en myndighet innan driftsättning innebär enligt Säkerhetspolisens expert att den godkännande myndigheten till viss del övertar ansvaret från verksamhetsutövaren och förändrar den för svensk säkerhetsskyddslagstiftning grundläggande principen att det är verksamhetsutövaren som ansvarar för att säkerhetsskyddet i den egna verksamheten är tillräcklig. En sådan reglering innebär både för- och nackdelar.

Utredningen anser inte att ett förhandsgodkännande från en myndighet fråntar verksamhetsutövarens ansvar för säkerheten i sina informationssystem. Godkännandet av en driftsättning innebär visserligen att riskerna och säkerhetsnivån vid tidpunkten för godkännandemyndighetens granskning av verksamhetsutövarens dokumentation accepteras, men det är fortfarande verksamhetsutövaren som ansvarar för att se till att informationssystemet upprätthåller kraven på informationssäkerhet. Utöver skyldigheterna att anmäla sin säkerhetskänsliga verksamhet och se till att berörda system är godkända skulle verksamhetsutövaren ha att fortlöpande kontrollera säkerheten och åtgärda eventuella brister i systemen.[44] Dock kan det uppstå svårigheter att närmare bedöma innehållet i det formella godkännan-

[42] Ett sådant agerande skulle förmodligen innebära att verksamhetsutövaren blir föremål för tillsyn, men eftersom driftsättningen av informationssystemet redan skett har då även den eventuella skadan för Sveriges säkerhet inträffat. Tillsynen syftar till att kontrollera att regelverket följs och är inte en förebyggande åtgärd.

[43] Den föreslagna anmälningsplikten bör också underlätta tillsynsverksamheten.

[44] Andra aspekter är tillräckligt fysiskt skydd och att endast behörig personal får tillgång till systemet.

det och vid efterföljande tillsyn av verksamheten förhålla sig till godkännandemyndighetens tidigare godkännande. T.ex. kan en tillsynsmyndighets benägenhet att utdöma sanktioner för observerade säkerhetsbrister i ett informationssystem påverkas om myndigheten tidigare godkänt driftsättning av systemet och det inte genomgått någon väsentlig förändring. En annan fråga som uppstår är om ett godkännande kan överföras till annan myndighet.

För- och nackdelar med ett myndighetsgodkännande av informationssystem

Det kan noteras att it-system blir alltmer komplexa. Risk för skada på Sveriges säkerhet – orsakad av försumlighet, olyckshändelse eller antagonistiskt angrepp – kan uppstå omedelbart vid driftsättning av ett informationssystem i säkerhetskänslig verksamhet. Skada kan uppkomma genom att säkerhetsskyddsklassificerade uppgifter röjs, förvanskas eller förstörs. T.ex. kan ett dataintrång röja alla uppgifter i ett system,[45] och det som väl är röjt går inte att ta tillbaka. Skada kan också uppstå genom att it-systemet förstörs och funktionalitet slås ut varpå kontinuitet i den säkerhetskänsliga verksamheten inte kan upprätthållas.[46] Därför är det viktigt att tillräckliga skyddsåtgärder vidtas före driftsättningen. Ett krav på förhandsgodkännande av berört informationssystems driftsättning från en kompetent oberoende tredje part kan medverka till att reducera sådana säkerhetsrisker ytterligare.

En fördel med ett godkännandeförfarande med en central myndighet som godkännandeorgan är att det bidrar till skapandet av en minimistandard för kontroll av säkerhet och mer enhetliga säkerhetskrav hos verksamhetsutövarna på de aktuella nivåerna. Särskilt för system som behandlar hemliga eller kvalificerat hemliga uppgifter, dvs. det mest skyddsvärda för Sverige, finns anledning att ställa långtgående krav på säkerheten. Här gör sig nämligen de största ris-

[45] Ett dataintrång behöver emellertid inte nödvändigtvis innebära att alla uppgifter i systemet röjs. En annan fråga är om uppgifterna ändå *betraktas* som röjda. Normalt sett bör man betrakta alla uppgifter som röjda om det inte går att visa att de inte kan ha röjts för obehöriga med anledning av intrånget. I vissa undantagsfall kan dock konstateras att intrånget är avgränsat till vissa delar och då behöver inte uppgifter som finns i andra delar av systemet betraktas som röjda. Således bör information i ett system där dataintrång kunnat påvisas betraktas som röjd tills tekniska undersökningar kunnat fastställa omfattning av intrånget.
[46] Säkerhetsskyddet syftar inte till att motverka påverkan på uppgifternas riktighet och tillgänglighet genom försumlighet eller olyckshändelse.

kerna gällande, vilket – även om inte behovet av teknisk kompetens nödvändigtvis ökar – kan motivera en oberoende tredjepartsbedömning av en central nationell myndighet.

Å ena sidan är det en rimlig utgångspunkt att verksamhetsutövaren själv ansvarar för verksamhetens skyddsvärden. Å andra sidan måste fördelarna med ett absolut ansvar för informationssäkerheten i informationsbehandlingen ställas mot vikten av kvalitetssäkring av att säkerhetskraven är uppfyllda för att förhindra allvarlig skada för Sveriges säkerhet. Till risken att informationssystemen annars blir angripna hör att informationssäkerhetsarbetet i stor utsträckning är eftersatt och utmaningarna på området är betydande.[47]

Ett argument för att ansvaret att godkänna informationssystemets driftsättning bör kvarstå på verksamhetsutövaren är att denne torde ha bäst inblick i den egna verksamhetens förutsättningar och prioriteringar, särskilt när det gäller att acceptera kvarvarande säkerhetsrisker. En utomstående, även med god kompetens och omfattande erfarenhet av informationssäkerhet och IKT-system, kan svårligen överblicka verksamhetens förutsättningar på samma sätt. Detta talar för att beslut om godkännande och därmed om hantering av residualrisker bör ske inom den egna organisationen.

Det kan tilläggas att s.k. godkännandemyndigheter i utlandet ofta har omfattande ansvar, kompetens respektive tillsynsbefogenheter på informationssäkerhetsområdet. Detta kan jämföras med Försvarsmaktens roll på säkerhetsskyddsområdet (särskilt i fråga om krypto). Trots de nyligen föreslagna bestämmelserna om säkerhetsskydd finns utrymme för en aktör att i vissa fall driftsätta ett informationssystem i säkerhetskänslig verksamhet utan att tillsynsmyndigheten gjort en mer ingående granskning av riskerna.[48] I t.ex. Norge utgör godkännandemyndighetens process för godkännande av informationssystem som behandlar säkerhetsklassificerad information en planerad och systematisk granskning av systemet – i form av en dokumentationsgenomgång – för att fastställa om det uppnås en lämplig säkerhetsnivå. Genomgången tar också fasta på om och hur negativa IKT-händelser hanteras. Vid granskningen utvärderas även informationssystemets

[47] Med undantag för Säkerhetspolisens och Försvarsmaktens områden råder i sektorerna allvarliga brister när det gäller systemsäkerhet och kompetens, såväl vid offentliga som privata aktörer.

[48] Försvarsmakten gör dock i tillämpliga fall en ingående granskning innan driftsättning, så länge berörd myndighet hemställer om samråd.

operativa miljö, dess behov av skydd och om föreslagna säkerhetsåtgärder är tillräckliga för att uppnå en lämplig skyddsnivå.

Den föreslagna möjligheten för tillsynsmyndigheterna på säkerhetsskyddsområdet att besluta en förhållandevis hög sanktionsavgift för överträdelser, som komplement till vitesföreläggande, kan i sig vara en tydlig och effektiv ekonomisk sanktion för den som har ett otillräckligt skydd för säkerhetsskyddsklassificerade uppgifter. Åtgärden riktar sig vanligen mot en konstaterad överträdelse och är i huvudsak en tillbakaverkande sanktion som är handlingsdirigerande genom att verka avskräckande. När säkerhetsskyddsklassificerade uppgifter väl röjts uppstår dock oåterkallelig risk för skada för Sveriges säkerhet, oavsett eventuellt efterföljande repressalier. I stället för att vara avhängig huruvida incitamenten i det enskilda fallet kan förutses tillräckligt motverka risktagande, t.ex. för stora och resursstarka aktörer, kan ett krav på formellt förhandsgodkännande förhindra att säkerhetskänsliga uppgifter över huvud taget hanteras före det att behörig myndighet finner säkerhetsriskläget acceptabelt. Ett godkännandeförfarande kan också minska risken för att Sveriges säkerhet skadas av misstag. Åtgärderna har olika skyddsändamål då kravet på godkännande syftar till att säkerställa att alla säkerhetskrav är uppfyllda i förväg (innan informationssystemet används), medan sanktionssystemet i sig primärt har en repressiv verkan. Sanktioner är alltså en för sen åtgärd då skadliga uppgifter redan kan vara röjda.

Utredningen noterar vidare att Sverige inte har något sådant godkännandeförfarande som förekommer i merparten av jämförbara länder. Den svenska samrådsmodellen framstår i sammanhanget som säregen. Regleringen som innebär att verksamhetsutövaren ska testa sina säkerhetsskyddsåtgärder och godkänna sitt informationssystem innan det får tas i drift i säkerhetskänslig verksamhet motsvarar närmast vad som brukar gälla i utlandet för information som inte är hemlig eller kvalificerat hemlig.

Sammanfattande bedömning av behovet av myndighetsgodkännande

Sammantaget kan det enligt utredningen inte antas att effekterna av den nya säkerhetsskyddsregleringen blir att likställa med ett krav på formellt förhandsgodkännande från en utpekad myndighet. Även om det kommande systemet är tämligen omfattande är det enligt ut-

redningens mening inte tillräckligt heltäckande. Mot bakgrund av de allvarliga följder som nationell säkerhet riskerar bedömer utredningen att det finns starka skäl att överväga införandet av ett sådant godkännandeförfarande som finns i flertalet andra jämförbara länder.[49] Ett motsvarande krav kan fylla funktionen som en ytterligare välbehövlig kontrollstation och därmed bidra till stärkt informationssäkerhet i säkerhetskänslig verksamhet.[50] Som anförts ovan medför emellertid ett sådant krav även ett antal svårigheter. Ändå finner utredningen att det finns behov av att införa ytterligare krav när det gäller driftsättning av informationssystem i säkerhetskänslig verksamhet. I linje med regleringen i flertalet jämförbara länder hade ett krav på myndighetgodkännande lämpligen kunnat avse informationssystem som ska hantera hemlig och/eller kvalificerat hemlig information.[51]

Ett alternativ till att nu införa ett nytt krav är att avvakta tills effekterna av de kompletterande bestämmelserna till säkerhetsskyddslagen utvärderats.[52] Utredningen anser dock inte att det finns tillräcklig anledning att vänta med att införa ytterligare krav på informationssystem i säkerhetskänslig verksamhet för att se effekten av de nya åtgärderna. Det är snarare angeläget att i samband med övriga skärpningar av tillsynssystemet också införa krav på myndighetsgodkännande av särskilt skyddsvärda informationssystem, eller ett likvärdigt förfarande, som ytterligare en säkerhetsskyddsåtgärd.

Säkerhetspolisen har, efter samverkan med Försvarsmakten, argumenterat för att varken samråd, ett negativt samrådsyttrande eller tillsyn formellt förhindrar driftsättning av informationssystem i säkerhetskänslig verksamhet. Mot denna bakgrund har myndigheterna föreslagit att samrådsrollen inför driftsättning och vid väsentlig förändring av informationssystem stärks genom att Säkerhetspolisen och Försvarsmakten ges möjlighet att förelägga verksamhetsutövare att vidta säkerhetsskyddsåtgärder och, om föreläggandet inte följs, besluta om att det ifrågavarande systemet inte får tas i drift eller för-

[49] Med tanke på de likheter som finns mellan Sverige och de övriga länderna i Norden är det naturligt att dessa system kan tjäna som vägledning i frågan om krav på godkännande.
[50] Ställningstagande i fråga om kvalificerat hemlig information kräver även särskilt god förmåga att göra en hotbildsanalys.
[51] Dock bör observeras att inte särskilt många aktörer hanterar sådana system. Antalet system som behandlar kvalificerat hemliga uppgifter är begränsat och återfinns främst hos Försvarsmakten, FRA och Säkerhetspolisen.
[52] Även etablerandet av cybersäkerhetscentret och dess planerade arbete är relevant i sammanhanget.

ändras i väsentliga avseenden. En sådan lösning innebär inte någon ändring av ansvarsförhållandena och kan enligt utredningens mening vara ett lämpligt alternativ till ett krav på förhandsgodkännande från en myndighet. Fråga uppkommer således om de föreslagna verktygen i praktiken skulle omhänderta eventuella risker vid behandling av säkerhetsskyddsklassificerade uppgifter på ett likvärdigt och fullgott sätt, trots att det inte rör sig om ett formellt myndighetsgodkännande. Denna lösning utvärderas i avsnitt 13.8.

När det gäller frågan om behov av ett samordnat samråd och nationellt godkännande inför driftsättning av ett informationssystem, som används av flera verksamhetsutövare i säkerhetskänslig verksamhet, delar utredningen Säkerhetspolisens uppfattning (se avsnitt 13.6). På de av Säkerhetspolisen anförda skälen behöver frågan om ett sådant nationellt godkännande för säkerhetskänslig verksamhet utredas närmare i särskild ordning och behandlas därför inte vidare i detta betänkande.

13.8 Ytterligare stärkt samrådsroll

Enligt Säkerhetspolisen och Försvarsmakten bör uppgiften att godkänna driftsättning av informationssystem ligga kvar hos verksamhetsutövaren. Även om verksamhetsutövaren i vissa säkerhetskänsliga fall även ska samråda med Säkerhetspolisen eller Försvarsmakten bedömer dessa myndigheter att man för närvarande inte har möjlighet att vidta åtgärder inför eller förbjuda en driftsättning eller väsentlig förändring av informationssystem i säkerhetskänslig verksamhet. Däremot kan dessa myndigheter inleda tillsyn.

Tillsyn är emellertid en reaktiv åtgärd. Ett dataintrång kan ske redan under själva driftsättningen varför tillsyn inte är en ändamålsenlig åtgärd för att skydda mot röjandet av säkerhetsskyddsklassificerade uppgifter och därmed skada på Sveriges säkerhet. För att undvika dessa följder vid driftsättning eller väsentlig förändring av informationssystem behövs således möjlighet att vidta åtgärder innan en driftsättning sker. En samrådsskyldighet och möjlighet att både förelägga verksamhetsutövaren att vidta säkerhetsskyddsåtgärder och förbjuda en driftsättning eller förändring av ett informationssystem är i sammanhanget tänkbara förebyggande åtgärder.

Säkerhetspolisen och Försvarsmakten har bedömt att det inte finns skäl att flytta ansvaret för säkerhetsskyddet från verksamhetsutövare på det sätt som ett godkännande av en myndighet innan driftsättning skulle innebära. I stället har Säkerhetspolisen och Försvarsmakten föreslagit att deras samrådsroll inför driftsättning och vid väsentlig förändring av informationssystem stärks på samma sätt som nu sker när det gäller utkontraktering och överlåtelse av säkerhetskänslig verksamhet. Härigenom ges myndigheterna möjlighet att besluta åtgärdsföreläggande inom ramen för samrådet och, om föreläggandet inte följs, förbjuda det planerade förfarandet. Utredningen kan konstatera att de av regeringen föreslagna kompletteringarna till säkerhetsskyddslagen inte ger tillsyns- eller samrådsmyndigheterna rätt att besluta att en driftsättning eller väsentlig förändring av ett informationssystem inte får genomföras (förbud). En sådan stärkt samrådsroll har betydande likheter med ett krav på förhandsgodkännande från en myndighet.

Nedan följer en beskrivning av hur en driftsättning eller väsentlig förändring av ett informationssystem i säkerhetskänslig verksamhet bör gå till enligt Säkerhetspolisen – från det att behovet uppstår till driftsättning.

1. Behov av nytt informationssystem, digitalisering, (verksamhetsutövaren).
2. Lämplighetsprövning (verksamhetsutövaren, se nedan).
3. Särskild säkerhetsskyddsbedömning (verksamhetsutövaren) (kravställning + lämplighetsprövning).
4. Beslut om utveckling om så bedömts lämpligt (verksamhetsutövaren).
5. Begäran om samråd – inkluderat särskild säkerhetsskyddsbedömning (verksamhetsutövaren).
6. Utveckling (verksamhetsutövaren).
7. Test av säkerhetsskyddsåtgärder (verksamhetsutövaren).
8. Uppdatering av särskild säkerhetsskyddsbedömning skickas till Säkerhetspolisen (verksamhetsutövaren).
9. Samrådsyttrande inklusive förelägganden (Säkerhetspolisen)
10. Hantera förelägganden (verksamhetsutövaren).

11. Meddela Säkerhetspolisen planerat driftsättningsdatum (eventuellt behöver minsta tid från meddelande till driftsättning regleras) (verksamhetsutövaren).
12. Eventuellt förbud (Säkerhetspolisen).
13. Godkännande ur säkerhetsskyddssynpunkt (verksamhetsutövaren).
14. Driftsättning (verksamhetsutövaren).

Det kan tilläggas att driftsättning av informationssystem i säkerhetskänslig verksamhet endast föranleder samråd med Säkerhetspolisen eller Försvarsmakten (beroende på vilket tillsynsområde verksamhetsutövaren tillhör). Endast Säkerhetspolisen och Försvarsmakten har den samlade bilden av hoten mot Sveriges säkerhet och Sveriges samlade skyddsvärden. Med hänsyn till dessa myndigheters unika sakkunskap och utpräglade roll på området finns inte skäl att ändra ordningen för vem verksamhetsutövaren ska samråda med vid driftsättning eller förändring av informationssystem.[53] Att ytterligare öka Säkerhetspolisens och Försvarsmaktens befogenheter att inrikta säkerhetsarbetet, överpröva analyser respektive beslut, begära kompletterande säkerhetsåtgärder och förbjuda olämpliga driftsättningar eller förändringar av informationssystem är att anse som ett rimligt alternativ till det övervägda kravet på förhandsgodkännande. En sådan lösning innebär inte heller någon ändring av ansvaret för säkerhetsskyddet i informationssystemet. Ett förfarande för godkännande av driftsättning hanterar inte heller helheten då framtida förändringar inte omhändertas.[54] Det bör vidare framhållas att det finns betydande organisatoriska skillnader mellan å ena sidan Sverige, å andra sidan merparten av jämförbara länder där man har en central nationell cybersäkerhetmyndighet (t.ex. Danmark, Finland och Norge)[55] med långtgående befogenheter och samlad kompetens inom informations- och cybersäkerhet, medan ansvaret för nationell informationssäkerhet i

[53] För att samrådet ska vara verkningsfullt och motverka potentiellt skadlig exponering av uppgifter eller verksamhet i övrigt, bör det, liksom tidigare, påbörjas innan verksamhetsutövaren inleder det förfarande som medför krav på samråd.
[54] Som tidigare berörts kan baskrav för system bygga på befintliga internationella standarder och certifieringsordningar. Sedan behöver den specifika applikationen och dess fysiska miljö säkerställas. Den myndighet som hanterar kommande tillsyn behöver också på ett tydligt sätt ge återkoppling till verksamhetsutövaren på insänd anmälan att föreslagen specifik applikations driftsättning kan accepteras. Detta skall inte ses som ett generellt godkännande utan som en accept för driftsättning för just denna situation. Denna specifika applikation kommer därefter att vid behov vara föremål för tillsyn.
[55] *Nasjonal sikkerhetsmyndighet* i Norge har cirka 300 anställda.

Sverige är påtagligt splittrat och placerat på ett flertal olika myndigheter, däribland sektors-/tillsynsmyndigheter. Införandet av ett generellt krav på att informationssystem, som behandlar hemliga och/eller kvalificerat hemliga uppgifter, ska godkännas av en utpekad myndighet hade sålunda bl.a. medfört behov av substantiella tillskott och omallokering av resurser.[56] Sammantaget bedömer utredningen att det lämpligaste alternativet i nuläget är att stärka samrådsrollen på det sätt som Säkerhetspolisen och Försvarsmakten föreslagit och efter viss tid utvärdera säkerhetseffekterna av myndigheternas nya verktyg. Tillkommande erfarenheter får utvisa eventuella behov av kompletterande krav på myndighetsgodkännande.

