CS-ST
Johan Turell

Johan.turell@msb.se

Regeringskansliet
Försvarsdepartementet
103 33 Stockholm

Delbetänkandet 2024:18 Nya regler om cybersäkerhet

Sammanfattning

Myndigheten för samhällsskydd och beredskap (MSB) har tagit del av rubricerat betänkande och lämnar följande synpunkter på utredningens förslag.

MSB konstaterar att utredningen har gjort en stor insats med en komplex uppgift under mycket knappa tidsförhållanden och tillstyrker till del utredningens förslag om hur Europaparlamentets och rådets direktiv av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) ska implementeras i Sverige.

MSB välkomnar utredningens förslag att MSB fortsatt utgör gemensam kontaktpunkt, CSIRT-enhet och får den nya rollen som nationell cyberkrishanteringsmyndighet.

MSB konstaterar samtidigt att möjligheterna att stärka motståndskraften i samhällsviktig verksamhet inte fullt ut har tillvaratagits. Privata och offentliga verksamhetsutövares perspektiv och behov har inte beaktats tillräckligt och vissa förslag kommer att aktivt försvåra för dem att tillvarata sina rättigheter och uppfylla sina förpliktelser. Utredningens förslag kommer i vissa fall att innebära dubbelarbete och ett ineffektivt nyttjande av statens resurser. Den befintliga kompetensen hos expertmyndigheterna har heller inte nyttjats till fullo, vilket hade varit önskvärt under rådande förhållanden.

Utredningens förslag leder enligt MSB:s bedömning till en mängd nya frågeställningar och gränsdragningsproblem när det gäller föreskrifter, efterlevnad och tillsyn som, om de inte adresseras, riskerar att ta omfattande resurser i anspråk att försöka lösa av aktörerna själva, på bekostnad av själva säkerhetsarbetet.

Sammanfattningsvis har myndigheten följande huvudsakliga synpunkter:

1. Tillämpningsområdet för NIS2 behöver utökas för att svara mot totalförsvarets behov
2. NIS2- och CER-regleringarna behöver bli en bottenplatta till säkerhetsskydd.
3. En gemensam tjänst för myndighetskontakter behöver skapas.
4. Överlappande reglering ska i möjligaste mån undvikas.
5. Använd etablerade begrepp
6. Förtydliga språk och krav avseende incidentrapportering.
7. Sanktionsmöjligheter för systematiskt och riskbaserat informations- och cybersäkerhetsarbete behöver införas.
8. Tillsynssamordningen behöver stärkas.
9. Konsekvensanalysen behöver fördjupas

10. NIS2-implementeringen behöver integreras i beredskapssystemet.

Genom den nära kopplingen till CER-direktivet kommer vissa av synpunkterna ha bäring på implementeringen av CER-direktivet, där utredningen återkommer med slutbetänkande i höst.

Inledning

NIS2- och CER-direktiven ökar motståndskraften i samhällsviktig verksamhet på ett samordnat sätt inom hela EU. Målsättningen är att förbättra den inre marknadens funktion. För att uppnå detta har EU kommissionen och regeringen varit tydlig med att de kompletterande NIS2- och CER-direktiven ska implementeras samlat. Sverige saknar idag en sammanhållen reglering som säkerställer motståndskraften i samhällsviktig verksamhet. Informations- och cybersäkerhet, fysisk säkerhet och personalsäkerhet är viktiga komponenter för att stärka motståndskraften för samhällets funktionalitet.

1. Utöka tillämpningsområdet

Utredningen föreslår ett tillämpningsområde för cybersäkerhetslagen som med vissa enstaka undantag motsvarar en minimiimplementering av NIS2-direktivet.

Sverige har en struktur för den krisberedskapen och det civila försvaret med 10 beredskapssektorer och sex civilområden. En viktig del i att bygga motståndskraft inom det beredskapssystemet är upprätthållandet av samhällsviktig verksamhet. All samhällsviktig verksamhet är beroende av nätverk och informationssystem för att kunna upprätthålla service till medborgarna.

I delbetänkandets redogörelse för de nya NIS2-sektorerna förs inget resonemang om hur dessa relaterar till det krisberedskap och civilt försvar samt de 10 beredskapssektorerna.

MSB anser att arbetet med NIS2-regleringen är en naturlig del av arbetet i beredskapssektorerna och att det på ett resurseffektivt sätt stärker både skyddet för den samhällsviktiga verksamheten och samhällets krisberedskap och civilt försvar i stort.

Enligt delbetänkandet ska endast vissa samhällsviktiga verksamheter omfattas av krav på att vidta säkerhetsåtgärder, tillsyn samt skyldighet att rapportera incidenter.[1] Andra viktiga samhällsfunktioner får därmed inte alls samma krav på sig.

Ur ett totalförsvarsperspektiv är det enligt MSB:s mening centralt att all samhällsviktig verksamhet på sikt behöver omfattas av NIS2-regleringen. MSB har i bred samverkan med samhällets aktörer tagit fram en lista över viktiga samhällsfunktioner.[2] Listan utgör en sammanställning av de viktiga samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet – i vardagen, krisen och kriget. De viktiga samhällsfunktionerna utgör grunden för att identifiera samhällsviktig verksamhet.

