Yttrande över betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36)

28

LS 2017-0831

Landstingsrådsberedningen

SKRIVELSE
2017-08-16

LS 2017-0831

Landstingsstyrelsen

Yttrande över betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster

Föredragande landstingsråd: Daniel Forslund

Ärendebeskrivning

Justitiedepartementet har genom remiss bjudit in Stockholms läns landsting att lämna synpunkter på betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36).

Förslag till beslut

Landstingsrådsberedningen föreslår landstingsstyrelsen besluta

att avge yttrande till Justitiedepartementet över betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36) i enlighet med landstingsdirektörens förslag till yttrande

att omedelbart justera beslutet.

Landstingsrådsberedningens motivering

Stockholms läns landsting tar de aktuella frågorna kring IT-säkerhet på stort allvar, och har under de senaste åren stegvis skärpt både rutiner och styrdokument samt tydliggjort ledningsansvaret för dessa frågor. Ökad digitalisering, informationsdelning och ett förändrat omvärldsläge gör att samhällets behov av informations- och cybersäkerhet ökar. Stockholms läns landsting välkomnar därför att utredningen föreslår flera förändringar som förbättrar säkerhetskraven och incidentrapporteringen för samhällsviktiga och digitala tjänster.

Stockholms läns landsting ställer sig i allt väsentligt positivt till utredningens förslag men lämnar vissa synpunkter på områden som berör landstingets verksamhet. Det finns idag en omfattande mängd IT-system inom hälso- och sjukvården. På en rad områden försvåras värdefull utveckling av hälso- och sjukvården av att lagstiftningen inte är anpassad

till de förändringar som hälso- och sjukvården genomgår eller till de nya möjligheter som skapas genom teknikutvecklingen.

Tydliga definitioner från lagstiftarens sida av vad som är särskilt skyddsvärda funktioner inom hälso- och sjukvården är viktigt för att Stockholms läns landsting ska kunna bedöma kravmässig tillämplighet i säkerhetskänslig verksamhet. Dessvärre är beskrivningarna i utredningen för de samhällsviktiga tjänsterna kring hälso- och sjukvård alltför vaga och övergripande.

Stockholms läns landsting föreslår därför att utredningen kompletteras med en fördjupad genomgång av vad som anses vara skyddsvärt inom hälso- och sjukvården, alternativt att MSB får i uppdrag att, tillsammans med Inspektionen för vård och omsorg, göra nödvändiga preciseringar av vilka delar av hälso- och sjukvården som träffas av de nya bestämmelserna.

Stockholms läns landsting ser positivt på utredningens förslag på incidentrapportering men ser en betydande risk för svårigheter för landstingen i samband med rapporteringen. Rapportering av allvarliga IT-incidenter behöver ske effektivt och utan dröjsmål. Det finns en risk för att en och samma incident kan kräva relativt många bedömningssteg för att klargöra och uppfylla rapporteringsskyldigheten till statliga myndigheter.

Stockholms läns landsting anser därför att det är viktigt att en fungerande rutin för landstingens rapportering etableras, så att identifierade risker kan rapporteras och åtgärdas så snabbt och effektivt som dagens snabba teknikutveckling kräver.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 24 juli 2017
Förslag till yttrande
Sammanfattning av betänkandet
betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36)

Irene Svenonius

Daniel Forslund

Gustaf Drougge

2017-07-24
LS 2017-0831

Landstingsstyrelsen
Landstingsstyrelsens förvaltning
SLL Informationssäkerhet
Vesna Lucassi

Landstingsstyrelsen

Yttrande över betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36)

Ärendebeskrivning
Justitiedepartementet har genom remiss bjudit in Stockholms läns landsting att lämna synpunkter på betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36).

Beslutsunderlag
Landstingsdirektörens tjänsteutlåtande den 24 juli 2017
Förslag till yttrande
Sammanfattning av betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36)

Förslag till beslut
Landstingsstyrelsen föreslås besluta

att avge yttrande till Justitiedepartementet över betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36) i enlighet med landstingsdirektörens förslag till yttrande

att omedelbart justera beslutet.

Förvaltningens förslag och motivering

Sammanfattning
Ärendet gäller yttrande över betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36). Utredningen behandlar frågan om hur det av Europaparlamentet och rådet antagna så kallade NIS-direktivet ska genomföras i svensk rätt och föreslår en ny lag och en ny förordning för vissa leverantörer av samhällsviktiga och digitala tjänster. Förslagen gäller vissa offentliga och enskilda verksamheter som

tillhandahåller samhällsviktiga tjänster inom sju skyddsvärda sektorer; däribland hälso- och sjukvård samt transporter. Även leverantörer av digitala tjänster omfattas av förslagen. Den nya lagen föreslås träda i kraft den 10 maj 2018. Förvaltningen ställer sig i allt väsentligt positivt till utredningens förslag men lämnar vissa synpunkter på områden som berör landstingets verksamhet.