En möjlig form för hur verksamhetsutövarens beslut om godkännande av driftsättning kan ske med en ökad roll för samrådsmyndigheten är att beslutet föregås av en lämplighetsprövning och samråd med Säkerhetspolisen eller Försvarsmakten. Omfattningen av ett sådant samråd behöver dock öka om en sådan stödjande process ska träffa de organisationer som är i behov av stöd. Därför bör ett förslag om sådan process kring samråd inför driftsättning eller väsentlig förändring av informationssystem utsträckas till att omfatta även system för hantering av uppgifter i säkerhetsskyddsklassen *konfidentiell* och *högre*. Utformningen av kraven bör i övrigt i möjligaste mån följa systematiken i det av regeringen föreslagna kapitlet om skyldigheter när en annan aktör kan få tillgång till säkerhetskänslig verksamhet (kapitel 4 i säkerhetsskyddslagen). Säkerhetsskyddsförordningens bestämmelser om förberedande åtgärder inför driftsättning av informationssystem (3 kap. 1–3 §§) bör därför överföras till ett nytt kapitel i säkerhetsskyddslagen. Även om samtliga dessa regler inte avser skyldigheter för enskilda finns ett värde i att ha en sammanhållen ordning för frågorna som relaterar till samrådsprocessen (se vidare nedan). Någon ändring i sak är här inte avsedd, utöver att samma krav vid driftsättning bör gälla också för väsentlig förändring av informationssystemen samt att samråd med Säkerhetspolisen eller Försvarsmakten inte längre begränsas till en skriftlig process.

[56] I Sverige medför Säkerhetspolisens och Försvarsmaktens unika kunskaper och utpräglade roller på säkerhetsskyddsområdet att dessa myndigheter framstår som naturligt val i fråga om godkännandemyndighet, men uppgiften att godkänna hade ändå inneburit ytterligare och mer djupgående insatthet i många verksamheter.

Närmare om väsentlig förändring av informationssystem

En väsentlig förändring av ett informationssystem kan, i likhet med driftsättning i säkerhetskänslig verksamhet, innebära att systemet börjar hantera säkerhetsskyddsklassificerade uppgifter. En väsentlig förändring av ett informationssystem kan exempelvis vara att

- ett befintligt informationssystem ska hantera uppgifter med en högre säkerhetsskyddsklassificering än tidigare,
- ett befintligt informationssystem ska integreras eller kommunicera med andra informationssystem, eller när exponering av annat skäl väsentligen ökar, eller
- ett befintligt informationssystem ska användas i en annan säkerhetskänslig verksamhet (om inte en sådan hantering omfattas av det ursprungliga samrådet).

Man kan också uttrycka det som att verksamhetsutövaren driftsätter en förändring av informationssystemet. Utredningen ser följaktligen inte bärande skäl för att kravmässigt göra en distinktion mellan dessa förfaranden.

Det kan noteras att den särskilda säkerhetsskyddsbedömning som ska göras vid driftsättning och väsentlig förändring av informationssystem är mer långtgående än säkerhetsskyddsbedömningarna vid förfarandena som kräver säkerhetsskyddsavtal. Skillnaden är emellertid befogad med hänsyn till det särskilt känsliga läge en driftsättning innebär (se ovan).

Närmare om samråd och befogenheter

För att Säkerhetspolisen och Försvarsmakten ska få likvärdiga förutsättningar som tillsynsmyndigheterna, för det fall de inte utövar tillsyn, bör också samrådsmyndigheten på motsvarande sätt kunna initiera samråd vid verksamhetsutövarens underlåtelse. Som tidigare berörts är det också motiverat med befogenheter att inom ramen för samrådet besluta åtgärdsföreläggande och vid behov besluta om förbud. Samrådet med samrådsmyndigheten bör, i likhet med samråd med tillsynsmyndigheterna, inte vara begränsat till en skriftlig process. Även muntliga samråd med tillsynsmyndigheterna är avsedda att dokumenteras. Det följer redan av förvaltningslagen (2017:900)

att en myndighet som får uppgifter på något annat sätt än genom en handling snarast ska dokumentera dem, om de kan ha betydelse för ett beslut i ärendet (21 §). Vidare underlättar upphävandet av formkravet för berörd myndighet att göra en lämplig anpassning av samrådet utifrån föreliggande omständigheter och behov av skyndsamhet. Samrådsmyndigheten bör på samma sätt som gäller för tillsynsmyndigheterna, inom ramen för samrådet få besluta att förelägga verksamhetsutövaren att vidta åtgärder för att fullgöra sina skyldigheter enligt säkerhetsskyddslagen och föreskrifter som har meddelats i anslutning till den lagen. Åtgärdsföreläggandet fyller, även inför driftsättning eller förändring av informationssystem, funktionen att beskriva vad som behöver göras för att det planerade förfarandet ska vara godtagbart från säkerhetsskyddssynpunkt.[57] Befogenheten möjliggör för samrådsmyndigheten att förelägga verksamhetsutövaren att vidta säkerhetsskyddsåtgärder för att avhjälpa brister i ett informationssystem som kan komma att behandla säkerhetsklassificerade uppgifter. Frågan är kopplad till vilka krav på säkerhetsskyddsåtgärder som Säkerhetspolisen har föreskrivit. Det skulle t.ex. kunna vara föreläggande om att vidta konkreta säkerhetsskyddsåtgärder såsom flerfaktorsautentisering[58] eller att åtgärda brister i separationen av informationssystem. Samrådsmyndigheten kan vidare t.ex. förelägga verksamhetsutövaren att göra en dimensionerad hotbildsbedömning (jfr avsnitt 6.4.2) om sådan underlåtits. Ytterligare ett exempel är att det finns krav på att verksamhetsutövaren ska genomföra egna granskningar av informationssystem och samrådsmyndigheten anser att genomförda granskningar inte är tillräckliga, då skulle myndigheten kunna förelägga verksamhetsutövaren att genomföra kompletterande granskningar. Förutsatt att Säkerhetspolisen eller Försvarsmakten föreskrivit ett krav på användande av certifierad IKT-produkt så skulle samrådsmyndigheten även kunna förelägga verksamhetsutövaren att använda en sådan certifierad produkt vid driftsättning eller förändring av sitt informationssystem. Dessa åtgärdsföreläggan-

[57] Behovet av att säkerhetsbrister åtgärdas kan öka när det rör sig om driftsättning av ett informationssystem av påtaglig betydelse för samhällsviktig verksamhet och nationell säkerhet. Förvaltningslagen innehåller allmänna krav på skyndsam handläggning. Å andra sidan kan en verksamhetsutövares planering av en driftsättning i vissa fall ta ett par år.

[58] Flerfaktorsautentisering är en metod för åtkomstkontroll där användare endast beviljas åtkomst efter att framgångsrikt ha presenterat flera separata bevis för en autentiseringsmekanism. En lyckad identitetskontroll förutsätter vanligtvis två eller flera former av information (t.ex. lösenord, smartkort och biometrisk autentisering) inom kategorierna kunskap, innehav och inneboende.

den behöver enligt utredningen inte kunna förenas med vite. Ett skäl till detta är att följden av att inte följa ett föreläggande är att det planerade förfarandet inte får genomföras, och att något ytterligare incitament för verksamhetsutövaren att följa föreläggandet inte lär behövas. Därutöver bör överträdelser av samrådsskyldigheten eller agerande i strid mot meddelat förbud kunna föranleda sanktionsavgift (se nedan).

Ett förbud bör även kunna aktualiseras när den planerade driftsättningen eller förändringen av ett informationssystem bedöms olämpligt även om ytterligare åtgärder vidtas. Möjligheten att besluta sådana förbud är av stor vikt för att förhindra att förfaranden som kan skada Sveriges säkerhet genomförs. Befogenheten bör tillkomma respektive samrådsmyndighet, bl.a. eftersom samrådsmyndigheten genom samrådet redan är insatt i ärendet och ett sådant förfarande är i linje med vad som gäller för tillsyn vid anskaffning och överlåtelse av säkerhetskänslig verksamhet.[59] Det bör framhållas att ett beslut om att förbjuda ett visst förfarande är en mycket långtgående åtgärd och bör användas restriktivt. Samrådsmyndigheten måste också i varje enskilt fall göra en proportionalitetsbedömning.[60]

Ett krav på lämplighetsprövning bör införas

Säkerhetspolisen anser att verksamhetsutövaren även inför driftsättning och väsentlig förändring av informationssystem bör göra en lämplighetsprövning i enlighet med vad som gäller vid anskaffning, utkontraktering och överlåtelse av säkerhetskänslig verksamhet. Verksamhetsutövaren ska således pröva lämpligheten av införandet av ett informationssystem baserat på dess möjliga påverkan på Sveriges säkerhet. Prövningen avser att hantera situationer där introducerandet av ett informationssystem kommer innebära stora risker för Sveriges säkerhet och som inte kan hanteras genom att vidta säkerhetsskyddsåtgärder. Det kan exempelvis röra som om funktioner som:

[59] Överklagande av dessa förbudsbeslut ska dock ske till förvaltningsdomstol och inte regeringen (se kapitel 15).
[60] I fall Säkerhetspolisen och Försvarsmakten har tillsynsansvar ska de enligt regeringens proposition 2020/21:194 även ha möjlighet att ingripa i vissa pågående förfaranden genom föreläggande.

– kraftigt påverkar samhällets motståndskraft, t.ex. att flera redundanta samhällsviktiga funktioner ersätts av ett informationssystem, och/eller
– sammanställningar av olika datamängder som inte ska vara möjliga att sammanställa (s.k. aggregat-problematik).

Det rör sig alltså om funktioner som oavsett hur väl dessa skyddas innebär ett stort risktagande för Sveriges säkerhet. Lämplighetsprövningen syftar således primärt till att verksamhetsutövaren i ett tidigt skede ska vara tvungen att ta ställning till om digitaliseringen är lämplig med tanke på dess effekt på Sveriges säkerhet. Lämplighetsprövningens största effekt är dock att i ett tidigt skede få upp frågor gällande Sveriges säkerhet och att tvinga verksamhetsutövaren att ta ställning. Det innebär också, i de fall som digitaliseringen bedöms olämplig, att onödigt utvecklingsarbete inte behöver genomföras.[61]

Som framgår ovan bör enligt Säkerhetspolisen lämplighetsprövningen göras före den särskilda säkerhetsskyddsbedömningen, direkt efter att verksamhetsutövaren har konstaterat att det finns ett behov av ett nytt informationssystem eller en väsentlig förändring. Regeringen har emellertid föreslagit att säkerhetsskyddsbedömningen ska göras först, när det gäller anskaffning och överlåtelse av säkerhetskänslig verksamhet. Ett skäl till den omvända ordning som Säkerhetspolisen förespråkar är att inga skyddsåtgärder kan minska framtida säkerhetsrisker när en driftsättning i säkerhetskänslig verksamhet väl sker, och att den särskilda säkerhetsskyddsbedömningen syftar till att identifiera just åtgärder för ökad säkerhet i systemet. Denna prövning syftar till att i ett tidigt skede tydliggöra för verksamhetsutövaren, i ett bredare perspektiv, huruvida planerad digitalisering är lämplig och erforderliga krav över huvud taget kan mötas (se ovan). Å andra sidan torde sådana slutsatser till följd av en lämplighetsprövning i sig förutsätta en bedömning av risker och hot, vilket en säkerhetsskyddsbedömning inbegriper.

Utredningen finner mot bakgrund av det ovan anförda att verksamhetsutövaren, i likhet med vad som gäller när en annan aktör kan få tillgång till säkerhetskänslig verksamhet, även ska vidta en lämplighetsprövning inför driftsättning eller väsentlig förändring av informationssystem i säkerhetskänslig verksamhet och att prövningen

[61] Säkerhetspolisen och Försvarsmakten torde kunna meddela närmare vägledning om förfarandet i sina föreskrifter.

ska dokumenteras. Tillräckliga skäl att avvika från den ordningsföljd som föreslås gälla vid anskaffning och överlåtelse av säkerhetskänslig verksamhet – genom att föreskriva att lämplighetsprövningen ska ske före den särskilda säkerhetsskyddsbedömningen – föreligger inte. Då lämplighetsprövningen fyller en annan funktion än verksamhetsutövarens godkännande av driftsättning, som innebär ett beslut att kvarstående risker med användning av informationssystemet accepteras, ska befintligt krav på godkännande kvarstå. Godkännandet sker lämpligen efter fullbordat samråd.

Närmare om överlappningar, undantag och samverkan

Fråga uppkommer om skyldigheten att pröva det planerade förfarandets lämplighet även kan överlappa med motsvarande krav vid anskaffning, utkontraktering och överlåtelse av säkerhetskänslig verksamhet. Om ett sådant förfarande omfattas av reglerna om överlåtelse av säkerhetskänslig verksamhet kan sättas ifråga om förfarandet även behöver omfattas av den nu föreslagna skyldigheten att göra en lämplighetsprövning. Samma sak gäller förslaget om krav på samråd. Samråd vid utkontraktering respektive driftsättning prövar emellertid olika saker. Ett samråd vid utkontraktering ska göras före upphandlingen där leverantören vidtar åtgärder som medför att denne får tillgång till säkerhetskänslig verksamhet. Efter samrådet för utkontraktering sker själva upphandlingen. Om driftsättning av ett informationssystem omfattas av det som upphandlas bör själva driftsättningen också blir föremål för samråd. I det samrådet ska då prövas om tillräckliga skyddsåtgärder i systemet är vidtagna. I detta avseende kan samråden således inte anses vara överlappande.[62]

När det gäller frågan om att undvika överlappande regleringar anser Säkerhetspolisen att det i nuläget inte är påkallat med en rätt att besluta om undantag från de föreslagna skyldigheterna i säkerhetsskyddslagen avseende samråd m.m. Ett sådant behov av undantag kan möjligen minska av den av regeringen övervägda[63] skyldigheten för tillsynsmyndigheten att i vissa fall ge samrådsmyndigheten

[62] I t.ex. fall då verksamhetsutövaren köper in ett färdigt informationssystem, som inte heller ska driftsättas av leverantören, kommer leverantören aldrig att få tillgång till de säkerhetsskyddsklassificerade uppgifterna.
[63] Regeringen utreder för närvarande frågan om yttrande vid samråd i sitt fortsatta arbete med säkerhetsskyddsförordningen.

tillfälle att yttra sig vid ett samråd. Utredningen finner således inte anledning att i denna del lämna förslag på föreskriftsrätt i fråga om undantag.

Vidare torde samrådsmyndigheterna, när dessa inte utövar tillsyn, i behövliga fall informeras av tillsynsmyndigheten om verksamhetsutövare planerar driftsättning av informationssystem och därmed få kännedom om denne vidtar erforderliga åtgärder. Denna samverkan kan lösas praktiskt.

Sanktionsavgift som ett komplement

En avsaknad av ingripandebefogenheter gör att det finns en risk att verksamhetsutövare är mindre benägna att efterleva säkerhetsskyddslagstiftningens krav, särskilt eftersom säkerhetsskyddsåtgärder kan vara kostsamma. Det har också framkommit att det finns fall där påpekade brister inte rättats till (se bl.a. SOU 2015:25 s. 476–478). Detta är inte en acceptabel ordning när det gäller åtgärder som ska motverka risker för Sveriges säkerhet. Utredningen anser därför att det, i linje med regeringens förslag i proposition 2020/21:194, bör införas en möjlighet även för samrådsmyndigheten att besluta om sanktionsavgift för att säkerställa säkerhetsskyddslagstiftningens efterlevnad. Utredningen finner på de av regeringen anförda skälen att sanktionsavgift är ett lämpligt ingripande vid överträdelser som avser samrådsskyldigheten och meddelat förbud (se prop. 2020/21:194, s. 85 ff.). Samrådsmyndigheternas befogenhet bör i denna del motsvara tillsynsmyndigheternas och följa samma system som regeringen föreslagit (se avsnitt 13.4.4 och det av regeringen föreslagna 7 kap. i säkerhetsskyddslagen om administrativa sanktionsavgifter). Således ska det inte vara obligatoriskt att ta ut sanktionsavgift när en överträdelse konstaterats, utan det är samrådsmyndigheten som avgör om en avgift ska tas ut i det enskilda fallet. De omständigheter som särskilt ska beaktas vid den bedömningen anges i den av regeringen föreslagna 7 kap. 3 § i säkerhetsskyddslagen. Även statliga myndigheter, kommuner och regioner ska kunna påföras sanktionsavgift. Innan samrådsmyndigheten tar ut en sanktionsavgift ska verksamhetsutövaren, enligt förvaltningslagen, ges tillfälle att yttra sig.

För ett effektivt samrådsförfarande som bidrar till ett bättre säkerhetsskydd är det av stor vikt att den verksamhetsutövare som är skyl-

dig att samråda lämnar korrekta uppgifter till samrådsmyndigheten i samband med samrådet. I syfte att motverka att oriktiga uppgifter lämnas vid samråd bör det vara möjligt att besluta om sanktionsavgift mot verksamhetsutövare när så ändå har skett.[64]

Försvarsmakten har väckt frågan om inte även en underlåtelse av verksamhetsutövaren att godkänna driftsättningen av ett informationssystem i säkerhetskänslig verksamhet bör kunna föranleda sanktionsavgift från samrådsmyndigheten. Utredningen lämnar förslag om *samråds*myndighetens möjlighet att ta ut sanktionsavgift, och bedömer att utgångspunkten bör vara att godkännandet sker efter det att samrådet avslutats. En risk med en sådan befogenhet som Försvarsmakten föreslår är således att samrådsrollen blir alltför utsträckt. Överträdelser som enligt utredningens förslag ska kunna rendera en sanktionsavgift är om samrådsskyldigheten åsidosatts, förbud inte respekteras eller oriktiga uppgifter lämnats vid samråd. Verksamhetsutövaren får inte – utan att först samråda – driftsätta eller väsentligen ändra informationssystem som kan förutses komma att behandla *konfidentiella* uppgifter och *högre*, eller andra system där åtkomst kan medföra inte obetydlig skada för Sveriges säkerhet. Om denna skyldighet överträds ska alltså sanktionsavgift kunna utdömas av samrådsmyndigheten. En annan fråga är om *tillsynsmyndigheterna* bör ha befogenheten att ta ut sanktionsavgift vid bristande godkännande och vilken skada som annars riskeras för Sveriges säkerhet. Mot bakgrund av de förslag som regeringen respektive utredningen lämnar om anmälningsplikt, lämplighetsprövning, nya kraftfulla verktyg för samråds- och tillsynsmyndigheterna (bl.a. åtgärdsföreläggande och förbud) och sanktionssystemet i övrigt finns, enligt utredningens mening, för närvarande inte tillräckliga skäl att även sanktionsbelägga godkännandkravet. Om det med tillkommande erfarenheter visar sig finnas behov av sanktioner även i denna del får den frågan behandlas närmare i kommande lagstiftningsärende.

[64] I vilken mån oriktiga uppgifter lämnats uppsåtligen eller i vilken utsträckning det varit oaktsamt ska beaktas vid bedömningen av om sanktionsavgift ska tas ut (se den av regeringen i proposition 2020/21:194 föreslagna 6 kap. 3 § i säkerhetsskyddslagen).

13.8.1 Certifiering som komplement

Säkerhetspolisen och Försvarsmakten får anses ha möjlighet att inom befintligt mandat föreskriva bl.a. om krav på användning av certifierad IKT, när så bedöms lämpligt, som en säkerhetsskyddsåtgärd som ger möjlighet att öka säkerheten i informationssystemet. Dessutom kommer den föreslagna befogenheten att besluta åtgärdsföreläggande att inrymma sådana krav på certifiering som en säkerhetsskyddsåtgärd. Även om det från experthåll lämnats synpunkter på att det är oklart i vilken utsträckning en sådan åtgärd har ändamålsenliga effekter för säkerheten i systemet bedömer utredningen att en användning av certifierade IKT-produkter kan stärka säkerheten i nätverks- och informationssystemen (se utförligare redogörelse i kapitel 12).