[1] Delbetänkandet 8 § förordning om cybersäkerhet
[2] https://www.msb.se/sv/publikationer/identifiering-av-samhallsviktig-verksamhet--lista-med-viktiga-samhallsfunktioner/

I utredningens direktiv gavs möjlighet att föreslå utvidgning om en sådan följdes av en konsekvensanalys. Utredningen har under utredningsarbetet dock konstaterat att tillgänglig tid och resurser inte givit något utrymme för ett sådant arbete varför förslagen i betänkandet utgör en minimiimplementering.

Förslag:

1. Ge MSB i regeringsuppdrag att, som underlag till den fortsatta lagstiftningsprocessen, föreslå och ta fram konsekvensanalyser för att utvidga tillämpningsområdet med de sektorer som det ur ett totalförsvarsperspektiv är särskilt angeläget att få med i NIS2-regleringen.[3]

2. Skapa en bottenplatta till säkerhetsskydd

Utredningen föreslår, precis som gäller inom nuvarande NIS-reglering, att den del av verksamheten som omfattas av säkerhetsskydd ska undantas helt från cybersäkerhetslagens krav på riskhanteringsåtgärder och incidentrapportering.[4]

Den bottenplatta av säkerhetskrav som etableras genom NIS2- och CER-direktiven kommer att på ett påtagligt sätt bidra till samhällets robusthet. Kraven i NIS2- och CER-direktiven utgår från ett allriskperspektiv medan säkerhetsskyddslagstiftningen har som syfte att skydda det mest skyddsvärda i samhället mot antagonistiska hot.

Hur förhållandet mellan kommande CER-reglering och säkerhetsskydd föreslås se ut kommer att framgå i slutbetänkandet men det är inte orimligt att anta att motsvarande upplägg väljs även där, ett upplägg som innebär att den del av en verksamhet som omfattas av säkerhetsskydd inte kommer att omfattas av CER-direktivet och därmed inte CER-direktivets krav på exempelvis riskanalys och kontinuitetshantering.

Vilka hot och risker en organisation ska hantera påverkar valet av åtgärder. MSB anser därför att det ur ett totalförsvarsperspektiv inte är rimligt att underlåta att ställa krav på säkerhetsarbetet utifrån ett allriskperspektiv på den verksamhet i en organisation som är av störst betydelse för nationell säkerhet och där funktionen hos verksamheten kan vara av stor betydelse för samhällets funktionalitet under kris och krig.

Utredningen för vidare ett resonemang kring relationen mellan NIS2-regleringen och säkerhetsskydd och möjligheterna till att etablera en föreslagen bottenplatta. Detta resonemang begränsas dock till att endast röra sådana myndigheter som helt undantas från NIS2-direktivets tillämpningsområde vilket resulterar i att utredningen konstaterar att det rör för få för att ge någon reell skillnad.[5]

[3] Försvarsberedningen har i sitt senaste delbetänkande Kraftsamling DS 2023:34 föreslagit fyra nya beredskapssektorer, 1) Sektor utrikeshandel, 2) Sektor försörjning med industrivaror, 3) Sektor arbetskraftsförsörjning, 4) Sektor planering, ledningsförmåga och samordning. https://www.regeringen.se/rattsliga-dokument/departementsserien-och-promemorior/2023/12/ds-202334-kraftsamling/
[4] Delbetänkandets förslag på 1 kap 12 § lag om cybersäkerhet samt avsnitt 5.5.4 och 5.5.5
[5] Delbetänkandet sid 137f.

MSB anser att utredningen belyst behovet alltför snävt. Frågan behöver utvidgas till att gälla alla verksamhetsutövare och deras behov av tydliga krav på åtgärder för att möta andra hot och risker än antagonistiska i säkerhetsskyddad verksamhet.

MSB är vidare av uppfattningen att alla delar i en samhällsviktig verksamhet, även den säkerhetsskyddade, behöver omfattas av krav på systematiskt och riskbaserat informations- och cybersäkerhetsarbete och att vidta säkerhetsåtgärder samt utbildning utifrån ett allriskperspektiv för att på så sätt även ge den säkerhetsskyddade delen ett allriskskydd. Detta blir än viktigare i CER-regleringen där säkerhetsskyddslagstiftningen till ännu större del saknar motsvarande krav. Även Säkerhetspolisen för fram NIS-direktivets krav som lämplig ”bottenplatta” som i förkommande fall kan kompletteras av säkerhetsskyddsregleringens bestämmelser.[6]

Däremot bedömer MSB att det är mer problematiskt att låta NIS2- (och CER-) regleringen avseende incidentrapportering och tillsyn även gälla säkerhetsskyddad verksamhet. För att inte överlappa och skapa otydliga gränsytor mot tillsyn respektive rapportering enligt säkerhetsskyddslagen bör därför cybersäkerhetslagens krav på incidentrapportering och tillsyn undantas när det gäller den säkerhetsskyddade verksamheten. Syftet med förslaget är att komplettera kraven som gäller för säkerhetsskydd och i den utsträckning säkerhetsskyddsregleringen innebär strängare krav gäller givetvis dessa framför NIS2- och CER-regleringens krav.

