Regionrådsberedningen

SKRIVELSE
2021-12-01

RS 2021-0750

Regionstyrelsen

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

Föredragande regionråd: Irene Svenonius

Ärendebeskrivning

Region Stockholm har beretts möjlighet att lämna yttrande över betänkande från Cybersäkerhetsberedningens ”Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem” (SOU 2021:63).

Förslag till beslut

Regionrådsberedningen föreslår att regionstyrelsen beslutar följande.

> Regiondirektörens tjänsteutlåtande utgör Region Stockholms yttrande över betänkandet Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63).

Regionrådsberedningens motivering

Regionstyrelsen har beretts möjlighet att lämna yttrande över betänkande från Cybersäkerhetsberedningens ”Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem” (SOU 2021:63).

I syfte att göra användningen av ett informationssystem i säkerhetskänslig verksamhet säkrare, vilket anses stärka skyddet för Sveriges säkerhet, föreslår utredningen överföring av säkerhetsskyddsförordningens bestämmelser om förberedande åtgärder inför driftsättning av informationssystem till säkerhetsskyddslagen med tillkommande reglering.

För Region Stockholms samhällsviktiga och integritetskänsliga verksamheter är cybersäkerhet oerhört viktigt. Regionrådsberedningen delar därför regionledningskontorets bedömning att de föreslagna åtgärderna och författningsändringarna är positiva, trots att de innebär en viss påverkan av det kommunala självstyret. Regionrådsberedningen tillstyrker sålunda betänkandets förslag till författningsändringar.

Beslutsunderlag

1. Regiondirektörens tjänsteutlåtande

2. Sammanfattning av SOU 2021:63, Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem
3. Karolinska universitetssjukhuset yttrande den 21 oktober 2021
4. Stockholms läns sjukvårdsområdes yttrande den 20 oktober 2021
5. Fastighets- och servicenämndens yttrande den 28 oktober 2021

Irene Svenonius

Regionledningskontoret
Vesna Lucassi

TJÄNSTEUTLÅTANDE
2021-11-08

RS 2021-0750

Regionstyrelsen

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

Regionledningskontorets förslag till beslut

Regionrådsberedningen föreslår att regionstyrelsen beslutar följande.

> Regiondirektörens tjänsteutlåtande utgör Region Stockholms yttrande över betänkandet Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63).

Sammanfattning

Region Stockholm har beretts möjlighet att lämna yttrande över betänkande från Cybersäkerhetsberedningens ”Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem” (SOU 2021:63).

För att göra användningen av ett informationssystem i säkerhetskänslig verksamhet säkrare, och därmed stärka skyddet för Sveriges säkerhet, föreslår utredningen överföring av säkerhetsskyddsförordningens bestämmelser om förberedande åtgärder inför driftsättning av informationssystem till säkerhetsskyddslagen med tillkommande reglering. Åtgärder som föreslås berör driftsättning och väsentlig förändring av informationssystem i säkerhetskänslig verksamhet, bl.a. krav på godkännande, särskild säkerhetsskyddsbedömning och lämplighetsprövning, liksom utvidgad samrådsskyldighet. Samrådsmyndigheterna (Säkerhetspolisen och Försvarsmakten) föreslås ges möjligheter att besluta åtgärdsföreägganden och att förbjuda en ur säkerhetsskyddssynpunkt olämplig driftsättning eller förändring av informationssystem.

Region Stockholm tillstyrker betänkandets förslag till författningsändringar.

Bakgrund

Europeiska unionen (EU) har antagit ett antal strategier, policys och förordningar för att stärka cybersäkerheten i unionen och medlemsstaterna.[1] Det huvudsakliga

[1] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av

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. [2]

Utredningen överlämnade sitt delbetänkande Kompletterande bestämmelser till EU:s cybersäkerhetsakt (SOU 2020:25). Riksdagen har fattat beslut om att lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt ska träda i kraft den 28 juni 2021.[3] I lagen finns kompletterande nationella bestämmelser om bl.a. nationell myndighet för cybersäkerhetscertifiering, tillsyn, sanktioner och förfarandet vid cybersäkerhetscertifiering.

Utredningens uppdrag 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[4] 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 konstaterar 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.

För att göra användningen av ett informationssystem i säkerhetskänslig verksamhet säkrare, och därmed stärka skyddet för Sveriges säkerhet, föreslår utredningen ändringar i säkerhetsskyddslagen, bl.a. överföring av bestämmelser från säkerhetsskyddsförordningen till säkerhetsskyddslagen, samt utvidgad samrådsskyldighet och möjligheter att besluta åtgärdsföreläggande och förbud mot driftsättning av informationssystem i säkerhetskänslig verksamhet.