Krav på ökad användning av IKT-produkter certifierade inom det europeiska ramverket för cybersäkerhetscertifiering, med tillägg av de nationella krav som kan komma att ställas, är ett sätt att höja säkerheten i informations- och nätverkssystem. Utredningen kan samtidigt notera att användning av certifierad IKT, oavsett tillägg av nationella krav, inte ger någon garanti för fullständig säkerhet i systemen. Utredningen bedömer att möjligheten till ökad användning av certifierad IKT i förening med samrådsmyndigheternas möjlighet att närmare reglera denna fråga (genom föreskrifter och förelägganden vid samråd om att vidta säkerhetsskyddsåtgärder) torde medföra ökad säkerhet i informationssystemen. Härtill kommer rätten att förbjuda planerade förfaranden som inte uppfyller tillräckliga säkerhetskrav.

Sammanfattande slutsatser

Mot bakgrund av det ovan anförda, och med beaktande av de ändringar i säkerhetsskyddslagen som regeringen föreslagit, anser utredningen att nu nämnda åtgärder bör utvärderas innan kompletterande krav på myndighetsgodkännande, eller införande av en nationellt särskilt anpassad ordning för certifiering av IKT i säkerhetskänslig verksamhet, övervägs.

13.8.2 Bestämmelserna ska tas in i säkerhetsskyddslagen

Bestämmelserna om samråd, förelägganden och förbud kommer med den utvidgning som utredningen föreslår delvis att avse förhållanden mellan enskilda och det allmänna. De innehåller också skyldigheter för enskilda. De bör därför tas in i säkerhetsskyddslagen.[65] I lagen bör anges att myndigheten som verksamhetsutövaren ska samråda med är den myndighet som regeringen bestämmer. I förordning om ändring i säkerhetsskyddsförordningen bör föreskrivas att Säkerhetspolisen och Försvarsmakten är samrådsmyndigheter enligt säkerhetsskyddslagen inom sitt respektive ansvarsområde.

[65] Säkerhetsskyddsförordningens bestämmelser om förberedande åtgärder inför driftsättning av informationssystem (3 kap. 1–3 §§) ska överföras till säkerhetsskyddslagen.

14 Tillgång till informationssystem vid tillsyn

Förslag: I säkerhetsskyddslagen införs en ny bestämmelse med innebörden att tillsynsmyndigheten ska, i den omfattning som det behövs för tillsynen, ha rätt att få tillgång till informationssystem som används i verksamhet som omfattas av tillsyn. Tillsynsmyndigheten ska även få besluta att förelägga den som står under tillsyn att ge tillgång till sådana informationssystem samt ha möjlighet att förena föreläggandet med vite.

Bedömning: Tillsynsmyndigheten kommer kunna begära handräckning av Kronofogdemyndigheten för att genomföra den ovan nämnda tillsynsåtgärden.

14.1 Inledning

Den som står under tillsyn enligt säkerhetsskyddslagen (2018:585) ska enligt regeringens lagförslag i propositionen *Ett starkare skydd för Sveriges säkerhet* (prop. 2020/21:194) ge tillsynsmyndigheten den information som behövs för tillsynen och, i nödvändig omfattning, tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamhet som omfattas av tillsyn. Tillsynsmyndigheten ska vidare enligt förslaget få förelägga den som står under tillsyn att tillhandahålla informationen och ge tillträde till utrymmena vid äventyr av vite (6 kap. 3 och 4 §§). Tillsynsmyndigheten ska även få begära handräckning av Kronofogdemyndigheten för att genomföra tillsynsåtgärderna (6 kap. 5 §).

Utredningen noterar att ovan nämnda undersökningsbefogenheter inte inbegriper någon uttrycklig rätt för tillsynsmyndigheten

att få tillgång till verksamhetsutövarens informationssystem. Behovet av en sådan befogenhet behandlas nedan.

14.2 Det finns skäl att införa ytterligare en undersökningsbefogenhet

Ett skäl för regeringens förslag (prop. 2020/21:194) att införa undersökningsbefogenheter är att en tillträdesrätt bedöms vara nödvändig för att tillsynsmyndigheterna ska kunna bedriva ett effektivt arbete med att kontrollera att säkerhetsskyddslagen följs och att därigenom motverka skador på Sveriges säkerhet. Varken befintlig eller föreslagen säkerhetsskyddsreglering innehåller emellertid befogenheter för utövande av tillsyn över verksamhetsutövarens informationssystem av betydelse för säkerhetskänslig verksamhet. Befogenhet att få tillgång till information och uppgifter om ett informationssystem är inte samma sak som att få tillträde eller tillgång till själva informationssystemet (se nedan).

Utredningen anser att ett effektivt system för tillsyn inte kan bygga på antagandet att det finns samförstånd mellan tillsynsmyndigheten och tillsynsobjektet. Detta gäller inte minst med hänsyn till de skyddsvärden det är fråga om samt eftersom antalet verksamheter av betydelse för Sveriges säkerhet har ökat i takt med privatiseringen av offentlig verksamhet och får antas fortsätta öka framöver (se prop. 2017/18:89 s. 125).

Samhällets utveckling och den ökande digitaliseringen av säkerhetskänslig verksamhet innebär att tillsynsmyndigheten vid tillsyn som regel behöver kontrollera vilka säkerhetsskyddåtgärder som vidtagits i informationssystem. För att genomföra en sådan kontroll är det, till skillnad från t.ex. kontroll av fysiska säkerhetsskyddsåtgärder, i de flesta fall inte tillräckligt att passivt besiktiga informationssystemet genom designgranskning, granskning av olika dokument och underlag samt intervjuer. Det är först efter genomförandet av aktiva tekniska kontroller, t.ex. simulerade angreppsförsök, som det går att bedöma om de säkerhetsskyddsåtgärder som vidtagits i systemet är tillräckliga, eller det kan påvisas att ett informationssystem inte är exponerat mot oskyddade nätverk. Kontroll av informationssäkerheten i ett informationssystem kan därmed endast ske genom att aktivt kontrollera och testa säkerhetsskyddsåtgärderna i systemet

tillsammans med dess omkringliggande infrastruktur, s.k. teknisk säkerhetsgranskning.[1]

För att tillsynsmyndigheten ska kunna bedriva en effektiv tillsyn även avseende informationssystem bör den därför ha rätt att, i den omfattning som det behövs för tillsynen, få tillgång till de informationssystem som är av betydelse för säkerhetskänslig verksamhet och som används i verksamhet som omfattas av tillsyn.[2] Mot detta intresse måste man ställa den enskildes rättigheter. Var och en har bl.a. rätt till skydd mot husrannsakan och liknande intrång samt mot intrång i den personliga integriteten och för sin korrespondens.[3] Husrannsakan kan också göras i it-miljö. Även en undersökning i ett informationssystem på distans, som inte inbegriper fysisk tillgång till systemet, motsvarar, i fråga om integritetsintrång, i princip en husrannsakan (jfr SOU 2017:100, s. 314–316). Det kan tilläggas att undersökningsmetoden inte syftar till beslagtagande av den elektroniskt lagrade informationen. Inskränkningar i den enskildes skydd kan godtas, under förutsättning att de är lagliga och nödvändiga i ett demokratiskt samhälle för att tillgodose något av de intressen som artikel 8 i Europakonventionen anger, däribland den nationella säkerheten. Den nu föreslagna rätten till tillgång avser en avgränsad krets, nämligen aktörer som använder informationssystem i säkerhetskänslig verksamhet. Förslaget bedöms vara nödvändigt för att tillsynsmyndigheterna ska kunna bedriva ett effektivt arbete med att kontrollera att säkerhetsskyddslagen följs och att därigenom motverka skador på Sveriges säkerhet. Den föreslagna tillgångsrätten bedöms således utgöra en godtagbar inskränkning av enskildas fri- och rättigheter. Det ankommer dock alltid på de rättstillämpande myndigheterna att göra en bedömning av om den vidtagna undersökningsåtgärden är proportionerlig i det enskilda fallet (jfr 5 § tredje stycket förvaltningslagen [2017:900]).

[1] I t.ex. Finland har Transport- och kommunikationsverket rätt att av myndigheter få tillgång till uppgifterna om de informationssystem och den datakommunikation som verket ska bedöma eller som är föremål för utredning samt, i den utsträckning det behövs för bedömningens utförande, tillträde till informationssystemet och lokaler där uppgifter som ingår i systemet behandlas (6 § lagen [2011/1406] om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation).

[2] Därmed kan undersökningar komma att göras i informationssystem som innehåller säkerhetsskyddsklassificerade uppgifter.

[3] Se 2 kap. 6 § regeringsformen och artikel 8 i Europakonventionen. En genomsökning av datalagrad information på ett kontor kan utgöra en inskränkning av verksamhetsutövarens rätt till respekt för sin korrespondens (se bl.a. *Wieser and Bicos Beteiligungen GmbH mot Österrike*, mål nr 74336/01 och dom den 16 oktober 2007).

På samma sätt som när det gäller tillträde till lokaler och liknande bör tillsynsmyndigheten även få förelägga den som står under tillsyn att ge tillgång till informationssystem vid äventyr av vite, samt få begära handräckning av Kronofogdemyndigheten för att genomföra tillsynsåtgärden.

14.3 Bestämmelserna ska tas in i säkerhetsskyddslagen

Bestämmelserna om tillgång till informationssystem avser, på samma sätt som tillsynsmyndighetens övriga befogenheter, delvis förhållandet mellan enskilda och det allmänna och gäller delvis även skyldigheter för enskilda gentemot det allmänna. De ska därför tas in i säkerhetsskyddslagen, lämpligen genom ett tillägg till de av regeringen föreslagna bestämmelserna om undersökningsbefogenheter i 6 kap. 3 och 4 §§ (se prop. 2020/21:194, s. 12).

Utredningen bedömer att tillsynsmyndigheten redan med stöd av den av regeringen föreslagna bestämmelsen i 6 kap. 5 § säkerhetsskyddslagen kan begära handräckning av Kronofogdemyndigheten för att genomföra den ovan nämnda tillsynsåtgärden, utan att lydelsen behöver ändras. Denna bestämmelse hänvisar nämligen tillbaka till 6 kap. 3 §.

15 Handläggning och överklagande

Förslag: Samrådsmyndighetens beslut om föreläggande under samråd samt om förbud och sanktionsavgift ska få överklagas till Förvaltningsrätten i Stockholm. På samma sätt ska även tillsynsmyndighetens beslut att förelägga tillsynsobjekt att ge tillgång till informationssystem få överklagas. När sådana beslut överklagas ska samråds- eller tillsynsmyndigheten vara motpart i domstolen. Det ska krävas prövningstillstånd vid överklagande till kammarrätten.

Tillsynsmyndighetens beslut att förelägga tillsynsobjektet att ge tillgång till informationssystem ska kunna överklagas.

Bedömning: Det behövs inga kompletterande regler om ärendehandläggningen hos myndigheterna.[1]

15.1 Förvaltningslagen bör gälla vid handläggningen

Förvaltningslagen gäller för handläggning av ärenden hos förvaltningsmyndigheterna och handläggning av förvaltningsärenden hos domstolarna. Lagen innehåller bl.a. bestämmelser om grunderna för god förvaltning och allmänna krav på handläggning av ärenden. Utredningen bedömer att samrådsmyndigheternas handläggning av samrådsärenden och deras möjlighet att besluta om förelägganden och förbud kommer att utgöra sådan handläggning av ärenden som medför att förvaltningslagen är tillämplig. Detsamma gäller i fråga om andra ärenden enligt säkerhetsskyddslagen, såsom tillsynsärenden.

[1] Ovan angivet förslag om rätten till klagomål avseende samrådsmyndighetens beslut kan införas genom tillägg till den av regeringen i proposition 2020/21:194 förslagna bestämmelsen om överklagande, 8 kap. 4 § första stycket i säkerhetsskyddslagen (2018:585).

I 3 § förvaltningslagen finns emellertid ett undantag för handläggning av ärenden i den brottsbekämpande verksamheten hos bl.a. Säkerhetspolisen. Utredningen anser dock att starka skäl talar för att förvaltningslagens bestämmelser bör gälla fullt ut vid Säkerhetspolisens handläggning av ärenden om samråd, förelägganden, förbud och sanktionsavgift. En sådan ordning skulle skapa en stadga och förutsebarhet i förfarandet som är önskvärd, inte minst med hänsyn till att den föreslagna regleringen delvis rör myndighetsutövning mot enskilda. Vidare ligger denna lösning i linje med regeringens förslag om handläggningsregler för tillsynsmyndigheterna på säkerhetsskyddsområdet. Utredningen noterar att regeringen redan förutskickat att det på förordningsnivå införs en bestämmelse om att undantaget i 3 § förvaltningslagen inte gäller för Säkerhetspolisen vid nu aktuella ärendetyper (se prop. 2020/21:194, s. 68).

15.2 Beslut som bör få överklagas

Enskildas rätt enligt artikel 6 i Europakonventionen till en rättvis domstolsprövning innebär att det bör finnas möjlighet att överklaga beslut om sanktionsavgift, förelägganden och förbud för en verksamhetsutövare att genomföra en driftsättning eller förändring av informationssystem. Även myndigheter och andra offentliga aktörer som samrådsmyndighetens beslut gått emot bör ha rätt att överklaga.[2]

Likaledes bör tillsynsmyndighetens beslut att förelägga tillsynsobjekt att ge tillgång till informationssystem få överklagas. Utredningen bedömer att ett sådant överklagande ska vara möjligt enligt den av regeringen föreslagna lydelsen av 8 kap. 4 § säkerhetsskyddslagen. Denna bestämmelse hänvisar nämligen tillbaka till 6 kap. 4 § (se prop. 2020/21:194, s. 15).

[2] Regeringen har föreslagit att tillsynsmyndigheters beslut om föreläggande under samråd eller vid tillsyn samt om förbud och sanktionsavgift ska få överklagas. I samband med det har regeringen bedömt att övriga beslut enligt säkerhetsskyddslagen inte bör få överklagas (prop. 2020/21:194, s. 109 ff.).

15.3 Överklagandeinstans

Eftersom beslut om sanktionsavgift och förelägganden vid samråd är förvaltningsbeslut är det en naturlig utgångspunkt att besluten överklagas till allmän förvaltningsdomstol, även om det kan vara fråga om känsliga uppgifter ur ett säkerhetsperspektiv. Genom att besluten får överklagas till allmän förvaltningsdomstol kan vidare prövningen ansluta till en befintlig processordning.

Målen enligt de föreslagna bestämmelserna är av ett så särpräglat slag att det kan bli svårt att skapa och upprätthålla tillräcklig kompetens hos alla förvaltningsrätter. Detta gäller särskilt eftersom antalet mål kan förväntas bli få. Dessutom bör den typen av känsliga uppgifter som kan förekomma i ärendena hållas inom en så begränsad krets som möjligt. Det finns därför skäl att koncentrera mål enligt de föreslagna bestämmelserna till en domstol. Domstolen kan därmed upparbeta den särskilda kompetens på området som krävs, organisera arbetet med dessa mål på ett lämpligt sätt och vidta de säkerhetsskyddsåtgärder som kan behövas. Anförda argument har föranlett regeringen att föreslå att överklagande av tillsynsmyndighetens beslut om förelägganden och sanktionsavgift ska få ske till Förvaltningsrätten i Stockholm (se prop. 2020/21:194, s. 109 f.).[3] Denna domstol bör av samma skäl även vara första överklagandeinstans för samrådsmyndighetens motsvarande beslut.[4] Även tillsynsmyndighetens beslut att förelägga tillsynsobjekt att ge tillgång till informationssystem bör, i likhet med vad som gäller för övriga undersökningsbefogenheter, följa angiven ordning för klagomål.

När det gäller tillsynsmyndigheters ärenden om förbud kan dessa kräva känsliga utrikespolitiska bedömningar och innehålla känslig information. Regeringen har med detta föreslagit att tillsynsmyndighetens beslut om förbud mot överlåtelser och andra förfaranden ska få överklagas till regeringen (se prop. 2020/21:194, s. 111). En verksamhetsutövares driftsättning eller förändring av ett informationssystem innebär emellertid, till skillnad från en anskaffning eller överlåtelse av säkerhetskänslig verksamhet, inte nödvändigtvis att säkerhetsskyddsklassificerade uppgifter exponeras för utomstående. I dessa fall torde en prövning av ett förbudsbeslut mer sällan aktualisera den sorts ut-

[3] Det kan vidare konstateras att den organisatoriska frågan om säkerhetsskydd avgörs av domstolen.
[4] De angivna fördelarna gäller också Kammarrätten i Stockholm, som i förekommande fall överprövar förvaltningsrättens avgöranden.

rikes-, försvars- och säkerhetspolitiska överväganden som bör hanteras av regeringen. Vidare bör samrådet i de allra flesta fall vara tillräckligt för att verksamhetsutövare självmant ska avstå från förfaranden som samrådstillsynsmyndigheten anser vara olämpliga från säkerhetsskyddssynpunkt. Utredningen anser således att även samrådsmyndighetens beslut om förbud ska få överklagas till förvaltningsdomstol. Med denna ordning undgår man dessutom risken för parallella processen hos domstol respektive regeringen om samma sak.

Om en enskild överklagar en myndighets beslut följer det av 7 a § förvaltningsprocesslagen (1971:291) att myndigheten är den enskildes motpart i domstol. Detsamma bör gälla om beslut överklagas av en myndighet. Det bör därför anges i bestämmelsen om rätt till överklagande att samrådsmyndigheten är motpart i domstolen när ett beslut överklagas. Vidare bör det anges att prövningstillstånd krävs vid överklagande till kammarrätten.

16 Offentlighet och sekretess

Bedömning: Förslagen medför inga behov av ändringar i offentlighets- och sekretesslagen.

Det finns inte skäl att överväga några inskränkningar av reglerna i förvaltningslagen och förvaltningsprocesslagen om partsinsyn och kommunikation.

16.1 Sekretesskyddet hos samrådsmyndigheten

I ärenden om samråd kan det förekomma uppgifter som är mycket känsliga och som omfattas av sekretess hos verksamhetsutövaren. Aktuell sekretessgrund kan antas vara primärt försvarssekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400), OSL. I vissa fall kan även utrikessekretess och underrättelsesekretess enligt 15 kap. 1 § respektive 18 kap. 2 § OSL aktualiseras. Sekretess enligt de nu nämnda paragraferna gäller oavsett hos vilken myndighet uppgifterna finns. Om samrådsmyndigheten genom samrådet får tillgång till uppgifter som är sekretessbelagda enligt dessa bestämmelser, kommer uppgifterna därför att ha samma sekretesskydd hos samrådsmyndigheten som de haft hos verksamhetsutövaren.

Det finns enligt utredningens bedömning inte skäl att utöka det befintliga sekretesskyddet för allmänna intressen genom ändringar i OSL. När det gäller sekretess med hänsyn till enskildas intressen för uppgifter som lämnas till samrådsmyndigheterna inom ramen för samråd kan det finnas behov av ett kompletterande skydd, som företrädesvis bör åstadkommas genom ändringar i offentlighets- och sekretessförordningen (2009:641).[1]

[1] Regeringen har bedömt att ett kompletterande sekretesskydd för uppgifter som enskilda lämnar till tillsynsmyndigheterna inom ramen för samråd och tillsyn skulle kunna åstadkommas genom ändringar i offentlighets- och sekretessförordningen (prop. 2020/21:194, s. 113). Utredningen har erfarit att frågan övervägs inom Regeringskansliet (Justitiedepartementet).