MSB noterar även att den nuvarande säkerhetsskyddslagstiftningen har utformats med ingångsvärdet att det inte finns en bottenplatta av reglering motsvarande NIS2- och CER-regleringen att utgå från. För att minska fragmenteringen på området i form av både överlappningar och luckor i regelverken kan det enligt myndigheten, efter att NIS2- och CER-direktiven har implementerats, finnas skäl att också på ett mer heltäckande sätt se över utformningen av regler om skydd av säkerhetsskyddad verksamhet där det finns ett heltäckande regelverk med krav på svensk samhällsviktig verksamhet att utgå från. MSB bedömer att ensad struktur, terminologi med mera skulle underlätta för verksamhetsutövarna som bedriver både samhällsviktig och säkerhetsskyddad verksamhet att hantera samhällets krav. Ett sådant arbete är givetvis omfattande och förutsätter sannolikt en särskild utredning.

Förslag:

2. Låt kraven att arbeta systematiskt och riskbaserat med cybersäkerhet samt kraven på att vidta säkerhetsåtgärder gälla för alla delar i verksamhetsutövarens organisation.

3. Tillsätt en utredning efter att NIS2- och CER-direktiven har implementerats med uppdrag att ta fram förslag på hur de säkerhetsrelaterade regelverken såsom NIS2- och CER-regleringen, säkerhetsskyddsregleringen och beredskapsförordningen på ett tydligare sätt kan kopplas samman i syfte att minska fragmenteringen på området.

[6] Delbetänkandet s 137.

3. Etablera en gemensam systemplattform för myndighetskontakter

Utredningen föreslår att en verksamhetsutövares anmälan om att den omfattas av NIS2-regleringen ska göras till respektive tillsynsmyndighet. Varje tillsynsmyndighet ska inom sitt tillsynsområde upprätta ett register över väsentliga och viktiga verksamhetsutövare.[7] Tillsynsmyndigheterna ska sedan senast den 1 mars 2025 och därefter, i vart fall, vartannat år dela dessa uppgifter med MSB för att myndigheten i sin tur (i egenskap av den gemensamma kontaktpunkten) vartannat år ska dela dessa uppgifter med EU-kommissionen och NIS Samarbetsgruppen.

Med anledning av att anmälningarna ska innehålla en del känsliga uppgifter, exempelvis organisationens IP-adressrymd, behöver en sådan anmälan enligt MSB:s bedömning göras i ett informationssystem som uppfyller en tillräcklig nivå av säkerhet vid användning, överföring och lagring för att kunna hantera information som kan omfattas av sekretess. Det gäller givetvis inte bara i samband med att anmälan görs utan kanske i än högre grad den samlade listan på vilka som anmälts, d.v.s. vilka som bedriver samhällsviktig verksamhet i sektorn.

MSB anser att det ur ett samhällsekonomiskt perspektiv inte är rimligt eller resurseffektivt att varje tillsynsmyndighet lägger ned resurser på att ta fram nya egna system som kan hantera verksamhetsutövarnas anmälningar och känsliga uppgifter däri med tillräcklig säkerhet. Verksamhetsutövare ska inte endast dela känslig information med de myndigheter som har utpekade uppdrag utifrån NIS2-regleringen i form av anmälningar. Samtliga verksamhetsutövare ska även skicka in incidentrapporter till MSB/CSIRT-enheten. Även incidentrapporter behöver hanteras med motsvarande säkerhetsnivå.

MSB:s inriktning är att de organisationer som omfattas av NIS2- och CER-regleringarna ska ha lätt att göra sin plikt, och ha lätt att kräva sin rätt. MSB utvecklar nu därför en systemplattform för att på ett säkert sätt kunna hantera informationsdelning och incidentrapportering från samtliga verksamhetsutövare. Funktionaliteten byggs också ut så att det även kan hantera anmälningar och andra myndighetskontakter som organisationer som omfattas av NIS2- och CER-regleringarna är ålagda, eller kan ha nytta av, att ha. Användning av systemplattformen för detta ändamål minskar behovet för respektive tillsynsmyndighet att investera i egna informationssystem.

Ett decentraliserat anmälningsupplägg riskerar enligt MSB:s mening inte bara bli mer resurskrävande än nödvändigt för de utpekade tillsynsmyndigheterna utan även för verksamhetsutövarna. Detta eftersom samtliga privata och offentliga verksamhetsutövare i så fall kommer att behöva hantera minst ett anmälningssystem (om de hör till flera tillsynssektorer behöver de anmäla sig motsvarande antal gånger i olika system) och dessutom i MSB:s systemplattform i samband med incidentrapporteringen. Det finns därför enligt MSB:s uppfattning fördelar med att all informationsdelning som behöver omfattas av en viss grad av säkerhet görs centralt i systemplattformen. På så sätt skulle verksamhetsutövaren endast behöva göra en anmälan som sedan distribueras till den eller de tillsynsmyndigheter som berörs.