Föreslagna ändringar innebär bl.a. följande åtgärder.

---

informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) trädde i kraft den 27 juni 2019.

[2] Åtgärder som bl.a. rör försvar och nationell säkerhet faller utanför EU:s kompetens (art. 4.2 EU-fördraget).

[3] Lag (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.
Förordning (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt

[4] För nätverks- och informationssystem som används i eller har betydelse för säkerhetskänslig verksamhet finns i dag särskilda krav i säkerhetsskydds-förordningen (2018:658). 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.

- Säkerhetsskyddsförordningens bestämmelser om förberedande åtgärder inför driftsättning av informationssystem ska överföras till säkerhetsskyddslagen.
- Befintligt krav på verksamhetsutövare att göra en särskild säkerhets-skyddsbedömning 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 säkerhetsskydds-bedömningen, 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 ansvarig tillsynsmyndighet (Säkerhetspolisen).
- 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 verksamhets-utövaren att vidta en säkerhetsskyddsåtgärd i berört informationssystem.
- Samrådsmyndigheterna ska även få möjlighet att förbjuda en ur säkerhetsskyddssynpunkt olämplig driftsättning eller förändring 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.

Utredningen föreslår 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.

Lagändringarna föreslås träda i kraft 2022-07-01.

Fastighets- och servicenämnden, Trafiknämnden, Karolinska universitetssjukhuset och Stockholms läns sjukvårdsområde (SLSO) har beretts möjlighet att lämna synpunkter på betänkandet.

Karolinska universitetssjukhuset har i yttrande 2021-10-21 avstått från att lämna specifika synpunkter.

SLSO har i beslut 2021-10-20, § 9, påtalat att förslagen för SLSO:s del bedöms vara av begränsad betydelse. Bedömningen är att de förslag som utredningen presenterar är bra och skulle innebära en trygghet och säkerhet i arbetet med att driftsätta ett system som är av betydelse för Sveriges säkerhet.

Fastighets- och servicenämnden har genom tjänstemannayttrande på delegation från nämnden 2021-10-28 ställt sig positiva till utredningens förslag, men menar också att konsekvenserna för regioner inte är tillräckligt utredda. Förvaltningen ser en risk för administrativa kostnader och ökade ledtider. Förvaltningen lyfter även behovet av begreppsförtydliganden och vägledningar, och betonar vikten av beställarkompetens och expertis i framtida upphandlingar.

Trafiknämnden har vid remisstidens utgång inte inkommit med yttranden.

Region Stockholms yttrande
Regionledningskontoret är positiva till utredningens förslag och tillstyrker betänkandets förslag till författningsändringar.

Med den tilltagande digitaliseringen och globaliseringen skapas nya former för kommunikation och informationslagring i snabb takt, och med det nya hot och risker mot offentliga och privata aktörer. Region Stockholm noterar den av utredningen framförda bedömningen att den föreslagna regleringen i viss mån påverkar den kommunala självstyrelsen, och tillstyrker utredningens bedömning att författningsändringarna är nödvändiga för att skydda de mest skyddsvärda verksamheterna i samhället.

Ekonomiska konsekvenser
Regionstyrelsens beslut innebär inga ekonomiska konsekvenser.

De ekonomiska konsekvenserna av utredningens förslag bedöms troligen vara begränsade och bör ställas mot det stärkta skydd som förslagna

författningsändringar medför för de mest skyddsvärda verksamheterna i Sverige.

Carina Lundberg Uudelepp
Regiondirektör

Susanne Bayard
IT-direktör

Beslutsunderlag

1. Sammanfattning av SOU 2021:63, Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem
2. Karolinska universitetssjukhuset yttrande den 21 oktober 2021
3. Stockholms läns sjukvårdsområdes yttrande den 20 oktober 2021
4. Fastighets- och servicenämndens yttrande den 28 oktober 2021

Beslutsexpediering

1. Karolinska universitetssjukhuset
2. Stockholms läns sjukvårdsområde
3. Fastighets- och servicenämnden

Godkänd av Carina Lundberg Uudelepp, 2021-11-08

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.

KAROLINSKA UNIVERSITETSSJUKHUSET

2021-10-21 Dnr K2021-7823

Regionsledningskontoret
registrator.rlk@sll.se
Box 22550
104 22 Stockholm

Yttrande över remiss Sveriges säkerhet - behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63), RS 2021-0750

Karolinska Universitetssjukhuset tackar för möjligheten att lämna yttrande över rubricerad remiss och önskar inte lämna några specifika synpunkter.