16.2 Utlämnande av uppgifter i samband med samråd

En annan fråga är i vilken mån en verksamhetsutövare som omfattas av OSL över huvud taget kan överlämna uppgifter som omfattas av sekretess till samrådsmyndigheten i ett ärende om samråd. Sekretess gäller nämligen även mellan myndigheter, vilket innebär att uppgifter som omfattas av sekretess hos en verksamhetsutövare inte kan överlämnas till samrådsmyndigheten med mindre än att det tillåts med stöd av en sekretessbrytande bestämmelse. I samrådsärenden torde uppgifter som begärs från samrådsmyndigheten och som omfattas av sekretess hos verksamhetsutövaren kunna lämnas över med stöd av 10 kap. 2 § OSL, som föreskriver att sekretess inte hindrar att en uppgift lämnas till en enskild eller till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet.[2] Eftersom myndigheten i de aktuella fallen har en skyldighet att samråda med samrådsmyndigheten bör ett överlämnande av sekretessbelagda uppgifter inom ramen för samrådet regelmässigt kunna ske med stöd av 10 kap. 2 § OSL. Ett överlämnande bör i många fall också kunna ske enligt 10 kap. 27 § OSL, s.k. generalklausulen, som medger utlämnande om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som uppgiften ska skydda. Det finns därmed stöd för de verksamhetsutövare som omfattas av OSL att lämna över de sekretessbelagda uppgifter som krävs för samrådet till samrådsmyndigheten.

När det gäller frågan i vilken utsträckning tillsynsmyndigheten kan lämna sekretessbelagda uppgifter till samrådsmyndigheten,[3] t.ex. rörande en enskild verksamhetsutövare, bedömer utredningen, med utgångspunkt i de förslag som lämnats rörande samrådsmyndigheternas roll (se kapitel 13), att ett sådant överlämnande bör kunna ske med stöd av 10 kap. 27 § OSL.[4]

[2] I de fall samrådsmyndigheten även utövar tillsyn kan tillsynsobjektet lämna över begärda uppgifter med stöd av 10 kap. 17 § OSL, som bl.a. föreskriver att sekretess inte hindrar att en uppgift lämnas till en myndighet om uppgiften behövs där för tillsyn över den myndighet där uppgiften förekommer.

[3] Regeringen har anfört att man vid behov får återkomma till frågan i vilken utsträckning tillsynsmyndigheterna kan lämna sekretessbelagda uppgifter till samordningsmyndigheterna (prop. 2020/21:194, s. 113 f.).

[4] Om information rutinmässigt kommer att utbytas kan det finnas ett behov av att införa en uppgiftsskyldighet för uppgiftslämnande myndighet som möjliggör ett utlämnande enligt 10 kap. 28 § OSL.

16.3 Sekretess vid tillsyn

Också i tillsynsärenden kan det förekomma uppgifter som är mycket känsliga och som omfattas av sekretess hos tillsynsobjekten. Utöver de i föregående avsnitt angivna sekretessgrunderna, och i förekommande fall sekretess i det internationella samarbetet enligt 15 kap. 1 a § OSL, kan vid tillsyn eventuell sekretess enligt andra bestämmelser överföras från tillsynsobjektet till tillsynsmyndigheten enligt 11 kap. 1 § OSL. Vidare kan i tillsynsärenden uppgifter som begärs från tillsynsmyndigheten och som omfattas av sekretess hos tillsynsobjektet lämnas över för tillsynen med stöd av 10 kap. 17 § OSL.[5] Utredningen anser således inte att den undersökningsbefogenhet som föreslås, vilken kan möjliggöra tillgång till känsliga uppgifter, ger anledning till ändringar i OSL (jfr regeringens överväganden i prop. 2020/21:194, s. 112 ff.).

16.4 Partsinsyn och kommunikation

Vid samrådsmyndighetens handläggning enligt den föreslagna regleringen om samråd gäller förvaltningslagen (2017:900). När ett beslut om föreläggande i ett samrådsärende överklagas till förvaltningsdomstol gäller förvaltningsprocesslagen (1971:291). De nu nämnda lagarna innehåller vissa bestämmelser om partsinsyn och kommunikation. I 10 § förvaltningslagen föreskrivs att den som är part i ett ärende har rätt att ta del av allt material som har tillförts ärendet. Av 25 § samma lag följer att en myndighet innan den fattar beslut i ett ärende, om det inte är uppenbart obehövligt, ska underrätta den som är part om allt material av betydelse för beslutet och ge parten tillfälle att inom en bestämd tid yttra sig över materialet. Av 18 § förvaltningsprocesslagen framgår att en part, innan ett mål avgörs, som huvudregel ska ha fått kännedom om det som tillförts målet genom annan än honom eller henne själv och fått tillfälle att yttra sig över det. Även enligt 10 § första stycket och 12 § förvaltningsprocesslagen gäller en viss underrättelseskyldighet gentemot part.

De nu nämnda bestämmelserna gäller, enligt 10 § och 25 § tredje stycket förvaltningslagen respektive 19 § förvaltningsprocesslagen, med de begränsningar som följer av 10 kap. 3 § OSL. Av 10 kap. 3 §

[5] Bestämmelsens tillämplighet förutsätter att tillsynsobjektet är en myndighet där uppgiften förekommer.

första stycket OSL framgår att sekretess inte hindrar att en enskild, som är part i ett mål eller ärende hos domstol eller annan myndighet och som på grund av sin partsställning har rätt till insyn i handläggningen, tar del av en handling eller annat material i målet eller ärendet. En sådan handling eller ett sådant material får dock inte lämnas ut till parten i den utsträckning det av hänsyn till allmänt eller enskilt intresse är av synnerlig vikt att sekretessbelagd uppgift i materialet inte röjs. I sådana fall ska parten på annat sätt få upplysning om vad materialet innehåller i den utsträckning det behövs för att parten ska kunna ta till vara sin rätt och det kan ske utan allvarlig skada för det intresse som sekretessen ska skydda. Upplysningsskyldigheten kan fullgöras både skriftligen och muntligen, t.ex. genom en muntlig redogörelse för innehållet i vissa handlingar (prop. 1971:30 s. 431 och 443).

Som framgår ovan kan det i ett samrådsärende förekomma sekretessbelagda uppgifter av mycket känslig natur. Ett röjande av sådana uppgifter, även till någon som är part i ärendet, skulle i vissa fall kunna skada Sveriges säkerhet. Sveriges säkerhet är ett synnerligen starkt allmänt intresse. När det finns anledning att ingripa med stöd av de föreslagna bestämmelserna torde därför en tillämpning av 10 kap. 3 § OSL regelmässigt resultera i bedömningen att det är av synnerlig vikt att inte röja uppgifter av sådan karaktär att det skulle innebära skada för Sveriges säkerhet att lämna ut dem. En annan bedömning kan göras när det gäller mindre känsliga uppgifter av mer teknisk karaktär, som t.ex. vilken typ av säkerhetsskyddsåtgärd som är nödvändig för att uppnå ett väl anpassat säkerhetsskydd i det planerade förfarandet. Utredningen anser mot denna bakgrund att bestämmelserna i förvaltningslagen och förvaltningsprocesslagen tillsammans med kravet på synnerlig vikt i 10 kap. 3 § OSL på ett rimligt sätt balanserar intresset av partsinsyn och kommunikation mot intresset av att skydda känsliga uppgifter i de aktuella ärendena. Mot denna bakgrund bedöms det inte behövas några inskränkningar av reglerna om partsinsyn och kommunikation.

17 Konsekvensbeskrivning

Bedömning: Skyddet för Sveriges säkerhet stärks genom förslagen.

Utredningens förslag att Försvarets materielverk (FMV) ges i uppdrag att – i samråd och samverkan med andra myndigheter och aktörer – ta fram formerna för arbetet med en nationell gemensam hot-, sårbarhets- och riskbedömning medför vissa kostnader. Med anledning av dessa kostnader bör FMV:s anslag ökas. Eventuella kostnader för övriga myndigheter bedöms rymmas inom respektive myndighets befintliga anslagsram.

För de verksamhetsutövare som kommer att träffas av övriga förslag kan de innebära ökade kostnader och administrativa bördor. Eventuella kostnader för statliga myndigheter bedöms rymmas inom respektive myndighets befintliga anslagsram.

Förslagen innebär även vissa ökade förvaltningskostnader för de myndigheter som kommer att vara samrådsmyndigheter (Säkerhetspolisen och Försvarsmakten). Dessa begränsade kostnader bedöms emellertid rymmas inom befintlig anslagsram och förväntat utökat anslag (se prop. 2020/21:30).

Förslagen medför dessutom att Kronofogdemyndigheten och de allmänna förvaltningsdomstolarna får något fler arbetsuppgifter. De kostnadsökningarna bedöms inte bli större än att de ryms inom befintliga anslag.

Utredningens bedömningar i övrigt, bl.a. att certifierade IKT-produkter, -tjänster och -processer i ökad utsträckning bör användas av statliga myndigheter, kan antas medföra kostnader men också besparingar om sådana åtgärder genomförs, samtidigt som dessa är svåra att beräkna.

17.1 Inledning

I utredningens uppdrag ingår att analysera konsekvenserna av lämnade förslag i enlighet med 14–15 a §§ kommittéförordningen (1998:1474). Eftersom utredningen lämnar författningsförslag ska konsekvensanalysen också göras i enlighet med 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning.

I utredningsdirektiven anges att utredningen ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för enskilda. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna ska utredningen föreslå hur dessa ska finansieras. Utredningen ska särskilt ange konsekvenserna för företag i form av kostnader och ökade administrativa bördor samt personella konsekvenser för berörda myndigheter.

I detta kapitel redovisas utredningens bedömning av konsekvenserna av de förslag utredningen lämnar. Förslagen syftar framför allt till att ytterligare skärpa säkerhetsskyddslagstiftningen.

17.2 Utgångspunkter

Säkerhetsskydd handlar om skyddet för Sveriges mest skyddsvärda verksamheter. Konsekvenserna av att skyddet fallerar kan därför bli mycket allvarliga. Den föreslagna regleringen syftar bl.a. till att göra vissa säkerhetsskyddsfrågor mer centrala hos verksamhetsutövare, att förhindra driftsättningar och väsentliga förändringar av informationssystem som är olämpliga ur säkerhetsskyddssynpunkt samt att öka efterlevnaden av säkerhetsskyddslagstiftningen. Förslagen innebär på detta sätt en förstärkning av skyddet för Sveriges säkerhet.

17.3 De som berörs av förslagen

Förslagen ska bidra till att stärka skyddet för Sveriges säkerhet. Utredningens förslag berör, förutom uppdraget till Försvarets materielverk (FMV), framför allt de statliga myndigheter som utredningen föreslår ska vara samrådsmyndigheter med tillkommande befogenheter enligt säkerhetsskyddslagen (Säkerhetspolisen och Försvarsmakten) och verksamhetsutövare som har informationssystem av betydelse för säkerhetskänslig verksamhet. Förslagen kan även beröra

tillsynsmyndigheter på säkerhetsskyddsområdet som samverkar med samrådsmyndigheterna samt Kronofogdemyndigheten och domstolar.

17.4 Frågan om krav på certifiering

Utredningen föreslår att regeringen ska ge Försvarets materielverk (FMV) i uppdrag att – i samråd och samverkan med andra myndigheter och berörda aktörer – ta fram formerna för arbetet med en nationell gemensam hot-, sårbarhets- och riskbedömning. Uppdraget medför vissa kostnader för såväl FMV som andra myndigheter och aktörer som deltar i arbetet. Med anledning av dessa kostnader bör FMV:s anslag ökas. Eventuella kostnader för övriga myndigheter kan antas vara begränsade och bedöms rymmas inom myndigheternas befintliga anslag. Utredningen lämnar i övrigt inga förslag i denna del. Vidare konsekvenser som kan följa av uppdraget går inte att bedöma i dag utan får analyseras i anslutning till det fortsatta arbetet.

Utredningens bedömningar i övrigt, bl.a. att certifierade IKT-produkter, -tjänster och processer i ökad utsträckning bör användas av myndigheter, kan initialt antas medföra ökade kostnader i samband med att sådana åtgärder genomförs, samtidigt som dessa är svåra att beräkna. Däremot kan en ökad användning av certifierad IKT minska behovet av egen testning och kvalitetssäkring, vilket kan medföra framtida kostnadsbesparingar. Kostnaderna och besparingarna går emellertid inte att beräkna och ligger dessutom utanför utredningens uppdrag att beskriva då åtgärderna inte direkt följer av förslag som utredningen lämnar.

När det gäller de konsekvenser som följer av det europeiska ramverket för cybersäkerhetscertifiering är dessa fortfarande svårbedömda då europeiska ordningar för sådan certifiering inte börjat tillämpas[1] och den närmare omfattningen av framtida frivillig eller obligatorisk cybersäkerhetscertifiering enligt det europeiska ramverket inte är känd.

[1] Dock har Enisa den 26 maj 2021 formellt överlämnat den första slutliga versionen av en europeisk certifieringsordning (EUCC) till EU-kommissionen.

Internationell handel med tredje land och ömsesidigt erkännande av certifikat

I utredningsdirektiven anges att utredningen även ska beakta de konsekvenser som bl.a. införandet av det europeiska ramverket för cybersäkerhetscertifiering kan få när det gäller internationell handel med tredjeland samt hur det påverkar erkännande och utfärdande av certifikat och andra åtaganden som följer av Sveriges medlemskap i bl.a. CCRA.

Utredningen har i sitt delbetänkande (avsnitt 13.5) påbörjat att analysera sådana effekter av EU:s cybersäkerhetsakt. De slutsatser som presenterats Kommerskollegiums rapport *The Cyber Effect – the implications of IT security regulation on international trade* (2018) gör sig fortfarande gällande. Eftersom EU-kommissionen ännu inte formellt antagit någon europeisk ordning för cybersäkerhetscertifiering, och utredningen inte heller föreslagit en särskild nationell certifieringsordning utformad för säkerhetskänslig verksamhet, saknas skäl för ytterligare konsekvensanalys i dessa avseenden.

17.5 Förslaget om en stärkt samrådsroll

Konsekvenser för verksamhetsutövare

Förslagen innebär till viss del att verksamhetsutövare, dvs. myndigheter, andra offentliga aktörer och företag, påförs ytterligare krav som kan komma att medföra bl.a. ekonomiska konsekvenser.

Verksamhetsutövare ska redan i dag ha god kännedom om sina skyddsvärden och göra en särskild säkerhetsskyddsbedömning vid driftsättning av informationssystem i säkerhetskänslig verksamhet. Vad gäller förslaget om att verksamhetsutövare, utöver en säkerhetsskyddsbedömning, även ska göra en lämplighetsprövning inför driftsättning eller väsentlig förändring av informationssystemet bör de bedömningarna utgå från den säkerhetsskyddsanalys som alla verksamhetsutövare redan i dag har en skyldighet att göra enligt 2 kap. 1 § säkerhetsskyddslagen (2018:585)[2]. Kravet på att göra en särskild säkerhetsskyddsbedömning och lämplighetsprövning innebär att riskerna för de skyddsvärden som har identifierats i säkerhetsskyddsana-

[2] Regeringens lagförslag i proposition 2021/21:194 innebär inte någon ändring av kravet på säkerhetsskyddsanalys i 2 kap. 1 § säkerhetsskyddslagen.

lysen konkretiseras i förhållande till en viss situation. Detta medför därför inte något betydande merarbete eller annan kostnad. Utredningen har emellertid föreslagit att den särskilda säkerhetsskyddsbedömningen även ska göras innan en *väsentlig förändring* av informationssystem som har betydelse för säkerhetskänslig verksamhet. Att verksamhetsutövaren också i denna situation ska *se till* att säkerhetsskyddet utformas så att motiverade säkerhetskrav i systemet tillgodoses, kan innebära visst merarbete.[3] Om den föreslagna lämplighetsprövningen mynnar ut i bedömningen att förfarandet inte är olämpligt från säkerhetsskyddssynpunkt, ska verksamhetsutövaren även samråda med Säkerhetspolisen eller Försvarsmakten (samrådsmyndigheten) om övriga rekvisit enligt nuvarande 3 kap. 2 § säkerhetsskyddsförordningen (2018:658)[4] är uppfyllda. Samrådet bör bygga på det underlag som verksamhetsutövaren redan tagit fram inom ramen för den särskilda säkerhetsskyddsbedömningen. Utredningen anser därför att den faktiska arbetsinsatsen för att inleda och genomföra samrådet är begränsad. Däremot kan samrådsprocessen göra att det tar längre tid att inleda ett förfarande än vad som annars hade varit fallet, vilket kan påverka verksamheten negativt. Hur lång tid samrådet kommer att ta och vad det kommer att mynna ut i har dock verksamhetsutövaren ofta en möjlighet att själv påverka.

Det som kan ha störst ekonomisk påverkan är förslagen om att samrådsmyndigheten under vissa omständigheter ska få besluta om förbud mot att genomföra en planerad driftsättning eller förändring av informationssystem för att förhindra skada för Sveriges säkerhet. För den verksamhetsutövare som meddelas förbud kan det innebära t.ex. att verksamhetsutövaren måste köpa en tjänst av en annan motpart som kräver högre ersättning. Möjligheten att besluta om förbud är dock ett sistahandsalternativ när övriga möjligheter är uttömda eller bedöms som utsiktslösa.

Vidare innebär förslaget om att tillsynsmyndigheten ska få ytterligare en undersökningsbefogenhet att verksamhetsutövare kan behöva ge tillsynsmyndigheten tillgång till sina informationssystem. Kostnaderna för att bistå tillsynsmyndigheten bör dock som regel vara begränsade.

[3] Befintligt krav på särskild säkerhetsskyddsbedömning innebär att verksamhetsutövaren endast inför *driftsättning* av ett sådant system ska ta ställning till vilka säkerhetskrav i systemet som är motiverade och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses.
[4] Utredningen föreslår att denna bestämmelse överförs till säkerhetsskyddslagen.

Utredningens förslag innebär också möjlighet för samrådsmyndigheterna att besluta om sanktionsavgifter för vissa överträdelser av regelsystemet.[5] För verksamhetsutövare som följer gällande krav leder förslaget inte till några ökade kostnader. För de aktörer som inte följer gällande regler innebär förslaget ekonomiska konsekvenser och kan medföra ökade kostnader eftersom sanktionsavgifter ska kunna tas ut utan krav på uppsåt eller oaktsamhet. Det föreslås ingen begränsning av storleken på sanktionsavgifterna i förhållande till den ekonomiska aktörens årsomsättning vilket kan leda till att mindre aktörer riskerar relativt sett högre avgifter. Eftersom en sanktionsavgift kan uppgå till höga belopp beroende på bl.a. överträdelsens allvar kan förslaget i denna del även förväntas leda till en bättre regelefterlevnad.

Genom möjligheten att överklaga myndigheternas beslut om föreläggande, förbud och sanktionsavgift till domstol bedömer utredningen att ett fullgott skydd för enskildas rättigheter säkerställs.

Mot bakgrund av det ovan anförda bedömer utredningen att förslagen i de flesta fall endast kommer medföra begränsade administrativa och andra kostnader för offentliga och enskilda verksamhetsutövare. Kostnadsökningen för statliga myndigheter som är verksamhetsutövare bör enligt utredningen rymmas inom respektive myndighets befintliga anslagsram.

Konsekvenser för samråds- och tillsynsmyndigheterna

I syfte att höja ambitionsnivån för samrådsprocessen kommer Säkerhetspolisens och Försvarsmaktens roll inom säkerhetsskyddet delvis att förändras. Utredningens förslag innebär bl.a. en viss utvidgning av Säkerhetspolisens och Försvarsmaktens ansvar för samråd och rätt att inleda sådana. Vidare föreslår utredningen att Säkerhetspolisen och Försvarsmakten som samrådsmyndigheter ska få vissa nya befogenheter, t.ex. möjlighet att besluta om förbud mot driftsättning eller väsentlig förändring av informationssystem i säkerhetskänslig verksamhet samt besluta om åtgärdsföreläggande och sanktionsavgift mot den som inte efterlever säkerhetsskyddslagstiftningens krav. Även om utredningen föreslår att stärkt samrådsroll tillkommer be-

[5] Förslaget om sanktionsavgift tydliggör för ekonomiska aktörer vilka sanktioner som kan bli aktuella vid överträdelser och under vilka förutsättningar avgift kan beslutas.

fogenheterna befintliga myndigheter på säkerhetsskyddsområdet som redan har många liknande uppgifter.

