Regeringskansliet

Remiss

2017-05-23
Ju2017/03997/L4

Justitiedepartementet
Enheten för lagstiftning om allmän ordning och säkerhet och samhällets krisberedskap
Dan Leeman
dan.leeman@regeringskansliet.se
Telefon 08-405 8036

Remiss av betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36)

Remissinstanser:

1. Riksdagens ombudsmän
2. Riksrevisionen
3. Svea hovrätt
4. Attunda tingsrätt
5. Kammarrätten i Stockholm
6. Förvaltningsrätten i Stockholm
7. Justitiekanslern
8. Polismyndigheten
9. Säkerhetspolisen
10. Myndigheten för samhällsskydd och beredskap
11. Kustbevakningen
12. Datainspektionen
13. Försvarsmakten
14. Försvarets materielverk
15. Försvarets radioanstalt
16. Totalförsvarets forskningsinstitut
17. Socialstyrelsen
18. Inspektionen för vård och omsorg
19. Läkemedelsverket
20. E-hälsomyndigheten
21. Riksgäldskontoret
22. Finansinspektionen
23. Statistiska centralbyrån

24. Länsstyrelsen i Stockholms län
25. Länsstyrelsen i Västra Götalands län
26. Länsstyrelsen i Skåne län
27. Länsstyrelsen i Blekinge län
28. Statskontoret
29. Statens servicecenter
30. E-legitimationsnämnden
31. Fortifikationsverket
32. Strålsäkerhetsmyndigheten
33. Uppsala universitet (Juridiska fakulteten)
34. Stockholms universitet (Juridiska fakulteten)
35. Kungl. Tekniska Högskolan
36. Affärsverket Svenska kraftnät
37. Statens energimyndighet
38. Energimarknadsinspektionen
39. Post- och telestyrelsen
40. Trafikverket
41. Sjöfartsverket
42. Luftfartsverket
43. Lantmäteriet
44. Statens veterinärmedicinska anstalt
45. Transportstyrelsen
46. Regelrådet
47. Livsmedelsverket
48. Försvarshögskolan
49. Jönköpings läns landsting
50. Kalmar läns landsting
51. Kronobergs läns landsting
52. Norrbottens läns landsting
53. Skåne läns landsting
54. Stockholms läns landsting
55. Södermanlands läns landsting
56. Västra Götalands läns landsting
57. Östergötlands läns landsting
58. Boden kommun
59. Eskilstuna kommun
60. Flens kommun
61. Gotlands kommun
62. Gävle kommun

63. Göteborgs kommun
64. Halmstads kommun
65. Helsingborgs kommun
66. Karlsborgs kommun
67. Karlskrona kommun
68. Karlstads kommun
69. Kiruna kommun
70. Leksands kommun
71. Linköpings kommun
72. Luleå kommun
73. Malmö kommun
74. Norrköpings kommun
75. Nynäshamn kommun
76. Sigtuna kommun
77. Stockholms kommun
78. Svedala kommun
79. Vänersborgs kommun
80. Västerås kommun
81. Älvsbyns kommun
82. Östhammars kommun
83. ACR Aviation Capacity Resources AB
84. COWI AB
85. Dataskydd.net
86. Energiföretagen Sverige
87. Energigas Sverige
88. Eon AB
89. IP-only
90. It- och telekomföretagen
91. Journalistförbundet
92. Nasdaq Stockholm AB
93. Netnod
94. Preem AB
95. SJ AB
96. SME-D
97. Stiftelsen för internetinfrastruktur
98. Svensk handel
99. Svenska bankföreningen
100. Svenska Petroleum och Biodrivmedel Institutet
101. Svenskt Näringsliv

102. Svenskt vatten
103. Sveriges advokatsamfund
104. Sveriges Hamnar
105. Sveriges Kommuner och Landsting
106. Swedavia
107. Swedegas AB
108. Säkerhets- och försvarsföretagen
109. Transportföretagen
110. Tågoperatörerna
111. Vårdföretagarna

Remissvaren ska ha kommit in till Justitiedepartementet, 103 33 Stockholm, senast den 15 augusti 2017. Remissvaren ska även skickas per e-post till ju.l4@regeringskansliet.se i Worddokument eller PDF-format. Om PDF-format används ska texten vara kopierbar.

Med hänsyn till direktivets korta genomförandetid är utrymmet för anstånd ytterst begränsat.

I remissen ligger att regeringen vill ha synpunkter på förslagen eller materialet i betänkandet.