Beslut om detta yttrande har fattats av sjukhusdirektören på delegation av styrelsen för Karolinska Universitetssjukhuset. Yttrandet har föredragits av säkerhetschef Håkan Borgström och samråd har skett med informationssäkerhetssamordnare Bill Heiding.

Beslutat dag som ovan

Björn Zoëga
Sjukhusdirektör

Delges: Styrelsen för Karolinska Universitetssjukhuset (anmälan), Registrator K

Region Stockholm

Stockholms läns sjukvårdsområde
Nämnd

Utdrag
PROTOKOLL 7/2021
Sammanträdesdatum
2021-10-20

Justerat onsdagen den 20 oktober 2021

Protokollet anslogs torsdagen den 21 oktober 2021

Justerare: Barbro Naroskyin Ann-Christine Jenvén

---

§ 9
Yttrande över Remiss – Sveriges säkerhet - behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)
SLSO 2021-2620, RS 2021-0750

Nämnden för Stockholms läns sjukvårdsområde beslutade

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

att förklara paragrafen omedelbart justerad.

Vid protokollet
Annika Jerhamre, nämndsekreterare

Utdragsbestyrkande

.....
Annika Jerhamre, nämndsekreterare

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

Serviceförvaltningen
Fastighetsförvaltningen

YTTRANDE

2021-10-28

RS 2021-0750
FSN 2021-0405

Regionledningskontoret
registrator.rlk@regionstockholm.se

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

Ärendebeskrivning

Ärendet är ett tjänstemannayttrande och utgör fastighets- och servicenämndens yttrande över slutbetänkandet Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63).

Sammanfattning

Fastighets- och servicenämnden har beretts möjlighet att yttra sig över slutbetänkandet Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63). Betänkandet omfattar förslag på ändringar i säkerhetsskyddslagen med syftet att förbättra säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet.

Yttrandet görs som ett tjänstemannayttrande på delegation från nämnden då tillräcklig tid för nämndbehandling inte funnits. Förvaltningen ser positivt på utredningens förslag till författningsändringar. Dock menar förvaltningen att konsekvenserna inte är tillräckligt utredda för regioner och menar att det finns risk för administrativa kostnader och ökade ledtider. Förvaltningen lyfter i sitt yttrande också behovet av begreppsförtydliganden och vägledningar.

Bakgrund

Med anledning av EU:s cybersäkerhetsakt har den s.k. cyberhetsutredningen i sin första del analyserat och lämnat förslag på kompletterande nationella bestämmelser om cybersäkerhetscertifiering (SOU2020:58), och i sin andra del övervägt om det finns behov av att stärka säkerheten i nätverks- och informationssystem i säkerhetskänslig verksamhet.

Utredningen föreslår 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 att gemensamt ta

fram hot-, sårbarhets- och riskbedömningar samt skyddsprofiler för olika IKT-produkter, -tjänster och -processer som ska användas i nätverks- och informationssystem i säkerhetskänslig verksamhet.
I slutbetänkandet, framgår utredningens förslag av ändringar i säkerhetsskyddslagen, bl.a genom att säkerhetsskyddsförordningens bestämmelser om förberedande åtgärder inför driftsättning av informationssystem överförs till säkerhetsskyddslagen med tillägg av konkretiserande regleringar.

De föreslagna lagändringarna innebär skyldighet för verksamhetsutövare att göra en särskild dokumenterad lämplighetsprövning samt särskild säkerhetsskyddsbedömning inför planerade och väsentliga förändringar av informationssystem som har betydelse för säkerhetskänslig verksamhet innan driftsättning. Lämplighetsprövningarna, föreslås liksom den särskilda säkerhetsskyddsbedömningen, samrådas med tillsynsmyndigheten (Säkerhetspolisen), godkännas och dokumenteras. Verksamhetsutövarens skyldighet att samråda med samrådsmyndigheten föreslås att inte begränsas i form av en skriftlig process. Om lämplighetsprövningen leder till bedömningen att det planerade förfarandet är olämpligt, ska det inte inledas.

Vidare föreslås att samrådsmyndigheterna får möjlighet att förbjuda en ur säkerhetsskyddssynpunkt olämplig driftsättning eller förändring av informationssystem och besluta om sanktionsavgift mot den som åsidosätter samrådsskyldigheten eller agerar i strid med meddelat förbud. För den verksamhetsutövare som meddelas förbud mot en planerad driftsättning eller förändring av informationssystem, framgår det i slutbetänkandet att det kan innebära att verksamhetsutövaren måste köpa en tjänst av en annan motpart som kräver högre ersättning. Lagregleringen innebär också att tillsynsmyndigheterna får en ny undersökningsbefogenhet genom möjligheten att få tillgång till verksamhetsutövares informationssystem.