För att samrådsmyndigheterna ska kunna fullgöra sina nya skyldigheter enligt säkerhetsskyddslagen ska berörda verksamhetsutövare i större utsträckning samråda med och lämna uppgifter till myndigheterna. Detta innebär ett ökat administrativt arbete och därtill hörande kostnader för myndigheterna. Eftersom verksamhetsutövarens skyldighet att samråda enligt utredningens förslag även är beroende av att en lämplighetsprövning leder till bedömningen att det planerade förfarandet inte är olämpligt, bör en ökning av antalet samråd inte bli annat än begränsad.[6]

Den föreslagna sanktionsbestämmelsen är en komplettering till det av regeringen förslagna sanktionssystemet i säkerhetsskyddslagen och innebär en motsvarande befogenhet för samrådsmyndigheten att besluta att en avgift ska kunna tas ut oavsett om överträdelsen skett uppsåtligen eller av oaktsamhet.[7] Att sanktionsavgiftssystemet bygger på strikt ansvar underlättar för myndigheternas bedömning i fråga om att ta ut sanktionsavgift. Det ska emellertid inte vara obligatoriskt att ta ut sanktionsavgift för överträdelser som kan leda till sanktionsavgift. Genom att myndigheterna själva får besluta om sanktionsavgift kan sanktionsförfarandet antas bli effektivare och enklare. Förslaget bedöms ha positiva effekter för myndigheternas möjligheter till övervakning av skyldigheter utan att påverka kostnaderna i någon större utsträckning. Kostnader kan antas tillkomma för delgivning av beslut om sanktionsavgift.

Sammantaget kan utredningens förslag om kompletterande befogenheter för Säkerhetspolisen och Försvarsmakten förväntas leda till en effektivare samrådsprocess. Möjligheten att ingripa ligger i tillämpliga delar i linje med regeringens lagförslag i proposition 2020/21:194 beträffande tillsynsmyndigheternas befogenheter på säkerhetsskyddsområdet, med undantaget att vitesföreläggande vid pågående förfarande inte får beslutas av samrådsmyndigheten.

Säkerhetspolisen och Försvarsmakten måste ha tillräckliga resurser för att på ett effektivt sätt kunna utöva sin förstärkta samrådsroll

[6] Dessa kostnader är främst beroende av i vilken omfattning som samråd kommer att ske och är i dag svåra att uppskatta. Eventuella kostnader bedöms emellertid inledningsvis vara begränsade.
[7] För att samrådsmyndigheterna – i likhet med vad som enligt regeringen bör gälla för tillsynsmyndigheter vid verksamhetsutövares anskaffning, utkontraktering och överlåtelse av säkerhetskänslig verksamhet – ska kunna beivra regelöverträdelser innehåller den föreslagna regleringen bestämmelser om möjlighet att påföra en verksamhetsutövare en sanktionsavgift.

på säkerhetsskyddsområdet. Detta innebär att samrådsverksamheten ska ha de personella, tekniska och ekonomiska resurser som behövs för att på ett effektivt sätt kunna utföra sin uppgift. Med hänsyn till Säkerhetspolisens och Försvarsmaktens omfattande kompetens och utpräglade roller inom informationssäkerhet på säkerhetsskyddsområdet bör behovet av att, som en följd av att myndigheterna tilldelas nya befogenheter och sanktionsmöjligheter, initialt utbilda personal och ändra vissa arbetsformer, vara förhållandevis litet. Förslaget torde inte heller innebära att verksamheterna hos myndigheterna behöver omorganiseras nämnvärt, utan merparten av de nya uppgifterna bör kunna tilldelas den existerande organisationen. I den mån den utvidgade samrådsverksamheten hos Säkerhetspolisen och Försvarsmakten förutsätter planering av organisation och arbetssätt samt upprättande av anvisningar respektive föreskrifter för samrådsförfarandet och verksamhetsutövarens lämplighetsprövning bedöms vissa uppgifter kunna lösas genom en omorganisering av resurserna samtidigt som vissa resurstillskott kan behövas. Uppgifterna bedöms för övrigt inte ha annat än marginella konsekvenser för arbetsfördelningen med andra myndigheter.

Utredningen bedömer vidare att den ökade samverkan mellan samråds- och tillsynsmyndigheter som kan förekomma i samband med driftsättning och förändring av informationssystem inte får annat än marginella ekonomiska effekter för myndigheterna.

Sammanfattningsvis kommer alltså kostnaderna för samrådsmyndigheterna att öka, men de bedöms vara begränsade. Behovet av resurser som de nya uppgifterna kan föranleda inledningsvis avser främst viss personalförstärkning.

Utredningen föreslår dessutom att tillsynsmyndigheterna ska få en ny undersökningsbefogenhet: möjligheten att, vid äventyr av vite, få tillgång till verksamhetsutövarens informationssystem. Förslaget i denna del bedöms ha positiva effekter för myndigheternas möjligheter till effektiv tillsyn utan att påverka kostnaderna i någon större utsträckning.

Genom budgetpropositionen för 2021 utökades tillsynsmyndigheters anslag med 100 miljoner kronor från och med 2021 och med ytterligare 10 miljoner kronor från och med 2022. Regeringen har dessutom i propositionen *Totalförsvaret 2021–2025* (prop. 2020/21:30) aviserat en inriktning att anslagen kommer utökas med ytterligare 10 miljoner kronor från och med 2024.

De av utredningen föreslagna kompletteringarna förväntas inte påverka samråds- och tillsynsmyndigheternas verksamheter mer än att konsekvenserna kan hanteras inom nu nämnda anslag.

Konsekvenser för Kronofogdemyndigheten

Den nya bestämmelsen om sanktionsavgift kan komma att öka antalet ärenden hos Kronofogdemyndigheten något. Även förslaget om att tillsynsmyndigheterna ska ha rätt att få tillgång till verksamhetsutövares informationssystem kan leda till att Kronofogdemyndighetens hjälp behövs vid ett antal tillfällen, men ökningen bedöms inte bli särskilt stor och förväntas inte påverka Kronofogdemyndighetens verksamhet mer än att konsekvenserna kan hanteras inom befintliga anslag för myndigheten.

Konsekvenser för domstolarna

Samrådsmyndighetens beslut om föreläggande under samråd, förbud och om att ta ut sanktionsavgift ska enligt utredningens förslag få överklagas till Förvaltningsrätten i Stockholm.[8] För prövning i Kammarrätten i Stockholm kommer det enligt förslaget krävas prövningstillstånd. Utredningen bedömer att ökningen av antalet mål kommer att bli begränsad. Även med beaktande av att målen kan vara komplexa finner utredningen därför att kostnaderna för den ökade måltillströmningen torde vara begränsade. Domstolarnas säkerhetsskydd kan även behöva anpassas med anledning av de säkerhetsskyddsklassificerade uppgifter som kan förekomma i målen. Utredningen anser dock i nuläget att både kostnaderna för den något ökade måltillströmningen och eventuella anpassningar av säkerhetsskyddet bör rymmas inom befintliga anslagsramar.

[8] Det kan tilläggas att tillsynsmyndighetens beslut att förelägga den som står under tillsyn att ge tillgång till informationssystem enligt 6 kap. 3 § säkerhetsskyddslagen inte får överklagas (se 8 kap. 4 § tredje stycket, lydelse enligt proposition 2020/21:194).

Konsekvenser för den kommunala självstyrelsen

Kommuner och regioner kan bedriva verksamhet av betydelse för Sveriges säkerhet. Säkerhetskänslig verksamhet i sådan verksamhet som kommuner och regioner bedriver, t.ex. räddningstjänst, energi- eller dricksvattenförsörjning och sjukvård, kan påverkas av förslagen. Om samrådsmyndigheten beslutar om förbud mot att inleda ett förfarande innebär det att kommunen eller regionen ifråga inte fritt kan förfoga över sin egendom. Förslagen påverkar alltså i viss mån den kommunala självstyrelsen. Den föreslagna regleringen går dock inte utöver vad som är nödvändigt för att skydda de mest skyddsvärda verksamheterna i samhället. Dessutom ska förbud användas restriktivt och som en sista utväg när andra åtgärder inte är tillräckliga. Förslagen berör därför den kommunala självstyrelsen på det minst ingripande sätt som är möjligt.

Kompetensförsörjning

Det finns i dag ett stort behov av kompetensförsörjning inom säkerhetsskyddsområdet. Många tillsynsmyndigheter och andra aktörer har påpekat att det redan i dag är svårt att rekrytera personal med rätt kompetens. Bl.a. finns det brist på personer med kunskap om it-säkerhet, informationssäkerhet och allmän kunskap om säkerhetsskydd. Om kompetensförsörjningen inte hanteras finns det en risk att förslagen inte får det genomslag som behövs för att höja ambitionsnivån inom säkerhetsskyddet. Förslagen i detta betänkande kommer emellertid endast innebära att behovet av kompetensförsörjning ökar i begränsad utsträckning. Betänkandets förslag kan samtidigt medföra att den spetskompetens inom säkerhetsskydd och cybersäkerhet som finns vid expertmyndigheterna, genom det samrådsförfarandet, i större utsträckning kan tas till vara som resurs för samhällets cybersäkerhet. Vidare har regeringen den 20 maj 2021 gett Säkerhetspolisen och Försvarsmakten i uppdrag att utreda hur kompetensförsörjningen kan tryggas (Ju2021/02005)[9]. Lösningar för hantering av eventuella konsekvenser på grund av kompetensbrist kan således i första hand identifieras genom pågående utredningsåtgärder.

[9] Uppdraget ska redovisas till Regeringskansliet (Justitiedepartementet och Försvarsdepartementet) senast den 1 mars 2022.

17.6 Konsekvenser för samhället

Syftet med det föreslagna systemet är att förbättra säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet. Eftersom även skyddet för Sveriges säkerhet därmed stärks kan regleringen anses ha övergripande positiva konsekvenser för hela samhället.

17.7 Brottsförebyggande effekter

Även om någon ny kriminalisering inte används kan förslaget antas ha vissa brottsförebyggande effekter. Regeringen har gjort bedömningen att all Säkerhetspolisens verksamhet, även på säkerhetsskyddsområdet, i någon mening är brottsbekämpande (se prop. 2013/14:110 s. 481 och prop. 2015/16:65 s. 40). De föreslagna befogenheterna kommer således i viss mån att underlätta för den brottsbekämpande verksamheten. Säkerhetsskyddet stärks och den skärpta regleringen av säkerhet i nätverks- och informationssystem bör vidare försvåra fullbordandet av dataintrång, bl.a. då ökade krav ställs för verksamhetsutövares driftsättning respektive förändring av system som har betydelse för säkerhetskänslig verksamhet.

17.8 Övriga konsekvenser

Följande områden berörs inte av förslagen (15 § kommittéförordningen):

- sysselsättning och offentlig service i olika delar av landet,
- jämställdheten mellan kvinnor och män, eller
- möjligheterna att nå de integrationspolitiska målen.

Förslagen bedöms inte heller i övrigt medföra några konsekvenser som behöver redovisas i detta sammanhang.

18 Författningskommentar

18.1 Förslaget till lag om ändring i säkerhetsskyddslagen (2018:585)

3 a kap. Skyldigheter inför driftsättning av informationssystem

1 § *Innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift, eller i väsentliga avseenden förändras, ska verksamhetsutövaren genom en särskild säkerhetsskyddsbedömning ta ställning till vilka säkerhetskrav i informationssystemet som är motiverade och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses.*

Med utgångspunkt i den särskilda säkerhetsskyddsbedömningen och övriga omständigheter ska verksamhetsutövaren pröva om driftsättningen eller förändringen av informationssystemet är lämplig från säkerhetsskyddssynpunkt. Verksamhetsutövaren ska också samråda enligt 2 §.

Den särskilda säkerhetsskyddsbedömningen och lämplighetsprövningen ska dokumenteras.

Om lämplighetsprövningen leder till bedömningen att det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt, får det inte inledas.

Övervägandena finns i avsnitt 13.8.

Paragrafen, som är ny, innehåller bestämmelser om särskild säkerhetsskyddsbedömning, lämplighetsprövning och samråd inför driftsättning och väsentlig förändring av informationssystem i säkerhetskänslig verksamhet. Bestämmelserna motsvarar delvis nuvarande 3 kap. 1 § i säkerhetsskyddsförordningen (2018:658).

Av *första stycket* framgår att en verksamhetsutövare ska göra en särskild säkerhetsskyddsbedömning innan denne inleder ett sådant förfarande som avses i bestämmelsen. Det innebär att verksamhetsutövaren ska dels identifiera de säkerhetskrav som informationssystemet behöver, dels se till att säkerhetsskyddet utformas så att

dessa krav tillgodoses. Bestämmelsen motsvarar nuvarande 3 kap. 1 § säkerhetsskyddsförordningen med det tillägget att den särskilda säkerhetsskyddsbedömningen ska omfatta även väsentliga förändringar av informationssystem som kan ha betydelse för säkerhetskänslig verksamhet. Den särskilda säkerhetsskyddsbedömningen ska utgöra ett underlag för den lämplighetsprövning som ska göras och som regleras i andra stycket.

Enligt *andra stycket* ska verksamhetsutövaren, med utgångspunkt i den särskilda säkerhetsskyddsbedömningen och övriga omständigheter, pröva om det planerade förfarandet är lämpligt från säkerhetsskyddssynpunkt. Verksamhetsutövaren ska därvid bl.a. beakta behovet av säkerhetsskydd och om det är möjligt att uppnå ett tillräckligt säkerhetsskydd. Det kan finnas förfaranden som inte är lämpliga oavsett vilka säkerhetsskyddsåtgärder som vidtas, t.ex. när flera redundanta samhällsviktiga funktioner ersätts av ett informationssystem, eller vid sammanställningar av olika datamängder, s.k. aggregering av uppgifter, som inte ska vara möjliga att sammanställa. Sådana funktioner innebär stora risker för Sveriges säkerhet och kan inte skyddas i tillräcklig utsträckning. En driftsättning eller väsentlig förändring av informationssystem i säkerhetskänslig verksamhet kan även vara olämplig av andra skäl.

Lämplighetsprövningen ska grundas på säkerhetsskyddsanalysen och den särskilda säkerhetsskyddsbedömningen samt sådan information om exempelvis hotbilder och kritiska beroenden mellan verksamheter som verksamhetsutövaren skaffat sig eller fått från samråds- eller tillsynsmyndigheten.

Både den särskilda säkerhetsskyddsbedömningen och lämplighetsprövningen ska avse samtliga moment i det planerade förfarandet. Säkerhetsskyddsklassificerade uppgifter kan röjas under såväl driftsättning som förändring av informationssystemet. Verksamhetsutövaren behöver inkludera aktuellt moment i den särskilda säkerhetsskyddsbedömningen och lämplighetsprövningen.

Av *tredje stycket* framgår att den särskilda säkerhetsskyddsbedömningen och lämplighetsprövningen ska dokumenteras. Bestämmelsen motsvarar delvis nuvarande 3 kap. 1 § säkerhetsskyddsförordningen.

I *fjärde stycket* klargörs att verksamhetsutövaren inte får inleda det planerade förfarandet om lämplighetsprövningen enligt andra

stycket leder till bedömningen att det är olämpligt från säkerhetsskyddssynpunkt.

2 § Om lämplighetsprövningen enligt 1 § leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt, ska verksamhetsutövaren samråda med den myndighet som regeringen bestämmer (samrådsmyndigheten), innan ett informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre tas i drift, eller i väsentliga avseenden förändras.

Samrådsskyldigheten gäller även i fråga om andra informationssystem än sådana som anges i första stycket, om obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är obetydlig.

Samrådsmyndigheten får besluta att förelägga verksamhetsutövaren att vidta åtgärder enligt denna lag och föreskrifter som har meddelats i anslutning till lagen.

Övervägandena finns i avsnitt 13.8.

Paragrafen, som är ny, innehåller bestämmelser om samråd och åtgärdsföreläggande. Bestämmelserna motsvarar delvis nuvarande 3 kap. 2 § säkerhetsskyddsförordningen.

Enligt *första stycket* ska verksamhetsutövaren, om lämplighetsprövningen enligt 1 § leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt, i vissa fall samråda med samrådsmyndigheten. I stycket anges även att regeringen ska utse samrådsmyndigheter enligt lagen. I övrigt motsvarar bestämmelserna i *första* och *andra stycket*, om skyldigheten att samråda, 3 kap. 2 § säkerhetsskyddsförordningen.

Verksamhetsutövaren ska ta initiativ till samråd efter det att den särskilda säkerhetsskyddsbedömningen och lämplighetsprövningen har genomförts men innan det planerade förfarandet inleds. Det kan dock vara av vikt att verksamhetsutövaren inte endast fokuserar på det enskilda moment som kräver samråd utan att denne ser det planerade förfarandet i dess helhet.

En naturlig utgångspunkt är att verksamhetsutövaren inleder samrådet genom att ge in dokumentationen av den särskilda säkerhetsskyddsbedömningen och lämplighetsprövningen till samrådsmyndigheten. Vilket ytterligare underlag som kan vara nödvändigt att ge in kan variera från fall till fall. En beskrivning av den planerade drift-

sättningen eller förändringen av informationssystemet bör ges in, liksom eventuell dokumentation avseende förfarandet. I många fall kan verksamhetsutövaren även behöva ge samrådsmyndigheten tillgång till relevanta delar av sin säkerhetsskyddsanalys.

Samrådet kan bl.a. omfatta frågan om en planerad driftsättning bör ändras, eller en förändring av ett informationssystem bör begränsas, på något sätt för att inte vara olämplig. Samrådsmyndighetens prövning bör också innefatta en bedömning av vad driftsättningen kan innebära på längre sikt, t.ex. vid omvärldsförändringar och ändrade hotbilder. Hur omfattande samrådet behöver vara får avgöras med hänsyn till omständigheterna i det enskilda fallet.

Enligt *tredje stycket* får samrådsmyndigheten inom ramen för samrådet förelägga verksamhetsutövaren att vidta åtgärder för att fullgöra sina skyldigheter enligt lagen och föreskrifter som har meddelats i anslutning till den. Ett föreläggande kan innehålla anvisningar om vilka ytterligare säkerhetsskyddsåtgärder för berört informationssystem som verksamhetsutövaren behöver vidta. Föreläggandet kan också innebära att verksamhetsutövaren vid en senare tidpunkt under samrådet ska återrapportera till samrådsmyndigheten hur olika åtgärder har utförts.

Utgångspunkten är att samrådet ska ha avslutats innan det planerade förfarandet inleds. Det innebär bl.a. att en driftsättning som utgångspunkt får påbörjas först när samrådet har genomförts och under förutsättning att samrådsmyndigheten inte har fattat beslut om förbud enligt 5 §.

Om samrådsmyndigheten bedömer att syftet med samrådet har uppfyllts och att verksamhetsutövaren kan gå vidare med det planerade förfarandet bör myndigheten fatta beslut om att avsluta samrådet utan vidare åtgärd.

I vilka fall samrådsmyndigheten får besluta om förbud mot att inleda det planerade förfarandet regleras i 5 §.

3 § *Om verksamhetsutövaren inte samråder med samrådsmyndigheten trots att det finns en skyldighet att göra det, får samrådsmyndigheten inleda samrådet.*

Övervägandena finns i avsnitt 13.8.

Paragrafen, som är ny, innehåller bestämmelser om när samrådsmyndigheten får inleda ett samråd.

Enligt paragrafen får samrådsmyndigheten inleda ett samråd om verksamhetsutövaren underlåter att göra det trots att samrådsskyldighet föreligger. Utgångspunkten är att verksamhetsutövaren ska ta initiativ till samrådet när det föreligger en samrådsskyldighet enligt 2 §. Det kan dock inträffa att samrådsmyndigheten får kännedom om att någon avser att genomföra ett samrådspliktigt förfarande och att något samråd inte har inletts av verksamhetsutövaren. I en sådan situation kan samrådsmyndigheten med stöd av bestämmelsen själv inleda ett samråd. Det som föreskrivs i 2 § tredje stycket om förelägganden och 5 § om förbud gäller även i fråga om ett sådant samråd.