[7] Delbetänkandet sid 177f.

Enligt MSB:s bedömning är det inte heller rimligt att staten, under den period då fokus ligger på uppbyggnad av totalförsvaret, endast en gång vartannat år ska ha en *samlad och uppdaterad* bild av vilka organisationer som bedriver samhällsviktig verksamhet. För totalförsvarsplaneringen behövs en ständigt tillgänglig, uppdaterad och samlad bild över vilka aktörer som bedriver samhällsviktig verksamhet, inte minst för privat-offentlig samverkan inom beredskapssystemet.

Mot bakgrund av myndighetens uppgift att verka för samordning av det civila försvaret men även som CSIRT-enhet och tillhandahållare av uppföljningsverktyget Cybersäkerhetskollen (tidigare Infosäkkollen och It-säkkollen) finns det fördelar med en central förvaltning av ett gemensamt register över anmälda verksamhetsutövare istället för att dela upp det mellan tillsynsmyndigheterna.

Utredningen föreslår att MSB fortsatt ska ha rollen som CSIRT-enhet. Information i de register som tillsynsmyndigheterna kommer att ansvara för innehåller viktig information som krävs för att MSB som CSIRT-enhet ska kunna utföra de uppgifter myndigheten har utifrån den rollen enligt NIS2-direktivet. MSB har även fått i uppdrag av regeringen att tillhandahålla Cybersäkerhetskollen till aktörer som omfattas av NIS-regleringen. Även för detta uppdrag utgör en uppdaterad tillgång till relevanta och aktuella kontaktuppgifter till leverantörerna en viktig förutsättning för att kunna ge stöd. Detsamma gäller exempelvis vid kontakter kring och inbjudningar till den årliga NIS-konferensen, ett arrangemang som anordnas exklusivt för NIS-leverantörer.

Förslag:

4. Säkerställ att anmälan, på samma sätt som incidentrapportering, görs på ett samlat sätt centralt till den gemensamma kontaktpunkten som stöd för totalförsvaret och för vidare distribution till berörd tillsynsmyndighet.

4. Överlappande reglering ska i möjligaste mån undvikas

Utredningen föreslår att lagen bör fyllas ut av föreskrifter som meddelas av tillsynsmyndigheterna. MSB ska ges tillfälle att yttra sig över föreskrifterna och regeringen föreslås ge MSB i uppdrag att skyndsamt utarbeta en vägledning om riskhanteringsåtgärder till stöd för tillsynsmyndighetens föreskriftsarbete. Enligt utredningens uppfattning är det angeläget att föreskrifterna kan sektorsanpassas och att den myndighet som har tillsyn också har föreskriftsrätten.[8]

MSB vill i sammanhanget erinra om följande:

Inom ramen för nuvarande NIS-reglering följer idag samtliga sektorer gemensamma föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete och sektorsspecifika föreskrifter om säkerhetsåtgärder. MSB utfärdar föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete medan föreskrifterna om säkerhetsåtgärder utfärdas av tillsynsmyndigheterna för nätverk och informationssystem i sina respektive sektorer.

[8] Delbetänkandet s 189 ff

Andelen av föreskriftskrav som innehåller krav på sektorsunika åtgärder, exempelvis krav på säkerhet i nätverk- och informationssystem som är särskilda för en specifik sektor, är i nuvarande NIS-reglering mycket liten. De befintliga föreskrifterna visar snarare att det som behöver regleras inte skiljer sig nämnvärt i sak, utan att skillnaderna snarare beror på olika prioriteringsnivå hos de föreskrivande myndigheterna men även på att olika myndigheter har olika sätt att reglera och olika grad av erfarenhet av att kravställa på cybersäkerhetsområdet. Kraven på säkerhetsåtgärder i nuvarande NIS-reglering är därmed mer fragmenterad än den ur ett systemperspektiv skulle behöva vara.

MSB:s bedömning är att skillnaderna i utformning av kraven i nuvarande NIS-reglering sannolikt utgjort ett mindre problem att hantera för tillsynsmyndigheter och verksamhetsutövare, eftersom de inte omfattat hela organisationen utan endast de nätverk och informationssystem som används för den samhällsviktiga tjänsten.

Med det utökade tillämpningsområdet för NIS2 kommer utredningens förslag att öka fragmenteringen av området ännu mer och resultera i ett flertal överlappande föreskrifter. Dels genom sektorsvisa krav på säkerhetsåtgärder men även genom att det som tidigare varit gemensamt – kraven på systematiskt och riskbaserat informations- och cybersäkerhetsarbete – nu ska regleras separat för varje sektor. Till det kommer att varje tillsynsmyndighet inom sin sektor ska föreskriva om utbildning inom systematiskt och riskbaserat cybersäkerhetsarbete och reglera krav på hur verksamhetsutövarna ska genomföra utbildningen.

Konsekvensen av förslaget blir därmed inte att varje tillsynsmyndighet reglerar separata sektorer. Tvärtom blir det så att en verksamhetsutövare som hör till fler än en sektor kommer att träffas av flera olika föreskrifter om samma sak (systematiskt och riskbaserat informations- och cybersäkerhetsarbete, säkerhetsåtgärder och utbildning).