Bakgrund

Betänkandets innehåll
Det av Europaparlamentet och rådet antagna så kallade NIS-direktivet fastställer åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverks- och informationssystem inom unionen. I betänkandet presenterar utredningen ett förslag på hur NIS-direktiv ska genomföras i svensk rätt.

Direktivet innehåller skyldigheter för varje medlemsstat att bland annat upprätta en förteckning över tjänster som är viktiga för att upprätthålla kritiskt samhällelig eller ekonomisk verksamhet, men även att identifiera de leverantörer som tillhandahåller dessa tjänster. Medlemsstaterna ska vidare utse myndigheter med särskilda uppgifter inom området, bland annat tillsynsmyndigheter och nationella kontaktpunkter för hantering av it-säkerhetsincidenter. Senast den 10 maj 2018 ska medlemsstaterna ha börjat tillämpa sina nya bestämmelser i lagar och författningar för att följa direktivet.

Utredningen föreslår i betänkandet en ny lag och en ny förordning för vissa leverantörer av samhällsviktiga och digitala tjänster: *Förslag till lag (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster* samt *Förslag till förordning (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster*. Verksamhet som är av betydelse för Sveriges säkerhet är undantagen från tillämpningsområdet.

Nedan följer en summering av betänkandets innehåll på utvalda områden (betänkandets kapitelindelning inom parentes).

Skyddsvärda sektorer och identifiering av leverantörer av samhällsviktiga tjänster (kap. 4 och kap. 6)
I betänkandet föreslås att Myndigheten för samhällsskydd och beredskap, MSB, ges i uppdrag att meddela föreskrifter (förteckning) om vilka tjänster

som är viktiga för att upprätthålla samhällsviktiga tjänster. För att en leverantör ska omfattas av direktivets bestämmelser och föreslagna författningskrav krävs att leverantören tillhandahåller en tjänst som finns på denna förteckning. Utgångspunkt för förteckningen är NIS-direktivets definition av vissa offentliga och enskilda verksamheter som tillhandahåller samhällsviktiga tjänster inom sju särskilt utpekade skyddsvärda sektorer (enligt i bilaga 2 till NIS-direktivet): energi, transporter, bank, finans-marknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur.

Säkerhetskrav (kap. 1 och kap. 7)
Betänkandet anger att det är verksamhetsutövaren som är ansvarig för att avgöra om denne omfattas av lagen. Verksamhetsutövaren åläggs enligt förslaget att genomföra en dokumenterad undersökning om tillhandahållen tjänst är beroende av nät eller informationssystem samt bedöma om en incident skulle kunna medföra en betydande störning enligt sektors-specifika och sektorsövergripande faktorer meddelade av tillsynsmyndighet.

I författningsförslaget ställs krav på leverantörer av samhällsviktiga tjänster att de ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

Såväl leverantörer av samhällsviktiga tjänster som leverantörer av digitala tjänster ska vidta ändamålsenliga tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem. Åtgärder ska även vidtas för att förebygga och minimera inverkan som säkerhetsincidenter.

Leverantörer av *digitala tjänster* ska utarbeta åtgärder för att hantera risker. Leverantörer av *samhällsviktiga tjänster* ska basera valet av säkerhetsåtgärder på dokumenterad riskanalys som ska uppdateras årligen och innehålla en åtgärdsplan.

Incidentrapportering och sekretess (kap. 11 och kap. 12)
I författningsförslaget ställs krav på att berörda leverantörer utan dröjsmål ska rapportera säkerhetsincidenter till CSIRT-enheten inom Myndigheten för samhällsskydd och beredskap. Rapporter ska innehålla information så att det blir möjligt för MSB att fastställa vilken gränsöverskridande inverkan incidenten har. Uppgifter som ska rapporteras omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400). Utredningen bedömer att befintliga bestämmelser är tillräckliga men föreslår vissa

ändringar för att skydda uppgifter om enskilds affärs- eller drifts-förhållande i samband med tillsyn.