4 § Ett informationssystem som ska användas i säkerhetskänslig verksamhet får inte tas i drift förrän det har godkänts från säkerhetsskyddssynpunkt av verksamhetsutövaren. Godkännandet ska dokumenteras.

Övervägandena finns i avsnitt 13.8.

Paragrafen, som är ny, innehåller bestämmelser om godkännande av ett informationssystems driftsättning i säkerhetskänslig verksamhet. motsvarar nuvarande 3 kap. 3 § säkerhetsskyddsförordningen.

Bestämmelsen innebär att verksamhetsutövaren måste fatta ett formellt beslut om att informationssystemet får tas i bruk. Beslutet ska dokumenteras. En naturlig utgångspunkt är att verksamhetsutövaren godkänner en driftsättning av informationssystemet först efter att samrådet har avslutats.

5 § Om ett beslut om föreläggande enligt 2 § inte följs eller om det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt även om ytterligare åtgärder vidtas, får samrådsmyndigheten besluta att driftsättningen eller förändringen av informationssystemet inte får genomföras (förbud).

Övervägandena finns i avsnitt 13.8.

Paragrafen, som är ny, innehåller bestämmelser om när samrådsmyndigheten får besluta att en driftsättning eller väsentlig förändring av ett informationssystem inte får genomföras (förbud).

Av paragrafen framgår att samrådsmyndigheten får besluta att det planerade förfarandet inte får genomföras om ett föreläggande inte

följs eller om förfarandet är olämpligt från säkerhetsskyddssynpunkt även om ytterligare åtgärder vidtas.

Så långt det är möjligt bör samrådsmyndigheten sträva efter att eventuella problem ska hanteras genom samrådet och förelägganden. Det kan dock finnas fall där en verksamhetsutövare, trots förelägganden, inte vidtar de åtgärder som behövs för att förfarandet ska vara lämpligt från säkerhetsskyddssynpunkt. Det kan också finnas förfaranden som är olämpliga oavsett vilka säkerhetsskyddsåtgärder som vidtas. Ett exempel kan vara att det i verksamheten förekommer säkerhetsskyddsklassificerade uppgifter som är så känsliga för Sveriges säkerhet att det inte under några förhållanden är lämpligt att de behandlas av verksamhetsutövaren i uppkopplade informationssystem. Samtidigt följer av 5 § förvaltningslagen (2017:900) att beslut om förbud får fattas bara om det är proportionerligt. En proportionalitetsbedömning ska göras i varje enskilt fall. Bedömningen ska bl.a. avse om det önskade resultatet kan uppnås på något annat och mindre ingripande sätt och om det avsedda resultatet står i rimligt förhållande till de olägenheter som kan antas uppstå för den som åtgärden riktas mot. Av kravet på proportionalitet följer att möjligheten att förbjuda verksamhetsutövaren att genomföra ett visst förfarande ska användas restriktivt.

6 kap.

3 § Tillsynsmyndigheten har i den omfattning som det behövs för tillsynen rätt att få *tillgång till informationssystem och* tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamhet som omfattas av tillsyn.

4 § Tillsynsmyndigheten får besluta att förelägga den som står under tillsyn att tillhandahålla information och ge *tillgång eller* tillträde enligt 2 och 3 §§. Ett sådant beslut om föreläggande får förenas med vite.

Övervägandena finns i kapitel 14.

De av regeringen i proposition 2020/21:194 föreslagna paragraferna reglerar tillsynsmyndighetens rätt att få tillträde till områden, lokaler och andra utrymmen samt möjlighet att besluta föreläggan-

den om information och tillträde (6 kap. 3 och 4 §§ säkerhetsskyddslagen).

Ändringarna innebär att tillsynsmyndigheten dels ges en ny undersökningsbefogenhet som innebär rätt att få tillgång till själva informationssystemet, dels får möjlighet att förelägga den som står under tillsyn att ge sådan tillgång.

Som utgångspunkt ska tillsynsmyndigheten i första hand försöka få verksamhetsutövaren att frivillig ge myndigheten tillgång till informationssystemet. För att tillsynsmyndigheten ska ha rätt att få tillgång till informationssystem krävs att systemet används i verksamhet som omfattas av tillsyn enligt 6 kap. 1 § och att informationstillgången behövs för tillsynen. Rätten motsvaras av en skyldighet för den som står under tillsyn att tillhandahålla det begärda tillträdet. Det intrång som tillgången innebär måste stå i proportion till behovet av tillsynsåtgärden. Tillgångsrätten ger inte tillsynsmyndigheten rätt att bereda sig tillgång med tvång. Om den som står under tillsyn inte samarbetar kan dock tillsynsmyndigheten förelägga denna att ge tillgång vid äventyr av vite och i sista hand begära handräckning av Kronofogdemyndigheten. Om ett föreläggande förenas med vite är lagen (1985:206) om viten tillämplig.

7 kap.

2 a § *Samrådsmyndigheten får besluta att ta ut en sanktionsavgift av en verksamhetsutövare som*

1. har åsidosatt sin skyldighet enligt 3 a kap. 2 § första och andra stycket,

2. har driftsatt eller förändrat ett informationssystem i strid med ett förbud som har meddelats med stöd av 3 a kap. 5 §, eller

3. har lämnat oriktiga uppgifter i samband med samråd enligt 3 a kap. 2 §.

Övervägandena finns i kapitel 13.

Paragrafen, som är ny, reglerar uttömmande vid vilka överträdelser samrådsmyndigheten får ta ut en sanktionsavgift av en verksamhetsutövare, nämligen i fall samrådsskyldigheten åsidosatts, meddelat förbud inte respekteras samt då oriktiga uppgifter lämnats vid samrådet.

Det är inte obligatoriskt att ta ut sanktionsavgift när en överträdelse har konstaterats, utan det är samrådsmyndigheten som avgör om en avgift ska tas ut i det enskilda fallet. De omständigheter som särskilt ska beaktas vid den bedömningen anges i 7 kap. 3 § säkerhetsskyddslagen. Också statliga myndigheter, kommuner och regioner kan påföras sanktionsavgift.

Innan samrådsmyndigheten tar ut en sanktionsavgift ska verksamhetsutövaren ges tillfälle att yttra sig. Detta följer av förvaltningslagen.

9 § En sanktionsavgift ska betalas till *samråds-* eller tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

En sanktionsavgift tillfaller staten.

Övervägandena finns i kapitel 13.

Paragrafen innehåller bestämmelser om betalning och indrivning av sanktionsavgifter.

Ändringen i *första stycket* innebär att det som anges där om betalning till tillsynsmyndigheten också, i tillämpliga fall, gäller i förhållande till samrådsmyndigheten.

8 kap.

4 § Beslut om föreläggande enligt *3 a kap. 2 §*, 4 kap. 9 och 15 §§ och 6 kap. 4 och 6 §§ eller sanktionsavgift enligt 7 kap. 1, 2 och 2 a §§ *eller beslut om förbud enligt 3 a kap. 5 §* får överklagas till Förvaltningsrätten i Stockholm. När ett sådant beslut överklagas är *samråds-* eller tillsynsmyndigheten motpart. Prövningstillstånd krävs vid överklagande till kammarrätten.

Beslut om förbud enligt 4 kap. 11, 17 och 18 §§ och föreläggande enligt 4 kap. 12 och 19 §§ får överklagas till regeringen.

Andra beslut enligt denna lag får inte överklagas.

Övervägandena finns i kapitel 15.

Paragrafen innehåller bestämmelser om överklagande.

Ändringen i *första stycket* innebär att även samrådsmyndighetens beslut om föreläggande under samråd samt om förbud eller sanktionsavgift får överklagas till Förvaltningsrätten i Stockholm och att samrådsmyndigheten är motpart när sådana beslut överklagas.

Ikraftträdande

1. Denna lag träder i kraft den 1 juli 2022.

2. Äldre föreskrifter gäller fortfarande för ärenden om samråd som har inletts före ikraftträdandet.

3. En sanktionsavgift enligt 7 kap. 2 a § får beslutas endast för överträdelser som skett efter ikraftträdandet.

Eftersom de föreslagna lagändringarna är mycket angelägna bör förslagen, även med beaktande av att ett skyndsamt ikraftträdande ger berörda aktörer en relativt kort tid att förbereda sig, träda i kraft så snart som möjligt. Med hänsyn till den tid som de olika leden i lagstiftningsprocessen kan förväntas ta, anser utredningen att ett ikraftträdande är möjligt tidigast den 1 juli 2022.

Punkt 1 föreskriver att lagen träder i kraft den 1 juli 2022. De föreslagna bestämmelserna om skyldigheter vid driftsättning av informationssystem bör inte ges retroaktiv verkan för sådana system som tagits i drift före ikraftträdandet.

Enligt *punkt 2* gäller äldre föreskrifter fortfarande för ärenden om samråd som har inletts före ikraftträdandet. Det innebär att ärenden om samråd i samband med driftsättningar och väsentliga förändringar av informationssystem som har inletts före ikraftträdandet handläggs enligt äldre föreskrifter.

Enligt *punkt 3* får en sanktionsavgift beslutas av samrådsmyndigheten endast för överträdelser som har skett efter ikraftträdandet.

Referenser

Offentliga tryck

Propositioner

Prop. 2020/21:186, *Kompletterande bestämmelser till EU:s cybersäkerhetsakt.*

Prop. 2020/21:30, Totalförsvar 2021–2025.

Prop. 2020/21:1, *Budgetproposition för 2021*, utg.omr. 6.

Prop. 2017/18:205, *Informationssäkerhet för samhällsviktiga och digitala tjänster*.

Prop. 2017/18:1, *Budgetproposition för 2018*, utg.omr. 2.

Prop. 2017/18:89, *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag*.

Skrivelser

Statsrådsberedningen (2017): *Nationell säkerhetsstrategi.*

Skr. 2017/18:47, *Hur Sverige blir bäst i världen på att använda digitaliseringens möjligheter – en skrivelse om politikens inriktning*.

Skr. 2016/17:213, *Nationell strategi för samhällets informations- och cybersäkerhet*.

Lagrådsremisser

Regeringens lagrådsremiss 2021-03-18, *Ett starkare skydd för Sveriges säkerhet*.

Statens offentliga utredningar

SOU 2021:25 *Struktur för ökad motståndskraft*.

SOU 2021:1 *Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering*.

SOU 2020:25 *EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering*.

SOU 2018:82 *Kompletteringar till den nya säkerhetsskyddslagen*.

SOU 2018:25 *Juridik som stöd för förvaltningens digitalisering*.

SOU 2017:114 *reboot–omstart för den digitala förvaltningen*.

SOU 2017:36 *Informationssäkerhet för samhällsviktiga och digitala tjänster*.

SOU 2017:23 *digitalforvaltning.nu*.

SOU 2016:89 *För digitalisering i tiden*.

SOU 2016:85 *Digitaliseringens effekter på individ och samhälle – fyra temarapporter*.

SOU 2015:91 *Digitaliseringens transformerande kraft – vägval för framtiden*.

SOU 2015:65 *Om Sverige i framtiden – en antologi om digitaliseringens möjligheter*.

SOU 2015:28 *Gör Sverige i framtiden – digital kompetens*.

SOU 2015:25 *En ny säkerhetsskyddslag*.

SOU 2015:23 *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten*.

SOU 2014:13 *En digital agenda i människans tjänst – en ljusnande framtid kan bli vår*.

SOU 2013:31 *En digital agenda i människans tjänst – Sveriges digitala ekosystem, dess aktörer och drivkrafter*.

SOU 2010:25 *Översyn av verksamhet och organisation på informationssäkerhetsområdet*.

Departementspromemorior

Ds 2019:8 *Värnkraft: Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025*.

Ds 2018:6 *Granskning av Transportstyrelsens upphandling av it-drift*.

Ds 2017:66 *Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025*.

Rapporter

Digitaliseringsrådet (2018): *En lägesbild av digital ledning*.

Ekonomistyrningsverket (2018): *Digitalisering av det offentliga Sverige*.

Enisa (2021): *SECURITY IN 5G SPECIFICATIONS – Controls in 3GPP Security Specifications (5G SA)*.

FOI (2020): *Vilse i lasagnen? En upptäcktsfärd i den svenska Digitaliseringens mångbottnade problemstruktur* (FOI-R--4814--SE).

Försvarets radioanstalts *årsrapport 2016*.

Högskolan i Skövde (2017): *Länsstyrelsernas förutsättningar att stödja kommuner gällande informationssäkerhet*.

IT & Telekomföretagens (2020): *IT-kompetensbristen – en rapport om den svenska digitala sektorns behov av spetskompetens*.

Knowit (2020): *Övergripande studie av offentlig it-drift (informationssäkerhet) i Västra Götaland (slutrapport)*.

Kommerskollegiums rapport *The Cyber Effect – the implications of IT security regulation on international trade* (2018).

Kungl. Ingenjörsvetenskapsakademin (2019): *Digitalisering för ökad konkurrenskraft*.

Myndigheten för samhällsskydd och beredskap (2021): *En struktur för uppföljning av det systematiska informations-säkerhetsarbetet i den offentliga förvaltningen*.

Myndigheten för samhällsskydd och beredskap, m.fl. (2021): *Samlad informations- och cybersäkerhetshandlingsplan 2019–2022*, MSB1635.

Myndigheten för samhällsskydd och beredskap (2020): *Statliga myndigheters it-incidentrapportering 2020 – Utmaningar för en säker och robust informationshantering*.

Myndigheten för digital förvaltning (2019): *Myndigheters digitala mognad och it-kostnader*.

Myndigheten för samhällsskydd och beredskap (2017): *Bevakningsansvariga myndigheters informations- och cybersäkerhet*.

Myndigheten för samhällsskydd och beredskap (2016): *Nationell handlingsplan för samhällets informationssäkerhet*.

Myndigheten för samhällsskydd och beredskap (2016): *Informationssäkerheten i Sveriges kommuner – Analys och rekommendationer utifrån MSB:s kommunenkät 2015*.

Myndigheten för samhällsskydd och beredskap (2015): *En bild av kommunernas informationssäkerhetsarbete 2015*.

Myndigheten för samhällsskydd och beredskap (2014): *En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter*.

PricewaterhouseCoopers (2020): *Cyberhoten mot Sverige 2019 – En undersökning om hur 100 större svenska bolag ser på cyberbrott nu och i ett framtidsperspektiv.*

Riksrevisionen (2019): *Föråldrade it-system – hinder för en effektiv digitalisering*, (RIR 2019:28).

Riksrevisionen (2016): *Informationssäkerhetsarbete på nio myndigheter – En andra granskning av informationssäkerheten i staten*, (RiR 2016:8).

Riksrevisionen (2014): *Informationssäkerheten i den civila statsförvaltningen*, (RIR 2014:23).

Sveriges Kommuner och Regioner (2019): *Kommunernas informationssäkerhetsarbete – en övergripande kartläggning av kommunernas systematiska informationssäkerhetsarbete*.

Säkerhetspolisen (2019): *Vägledning i säkerhetsskydd – Informationssäkerhet*.

Säkerhetspolisen (2017): Säkerhetsskydd *hos myndigheter med mest skyddsvärd verksamhet*, Säkerhetspolisens offentliga redovisning till regeringen (2017-25007-5).

Säkerhetspolisens *årsbok 2016*.

Vetenskapsrådet (2018): *Att motverka överbelastning av samhällsviktiga webbplatser Slutrapport 2018 från projekt Särimner*.

Teknikföretagen (2019): *CYBERHOTEN – Så ser hotbilden och attackerna ut mot svenska teknikföretag*.

Unitalent AB (2020): *Cybersäkerhet – En kartläggning av Sveriges nuläge 2020 och framtidsutsikter för branschen*.

Vetenskapsrådet (2018): *Vetenskapsrådets guide till infrastrukturen*.

Vinnova (2018): *Artificiell intelligens i svenskt näringsliv och samhälle – Analys av utveckling och potential*, (slutrapport).

Övrigt

Finska regeringens proposition (RP 98/2020 rd) till riksdagen *med förslag till lagar om ändring av lagen om tjänster inom elektronisk kommunikation och av vissa lagar som har samband med den*.

Försvarsmakten (2013): *Handbok Försvarsmaktens säkerhetstjänst, Informationssäkerhet, H Säk Infosäk*.

ITU (2018): *Global Cybersecurity Index (GCI)*.

OECD (2019): *Digital Government Index*, resultat för 2019.

OECD (2019): *Digital Government Review of Sweden – Towards a Data-driven Public Sector*, 2019.

Säkerhetspolisen *Hotbild mot säkerhetskänslig verksamhet*, 2019.

Säkerhetspolisens *Vägledning i säkerhetsskydd Fysisk säkerhet*, 2020.

Säkerhetspolisens *Vägledning i säkerhetsskydd, Informationssäkerhet*, 2020.

Säkerhetspolisens *Vägledning i säkerhetsskydd – Introduktion till säkerhetsskydd*, 2019.

Säkerhetspolisens *Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys*, 2019.

Kommittédirektiv 2019:73

Cybersäkerhet – genomförandet av cybersäkerhetsakten och vissa åtgärder till skydd för säkerhetskänslig verksamhet

Beslut vid regeringssammanträde den 31 oktober 2019

Sammanfattning

En särskild utredare ska föreslå de anpassningar och kompletterande författningsbestämmelser som cybersäkerhetsakten ger anledning till. Syftet är att säkerställa att den kompletterande nationella reglering som behövs finns på plats när hela förordningen börjar tillämpas den 28 juni 2021. Utredaren ska också överväga om det finns anledning att införa ytterligare krav för att skydda verksamheter som är av betydelse för Sveriges säkerhet.

Utredaren ska bl.a.

- undersöka vilka kompletterande nationella föreskrifter, exempelvis processuella bestämmelser och bestämmelser om sanktioner, som förordningen kräver eller Sverige bör införa,
- föreslå vilken befintlig myndighet som ska få i uppdrag att vara tillsynsmyndighet,
- analysera om, och i så fall föreslå vilka kompletterande bestämmelser som bör införas dels om självbedömning av överensstämmelse med de krav som ställs i certifieringsordningar och dels om organ för bedömning av överensstämmelse i den svenska regleringen,

- bedöma om det bör införas krav på certifiering och godkännande av vissa produkter, tjänster och processer som ska användas i verksamheter som är av betydelse för Sveriges säkerhet och föreslå hur ett sådant system skulle kunna utformas, och
- lämna sådana författningsförslag som i övrigt behövs och är lämpliga.

Uppdraget ska i den del som avser anpassningar med anledning av EU-förordningen redovisas senast den 1 juni 2020. I den del som avser regler för verksamheter som är av betydelse för Sveriges säkerhet ska uppdraget redovisas senast den 1 mars 2021.

Den nya regleringen – cybersäkerhetsakten

Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) trädde i kraft den 27 juni 2019. Förordningen började tillämpas direkt med undantag för vissa artiklar som kräver kompletterande bestämmelser på nationell nivå och som därför ska börja tillämpas först den 28 juni 2021. Det huvudsakliga syftet med förordningen är att säkerställa en väl fungerande inre marknad och samtidigt sträva efter att uppnå en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen.