Exempelvis kommer kommuner och regioner, som bedriver verksamhet inom flera sektorer, att behöva förhålla sig till flera olika föreskrifter som alla behandlar kraven på systematiskt och riskbaserat informations- och cybersäkerhetsarbete, utbildning samt särskilda föreskrifter om säkerhetsåtgärder.

290 kommuner kan därmed komma att behöva följa ett flertal föreskrifter från olika tillsynsmyndigheter såsom Transportstyrelsen, Livsmedelsverket, Energimyndigheten, IVO och MSB som samtliga gäller för hela kommunens verksamhet och reglerar samma sak – dvs hur det systematiska informations- och cybersäkerhetsarbetet ska bedrivas, vilka säkerhetsåtgärder som ska vidtas och hur utbildning på området ska utformas.

Länsstyrelserna i Norrbottens, Skånes, Stockholms och Västra Götalands län föreslås som nya tillsynsmyndigheter för en rad sektorer inom varsitt utpekat geografiskt område. I tillsynsuppgiften ingår enligt utredningens förslag att som nämnts utfärda föreskrifter för hur det systematiska informations- och cybersäkerhetsarbetet ska bedrivas, vilka säkerhetsåtgärder som ska vidtas och hur utbildning på området ska utformas. Detta får till konsekvens att verksamhetsutövare inom sektorerna Avfallshantering, Forskning, Tillverkning, produktion och distribution av kemikalier Tillverkning av datorer, elektronikvaror och optik, Tillverkning av elapparatur och Tillverkning av övriga maskiner kommer att, trots att de tillhör samma sektor, omfattas av olika föreskrifter beroende på

verksamhetens geografiska placering. De enda av länsstyrelsernas tillsynssektorer som får en nationellt samlad reglering är offentlig förvaltning och lärosäten med examenstillstånd eftersom utredningen där föreslår att MSB utfärdar föreskrifterna.

MSB anser att förslaget på fördelning av föreskriftsmandat har påtagliga brister ur verksamhetsutövarnas perspektiv. Inte heller följer det reglerna för statlig regelgivning och resursanvändning. Det måste anses orimligt att flera myndigheter ska reglera samma sak i olika föreskrifter.

Flera expertmyndigheter, såsom Säkerhetspolisen, Transportstyrelsen och Integritetsskyddsmyndigheten, har föreslagit att MSB, för att förhindra fragmentering, överlappande regelverk och onödigt omfattande regelbestånd, ska ges befogenhet att meddela grundföreskrifter för samtliga sektorer. NIS-tillsynsmyndigheterna kan sedan, vid behov och med stöd av sin sektorsspecifika kompetens, komplettera grundföreskrifterna med särskilda föreskrifter med stärkta krav där behoven inom sektorn kräver det, exempelvis för särskilda industriella styr- och kontrollsystem.[9] MSB delar den uppfattningen.

Både privata och offentliga verksamhetsutövare samt tillsynsmyndigheter skulle gynnas av gemensamma grundföreskrifter. Dels för att underlätta efterlevnad och dels för att underlätta tillsyn. Ett sådant förfarande utgör otvetydigt även en väsentligt mer effektiv användning av det offentligas resurser eftersom tillsynsmyndigheterna kan fokusera på sina sektorsspecifika delar och verksamhetsutövarna kan fokusera på själva säkerhetsarbetet.

MSB bedömer även att gemensamma grundföreskrifter skulle gynna behovet av att höja den nationella nivån på informations- och cybersäkerhetsområdet i samhällsviktig verksamhet. Något som efterfrågas inom ramen för stärkt totalförsvar.

Utredningen har framfört att en sådan lösning skulle riskera leda till tolkningssvårigheter och motstridiga krav såvida inte det handlar om verkställighetsföreskrifter vilka i sin tur, enligt utredningen, inte är lämpliga att använda på grund av att de i första hand är tänkta att vara av administrativ karaktär.[10]

MSB delar inte utredningens bedömning att en lösning med grundföreskrifter som, där behov finns, kompletteras med starkare sektorsspecifika krav skulle leda till motstridiga krav och tolkningssvårigheter. Motsvarande upplägg tillämpas exempelvis i föreskrifterna för säkerhetsåtgärder i informationssystem för statliga myndigheter.[11] MSB ser snarare fullständigt överlappande föreskrifter som en betydligt större risk. Det skapar tolkningssvårigheter och en inbyggd konflikt som drabbar alla verksamhetsutövare som hör till flera sektorer.

