Datum	Diarienr
2017-08-21	2017-4770
Ert datum	Er referens
2017-05-23	Ju2017/03997/L4

Avdelningen för utveckling av samhällsskydd
Verksamheten för cybersäkerhet och skydd av samhällsviktig verksamhet
Helena Andersson
helena.andersson@msb.se

Regeringskansliet
Justitiedepartementet

103 33 Stockholm

Betänkandet SOU 2017:36 Informationssäkerhet för samhällsviktiga och digitala tjänster

Sammanfattning

Myndigheten för samhällsskydd och beredskap (MSB) tillstyrker merparten av utredningens förslag på hur direktivet (2016/1148) om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet) ska implementeras i Sverige.

Sammanfattningsvis har myndigheten följande synpunkter.

Avseende tillsyn:

- Inför tillsyn över statliga myndigheters informationssäkerhetsarbete
- Ge MSB starkare mandat att leda och samordna, inklusive föreskriftsrätt rörande tillsynsarbetet
- Förtydliga tillsynsmyndigheternas uppdrag.
- Utöka och förtydliga informationsutbytet mellan tillsynsmyndigheter och MSB

Avseende råd och stöd:

- Utse MSB till tillsynsvägledande myndighet.
- Tydliggör MSB:s roll att ge råd och stöd

Avseende krav på säkerhetsarbetet:

- Leverantörer ska informera tillsynsmyndigheter att de omfattas av NIS.
- Tydliggör att föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete är sektorsövergripande och föreskrifter om säkerhetsåtgärder enligt 11 och 12 §§ är komplement.
- Byt ut begreppet ”säkerhetsprinciper” mot ”styrande dokument”.

Avseende incidentrapportering:

- Samordna sektorsspecifika föreskrifter om incidentrapportering så långt möjligt.
- Inför absolut sekretess för it-incidenter.

Avseende resursbehov

- MSB behöver tillföras ytterligare resurser för att kunna utföra uppdragen inom NIS.

Synpunkter avseende tillsyn

Tillsyn över statliga myndigheter

Direktivet skapar förutsättningar för ett effektivt och ändamålsenligt informationssäkerhetsarbete i medlemsländerna genom att i ett antal samhällsviktiga sektorer införa krav på systematiskt och riskbaserat informationssäkerhetsarbete inklusive it-incidentrapportering samt tillsyn.

Behovet av att utöva tillsyn över myndigheters informationssäkerhetsarbete, utöver existerande tillsyn rörande säkerhetsskydd, har påpekats tidigare i flera sammanhang[1]. Att tillföra tillsyn som ett verktyg är av central betydelse för att komma längre i säkerhetsarbetet även hos myndigheter. Det i sin tur kommer också att bidra till att öka allmänhetens och privata aktörers tillit och förtroende för informationshantering i den offentliga sektorn, en sektor som i rask takt håller på att digitaliseras. Som bland annat NISU-utredningen (SOU 2015:23) och Riksrevisionen föreslagit kan ett tillsynsuppdrag med fördel läggas på MSB. Myndigheten utövar redan idag tillsyn över statliga myndigheter på flera områden, exempelvis inom brandfarliga och explosiva varor.

Starkare mandat att leda och samordna arbetet

Genom NIS-direktivet införs tillsyn i en rad sektorer. Genom att tillsynen ska utföras av flera olika myndigheter med olika erfarenhet av frågorna är det centralt att både säkerställa att tillsynen utförs på ett likartat sätt samt att samtliga berördas myndigheters erfarenheter och kunskap tillvaratas på ett ändamålsenligt sätt. Detta förutsätter en nära samverkan samt tydlighet avseende vad tillsynen ska utgå från.