Tillsyn och sanktioner (kap. 8 och kap. 9)
NIS-direktivet ställer krav på medlemsstaterna att utse en eller flera nationella behöriga myndigheter för säkerhet i nätverk och informations-system för minst de skyddsvärda sektorer som anges i bilaga 2 till NIS-direktivet. Tillsynsmyndigheterna ska ansvara för att övervaka att regelverket följs. För hälso- och sjukvården anges Inspektionen för vård och omsorg som tillsynsmyndighet. För transporter anges Transportstyrelsen. Tillsynsmyndigheten ska besluta att sanktionsavgift ska tas ut av den som underlåter att incidentrapportera eller att vidta säkerhetsåtgärder.

Vidare anges att MSB uppdras att leda ett samarbetsforum där samtliga tillsynsmyndigheter ska ingå samt ta emot tillsynsmyndighetens bedömning av brister i nätverk och informationssystem.

Överväganden
Förvaltningen välkomnar och ställer sig i allt väsentligt positivt till utredningens förslag. Förvaltningen lämnar dock i bilagt yttrande vissa synpunkter på betänkandet.

Identifiering av samhällsviktiga tjänster (kap. 4)
Utredningen ger en beskrivning av respektive skyddsvärd sektor som ska omfattas av de nya bestämmelserna. Beskrivningarna baseras dels på bilaga 2 till NIS-direktivet, dels på egna beskrivningar utifrån en inventering som genomförts efter att ha träffat företrädare för samtliga sektorer. Förvaltningen konstaterar att beskrivningarna är relativt precisa för flera av sektorerna, men vag och övergripande när det gäller hälso- och sjukvården.

Förvaltningen bedömer att de vaga beskrivningarna är olyckliga. Det existerar idag en omfattande mängd it-system och digitala tjänster inom hälso- och sjukvården. Landstinget står samtidigt inför en stor förändrings-process med framtidsplaner som omfattar stora satsningar på it och digitalisering. Redan idag uppstår problem till följd av att lagstiftningen inte är anpassad till de förändringar som hälso- och sjukvården genomgår, med ökande antal privata vårdgivare och större inslag av s.k. nätverks-sjukvård, där flera offentliga och privata vårdgivare samverkar kring vården av en patient.

Utöver detta finns det dessutom otydligheter från lagstiftarens sida gällande vad som är särskilt skyddsvärda funktioner inom hälso- och sjukvården. Det gör att landstingen många gånger har svårt att bedöma kravmässig tillämplighet i säkerhetskänslig verksamhet. Risken är därför stor att utredningens summariska genomgång av vad som är skyddsvärt inom sektorn hälso- och sjukvård kommer leda till problem när sedan landstingen ska identifiera vilka verksamheter som träffas av de nya bestämmelserna.

Förvaltningen föreslår därför i bilagt yttrande att utredningen kompletteras med en fördjupad genomgång av vad som anses vara samhällsviktigt och skyddsvärt inom hälso- och sjukvården. Om detta inte är möjligt är det önskvärt att istället MSB får i uppdrag att tillsammans med berörd tillsynsmyndighet, Inspektionen för vård och omsorg, göra nödvändiga preciseringar av vilka delar av hälso- och sjukvården som ska omfattas av bestämmelserna.

Incidentrapportering (kap. 8)
I betänkandet föreslår utredningen att leverantörer av samhällsviktiga tjänster och digitala tjänster utan dröjsmål ska rapportera alla allvarliga incidenter till CSIRT-enheten vid MSB. Förvaltningen ser positivt på detta förslag. En fungerande rutin för rapportering av allvarliga it-incidenter är av stor betydelse både ur ett nationellt perspektiv, för landstingen liksom för de enskilda förvaltningarna och bolagen inom Stockholms läns landsting. Förvaltningen ser dock en betydande risk för svårigheter för landstingen i samband med rapporteringen.

Förvaltningen bedömer att det kommer att krävas relativt många bedömningssteg för att uppfylla rapporteringsskyldigheten till statliga myndigheter i samband med allvarliga incidenter. Det skulle för landstingets del exempelvis kunna röra sig om CSIRT-enheten vid MSB (utredningens förslag), Säkerhetspolisen (säkerhetsskyddsförordningen), Datainspektionen (nya dataskyddsförordningen), Inspektionen för vård och omsorg (patientsäkerhetslagen) etc.

I bilagt förslag till yttrande föreslås att utredningen kompletteras med en analys av möjligheten att utarbeta former för samverkan mellan behöriga mottagande myndigheter i syfte att underlätta för rapporteringsskyldiga verksamheter i samband med att allvarliga incidenter inträffar. Det vore önskvärt om exempelvis MSB:s CSIRT-enhet får ett samordnande uppdrag

att bedöma vilka ytterligare myndigheter som behöver ta emot information om rapporterade incidenter samt tillse att så sker då behov uppstår.