Förordningen är uppdelad i två delar. Den första delen gäller fastställandet av mål, uppgifter och organisatoriska frågor som rör Enisa. Denna del kräver enligt regeringens bedömning ingen särskild kompletterande nationell reglering från medlemsstaternas sida. Den andra delen reglerar fastställandet av ett europeiskt ramverk för cybersäkerhetscertifiering. Syftet är att säkerställa en tillfredsställande nivå i fråga om cybersäkerhet för informations- och kommunikationsteknik (IKT) i unionen samt att undvika en fragmentering av den inre marknaden när det gäller certifieringsordningar i unionen. Skapandet av europeiska ordningar för cybersäkerhetscertifiering kommer att medföra att certifikat som utfärdas enligt dessa certifieringsordningar blir giltiga och erkända i alla medlemsstater. Förutom att beskriva de säkerhetsmålsättningar som ska beaktas i utformningen

av de europeiska ordningarna för cybersäkerhetscertifieringar, anger förordningen vad minimiinnehållet i sådana ordningar bör vara. Förordningen anger också väsentliga funktioner och uppgifter för Enisa inom cybersäkerhetscertifiering. Kommissionen kommer att utarbeta löpande arbetsprogram för europeisk cybersäkerhetscertifiering där det fastställs strategiska prioriteringar för framtida europeiska ordningar för cybersäkerhetscertifiering. De europeiska certifieringsordningarna kommer sedan att utarbetas av Enisa, med hjälp av expertråd och i nära samarbete med den europeiska gruppen för cybersäkerhetscertifiering (ECCG), som också har inrättats genom förordningen. Gruppens uppgifter regleras i förordningen och består bl.a. i att ge råd till och bistå kommissionen vad gäller cybersäkerhetscertifiering och utarbetande av de europeiska ordningarna för cybersäkerhetscertifiering. En annan uppgift för gruppen är att underlätta anpassningen av de europeiska ordningarna till internationellt erkända standarder och att, där så är lämpligt, lämna rekommendationer till Enisa om att samarbeta med relevanta internationella standardiseringsorganisationer för att åtgärda brister eller luckor i de befintliga internationellt erkända standarderna. Kommissionen ska, med stöd från Enisa, vara ordförande i gruppen. Kommissionen antar sedan de europeiska ordningarna för cybercertifiering genom genomförandeakter.

En europeisk ordning för cybersäkerhetscertifiering får innehålla en eller flera av följande assuransnivåer för IKT-produkter, IKT-tjänster och IKT-processer, dvs. på vilken nivå produkten, tjänsten eller processen har utvärderats: ”grundläggande”, ”betydande” eller ”hög”. Varje europeiskt cybersäkerhetscertifikat kan avse någon av assuransnivåerna medan EU-försäkran om överensstämmelse endast kan avse assuransnivån ”grundläggande”. De säkerhetskrav som motsvarar varje assuransnivå ska anges i den relevanta europeiska ordningen för cybersäkerhetscertifiering. Certifikatet eller EU-försäkran om överensstämmelse ska hänvisa till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, som syftar till att minska risken för eller förhindra cybersäkerhetsincidenter. Ett europeiskt cybersäkerhetscertifikat eller en EU-försäkran om överensstämmelse med assuransnivån ”grundläggande” ska försäkra att motsvarande säkerhetskrav är uppfyllda, inbegripet säkerhetsfunktioner, och att utvärderingen har skett på en nivå som avser att minimera kända grundläggande risker för inci-

denter och cyberattacker. Den utvärdering som ska göras ska innefatta åtminstone en granskning av den tekniska dokumentationen. Om en sådan granskning inte är lämplig ska alternativa utvärderingsinsatser med likvärdig effekt utföras. Om en europeisk ordning för cybersäkerhetscertifiering ger möjlighet till självbedömning av överensstämmelse bör det vara tillräckligt att tillverkaren eller leverantören har gjort en självbedömning av IKT-produktens, IKT-tjänstens eller IKT-processens överensstämmelse med certifieringsordningen. För assuransnivån ”betydande” bör utvärderingen, utöver kraven för assuransnivån ”grundläggande”, åtminstone omfatta en kontroll av överensstämmelsen mellan IKT-produktens, IKT-tjänstens eller IKT-processens säkerhetsfunktioner och den tekniska dokumentationen. För assuransnivån ”hög” bör utvärderingen, utöver kraven för assuransnivån ”betydande”, åtminstone omfatta ett effektivitetstest som bedömer resistensen hos IKT-produktens, IKT-tjänstens eller IKT-processens säkerhetsfunktioner gentemot genomtänkta cyberangrepp som utförs av personer med betydande kompetens och resurser. En europeisk ordning för cybersäkerhetscertifiering kan ha flera olika utvärderingsnivåer beroende på hur stringent och djupgående den aktuella utvärderingsmetoden är.

Enligt förordningen ska övervakning, tillsyn och verkställighetsuppgifter framför allt ligga hos medlemsstaterna. Medlemsstaterna ska utse en eller flera tillsynsmyndigheter, så kallade nationella myndigheter för cybersäkerhetscertifiering. Myndigheten eller myndigheterna kommer bl.a. att få i uppdrag att övervaka och kontrollera organ för bedömning av överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat och utfärdare av en EU-försäkran om överensstämmelse. Ett organ för bedömning av överensstämmelse är ett organ som utför bedömning av överensstämmelse, bl.a. genom kalibrering, provning, certifiering och kontroll.

Förordningens bestämmelser ska inte påverka tillämpningen av särskilda bestämmelser om frivillig eller obligatorisk certifiering i andra unionsrättsakter. Förordningen ska heller inte påverka medlemsstaternas befogenheter i fråga om verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på straffrättens område. Den delen av förordningen som rör cybersäkerhetscertifiering kommer att kräva anpassningar och kompletterande författningsbestämmelser på nationell nivå.

Uppdraget att genomföra EU:s cybersäkerhetsakt

Allmänna riktlinjer för uppdraget

Cybersäkerhetsakten kommer att reglera den cybersäkerhetscertifiering som följer av en europeisk certifieringsordning för cybersäkerhetscertifiering som fastställts av kommissionen. I dag bestämmer en producent själv om en produkt, tjänst eller process ska certifieras och i så fall vilket certifieringsorgan som ska utföra certifieringen. Utgångspunkten kommer att vara att certifieringen även i framtiden ska vara frivillig, oavsett om en europeisk ordning för cybersäkerhetscertifiering finns på plats eller inte. Detta är dock upp till varje medlemsstat att bestämma. Den största skillnaden är att när en sådan europeisk ordning för cybersäkerhetscertifiering finns på plats, får inte längre nationella cybersäkerhetscertifieringar utföras inom det område som täcks av den europeiska ordningen för cybersäkerhetscertifiering. Förordningen innebär också att när en europeisk ordning för cybersäkerhetscertifiering ska användas reglerar förordningen vilka krav som ställs på certifieringen, certifieringsorganen och de leverantörer och producenter som innehar ett sådant certifikat. Det finns därför ett behov av att ta fram en nationell reglering som kompletterar förordningen.

Utredaren ska därför

- lämna förslag till författningsbestämmelser som kompletterar cybersäkerhetsakten.

Vilken myndighet ska vara nationell myndighet för cybersäkerhetscertifiering?

Cybersäkerhetsakten föreskriver att varje medlemsstat ska utse en eller flera nationella myndigheter för cybersäkerhetscertifiering på sitt territorium som ansvariga för tillsynsuppgifterna. Alternativt kan medlemsstaten, efter överenskommelse med en annan medlemsstat, utse en eller flera nationella myndigheter för cybersäkerhetscertifiering som är etablerade i denna andra medlemsstat (artikel 58).

Flertalet av cybersäkerhetsaktens bestämmelser om nationella myndigheter för cybersäkerhetscertifiering gäller direkt och medför inga krav på eller behov av kompletterande nationella bestämmelser. Medlemsstaterna ska dock underrätta kommissionen om vilka myn-

digheter som utsetts och, om fler än en myndighet utsetts, vilka uppgifter de olika myndigheterna ska ha. Myndigheterna kommer bl.a. även att ha en roll när det gäller utfärdandet av europeiska cybersäkerhetscertifikat (på nivån ”hög”), och då måste medlemsstaterna säkerställa att denna verksamhet är avskild från uppgifterna som myndigheten ska utföra som tillsynsmyndighet och att den utförs av oberoende enheter.

Vissa andra frågor är i och för sig reglerade i förordningen men tillåter ytterligare nationell reglering. Detta gäller exempelvis regleringen om tillsynsmyndighetens befogenheter i artikel 58.8. Det är vidare upp till medlemsstaterna att inom vissa angivna ramar reglera bl.a. tillsynsmyndighetens organisation och se till att myndigheten har tillräckliga resurser.

Vid tillsynsmyndigheten kommer det att samlas känslig information om cybersäkerheten i vissa produkter, tjänster och processer eftersom myndigheten kommer att ha ett särskilt ansvar för utfärdande av certifikat enligt den högsta assuransnivån. Det är därför viktigt att myndigheten har personal med erfarenhet av och förmåga att bedöma och hantera uppgifter enligt de krav som ställs i offentlighets- och sekretesslagen (2009:400) och säkerhetsskyddslagen (2018:585). Sveriges certifieringsorgan för it-säkerhet som är lokaliserat vid Försvarets materielverk, CSEC, ska enligt sin instruktion i sin verksamhet beakta nationella säkerhetsintressen. Ett sådant krav bör därför införas även i den reglering som föreslås av utredaren.

Styrelsen för ackreditering och teknisk kontroll (Swedac) har i dag vissa av de uppgifter som den nationella myndigheten för cybersäkerhetscertifiering ska ha. Enligt sin instruktion ska Swedac bl.a. ansvara för frågor om teknisk kontroll, vilket inkluderar ackreditering och frågor i övrigt om bedömning av överensstämmelse. Swedac ska särskilt ansvara för ordningar för bedömning av överensstämmelse/teknisk provning och kontroll. Detta inbegriper att i EU, internationellt och nationellt verka för öppna och harmoniserade tekniska kontrollordningar, ackrediteringssystem och normer för ömsesidigt godtagande av resultat från provningar, certifieringar och andra bevis om överensstämmelse som undanröjer tekniska handelshinder samt upprätthålla och vidareutveckla öppna, kostnadseffektiva och behovsanpassade ordningar för teknisk kontroll och bedömning av överensstämmelse. Swedac är även nationellt ackrediteringsorgan i enlighet med Europaparlamentets och rådets förordning (EG) nr 765/2008

av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 och anmäler och utövar tillsyn över organ som enligt lagen (2011:791) om ackreditering och teknisk kontroll ska anmälas för uppgifter i samband med bedömning av överensstämmelse enligt bestämmelser som gäller inom EU.

För att undvika att den nationella myndigheten för cybersäkerhetscertifiering tilldelas uppgifter som redan utförs av Swedac bör utredaren kartlägga hur förhållandet mellan den nationella myndigheten för cybersäkerhetscertifiering och Swedac ska se ut, i vilka fall de två myndigheterna ska samarbeta och vilket behov av kompletterande nationella bestämmelser som behövs. Det är viktigt att utredaren i detta arbete beaktar de kostnader, den tid och andra aspekter som en dubbel granskning av såväl Swedac som den nationella tillsynsmyndigheten kommer att innebära för den som blir granskad.

Utredaren ska därför

- föreslå vilken befintlig myndighet som ska få i uppdrag att vara nationell tillsynsmyndighet för cybersäkerhetscertifiering,
- ta ställning till hur myndighetens organisation påverkas,
- kartlägga vilket förhållande den nationella myndigheten för cybersäkerhetscertifiering ska ha till Swedac och hur uppgifterna ska fördelas dem emellan för att undvika såväl överlappande granskningar som luckor i tillsynen, samt
- utarbeta nödvändiga kompletterande författningsförslag, inklusive om de befogenheter som den nationella myndigheten för cybersäkerhetscertifiering ska tilldelas, i syfte att myndigheten ska kunna utföra de uppgifter som följer av förordningen.

Ska det införas kompletterande bestämmelser om sanktioner?

Cybersäkerhetsakten innehåller i artikel 65 bestämmelser om att medlemsstaterna ska fastställa regler om sanktioner vid överträdelser av den delen av förordningen som reglerar ett ramverk för cybersäkerhetscertifiering och för överträdelser av europeiska ordningar för cybersäkerhetscertifiering. Medlemsstaterna ska också vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. I artikel 58.8 finns en

lista över de befogenheter som de nationella myndigheterna för cybersäkerhetscertifiering måste ha. I punkt f anges att myndigheterna ska utdöma sanktioner i enlighet med nationell rätt och kräva att överträdelser av skyldigheterna i förordningen omedelbart upphör. Medlemsstaterna ska vidare enligt artikel 65 anmäla dessa regler och åtgärder samt eventuella ändringar som berör dem till kommissionen utan dröjsmål. I förordningen saknas dock närmare bestämmelser om hur detta ska gå till och vilka som ska kunna drabbas av sanktioner. Till detta kommer också att det föreslagna systemet är frivilligt. Om sanktionerna för att bryta mot ett system som inte är obligatoriskt är för långtgående finns det risk för att aktörer inte kommer att använda sig av den europeiska cybersäkerhetscertifieringen eller att de vänder sig till länder med mildare sanktionssystem. Samtidigt får det europeiska systemet inte bli tandlöst för dem som trots allt väljer att använda sig av det. Det finns därför behov av att analysera och ta ställning till i vilken utsträckning överträdelser av förordningen bör bli föremål för sanktioner i Sverige.

Utredaren ska därför

- analysera vilka kompletterande bestämmelser om sanktioner som Sverige behöver eller bör införa,
- lämna sådana författningsförslag som behövs och är lämpliga.

Processuella frågor och rätten att klaga

Av artikel 58.8 i förordningen framgår det att utövandet av tillsynsmyndighetens befogenheter ska vara föremål för lämpliga skyddsåtgärder, bl.a. effektiva rättsmedel. Enligt artikel 58.8 d ska tillsynsmyndigheten ha befogenhet att få tillgång till lokaler hos organ för bedömning av överensstämmelse eller hos innehavare av ett europeiskt cybersäkerhetscertifikat i enlighet med unionsrätten eller nationell processrätt. Fysiska och juridiska personer ska, enligt förordningen, ha rätt att lämna in klagomål till utfärdaren av ett europeiskt cybersäkerhetscertifikat eller, när klagomålet rör ett europeiskt cybersäkerhetscertifikat som utfärdats av ett organ för bedömning av överensstämmelse, till den behöriga nationella myndigheten för cybersäkerhetscertifiering (artikel 63.1). Vidare ska fysiska och juridiska personer ha rätt till ett effektivt rättsmedel mot den myndighet eller de organ som nämnts ovan och som fattat ett beslut, och när det gäller underlåtenhet att

vidta åtgärder med anledning av ett klagomål som lämnats in till myndigheten eller organet (artikel 64.1). Detta torde för svensk del bäst tillgodoses genom en rätt för enskilda att överklaga tillsynsmyndighetens beslut till allmän förvaltningsdomstol.

Behovet av kompletterande nationella bestämmelser i de ovanstående frågorna behöver bli föremål för närmare analys.

Utredaren ska därför

- analysera i vilken utsträckning det behövs kompletterande bestämmelser om utövandet av tillsynsmyndighetens befogenheter,
- ta ställning till i vilken utsträckning det behövs kompletterande bestämmelser om de rättsmedel för enskilda som regleras i förordningen, och
- lämna sådana författningsförslag som behövs och är lämpliga.

Hur ska förordningens bestämmelser om organ för bedömning av överensstämmelse och självbedömning av överensstämmelse genomföras?

Förordningen reglerar även organ för bedömning av överensstämmelse, som bl.a. kan utfärda europeiska cybersäkerhetscertifikat. I bilagan till förordningen finns närmare bestämmelser med krav på dessa organ, bl.a. om upprätthållande av konfidentialitet och tystnadsplikt. Organen för bedömning av överensstämmelse ska ackrediteras av det nationella ackrediteringsorganet – i Sveriges fall är det Swedac. I fall där ett europeiskt cybersäkerhetscertifikat utfärdas av en nationell myndighet för cybersäkerhetscertifiering ska certifieringsorganet hos den nationella myndigheten för cybersäkerhetscertifiering ackrediteras som organ för bedömning av överensstämmelse.

En europeisk ordning för cybersäkerhetscertifiering kan också ge tillverkare eller leverantörer möjlighet att göra en självbedömning av överensstämmelse. Detta tillåts endast i förhållande till produkter, tjänster och processer där de uppfyllda säkerhetskraven är ställda på en lägre nivå. I förordningen finns bestämmelser om hur detta ska gå till (artikel 53). Där anges också att detta är frivilligt att utfärda, om inte annat anges i unionsrätten eller i medlemsstaternas nationella rätt.

Utredaren ska därför

- föreslå hur bestämmelserna om kraven på organen för överensstämmelse ska genomföras,
- analysera om nuvarande sekretessbestämmelser för offentliga organ och bestämmelser om tystnadsplikt för privata aktörer behöver anpassas eller ny lagstiftning föreslås, med anledning av förordningens reglering om tystnadsplikt och konfidentialitet hos organen för överensstämmelse, och
- lämna sådana författningsförslag som behövs och är lämpliga.

Frivillighet

Cybersäkerhetscertifieringen ska enligt förordningen vara frivillig, om inte annat anges i unionsrätten eller i medlemsstaternas nationella rätt (artikel 56.2). Förordningen ger dock kommissionen i uppdrag att regelbundet bedöma effektiviteten hos och användningen av de antagna europeiska ordningarna för cybersäkerhetscertifiering och huruvida en specifik europeisk ordning för cybersäkerhetscertifiering ska göras obligatorisk genom unionsrätten i syfte att säkerställa en adekvat cybersäkerhetsnivå och förbättra den inre marknadens funktion. Den första bedömningen ska göras senast den 31 december 2023, och efterföljande bedömningar ska göras minst en gång vartannat år. Kommissionen ska sedan på grundval av bedömningen fastställa om produkter, tjänster eller processer ska omfattas av en obligatorisk certifieringsordning.

Som tidigare nämnts upphör de nationella ordningarna för cybersäkerhetscertifiering och tillhörande förfaranden att gälla så fort det finns europeiska motsvarigheter. Befintliga certifikat kommer dock att förbli giltiga till dess att de löper ut. Medlemsstaterna förbinder sig också att inte införa nya nationella ordningar, som omfattas av en befintlig europeisk ordning för cybersäkerhetscertifiering, och ska meddela kommissionen och ECCG om alla avsikter att utarbeta nya nationella ordningar för cybersäkerhetscertifiering. Detta regleras i förordningen och kommer att påverka såväl innehavare av befintliga certifikat som de certifieringsorgan som i dag utfärdar certifikat enligt andra ordningar. Verksamheter måste anpassas till det nya systemet,

och branschen måste hålla sig uppdaterad om de förslag till europeiska ordningar för cybersäkerhetscertifiering som utarbetas.

Utredaren ska därför

- hålla sig uppdaterad om hur arbetet med att utarbeta europeiska ordningar för cybersäkerhetscertifiering fortgår, och
- lämna sådana författningsförslag som behövs och är lämpliga.

Certifiering på den högsta assuransnivån

I Sverige finns i dag vid Försvarets materielverk ett nationellt certifieringsorgan för it-säkerhet i produkter och system, CSEC. CSEC ska i sin verksamhet beakta nationella säkerhetsintressen och verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat. Dessutom är CSEC Sveriges signatär och representant inom den internationella överenskommelsen för ömsesidigt erkännande av certifikat, Common Criteria Recognition Arrangement (CCRA), och motsvarande överenskommelse inom Europa, Senior Officials Group Information Systems Security – Mutual Recognition Arrangement (SOG-IS MRA), (5 § förordningen [2007:854] med instruktion för Försvarets materielverk). Detta innebär att CSEC representerar och tar tillvara landets intressen inom organisationerna. Som nationellt certifieringsorgan ansvarar CSEC för att ta fram och utveckla regler för granskning av it-säkerhet i produkter och system enligt Common Criteria, CC. CSEC licensierar företag som utför granskningar enligt dessa regler samt utövar tillsyn över dessa företag. Produkter som certifierats av CSEC används bl.a. av Försvarsmakten. CC erkänns internationellt av världens ledande länder inom it-säkerhet och anses obligatoriskt för it-produkter i kritiska infrastrukturer i flera länder. CSEC har även som uppdrag att samverka internationellt med andra certifieringsorgan och säkerhetsmyndigheter.