Lagändringarna föreslås träda i kraft den 1 juli 2022.

Då det funnits kort om tid för att svara på remissen, och förslaget är relativt omfattande avges nämndens yttrande som ett tjänstemannayttrande med stöd av nämndens delegationsordning. Ärendet har beretts inom serviceförvaltningen i dialog med fastighetsförvaltningen. Yttrandet ska anmälas till fastighets- och servicenämnden vid nämndens nästkommande sammanträde.

Serviceförvaltningen
Fastighetsförvaltningen

YTTRANDE

2021-10-28

RS 2021-0750
FSN 2021-0405

Överväganden

Förvaltningen vill avge följande yttrande över remissen.

Med den tilltagande digitaliseringen och globaliseringen skapas nya former för kommunikation och informationslagring i snabb takt, och med det nya hot och risker mot offentliga och privata aktörer. Förvaltningen ser positivt på de lagändringar som föreslås för att stärka skyddet för Sveriges säkerhet och delar de förslag som framförs för att skärpa säkerhetsskyddslagstiftningen. Likaså är förvaltningen positiva till förslaget om formerna för arbetet med en nationell gemensam hot-, sårbarhets- och riskbedömning.

Förvaltningen menar också att utredningens konsekvensanalys inte i tillräcklig omfattning belyser kostnaderna för regioner och hade önskat se en mer genomarbetad konsekvensanalys i denna del. Förvaltningen menar att en mer djupgående konsekvensanalys skulle kunna visat att resurstillskott är nödvändigt i fler perspektiv än de som framgår av utredningen. Förvaltningen ser även behov av kompetens och vägledning som stödjer arbetet vid bedömningar och som säkerställer effektivitet i samrådsprocessen och i det förberedande arbetet inför driftsättningar.

Nedan följer mer detaljerade synpunkter på områden som berör förvaltningens verksamhet.

17.5 Förslaget om en stärkt samrådsroll

Konsekvenser för verksamhetsutövare

Förvaltningen ser positivt på samrådsförfarandet och verksamhetsutövares skyldigheter inför driftsättning, men vill samtidigt betona vikten av att samrådsmyndigheter får rätt kapacitet och förutsättningar att samråda med verksamhetsutövare. Om lagregleringen medför långa handläggningstider i samråd och lämplighetsprövning ser nämnden påtagliga risker för konsekvenser för verksamhetsutövaren. Förvaltningen vill också lyfta potentiell risk, att ökad administration och kostnader kan medföras förknippat med detta.

Verksamhetsutövare ska pröva och genomföra bedömningar om driftsättning eller förändring av nätverks- och informationssystem, är lämpligt från säkerhetsskyddspunkt och samråda med centralt utpekad myndighet. Förvaltningen önskar lyfta behovet av vägledning till verksamhetsutövare i denna del. Förvaltningen ser också behov av utvecklade kompetenser, arbetsprocesser och sambedömningar med nämnder och bolag för att fortsatt

stärka en god och patientsäker vård.

Vidare önskar förvaltningen lyfta behovet av att konkretisera lagstiftningens definition av vad som avses med *förändring* av informationssystem samt att det tydligt definieras vad som avses och innefattas med *begreppet* informationssystem. Vägledningar i dessa delar skulle underlätta implementering av lagstiftningen och effektivisera samrådsprocessen, liksom minska risken för varierad tolkning av definitionen.

Förvaltningen ser också att det är av betydelse att lyfta vikten av rätt beställarkompetens och expertis inom området vid framtida upphandlingar. Bedömningen är att de ökade upphandlingskraven initialt kommer att begränsa antalet anbudsgivare vilket under en övergångsperiod kan påverka konkurrensen.

Det finns en risk att utredningens förslag kan medföra ökade kostnader beroende på hur omfattande arbete och tidsåtgång som kommer att krävas i samråds- och godkännandeprocessen.

Ekonomiska konsekvenser

De ekonomiska konsekvenserna av utredningens förslag är för förvaltningen är svårbedömda. Utredningens förslag kan komma att innebära ökade administrativa kostnader. Sådana merkostnader är en del av en generellt höjd ambitionsnivå inom totalförsvar och säkerhetsskyddsarbete i Sverige. Den aktuella lagstiftens påverkan på kostnader bör tas i beaktande när statsbidrag för regionernas arbete med totalförsvarsfrågor utformas.

Stefan Schildt	Anette Henriksson
Förvaltningschef	Förvaltningschef
Serviceförvaltningen	Fastighetsförvaltningen

Region Stockholm