Konsekvensanalys (kap. 13)
I betänkandet redogör utredningen för en konsekvensanalys och konstaterar att det är ett förändrat omvärldsläge som gör att samhällets behov av informations- och cybersäkerhet ökar, inte föreskrifterna i sig. Förvaltningen delar utredningens syn i detta avseende och står även bakom klargörandet att det i uppdraget att tillhandahålla en samhällsviktig tjänst även ingår att vidta grundläggande säkerhetsåtgärder.

Förvaltningen menar dock att utredningens konsekvensanalys är för grund och inte i tillräcklig omfattning belyser kostnaderna för landstingen. Förvaltningen skulle se positivt på en mer genomarbetad konsekvensanalys med fokus inte bara på tillsynsmyndigheter, domstolar och MSB som mottagare för incidentrapportering utan även på landstingen som samhällsviktiga aktörer. Förvaltningen menar att en mer djupgående konsekvensanalys skulle visa att resurstillskott är nödvändigt i fler perspektiv än de utpekade, och att de anslagsmöjligheter som utredningen hänvisar till, exempelvis anslaget 2:4 Krisberedskap, behöver ses över.

Ekonomiska konsekvenser
Beslutet har inga ekonomiska konsekvenser.

Malin Frenning
Landstingsdirektör

Mats Nomberg
Tillförordnad Direktör Strategisk IT SLL

Beslutsexpediering:
Akt
Justitiedepartementet
Landstingsdirektörens stab
Godkänd av Malin Frenning, 2017-08-16

Landstingsstyrelsen

YTTRANDE
2017-08-29

Diarienummer
LS 2017-0831

Justitiedepartementet
Ju2017/03997/L4

Yttrande över betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36)

Stockholms läns landsting har beretts möjlighet att yttra sig över betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36). Utredningen behandlar frågan om hur det så kallade NIS-direktivet ska genomföras i svensk rätt och föreslår en ny lag och en ny förordning för vissa leverantörer av samhällsviktiga och digitala tjänster.

Stockholms läns landsting välkomnar och ställer sig i allt väsentligt positivt till utredningens förslag. Landstinget önskar dock lämna följande synpunkter.

Beskrivning av sektorer och förteckning över samhällsviktiga tjänster (kap. 4)
Utredningens förslag gäller vissa offentliga och enskilda verksamheter som tillhandahåller samhällsviktiga tjänster inom sju skyddsvärda sektorer som anges i bilaga 2 till NIS-direktivet: energi, transporter, bank, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Utredningen föreslår att Myndigheten för samhällsskydd och beredskap, MSB, ska meddela föreskrifter om vilka tjänster som är samhällsviktiga för var och en av dessa sektorer. Skyldigheter att vidta säkerhetsåtgärder faller sedan ut på den som är ansvarig för en verksamhet som tillhandahåller en samhällsviktig tjänst som finns upptagen i MSB:s föreskrifter.

Utredningen ger i kapitel 4 en beskrivning av respektive sektor genom att återge dels vad som anges i bilaga 2 till NIS-direktivet, dels egna beskrivningar utifrån en inventering som genomförts efter att ha träffat företrädare för samtliga sektorer.

Stockholms läns landsting konstaterar att beskrivningarna är relativt precisa för flera av sektorerna, men vag och övergripande när det gäller hälso- och sjukvården (t.ex. sid. 76, sid. 103). Stockholms läns landsting menar att de vaga beskrivningarna är olyckliga och riskerar att skapa otydlighet i instruktionen till MSB och i de föreskrifter som MSB ska meddela.

Det existerar idag en omfattande mängd it-system och digitala tjänster inom hälso- och sjukvården. Behoven att modernisera och digitalisera ytterligare är stora för att möta kommande behov. Samtidigt försvåras på en rad områden värdefull utveckling av hälso- och sjukvården av att lagstiftningen inte är anpassad sig till de förändringar som hälso- och sjukvården genomgår, med ökande antal privata vårdgivare och större inslag av s.k. nätverkssjukvård, där flera offentliga och privata vårdgivare samverkar kring vården av en patient.

Otydligheter från lagstiftarens sida vad som dessutom är särskilt skyddsvärda funktioner inom hälso- och sjukvården skapar problem för landstingen att bedöma kravmässig tillämplighet i säkerhetskänslig verksamhet. Med utredningens vaga och övergripande genomgång riskerar svårigheterna att bli ännu större att identifiera vilka verksamheter som träffas av de nya bestämmelserna.