CCRA och SOG-IS MRA tillåter endast statliga certifieringsorgan, vilket medför att det i dag bara är CSEC som utfärdar certifikat enligt den standarden i Sverige. Med cybersäkerhetsakten tillåts privata certifieringsorgan endast att utfärda certifikat på nivån ”grundläggande” eller ”betydande”. För nivån ”hög” är det den nationella myndigheten för cybersäkerhetscertifiering som är behörig. Myndigheten kan dock delegera detta till ett organ för bedömning av överensstämmelse genom en allmän delegering på förhand av uppgiften eller efter

förhandsgodkännande av varje enskilt europeiskt cybersäkerhetscertifikat.

Utredaren ska därför

- föreslå hur certifiering på assuransnivån ”hög” ska genomföras i Sverige och utreda om detta kan och bör regleras genom författning. Utredaren ska ha som utgångspunkt att CSEC ska ha en roll då det gäller denna typ av certifiering.

Uppdraget att överväga om det bör införas krav på certifiering och godkännande till skydd för Sveriges säkerhet

Särskilda krav på säkerhet måste kunna ställas på nät- och informationssäkerhet för att skydda nationell säkerhet. Åtgärder för att skydda nationell säkerhet faller utanför EU:s kompetens (art. 4.2 EU-fördraget). Av artikel 1.2 cybersäkerhetsakten framgår även att förordningen inte ska påverka medlemsstaternas befogenheter i fråga om nät- och informationssäkerhet, särskilt inte verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på strafflagstiftningens område.

Säkerhetsskyddslagen gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet). För informationssystem som används i eller har betydelse för säkerhetskänslig verksamhet finns särskilda krav i säkerhetsskyddsförordningen (2018:658). Det rör sig dels om förberedande åtgärder inför driftsättning av sådana informationssystem, dels om säkerhetskrav som kontinuerligt ställs på informationssystemen. Bestämmelserna innehåller även krav på samråd med Säkerhetspolisen eller Försvarsmakten i vissa fall. Detta gäller för informationssystem som kan komma att behandla säkerhetsskyddsklassificerade uppgifter av visst slag och informationssystem där obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är obetydlig. Bestämmelserna innebär att det är verksamhetsutövaren som ansvarar för att se till att informationssystemen upprätthåller kraven på informationssäkerhet.

Det finns anledning att överväga om ytterligare krav bör införas för att säkerställa att nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet uppfyller de krav som behövs

för att upprätthålla skyddet av sådana verksamheter. En möjlighet kan vara att införa krav på att produkter, tjänster och processer inom nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet ska vara certifierade enligt särskilda certifieringsordningar som ställer krav anpassade för användning i säkerhetskänslig verksamhet. En kompletterande eller alternativ möjlighet är att införa krav på godkännande från en utpekad myndighet innan en sådan produkt, tjänst eller process tas i drift i säkerhetskänslig verksamhet.

Utredaren ska därför:

- bedöma om det finns anledning att införa särskilda krav på att produkter, tjänster och processer som ingår i ett nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet, ska vara certifierade enligt särskilda certifieringsordningar utformade för säkerhetskänslig verksamhet,
- överväga om det finns anledning att införa krav på godkännande från en myndighet för att sådana produkter, tjänster och processer ska få tas i drift i viss eller all säkerhetskänslig verksamhet,
- göra en internationell jämförelse av lagstiftning som innebär särskilda krav med anledning av nationell säkerhet för produkter, tjänster och processer som ingår i ett nätverks- eller informationssystem i länder som utredaren bedömer vara av intresse,
- lämna förslag, förenliga med EU-rätten, på hur ett sådant regelverk skulle kunna se ut, inklusive vilken eller vilka myndigheter som skulle ansvara för uppgiften och vilka sanktioner en sådan reglering bör förenas med,
- lämna nödvändiga författningsförslag som behövs och är lämpliga.

Utredningen har i denna del att förhålla sig till betänkandet Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82) som för närvarande bereds i Regeringskansliet.

Övriga frågor

Utredaren är fri att inom de ramar som anges i de allmänna riktlinjerna ta upp och belysa även andra frågeställningar som är relevanta för uppdraget.

Om utredaren kommer fram till att det krävs eller är lämpligt med kompletterande nationella bestämmelser i andra delar ska sådana kunna föreslås.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för enskilda. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. Utredaren ska särskilt ange konsekvenserna för företag i form av kostnader och ökade administrativa bördor samt personella konsekvenser för berörda myndigheter.

Utredaren ska även beakta de konsekvenser som förordningens genomförande kan få när det gäller internationell handel med tredjeland och erkännande och utfärdande av certifikat och andra åtaganden som följer av Sveriges medlemskap i bl.a. CCRA.

Kontakter och redovisning av uppdraget

Utredaren ska hålla Regeringskansliet (Försvarsdepartementet) informerat om det löpande arbetet.

Vid genomförandet av uppdraget ska utredaren hålla sig informerad om och beakta relevant arbete som bedrivs inom Regeringskansliet (exempelvis arbetet med betänkandet Kompletteringar till den nya säkerhetsskyddslagen, SOU 2018:82), utredningsväsendet och inom EU. Under genomförandet av uppdraget ska utredaren, i den utsträckning som bedöms lämplig, också ha en dialog med och inhämta upplysningar från myndigheter, näringslivet och andra som kan vara berörda av de aktuella frågorna.

Uppdraget ska redovisas i den del som avser anpassningar med anledning av EU-förordningen senast den 1 juni 2020. I den del som avser regler till skydd för Sveriges säkerhet ska uppdraget redovisas senast den 1 mars 2021.

(Försvarsdepartementet)

Kommittédirektiv 2020:57

Tilläggsdirektiv till Cybersäkerhetsutredningen (Fö 2019:01)

Beslut vid regeringssammanträde den 14 maj 2020

Förlängd tid för en del av uppdraget

Regeringen beslutade den 31 oktober 2019 kommittédirektiv om att ge en särskild utredare i uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser som cybersäkerhetsakten ger anledning till samt att överväga om det finns anledning att införa ytterligare krav för att skydda verksamheter som är av betydelse för Sveriges säkerhet (dir. 2019:73). Enligt direktiven skulle utredaren redovisa den del av uppdraget som avser anpassningar med anledning av cybersäkerhetsakten senast den 1 juni 2020.

Utredningstiden förlängs för en del av uppdraget. Den del av uppdraget som avser anpassningar med anledning av cybersäkerhetsakten ska i stället redovisas senast den 31 augusti 2020.

(Försvarsdepartementet)

Kommittédirektiv 2021:10

Tilläggsdirektiv till Cybersäkerhetsutredningen (Fö 2019:01)

Beslut vid regeringssammanträde den 18 februari 2021

Förlängd tid för en del av uppdraget

Regeringen beslutade den 31 oktober 2019 kommittédirektiv om att ge en särskild utredare i uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser som cybersäkerhetsakten ger anledning till samt att överväga om det finns anledning att införa ytterligare krav för att skydda verksamheter som är av betydelse för Sveriges säkerhet (dir. 2019:73). Enligt direktiven skulle den del som avser regler för verksamheter som är av betydelse för Sveriges säkerhet redovisas senast den 1 mars 2021.

Utredningstiden förlängs för en del av uppdraget. Den del av uppdraget som avser regler för verksamheter som är av betydelse för Sveriges säkerhet ska i stället redovisas senast den 30 juni 2021.

(Försvarsdepartementet)

STATENS OFFENTLIGA UTREDNINGAR

[Date]

Komm2021/

SWEDISH GOVERNMENT OFFICIAL REPORTS

The Cyber Security Inquiry
Fö 2019:1

Request for information

To [whom it may concern]

(National authority)
(Att: Mr./Ms. Xx Yy)

The Swedish Government has appointed Chief Judge Nils Cederstierna as Inquiry Chair to examine the need to strengthen the cybersecurity in information and communication systems (networks) in activities relevant to national security.

Chief Judge Nils Cederstierna is assisted by Mr. Thomas Wallander, Principal Secretary, and Mr. Patrik Roos, Inquiry Secretary, as well as Government Advisors and experts from Government Authorities.

The directives to the Inquiry state that it should gather information and examine whether certification of information and communications technology (ICT-products, -services and -processes), or requirements for approval of such products, services and processes can contribute to strengthening security in information- and communication systems (networks).[1]

The directives also state that the Inquiry should gather information and examine regulatory systems in this area in comparable countries. It would be much appreciated if you could assist the Inquiry with information about

[1] In September 2020 the Inquiry Chair submitted an interim report to the Swedish Government. The report included proposed national provisions on cyber security certification in support of the EU Cybersecurity Act (2019/881). The report (including an English summary) *EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhet* (SOU 2020:58), is available online.

Telephone: +46 8 405 10 00
Fax: +46 8 723 11 89
Web: www.regeringen.se

Postal address: SE 103 33 Stockholm
Street address: Jakobsgatan 9
E-mail: fo.registrator@gov.se

regulatory systems in this area in your country. The information that is specifically requested can be found in the attached question compilation.

It would also be much appreciated if we could have the opportunity to ask supplementary questions and discuss the topic at a digital meeting in the near future. The information is of importance for the understanding and analysis of how a regulatory system in the field can be developed. The information will be included in the official report that is to be submitted to the Government. Please be advised that the report is to be submitted no later than 30 June 2021.

The Inquiry appreciate if the information is sent via email (Word-file).

Sincerely,

Nils Cederstierna
Inquiry Chair

Contact information to the Inquiry Secretary:
Tel. +46 73-067 12 41
patrik.roos@regeringskansliet.se

Compilation of questions

1 Please provide a short overview of regulatory systems (legislation) and responsible authorities in the field of information security within national security and critical infrastructure.

2 Please provide information regarding any special requirements (e.g. requirement for certification and/or approval) for information systems (including networks or ICT-products, -services and -processes) used in or of importance to national security? How is national security defined in your country?

3 Please provide information regarding special requirements (e.g. requirement for certification and/or approval) for information systems (including networks or ICT-products, -services and -processes) used in or of importance to critical infrastructure? How are essential entities and critical infrastructure defined?

Statens offentliga utredningar 2021

Kronologisk förteckning

1. Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering. I.
2. Krav på kunskaper i svenska och samhällskunskap för svenskt medborgarskap. Ju.
3. Skolbibliotek för bildning och utbildning. U.
4. Informationsöverföring inom vård och omsorg. S.
5. Ett förbättrat system för arbetskraftsinvandring. Ju.
6. God och nära vård. Rätt stöd till psykisk hälsa. S.
7. Förstärkt skydd för väljarna vid röstmottagningen. Ju.
8. När behovet får styra – ett tandvårdssystem för en mer jämlik tandhälsa. Vol. 1 & Vol. 2, bilagor + Sammanfattning (häfte). S.
9. Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen. I.
10. Radiologiska skador – skadestånd, säkerheter, skadereglering. M.
11. Bättre möjligheter för elever att nå kunskapskraven – aktivt stöd- och elevhälsoarbete samt stärkt utbildning för elever med intellektuell funktionsnedsättning. U.
12. Andra chans för krisande företag – En ny lag om företagsrekonstruktion. Ju.
13. En teknikneutral grundlagsbestämmelse för regeringsbeslut. Ju.
14. Boende på (o)lika villkor – merkostnader i bostad med särskild service för vuxna enligt LSS. S.
15. Föreningsfrihet och terroristorganisationer. Ju.
16. En väl fungerande ordning för val och beslutsfattande i kommuner och regioner. Fi.
17. Ett moderniserat konsumentskydd. Fi.
18. Bolags rörlighet över gränserna. Volym 1 & 2. Ju.
19. En stärkt försörjningsberedskap för hälso- och sjukvården. Del 1 och 2. S.
20. Ecris-TCN – ett mer effektivt utbyte av brottmålsdomar mot tredjelandsmedborgare. Ju.
21. En klimatanpassad miljöbalk för samtiden och framtiden. M.
22. Hårdare regler för nya nikotinprodukter. S.
23. Stärkt planering för en hållbar utveckling. Fi.
24. Äga avfall – en del av den cirkulära ekonomin. M.
25. Struktur för ökad motståndskraft. Ju.
26. Använd det som fungerar. M.
27. Ett förbud mot rasistiska organisationer. Ju.
28. Immunitet för utställningsföremål. Ku.
29. Ökade möjligheter att förhindra illegal handel via post. I.
30. Kampen om tiden – mer tid till lärande. U.
31. Kontroller på väg. I.
32. Papper, poddar och ... Pliktmateriallagstiftning för ett tryggat källmaterial. U.
33. En tioårig grundskola. Införandet av en ny årskurs 1 i grundskolan, grundsärskolan, specialskolan och sameskolan. U.
34. Börja med barnen! En sammanhållen god och nära vård för barn och unga. S.
35. En stärkt rättsprocess och en ökad lagföring. Ju.

36. Gode män och förvaltare – en översyn. Ju.
37. Stärkt rätt till personlig assistans. Ökad rättssäkerhet för barn, fler grundläggande behov och tryggare sjukvårdande insatser. S.
38. En ny lag om ordningsvakter m.m. Ju.
39. Ombuds tillgång till vård- och omsorgsuppgifter och förenklad behörighetskontroll inom vården. S.
40. Mervärdesskatt vid inhyrd personal för vård och social omsorg. Fi.
41. VAB för vårdåtgärder i skolan. S.
42. Stärkta åtgärder mot penningtvätt och finansiering av terrorism. Fi.
43. Ett förstärkt skydd mot sexuella kränkningar. Ju.
44. Tillgänglighetsdirektivet. S.
45. En EU-anpassad djurläkemedelslagstiftning. Del 1 och 2. N.
46. Snabbare lagföring – ett snabbförfarande i brottmål. Ju.
47. Ett nytt regelverk för bygglov. Del 1 och 2. Fi.
48. I en värld som ställer om. Sverige utan fossila drivmedel 2040. M.
49. Kommuner mot brott. Ju.
50. Fri hyressättning vid nyproduktion. Ju.
51. Skydd av arter – vårt gemensamma ansvar. Vol. 1 och 2. M.
52. Vilja välja vård och omsorg. En hållbar kompetensförsörjning inom vård och omsorg om äldre. S.
53. En rättssäker vindkraftsprövning. M.
54. Ändrade regler i medborgarskapslagen. Ju.
55. Mikroföretagarkonto – schabloniserad inkomstbeskattning för de minsta företagen. Fi.
56. Nya regler om utländska föräldraskap och adoption i vissa fall. Ju.
57. Om folkbokföring, samordningsnummer och identitetsnummer. Fi.
58. Läge och kvalitet i hyressättningen. Ju.
59. Vägen till tillgänglighet – långsiktig, strategisk och i samverkan. S.
60. Förenklingar för mikroföretag och modernisering av bokföringslagen. N.
61. Utvisning på grund av brott – ett skärpt regelverk. Ju.
62. Användning av e-legitimation i tjänsten i den offentliga förvaltningen. I.
63. Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem. Fö.

Statens offentliga utredningar 2021

Systematisk förteckning

Finansdepartementet

En väl fungerande ordning för val och beslutsfattande i kommuner och regioner. [16]

Ett moderniserat konsumentskydd. [17]

Stärkt planering för en hållbar utveckling. [23]

Mervärdesskatt vid inhyrd personal för vård och social omsorg. [40]

Stärkta åtgärder mot penningtvätt och finansiering av terrorism. [42]

Ett nytt regelverk för bygglov. Del 1 och 2. [47]

Mikroföretagarkonto – schabloniserad inkomstbeskattning för de minsta företagen. [55]

Om folkbokföring, samordningsnummer och identitetsnummer. [57]

Försvarsdepartementet

Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem. [63]

Infrastrukturdepartementet

Säker och kostnadseffektiv it-drift rättsliga förutsättningar för utkontraktering. [1]

Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen. [9]

Ökade möjligheter att förhindra illegal handel via post. [29]

Kontroller på väg. [31]

Användning av e-legitimation i tjänsten i den offentliga förvaltningen. [62]

Justitiedepartementet

Krav på kunskaper i svenska och samhällskunskap för svenskt medborgarskap. [2]

Ett förbättrat system för arbetskraftsinvandring. [5]

Förstärkt skydd för väljarna vid röstmottagningen. [7]

Andra chans för krisande företag – En ny lag om företagsrekonstruktion. [12]

En teknikneutral grundlagsbestämmelse för regeringsbeslut. [13]

Föreningsfrihet och terroristorganisationer. [15]

Bolags rörlighet över gränserna. Volym 1 & 2. [18]

Ecris-TCN – ett mer effektivt utbyte av brottmålsdomar mot tredjelandsmedborgare. [20]

Struktur för ökad motståndskraft. [25]

Ett förbud mot rasistiska organisationer. [27]

En stärkt rättsprocess och en ökad lagföring. [35]

Gode män och förvaltare – en översyn. [36]

En ny lag om ordningsvakter m.m. [38]

Ett förstärkt skydd mot sexuella kränkningar. [43]

Snabbare lagföring – ett snabbförfarande i brottmål. [46]

Kommuner mot brott. [49]

Fri hyressättning vid nyproduktion. [50]

Ändrade regler i medborgarskapslagen. [54]

Nya regler om utländska föräldraskap och adoption i vissa fall. [56]

Läge och kvalitet i hyressättningen. [58]

Utvisning på grund av brott – ett skärpt regelverk. [61]

Kulturdepartementet

Immunitet för utställningsföremål. [28]

Miljödepartementet

Radiologiska skador – skadestånd, säkerheter, skadereglering. [10]

En klimatanpassad miljöbalk för samtiden och framtiden. [21]

Äga avfall
– en del av den cirkulära ekonomin. [24]

Använd det som fungerar. [26]

I en värld som ställer om.
Sverige utan fossila drivmedel 2040. [48]

Skydd av arter – vårt gemensamma ansvar. Vol. 1 och 2. [51]

En rättssäker vindkraftsprövning. [53]

Näringsdepartementet

En EU-anpassad djurläkemedelslagstiftning. Del 1 och 2. [45]

Förenklingar för mikroföretag och modernisering av bokföringslagen. [60]

Socialdepartementet

Informationsöverföring inom vård och omsorg. [4]

God och nära vård. Rätt stöd till psykisk hälsa. [6]

När behovet får styra
– ett tandvårdssystem för en mer jämlik tandhälsa. Vol. 1 & Vol. 2, bilagor + Sammanfattning (häfte). [8]

Boende på (o)lika villkor – merkostnader i bostad med särskild service för vuxna enligt LSS. [14]

En stärkt försörjningsberedskap för hälso- och sjukvården. Del 1 och 2. [19]

Hårdare regler för nya nikotinprodukter. [22]

Börja med barnen! En sammanhållen god och nära vård för barn och unga. [34]

Stärkt rätt till personlig assistans. Ökad rättssäkerhet för barn, fler grundläggande behov och tryggare sjukvårdande insatser. [37]

Ombuds tillgång till vård- och omsorgsuppgifter och förenklad behörighetskontroll inom vården. [39]

VAB för vårdåtgärder i skolan. [41]

Tillgänglighetsdirektivet. [44]

Vilja välja vård och omsorg.
En hållbar kompetensförsörjning inom vård och omsorg om äldre. [52]

Vägen till ökad tillgänglighet – långsiktig, strategisk och i samverkan. [59]

Utbildningsdepartementet

Skolbibliotek för bildning och utbildning. [3]

Bättre möjligheter för elever att nå kunskapskraven – aktivt stöd- och elevhälsoarbete samt stärkt utbildning för elever med intellektuell funktionsnedsättning. [11]

Kampen om tiden
– mer tid till lärande. [30]

Papper, poddar och ...
Pliktmateriallagstiftning för ett tryggat källmaterial. [32]

En tioårig grundskola. Införandet av en ny årskurs 1 i grundskolan, grundsärskolan, specialskolan och sameskolan. [33]



Regeringskansliet

103 33 Stockholm Växel 08-405 10 00 www.regeringen.se

ISBN 978-91-525-0178-8 ISSN 0375-250X

Omslag: Elanders Sverige AB
Bild: Jackie Niam och Luerat Satichob
Bild och bildbearbetning:
Agneta S Öberg