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

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

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

Maria Lindeberg
Kanslirråd

Kopia till Wolters Kluwers kundservice, 106 47 Stockholm

Informationssäkerhet för samhällsviktiga och digitala tjänster

Betänkande av
Utredningen om genomförande av NIS-direktivet

Stockholm 2017

STATENS OFFENTLIGA UTREDNINGAR

SOU 2017:36

SOU och Ds kan köpas från Wolters Kluwers kundservice.
Beställningsadress: Wolters Kluwers kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@wolterskluwer.se
Webbplats: wolterskluwer.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Wolters Kluwer Sverige AB
på uppdrag av Regeringskansliets förvaltningsavdelning.
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck: Elanders Sverige AB, Stockholm 2017

ISBN 978-91-38-24602-3
ISSN 0375-250X

Till statsrådet Anders Ygeman

Regeringen beslutade den 31 mars 2016 att utse en särskild utredare med uppdrag att föreslå hur Europaparlamentets och rådet 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 ska genomföras i svensk rätt.

Utredarens uppdrag har varit att föreslå hur 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, med inriktningen att Myndigheten för samhällsskydd och beredskap ges en samordnande roll på området men att andra myndigheters ansvar för tillsyn inom särskilda sektorer ska fortsätta gälla, 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.

Lagmannen i Stockholms tingsrätt Stefan Strömberg förordnades att fr.o.m. den 2 maj 2016 vara särskild utredare.

Förordnade sakkunniga har under hela eller delar av utredningstiden varit rättssakkunnige Dan Leeman (Justitiedepartementet), kanslirådet Henrik Moberg (Socialdepartementet), rättssakkunniga Mia Persson (Försvarsdepartementet) och kanslirådet Jörgen Samuelsson (Näringsdepartementet).

Som experter att biträda utredningen förordnades fr.o.m. den 5 oktober 2016 numera stf. avdelningschefen Mia Arblom (Försvarsmakten), numera avdelningsdirektören Henrik Christiansson (Säkerhetspolisen), numera enhetschefen Linda Ericson (Myndigheten för samhällsskydd och beredskap), juristen Britt-Marie Jönson (Post- och telestyrelsen), informationssäkerhetsexperten Arvid Kjell (Försvarets Radioanstalt) och it-säkerhetschefen Josefine Östfeldt (Polismyndigheten) samt fr.o.m. den 23 november 2016 juristen Markus Lind (Datainspektionen).

Som ledamöter i en till utredningen knuten referensgrupp förordnades fr.o.m. den 5 oktober 2016 säkerhetschefen Per Ekegren (Livsmedelsverket), chefsjuristen Elisabeth Ekstrand (IIS), handläggaren Linda Eriksson (Statens Energimyndighet), säkerhetschefen Stefan Larsson (E-hälsomyndigheten), riskexperten Anders Lindgren (Finansinspektionen), juristen Markus Lind (Datainspektionen), säkerhetschefen Torbjörn Mellblom (Sjöfartsverket), näringspolitiske experten Pär Nygårds (IT-&Telekomföretagen), utredaren Margareta Palmqvist (Socialstyrelsen), verksjuristen Kim Reenaas (Elsäkerhetsverket), enhetschefen Gunilla Roos (Transportstyrelsen), enhetschefen Per-Olof Ström (Trafikverket), förbundsjuristen Jeanna Thorslund (SKL) och enhetschefen Tina Stödberg (Affärsverket svenska kraftnät). Jeanna Thorslund entledigades den 26 oktober 2016 och samma dag förordnades i stället sektionschefen Jörgen Sandström (SKL). Tina Stödberg entledigades den 28 oktober 2016 och samma dag förordnades i stället it-säkerhetssamordnaren Satu Hallikainen (Affärsverket svenska kraftnät). Markus Lind entledigades den 23 november 2016 för att i stället förordnas som expert.

Som sekreterare anställdes den 2 maj 2016 byrådirektören Annette Norman och den 1 augusti 2016 numera rådmannen Malin Stensbäck.

Utredningen överlämnar härmed betänkandet *Informationssäkerhet för samhällsviktiga och digitala tjänster* (SOU 2017:36). Experterna och de sakkunniga har i allt väsentligt ställt sig bakom utredningens överväganden och förslag. De särskilda ståndpunkter

som enskilda experter och sakkunniga kan ha haft i olika frågor har berörts i texterna eller som möjliga alternativa bedömningar. Utredningens uppdrag är med detta slutfört.

Stockholm i april 2017

Stefan Strömberg

/ Annette Norman
Malin Stensbäck

Innehåll

Bilagor

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.