I betänkandet presenteras argumentet att verksamhetsutövarna som regleras i annan nationell reglering i sektorn Elektronisk kommunikation nyligen infört reglering och att det skulle bli betungande med nya föreskrifter i form av grundföreskrifter. [12] Utredningen

[9] Delbetänkandet s. 190
[10] Delbetänkandet sid 229f.
[11] 2 § Om en annan författning innehåller en bestämmelse som ställer högre krav än kraven i dessa föreskrifter tillämpas den bestämmelsen.
[12] Delbetänkandet sid 228f

konstaterar även att verksamhetsutövare såsom leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster, leverantörer av marknadsplatser online, sökmotorer, plattformar för sociala nätverkstjänster samt kvalificerade tillhandahållare av betrodda tjänster kommer att omfattas av kommissionens genomförandeakt som ska antas senast den 17 oktober 2024.[13] Utredningen konstaterar att i och med detta kommer det att finnas skillnader i de krav som ställs på olika verksamhetsutövare redan på EU-nivå samt att med en gemensam föreskrift skulle det ändå finnas ett behov av sektorsspecifika regleringar

MSB vill framföra att ett alternativt sätt att tillgodose den sektorns önskemål är att låta sektorn undantas från de gemensamma lösningar som förordas.

Utredningens förslag att föreskrifterna ska ensas genom att MSB ges i regeringsuppdrag att utarbeta en vägledning som stöd för tillsynsmyndigheternas föreskriftsarbete är enligt MSB otillräckligt och adresserar inte problematiken med regelmängden.

Förslag:

5. Ge MSB bemyndigande att utfärda föreskrifter rörande systematiskt och riskbaserat informations- och cybersäkerhetsarbete, samt föreskrifter med grundläggande krav på säkerhetsåtgärder (riskhanteringsåtgärder) och utbildning.

6. Ge tillsynsmyndigheterna bemyndigande att där behov finns utfärda kompletterande föreskrifter med särskilda krav på säkerhetsåtgärder och utbildning samt MSB motsvarande bemyndigande när det gäller sektorerna offentlig förvaltning och lärosäten med examenstillstånd.

5. Använd etablerade begrepp

Utredningens utgångspunkt är som följer av avsnitt 5.2.1 att direktivet inte ska införlivas direktivnära utan att förslagen ska utformas utifrån den systematik och terminologi som används i svensk rätt och att ett normalt språkbruk ska eftersträvas. Utredningen konstaterar även att detta följer uttryckligen av regeringens direktiv att den terminologi som används i direktiven ska anpassas till vedertagna begrepp i nationell reglering.[14] Utredningen gör också bedömningen att det inte är möjligt att anpassa begreppen i cybersäkerhetslagen till begreppen i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster eftersom kraven på åtgärder i NIS-direktivet.[15]

MSB stödjer användningen av vedertagna begrepp och normalt språkbruk. Myndigheten menar därför att formuleringen ”systematiskt och riskbaserat informationssäkerhetsarbete” bör kompletteras med ”cybersäkerhet” med anledning av att EU nu har definierat cybersäkerhet i cybersäkerhetsakten och att begreppet används

[13] Delbetänkandet sid 229
[14] Delbetänkandet sid 194
[15] Delbetänkandet sid 191

genomgående i övriga delar av betänkandet.[16] Ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete är enligt MSB heltäckande och tydliggör ett allriskperspektiv i arbetet med skydd för nätverk och informationssystem. Det svarar även mot väletablerat sätt att arbeta och existerande standarder. Genom detta kopplas etablerat språkbruk i nationell reglering tydligt ihop med den nya legaldefinitionen i EU. MSB anser därför att det ska tydligt framgå att cybersäkerhet utgör en viktig del i det systematiska och riskbaserade informationssäkerhetsarbetet.

Myndigheten anser även att begreppet ”riskhanteringsåtgärder” ska ersättas med ”säkerhetsåtgärder” för att ansluta till etablerat språkbruk på området. MSB delar inte i utredningens bedömning att kraven i NIS2-direktivet i hög grad avviker från kraven i NIS-direktivet. Den huvudsakliga skillnaden är enligt MSB:s uppfattning att de har konkretiserats i NIS2-direktivet jämfört med kraven i nuvarande NIS-reglering. Det finns en etablerad uppsättning av åtgärder som kan införas för att skydda nätverk och informationssystem. Att byta begreppet ”säkerhetsåtgärder” mot ”riskhanteringsåtgärder” skapar en enligt MSB felaktig bild av att det är något annat än den etablerade uppsättningen av åtgärder som används för att skydda nätverk och informationssystem. Säkerhetsåtgärder är ett etablerat samlingsbegrepp för dessa åtgärder, både nationellt och internationellt.

Förslag:

7. Komplettera formuleringen systematiskt och riskbaserat informationssäkerhetsarbete med ”cybersäkerhet” och använd ”systematiskt och riskbaserat informations- och cybersäkerhetsarbete”.

Använd begreppet ”säkerhetsåtgärder” istället för ”riskhanteringsåtgärder”.

6. Förtydliga språk och krav avseende incidentrapporteringen

MSB instämmer i stort med utredningens förslag på utformningen av incidentrapporteringen men föreslår justeringar i 3 kapitlet i den föreslagna cybersäkerhetslagen för att förenkla för verksamhetsutövarna samt bättre spegla de krav som ställs i NIS2-direktivet.