Stockholms läns landsting föreslår därför att utredningen kompletteras med en fördjupad genomgång av vad som anses vara samhällsviktigt och skyddsvärt inom hälso- och sjukvården. Om detta inte är möjligt är det önskvärt att istället MSB får i uppdrag att tillsammans med berörd tillsynsmyndighet, Inspektionen för vård och omsorg, göra nödvändiga preciseringar av vilka delar av hälso- och sjukvården som ska omfattas av bestämmelserna.

Incidentrapportering (kap. 8)
Utredningen föreslår att leverantörer av samhällsviktiga tjänster och av digitala tjänster utan dröjsmål ska rapportera alla incidenter som har en allvarlig inverkan på tillhandahållandet av tjänsten till CSIRT-enheten vid MSB. Utredningen anger vidare att rapporterna ska innehålla information så att det blir möjligt för MSB att fastställa vilken gränsöverskridande inverkan incidenten har (sid. 213).

Stockholms läns landsting ser positivt på utredningens förslag på incidentrapportering men ser en betydande risk för svårigheter för landstingen i samband med rapporteringen. Som landstinget uppfattar det finns det risk för att det vid en och samma incident kan komma att krävas relativt många bedömningssteg för att, utan dröjsmål efter upptäckt, klargöra och uppfylla rapporteringsskyldigheten till statliga myndigheter. Det skulle för landstingets del exempelvis kunna röra sig om CSIRT-enheten vid MSB (utredningens förslag), Säkerhetspolisen (säkerhets-skyddsförordningen), Datainspektionen (nya dataskyddsförordningen), Inspektionen för vård och omsorg (patientsäkerhetslagen) etc.

Stockholms läns landsting anser att en fungerande rutin för rapportering av allvarliga it-incidenter är av stor betydelse både ur ett nationellt perspektiv, för landstingen liksom för de enskilda förvaltningarna och bolagen inom Stockholms läns landsting. För att undvika oönskade konsekvenser behöver det framgå hur rapporteringen för landstingen ska gå till. Stockholms läns landsting föreslår att utredningen kompletteras med en analys av möjligheten att utarbeta former för samverkan mellan behöriga mottagande myndigheter i syfte att underlätta den administrativa bördan för rapporteringsskyldiga verksamheter. Landstinget skulle exempelvis se positivt på om CSIRT-enheten som nationell kontaktpunkt får i uppdrag att bedöma vilka ytterligare myndigheter som behöver ta emot information om en rapporterad incident samt tillse att så sker.

Konsekvensanalys (kap. 13)
När det gäller konsekvenserna i övrigt av förslagen för Stockholms läns landstinget är det, som anges i betänkandet, ett förändrat omvärldsläge som gör att samhällets behov av informations- och cybersäkerhet ökar, inte föreskrifterna i sig (sid.265). Landstinget delar utredningens syn på att det i uppdraget att tillhandahålla en samhällsviktig tjänst även ingår att vidta grundläggande säkerhetsåtgärder (sid. 275). Dock menar landstinget att utredningens konsekvensanalys är för grund och inte i tillräcklig omfattning belyser kostnaderna för landstingen.

Landstinget skulle se positivt på en mer genomarbetad konsekvensanalys med fokus inte bara på tillsynsmyndigheter, domstolar och MSB som mottagare för incidentrapportering utan även på landstingen som samhällsviktiga aktörer. Landstinget menar att en mer djupgående konsekvensanalys skulle visa att resurstillskott är nödvändigt i fler perspektiv än de utpekade.

Landstinget hade även gärna sett att utredningen genomlyst och givit förslag på vidareutveckling av fördelningen gällande medel ur anslag 2:4 Krisberedskap som nämns i utredningen (sid. 268), som ett sätt att skapa att skapa förutsättningar för snabbare förändringar i de samverkande processerna.

Sammanfattning

Bakgrund

I juli 2016 antog Europaparlamentet och rådet NIS-direktivet[1]. Direktivet fastställer åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen, i syfte att förbättra den inre marknadens funktion.

Direktivet innebär bland annat skyldigheter för vissa leverantörer av samhällsviktiga tjänster och vissa leverantörer av digitala tjänster att vidta säkerhetsåtgärder för att hantera risker samt förebygga och hantera incidenter i nätverk och informationssystem som de är beroende av för att tillhandahålla tjänsterna. Leverantörerna ska också rapportera incidenter som har en betydande respektive avsevärd inverkan på kontinuiteten i tjänsten.

För att en leverantör ska anses vara en sådan leverantör av samhällsviktiga tjänster som omfattas av direktivet krävs att leverantören bedriver verksamhet inom någon av de i direktivet särskilt utpekade enheterna. Enheterna finns inom sju angivna sektorer. Sektorerna omfattar energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Dessutom krävs att den tjänst som tillhandahålls är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Medlemsstaterna är skyldiga att dels upprätta en förteckning över de tjänster på medlemsstatens territorium som är viktiga för att

[1] 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.

upprätthålla kritisk samhällelig eller ekonomisk verksamhet, dels identifiera de leverantörer som tillhandahåller sådana tjänster.