Utredningen föreslår att MSB ska få i uppdrag att leda ett samarbetsforum där samtliga tillsynsmyndigheter ska ingå. MSB har omfattande erfarenhet av att ha en samordnande roll och olika typer av nätverk och samarbeten, exempelvis samverkansområdena och Samfi. Samarbetsforumet kommer enligt MSB:s bedömning vara av avgörande betydelse för möjligheten att säkerställa att tillsynen inom området harmoniseras och därmed utförs på ett så likartat sätt

[1] Riksrevisionen, Informationssäkerheten i den civila statsförvaltningen, RiR 2014:23 s 81f, Informations- och cybersäkerhet i Sverige SOU 2015:23 s 227f

som möjligt avseende metod, utgångspunkter och syfte. I annat fall uppstår risk för spretig regeltillämpning och i förlängningen en ojämn nivå av informationssäkerhet i samhället och svårighet att dra nytta av kunskaper och erfarenheter som är gemensamma för alla organisationers informationssäkerhetsarbete. För att säkerställa att syftet med NIS direktivet uppfylls är det väsentligt att deltagande i samarbetsforumet prioriteras av samtliga berörda myndigheter samt att MSB ges ett tydligt uppdrag att leda och inrikta arbetet. Det bör därför införas ett krav på deltagande och bidrag till det gemensamma arbetet i samarbetsforumet i respektive tillsynsmyndighets instruktion samt att MSB:s uppgift att leda och samordna arbetet i samarbetsgruppen ska framgå av myndighetens instruktion.

Förtydliga tillsynsmyndigheternas uppdrag

De utpekade tillsynsmyndigheterna bedriver redan idag tillsyn i olika frågor. Det föreligger därför en risk att tillsyn enligt NIS som byggs upp utan sektorsövergripande harmonisering i praktiken kommer att utföras på många olika sätt och därmed inte stödja syftet med NIS-direktivet. MSB anser därför att det är angeläget att i förordningen förtydliga att tillsynsarbetet med koppling till NIS så långt möjligt ska harmoniseras. samt bygga på samma metodik som används i etablerad tillsynsreglering, exempelvis på skol- respektive miljöområdet rörande exempelvis tillsynsplaner, uppföljning och utvärdering.

Det bör även tydligt framgå att tillsynen i första hand ska utgå från de föreskrifter som MSB föreslås utfärda om ett systematiskt och riskbaserat informationssäkerhetsarbete.

MSB föreslår därför att nedan punkt läggs till i 6 § förordningen samt att författningskommentaren till 22 § i lagförslaget kompletteras på nedan föreslaget vis.

6 § Tillsynsmyndigheten ska X. bedriva tillsynsarbetet i enlighet med det metodstöd för tillsyn som tas fram av Myndigheten för samhällsskydd och beredskap tillsammans med tillsynsmyndigheterna.

22 § Paragrafen genomför artikel 8.1–2 i NIS-direktivet. Syftet med åtgärden tillsyn är att kunna bedöma hur leverantörerna bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete. I detta ingår att bedöma hur de uppfyller säkerhetskraven och kraven på incidentrapportering samt bedöma vilka effekter direktivets krav får på säkerheten i nätverk och informationssystem. Sättet att utföra behovsutredningar, planering rörande resurser och inriktning, kartläggning av tillsynsobjekt, uppföljning och utvärdering, hantering av upptäckta brister samt informationsinhämtning från leverantörer för en sådan tillsyn bör så långt möjligt harmoniseras.

Det innebär att tillsyn i form av självskattning eller kontroll av att relevant dokumentation finns på plats inte uppfyller direktivets krav. Resultatet från en tillsyn kan ligga till grund för sanktioner och förelägganden om att avhjälpa brister.
....