Utredningen har valt att inte, såsom det anges i artikel 23 p 4 i NIS2-direktivet, ta med kravet på att rapportering ska lämna information ” utan onödigt dröjsmål och under alla omständigheter” kopplat till respektive tidsintervall för rapportering.[17]

MSB bedömer att utredningens skrivning i 3 kapitlet 5 – 7 §§ cybersäkerhetslagen där endast kraven på tid för olika typer av rapportering anges som ”inom 24 timmar”, ”inom 72 timmar” respektive ”inom en månad” inte alls ger samma tydlighet för verksamhetsutövaren att informationsdelningen ska ske så snart som möjligt och att 24, 72

[16] Cybersäkerhet definieras i EU:s cybersäkerhetsakt som ”all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot”. Cyberhot definieras i samma reglering som ”en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare dessa system och andra personer.”
[17] Delbetänkandet sid 201

och en månad snarast ska ses som en bortre gräns. MSB anser därför att tidsangivelserna ska genomgående kompletteras med ” utan onödigt dröjsmål och under alla omständigheter” för att ansluta till direktivets skrivningar.

Utredningen har även i 5 § valt att använda begreppet *varning* om den initiala rapporteringen. Valet speglar begreppet *tidig varning* som används i direktivet.

MSB anser att det finns en påtaglig risk att ordvalet kan leda till förvirring. Dels eftersom en stor andel av de händelser som rapporteras är icke-antagonistiska och det inte föreligger någon omedelbar risk för fler liknande och efterföljande incidenter – det krävs inte en ”varning” i ordets vanliga betydelse, dels för att det riskerar att förväxlas med de varningar CSIRT-enheten skickar ut när verksamheter skyndsamt behöver vidta åtgärder. MSB föreslår därför i första hand att skrivningen endast innebär ett krav på att verksamhetsutövaren ska underrätta CSIRT-enheten och om det bedöms finnas ett behov av att benämna denna underrättelse särskilt att begreppet *notifiering* används istället för *varning* eftersom det ansluter till etablerat språkbruk.

Utredningen har vidare föreslagit i 6 § att verksamhetsutövaren ska inom 72 timmar från tidpunkten från kännedom göra en incidentanmälan till CSIRT-enheten om betydande incidenter. Den ska innehålla en inledande bedömning av hur allvarlig den betydande incidenten är, konsekvenserna av den och förekomsten av angreppsindikatorer.

MSB konstaterar att beskrivningen i artikel 23 p 4 b) i NIS2-direktivet av vilken information som ska lämnas är både mer omfattande och bättre motsvarar var en CSIRT-enhet behöver för att kunna stödja drabbade verksamhetsutövare. Det vill säga: ”en inledande bedömning av den betydande incidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer.”

För att CSIRT-enheten, i de fall där det behövs, ska kunna ge råd och stöd behöver en incidentanmälan innehålla en *bedömning av incidenten* och vad som har hänt, inte enbart hur allvarligt det inträffade är och vilka konsekvenser händelsen får. Vidare innebär *förekomsten* av angreppsindikatorer enbart om verksamheten har identifierat tecken på att incidenten kan ha sin grund i brottslig gärning. Detta är en förutsättning för CSIRT-enheten att kunna ge adekvata råd och stöd till både den drabbade och andra drabbade verksamheter och även förbättra sin lägesförståelse.

Förslag:

8. Justera skrivningarna i 3 kap. 5 - 7 §§ i förslaget till cybersäkerhetslag för att ansluta till etablerat språkbruk och spegla motsvarande krav i artikel 23 p 4:

5 § Verksamhetsutövaren ska ~~som en varning~~ underrätta CSIRT-enheten om betydande incidenter **utan onödigt dröjsmål och under alla omständigheter inom** 24 timmar efter det att verksamhetsutövaren fått kännedom om den. Av underrättelsen ska framgå om det finns misstanke om att incidenten orsakats uppsåtligen och om incidenten kan ha gränsöverskridande effekter.

6 § Verksamhetsutövaren ska också **utan onödigt dröjsmål och under alla omständigheter** inom 72 timmar från tidpunkten **för** kännedom göra en incidentanmälan till

CSIRT-enheten om betydande incidenter. Den ska innehålla en inledande bedömning av **en inledande bedömning av den betydande incidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer.** Vidare ska tidigare **underrättelse** enligt 5 § uppdateras.

7 § Verksamhetsutövaren ska **senast** en månad ~~från~~ **efter underrättelsen** i 5 § lämna en slutrapport till CSIRT-enheten. Om incidenten fortfarande är pågående ska i stället en lägesrapport lämnas. Lägesrapporten ska kompletteras med en slutrapport en månad efter det att incidenten har hanterats. Slutrapporten eller lägesrapporten ska innehålla en beskrivning av […]

7. Inför möjlighet att ingripa vid bristande systematiskt och riskbaserat informations- och cybersäkerhetsarbete

Enligt utredningens förslag ska en tillsynsmyndighet inte ha möjlighet att ingripa med förelägganden, sanktionsavgifter och liknande mot verksamhetsutövare som inte följer föreskriftskrav på att bedriva systematiskt och riskbaserat informations- och cybersäkerhetsarbete. Sådana ingripanden ska däremot kunna göras om verksamhetsutövaren inte uppfyllt krav när det gäller riskhanteringsåtgärder eller utbildning. Av förslaget till cybersäkerhetslag följer i 3 kapitlet 1 § att riskhanteringsåtgärder ska utgå från ett allriskperspektiv och en riskanalys och vara proportionella i förhållande till risken. De ska även utvärderas.