De leverantörer av digitala tjänster som omfattas av direktivet är sådana som tillhandahåller internetbaserade marknadsplatser, internetbaserade sökmotorer eller molntjänster. Dessa leverantörer ska inte identifieras på det sätt som gäller för leverantörer av samhällsviktiga tjänster och omfattas av direktivet utan att någon bedömning ska göras av om de är samhällsviktiga eller inte.

Medlemsstaterna ska enligt direktivet utse myndigheter med särskilda uppgifter på området, till exempel tillsynsmyndigheter, nationella kontaktpunkter och enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter). Medlemsstaterna ska också säkerställa att tillsynsmyndigheterna har befogenheter och medel för att kontrollera att leverantörerna uppfyller sina skyldigheter samt fastställa regler om sanktioner för överträdelse av de nationella bestämmelserna som antagits enligt direktivet.

Direktivet innehåller vidare en skyldighet för varje medlemsstat att anta en nationell strategi för säkerhet i nätverk och informationssystem.

Medlemsstaterna ska senast den 9 maj 2018 anta och offentliggöra de bestämmelser i lagar och andra författningar som är nödvändiga för att följa direktivet. Bestämmelserna ska tillämpas från och med den 10 maj 2018.

Utredningens uppdrag

Utredningens uppdrag har varit att föreslå hur NIS-direktivet ska genomföras i svensk rätt. Detta har innefattat bland annat att föreslå hur direktivets krav på utpekande av myndigheter med ansvar för vissa funktioner ska genomföras, hur identifiering av och krav på leverantörer som omfattas av direktivet kan genomföras i ett samlat regelverk med beaktande av gällande bestämmelser, sektorsansvar och vad som är mest effektivt utifrån olika perspektiv, föreslå nödvändiga ändringar i offentlighets- och sekretesslagen (2009:400) för att känslig information i incidentrapporter ska kunna skyddas, och lämna nödvändiga författningsförslag.

Frågan om hur en nationell strategi för säkerhet i nätverk och informationssystem bör utformas har inte omfattats av uppdraget.

Utredningens förslag

Ett samlat regelverk – en ny lag och en ny förordning

Utredningen föreslår en ny lag och en ny förordning som till utformning och innehåll ligger nära NIS-direktivet. Regelverket ska tillämpas endast på sådana leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster som omfattas av direktivet. I den utsträckning det finns bestämmelser om säkerhetskrav eller incidentrapporteringskrav på de aktuella leverantörerna i annan lag som minst motsvarar bestämmelserna i den föreslagna lagen ska emellertid de bestämmelserna tillämpas. Om sådana krav finns i bindande EU-rättsakter (lex specialis) ska den föreslagna lagen inte tillämpas alls.

Vissa företag och leverantörer är uttryckligen undantagna från direktivets tillämpningsområde. Dessa omfattas följaktligen inte heller av den föreslagna lagen. Detta innebär att regelverket inte ska tillämpas på företag som omfattas av kraven i artiklarna 13a och 13b i direktiv 2002/21/EG, dvs. tillhandahållare av ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst. I NIS-direktivet anges dock internetknutpunkter uttryckligen som en sådan enhet som ska regleras enligt direktivet. Tillhandahållare av internetknutpunkter omfattas därför av den föreslagna lagen trots att de enligt svensk rätt anses som sådana företag som omfattas av artiklarna 13a och 13b.

Regelverket ska inte heller tillämpas på leverantörer av betrodda tjänster som omfattas av kraven i artikel 19 i förordning (EU) nr 910/2014 (eIDAS).

Även verksamhet som är av betydelse för Sveriges säkerhet är undantagen från tillämpningsområdet. Detta innebär till exempel att verksamhet som omfattas av säkerhetsskyddslagen inte omfattas. Incidenter som inträffar i sådan verksamhet ska därmed inte rapporteras enligt bestämmelserna i den föreslagna lagen, utan även fortsättningsvis rapporteras enligt 10 a § säkerhetsskyddsförordningen (1996:633).

Föreskrifter med förteckning över samhällsviktiga tjänster

För att leverantörer av samhällsviktiga tjänster ska kunna identifieras ska Myndigheten för samhällsskydd och beredskap meddela föreskrifter (förteckning) om vilka tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet (samhällsviktiga tjänster) för varje sektor som omfattas av NIS-direktivet.