Stärkt informationsutbyte mellan tillsynsmyndigheter och MSB

MSB föreslås få i uppgift att ha en samlad bild av NIS-direktivets genomförande och tillämpning i Sverige. En förutsättning för att kunna dra väl underbyggda slutsatser om olika förhållanden är att det finns möjlighet att kombinera information från olika källor. Sådana kombinationer kan också tydliggöra förhållanden som inte skulle vara lika tydliga om information endast inhämtats från en källa. MSB måste därför starkt ifrågasätta utredningens slutsats att MSB, i motsats till den uttryckliga inriktningen i kommittédirektiv 2016:29, inte skulle få tillgång till tillsynsrapporter från andra sektorsmyndigheter. Att överlämna utformningen av informationsutbytet inom NIS rörande en sådan viktig informationskälla som tillsynsrapporter till separata överenskommelser mellan samtliga berörda myndigheter kan i praktiken ge en mycket ojämn tillgång till information, både avseende tidpunkt och omfattning.

MSB kan dessutom inte se att känslighetsgraden i någon nämnvärd utsträckning skulle skilja sig mellan en it-incidentrapport och en tillsynsrapport. Denna bedömning baserar MSB på flera år av hantering av it-incidentrapporter från olika typer av organisationer i samhället inklusive drygt ett års erfarenhet av obligatorisk it-incidentrapportering för statliga myndigheter. Om en leverantör som omfattas av direktivet skulle uppleva det som försvårande att information som ingår i en tillsynsrapport delas med fler myndigheter så gäller det i minst lika stor utsträckning för information som skickas in i en incidentrapport.

Att den ena informationsmängden kan hanteras centralt hos MSB men inte den andra ter sig som märkligt, särskilt med tanke på de andra känsliga informationsmängder som myndigheten hanterar, exempelvis inom civilt försvar. Istället borde informationsutbytet rörande båda informationsmängderna vara så omfattande och transparant som möjligt mellan respektive tillsynsmyndighet och MSB. MSB ser inte några problem med att dela it-incidentrapporter med respektive tillsynsmyndighet.

Utredningen föreslår att MSB i förordningen ska åläggas att skyndsamt överlämna it-incidentrapporter till respektive tillsynsmyndighet. Med tanke på att det handlar om att dela information samt att MSB överväger olika typer av systemlösningar för ett sådant tillhandahållande av it-incidentrapporter är det mer lämpligt att använda det mer neutrala begreppet tillgängliggöra.

MSB anser också att tidskravet kopplat till informationsutbytet mellan myndigheterna bör vara harmoniserat. Med tanke på att det handlar om flera olika aktörer och olika typer av informationsmängder behöver det vara något

mer generöst än ”skyndsamt”. Användningen av ”utan onödigt dröjsmål” torde på ett tillräckligt sätt uttrycka behovet av att informationsdelning sker i närtid både gällande it-incidentrapporter och information om genomförd tillsyn.

Med anledning av ovan föreslår MSB följande ändringar och tillägg i förordningen:

6 § Tillsynsmyndigheten ska p X. Utan onödigt dröjsmål tillgängliggöra för samordningsuppdraget relevant information om genomförd tillsyn till Myndigheten för samhällsskydd och beredskap.

8 § 3 st Myndigheten för samhällsskydd och beredskap p 7. ska utan onödigt dröjsmål tillgängliggöra incidentrapporter som lämnas enligt 16 och 19 §§ lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga och digitala tjänster till den tillsynsmyndighet som enligt 5 § denna förordning utövar tillsyn över den rapporterande leverantören.

Synpunkter avseende råd och stöd

MSB anser att myndigheten bör utses till tillsynsvägledande myndighet och menar, till skillnad från utredningen, att den roll som myndigheten föreslås få är just en tillsynsvägledande roll. Att använda den benämningen på MSB:s uppgifter skapar därför en nödvändig tydlighet.

Utredningen föreslår vidare att tillsynsuppgiften som ges tillsynsmyndigheterna även ska omfatta rådgivning. MSB ser detta som problematiskt eftersom det riskerar att råd och stöd kan komma att skilja sig mellan sektorerna, även på sektorsövergripande nivå. Det bör istället vara MSB.s uppgift att, i samverkan med tillsynsmyndigheterna, ta fram råd och stöd gällande de gemensamma kraven på leverantörerna.