Identifiering av leverantörer av samhällsviktiga tjänster

Det är i likhet med vad som gäller enligt säkerhetsskyddslagstiftningen verksamhetsutövaren som är ansvarig för att avgöra om denne omfattas av lagen. I detta syfte ska den som är ansvarig för en verksamhet som tillhandahåller en samhällsviktig tjänst som finns upptagen i de föreskrifter (förteckning) som Myndigheten för samhällsskydd och beredskap ska meddela, undersöka om tillhandahållandet av tjänsten är beroende av nätverk eller informationssystem och om en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Undersökningen ska dokumenteras. För att avgöra om en störning är betydande ska verksamhetsutövaren beakta vissa särskilda faktorer, bland annat det antal användare som är beroende av den aktuella tjänsten. Tillsynsmyndigheten får meddela föreskrifter om vilka sektorspecifika och sektoröverskridande faktorer som ska beaktas vid bedömningen av om en incident skulle medföra en betydande störning.

Säkerhetskrav och incidentrapportering

Såväl leverantörer av samhällsviktiga tjänster som leverantörer av digitala tjänster ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i deras nätverk och informationssystem. De ska också vidta lämpliga åtgärder för att förebygga och minimiera den inverkan som incidenter som påverkar säkerheten i deras nätverk och informationssystem har på de tjänster som tillhandahålls. Syftet med sistnämnda åtgärder är att säkerställa kontinuiteten i tjänsterna.

Leverantörer av digitala tjänster ska själva utarbeta åtgärder för att hantera risker. De ska i det arbetet beakta vissa i lagen angivna faktorer. Leverantörer av samhällsviktiga tjänster ska i stället göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder. I analysen, som ska dokumenteras och uppdateras årligen, ska en åtgärdsplan ingå. Tillsynsmyndigheten får också meddela föreskrifter om utformingen av säkerhetsåtgärderna. Leverantörer av samhällsviktiga tjänster ska också bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

Både leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster ska utan onödigt dröjsmål rapportera incidenter till CSIRT-enheten (se nedan) vid Myndigheten för samhällsskydd och beredskap. Leverantörer av samhällsviktiga tjänster ska rapportera incidenter som har en betydande inverkan på kontinuiteten i tjänsten, medan leverantörer av digitala tjänster ska rapportera incidenter som har en avsevärd inverkan på tillhandahållandet av tjänsten. I lagen anges ett antal faktorer som framför allt ska beaktas vid bedömningen av om incidenten har en sådan inverkan att den ska rapporteras.

Tillsynsmyndigheten får meddela närmare föreskrifter om faktorer som ska beaktas vid bedömningen av om en incident har betydande inverkan. Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om rapportering av incidenter och om förutsättningarna för frivillig incidentrapportering.

Tillsyn

För varje sektor och för de digitala tjänster som omfattas av lagen ska en tillsynsmyndighet ansvara för att övervaka att regelverket följs. Följande myndigheter föreslås vara tillsynsmyndigheter.

Sektor	Tillsynsmyndighet
Energi	Statens energimyndighet
Transporter	Transportstyrelsen
Bankverksamhet	Finansinspektionen
Finansmarknadsinfrastruktur	Finansinspektionen
Hälso- och sjukvård	Inspektionen för vård och omsorg
Leverans och distribution av dricksvatten	Livsmedelsverket
Digital infrastruktur	Post- och telestyrelsen

Digitala tjänster	Tillsynsmyndighet
Digitala tjänster	Post- och telestyrelsen

Vid tillsyn ska leverantören tillhandahålla tillsynsmyndigheten den information som behövs för en bedömning av säkerheten i leverantörens nätverk och informationssystem. Leverantörer av samhällsviktiga tjänster är skyldiga att tillhandahålla även bevis för att säkerhetsprinciper har genomförts effektivt.

Beträffande leverantörer av digitala tjänster får tillsynsåtgärder vidtas bara i efterhand, när tillsynsmyndigheten har fått kännedom om att leverantören inte uppfyller säkerhetskraven eller kravet att incidentrapportera.

Tillsynsmyndigheten ska försöka få en leverantör som inte följer regelverket att rätta sig. Tillsynsmyndigheten får meddela föreläggganden, dels i syfte att få tillgång till viss information som behövs för tillsynen, dels för att få leverantören att följa regelverket. Ett föreläggande får förenas med vite.

Myndigheten för samhällsskydd och beredskap ska inom ramen för sitt nuvarande uppdrag ha en samlad bild av NIS-direktivets genomförande och tillämpning i Sverige genom att leda ett samarbetsforum där samtliga tillsynsmyndigheter ska ingå samt ta emot tillsynsmyndighetens bedömning av brister i nätverk och informationssystem. I bedömningen bör ingå brister som upptäcks vid tillsyn men även svårigheter vid tillämpning och tolkning av regelverket. Myndigheten för samhällsskydd och beredskap ska vidare tillhandahålla tillsynsmyndigheterna det metodstöd för tillsyn som behövs för en effektiv tillsyn enligt det föreslagna regelverket.

Sanktionsavgift

Tillsynsmyndigheten ska besluta att sanktionsavgift ska tas ut av den som underlåter att incidentrapportera eller att vidta säkerhetsåtgärder. Vid bedömningen av avgiftens storlek ska tillsynsmyndigheten ta särskild hänsyn till skada eller risk för skada som uppstått till följd av överträdelsen, om leverantören tidigare har begått en överträdelse samt de kostnader som leverantören har undvikit till följd av överträdelsen. Sanktionsavgiften får under vissa förhållanden efterges helt eller delvis.

Nationell kontaktpunkt, samarbetsgrupp och CSIRT-enhet

För att underlätta gränsöverskridande samarbete och för att möjliggöra ett effektivt genomförande av NIS-direktivet ska det i varje medlemsstat finnas en *nationell gemensam kontaktpunkt*. Den nationella kontaktpunkten ska ansvara för samordningen av frågor angående nätverk och informationssystem och för gränsöverskridande samarbete på unionsnivå. Den nationella kontaktpunkten ska också lämna en sammanfattande rapport om antalet ingivna incidentrapporter och om de rapporterade incidenternas art till samarbetsgruppen.

Samarbetsgruppen syftar till att stödja och underlätta strategiskt samarbete mellan medlemsstaterna vad gäller säkerhet i nätverk och informationssystem. Gruppen ska bland annat utbyta bästa praxis i olika avseenden. Utöver företrädare för medlemsstaterna består gruppen av representanter från kommissionen och från Europeiska unionens byrå för nät- och informationssäkerhet (Enisa).

I varje medlemsstat ska det enligt NIS-direktivet också finnas en eller flera *enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter)*. CSIRT-enheten ska bland annat övervaka incidenter på nationell nivå och tillhandahålla tidiga varningar m.m. till relevanta aktörer om risker och incidenter. CSIRT-enheten ska också delta i ett CSIRT-nätverk inom unionen.

Utredningens förslag innebär att Myndigheten för samhällsskydd och beredskap ska vara både nationell kontaktpunkt och CSIRT-enhet samt representera Sverige i samarbetsgruppen. Myndigheten för samhällsskydd och beredskap har redan i dag ett sådant uppdrag samt den struktur och kompetens som krävs för detta.

Sekretess

Befintliga bestämmelser om sekretess omfattar uppgifter som ska rapporteras och delas med anledning av incidenter samt tillhandahållas i samband med tillsyn. Det har inte framkommit några exempel på att den nuvarande regleringen är otillräcklig. Det finns därmed inte skäl att införa starkare sekretess för uppgifter som lämnas inom ramen för incidentrapporteringen.

Till följd av tillsynen kan tillsynsmyndigheterna emellertid få del av känsliga uppgifter om enskilds affärs- eller driftförhållande. För att sistnämnda uppgifter ska kunna skyddas behöver sekretessförordningen ändras så att sekretess för sådana uppgifter gäller i verksamhet som består i tillsyn enligt det föreslagna regelverket.

Konsekvenser

NIS-direktivets genomförande kommer initialt att innebära kostnader för de föreslagna tillsynsmyndigheterna. Kostnaderna kan till viss del, i vart fall på lång sikt, finansieras genom de samhällsekonomiska vinster som en hög gemensam nivå av säkerhet i nätverk och informationssystem medför.

Utredningen föreslår att tillsynsmyndigheteras uppdrag enligt förslagen, i vart fall inledningsvis, ska vara anslagsfinansierade och fördelas på de utgiftsområden som respektive sektor tillhör. När det gäller kostnader för löpande tillsyn samt för kompetensförsörjning föreslår utredningen att Statskontoret ges i uppdrag att lämna ett förslag på genomförande och finansiering.

Ikraftträdande

Regelverket föreslås träda i kraft den 10 maj 2018, vilket är det datum som medlemsstaterna enligt NIS-direktivet ska tillämpa direktivets bestämmelser. För att lagen ska kunna tillämpas i enlighet med direktivet den dagen föreslår utredningen att vissa myndigheter dessförinnan ges i uppdrag att påbörja arbetet med myndighetsföreskrifter samt att vidta andra behövliga förberedelseåtgärder.