I utredningens förslag på förordning regleras i 9 § att MSB ska lämna råd och stöd till tillsynsmyndigheterna vid utarbetandet av myndighetsföreskrifter. MSB ser det som olyckligt begränsande. Utredningen föreslår att MSB ska genomföra en rad olika uppdrag som också innebär råd och stöd av olika typer samt därutöver, rörande tillsyn, ska ha en tydligt samordnande roll som även behöver innefatta uppföljning och utvärdering för att kunna ge nödvändigt stöd till tillsynsmyndigheterna. Författningstexten bör därför justeras:

9 § Myndigheten för samhällsskydd och beredskap ska lämna råd och stöd till tillsynsmyndigheterna vid utarbetandet av myndighetsföreskrifter samt utöva en tillsynsvägledande roll genom att tillhandahålla metodstöd för tillsynsarbetet, samordna, följa upp och utvärdera tillsynen.

Synpunkter avseende säkerhetskrav

Informera om status som leverantör av samhällsviktig tjänst

Utredningen föreslår att det ska ankomma på aktörerna i de olika utpekade sektorerna att själva undersöka om de uppfyller kraven för att vara en leverantörer av samhällsviktiga tjänster eller inte. Att endast ställa krav på leverantörerna att genomföra en sådan undersökning utan att delge resultatet till tillsynsmyndigheten minskar tillsynsmyndighetens möjlighet att på ett enkelt sätt få en uppfattning om hur många leverantörer av samhällsviktiga tjänster som de facto finns inom respektive sektor. De aktörer som vid en sådan undersökning kommer fram till att de uppfyller kraven för att vara leverantörer av samhällsviktiga tjänster bör därför även åläggas att informera tillsynsmyndigheten om detta förhållande. Detta är även viktigt för MSB för att exempelvis kunna skicka ut teknisk information med koppling till incidentrapportering.

Föreskrifter om säkerhetskrav

Tillsynsmyndigheterna föreslås få mandat att meddela närmare föreskrifter om utformningen av säkerhetsåtgärder enligt 11 och 12 §§ i den föreslagna lagen. De säkerhetsåtgärder som beskrivs i författningskommentaren till 11 § ingår samtliga som en naturlig del i ett systematiskt och riskbaserat informationssäkerhetsarbete, det vill säga det som åläggs leverantörerna i 10 § lagförslaget. För att motverka otydlighet och en spretig regelflora som skapar onödiga skiljelinjer mellan olika sektorer avseende vad de har att förhålla sig till anser MSB det centralt att det tydliggörs i författningskommentaren till 11 § att åtgärderna utgör ett komplement till det systematiska arbetet.

> 11 § Paragrafen genomför artikel 14.1 i NIS-direktivet.
>
> Med säkerhet i nätverk och informationssystem avses systemens förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de besläktade tjänster som erbjuds genom eller är tillgängliga via dessa nätverk och informationssystem (7 § 2). Åtgärderna ska utgöra ett komplement till det systematiska och riskbaserade informationssäkerhetsarbetet som behandlas i lagens 10 §.

Begreppsproblematik

Byt genomgående ut begreppet ”säkerhetsprinciper” mot ”styrande dokument. I direktivstexten samt i lagförslaget används begreppet säkerhetsprinciper. Av författningskommentaren framgår att det är hämtat från den engelska termen security policies och avser olika typer av styrande dokument. Inom ramen för ett systematiskt informationssäkerhetsarbete i enlighet med internationella standarder på området finns i nuläget inte någon motsvarande användning av begreppet säkerhetsprinciper. Genom att introducera ett begrepp som inte är etablerat och dessutom låta det beteckna en informationsmängd som redan benämns på ett allmänt accepterat sätt (styrande dokument) riskeras att skapas

mer osäkerhet än tydlighet rörande innebörden av kraven. Med anledning av detta ser MSB det som mycket angeläget att begreppet ”säkerhetsprinciper” genomgående byts ut mot det mer rättvisande och etablerade begreppet ”styrande dokument”.

Synpunkter avseende incidentrapportering

Harmoniserad rapportering

Med hänsyn till att incidenter som kan orsaka rapporteringsplikt sällan endast drabbar en enda sektor är det enligt MSB:s uppfattning av stor betydelse att det sker en harmonisering av vad som ska rapporteras. MSB anser att det är centralt att även den här typen av frågor tas upp i samarbetsforumet samt att föreskrifterna som tillsynsmyndigheterna ska ta fram för att avgöra om en incident har en betydande inverkan på kontinuiteten samordnas.

Absolut sekretess

Erfarenheterna från den obligatoriska it-incidentrapporteringen för statliga myndigheter visar på att vissa myndigheter inte upplever sekretesskyddet, främst i form av OSL 18:8, vara tillräckligt heltäckande för att de ska välja att lämna utförliga rapporter över inträffade incidenter, detta trots föreliggande kammarrättsavgöranden. Med hänsyn till att statliga myndigheter, som får anses ha en god förståelse för regelverket kring offentliga och sekretessbelagda handlingar, väljer en sådan handlingslinje ser MSB det föreligga en mycket hög risk för att privata aktörer som åläggs rapportera genom NIS-direktivet i ännu högre utsträckning kommer att välja att lämna endast knapphändig information i sina incidentrapporter. Kontakter med privata aktörer i samband med informationsdelning vid incidenter visar att det förhållandet att det inte går att på förhand garantera resultatet av en sekretessprövning upplevs som ett hinder att lämna känslig information.

Informationssäkerhetsområdet är komplext och den tekniska utvecklingen går mycket snabbt. En uppgift som tidigare har bedömts som förhållandevis harmlös kan plötsligt användas för avancerade angrepp. Bedömningen av om syftet med säkerhetsåtgärden motverkas och därmed omfattas av sekretess kräver kontinuerlig insikt i utvecklingen på området. Att it-incidentrapporterna inte bara ska hanteras av MSB utan även av samtliga tillsynsmyndigheter kommer att ställa mycket höga krav på samtliga berörda myndigheter att ha förmåga att göra nödvändiga, uppdaterade och samstämmiga riskanalyser om kritiska tjänster i samhället. Privata aktörer behöver etablera ett mycket högt förtroende för samtliga myndigheters förmåga att hantera informationen. Absolut sekretess ger aktörerna möjlighet att i förväg få en förvissning om hur känslig information ska hanteras och kan då välja att lämna in fullständig information. Enligt MSB:s uppfattning är införandet av absolut sekretess för de inlämnade it-incidentrapporter, särskild de känsligaste uppgifterna, en grundläggande förutsättning för att rapportering enligt NIS ska få avsedd effekt för samhällets informationssäkerhet. Motsvarande reglering finns redan på plats i ett antal medlemsstater med anledning av NIS.

Synpunkter avseende resurser

MSB ser mycket positivt på de möjligheter att stödja samhällets informationssäkerhet som utredningens förslag innebär. Även om uppgifterna sakmässigt harmonierar väl med MSB:s nuvarande uppdrag och kompetensområde innebär de i många delar en mycket kraftig utökning av mängden arbete, exempelvis rörande incidentrapportering. Sammantaget innebär detta att myndigheten, till skillnad från utredningens slutsats, har behov av ytterligare resurser. Enligt MSB:s bedömning finns ett behov av ytterligare resurser för att genomföra myndighetens uppdrag inom NIS. I budgetunderlaget för 2018 har myndigheten äskat 25 miljoner för att utveckla arbetet med informationssäkerhet i samhället.

I detta ärende har vikarierande generaldirektören Nils Svartz beslutat. Helena Andersson har varit föredragande. I den slutliga handläggningen har också avdelningschefen Cecilia Nyström, verksamhetschefen Richard Oehme och enhetschefen Linda Ericson deltagit.

Nils Svartz

Helena Andersson