MSB:s bedömning är att tillsynsmyndigheterna behöver ha möjlighet att både tillsyna och ingripa, på ett sådant sätt att organisationer bygger den säkerhet de behöver. Tillsyns- och ingripandemandaten måste därför vara ordnade så att en tillsynsmyndighet kan följa upp, och vid behov ingripa, så att verksamhetsutövare på ett ändamålsenligt sätt först identifierar, analyserar och bedömer sina risker, därefter identifierar, analyserar, bedömer, väljer och inför åtgärder för att i tillräcklig utsträckning åtgärda de risker som behöver åtgärdas, samt i efterhand följer upp att de införda åtgärderna fick avsedd verkan och tillräcklig verkan.

Återkommande undersökningar, bland annat genom Cybersäkerhetskollen[18], visar att det systematiska och riskbaserade informations- och cybersäkerhetsarbetet inte prioriteras. Det leder i sin tur till att det inträffar incidenter som hade kunnat undvikas om organisationer bedrev ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete. MSB vill betona att ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete är grunden för att en verksamhetsutövare ska kunna välja och utforma riskhanteringsåtgärder (säkerhetsåtgärder) inklusive att hålla skyddet proportionellt över tid utifrån förändringar av hot mot verksamhetsutövarens informationsbehandling och sårbarheter i verksamhetsutövarens nätverk- och informationssystem. Arbetet med riskanalys och utvärdering är grundläggande beståndsdelar i ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete.

[18] Tidigare Infosäkkollen och It-säkkollen, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/arbeta-systematiskt-informationssakerhet-och-cybersakerhet/cybersakerhetskollen/

Brister när det gäller det systematiska och riskbaserade informations- och cybersäkerhetsarbetet påverkar därför riskhanteringsåtgärderna.

MSB noterar också att i nu gällande NIS-reglering, till skillnad mot utredningens förslag, omfattas arbetet med riskanalys som ska ligga till grund för val av säkerhetsåtgärder av tillsyn och möjligheter att utfärda både förelägganden och sanktioner vid bristande kravuppfyllnad.[19]

Enligt myndighetens bedömning innebär därför avsaknaden av ingripandemöjligheter för systematiskt och riskbaserat informations- och cybersäkerhetsarbete till och med sämre möjligheter att styra verksamhetsutövarna mot ändamålsenliga riskhanteringsåtgärder (säkerhetsåtgärder) än vad nuvarande reglering ger.

MSB anser att detta är problematiskt. Det är inom ramen för det systematiska och riskbaserade informations- och cybersäkerhetsarbetet som information och underlag inhämtas och förutsättningar skapas för att lära av incidenter, identifiera och analysera risker, samt bedöma om införda säkerhetsåtgärder är ändamålsenliga. Om det systematiska och riskbaserade informations- och cybersäkerhetsarbetet inte bedrivs på en tillräckligt hög nivå så kommer i allmänhet inte riskanalyserna som organisationen genomför i tillräcklig utsträckning identifiera och korrekt analysera organisationens risker. Det leder i sin tur till att organisationer riskerar att införa säkerhetsåtgärder i otillräcklig utsträckning, eller att de inför fel säkerhetsåtgärder.

MSB anser därför att tillsynsmyndigheterna ska ges möjligheter att ingripa även när verksamhetsutövarna brister i att följa föreskriftskrav rörande det systematiska och riskbaserade informations- och cybersäkerhetsarbetet. Utredningens förslag snarast försämrar möjligheterna att stärka ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete i samhällsviktig verksamhet vilket inte gynnar vare sig verksamhetsutövarna eller arbetet med att stärka totalförsvaret.

Förslag:

9. Ge tillsynsmyndigheter möjligheter att ingripa mot verksamhetsutövares brister i sitt systematiska och riskbaserade informations- och cybersäkerhetsarbete genom en ny punkt 4 i 5 kap 1 § i förslaget till Cybersäkerhetslag:

p4. systematiskt och riskbaserat informations- och cybersäkerhetsarbete enligt 3 kap. 2 §.

8. Stärk tillsynssamordningen

Enligt utredningen ska MSB fortsatt leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn. MSB ges inget ytterligare mandat vad gäller tillsynssamordningen. Inte heller ålägger utredningen tillsynsmyndigheterna att samordna sig.[20]

[19] 12, 28 – 29 §§ lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
[20] Delbetänkandet sid 209ff och 240ff

I betänkandet redogörs för hur det i olika forum och analyser[21] har framförts ett behov av ökad tillsynssamordning redan vid tillämpningen av nu gällande NIS-reglering. I samband med utredningsarbetet har flera expertmyndigheter och andra organisationer framfört att NIS2-regleringen kommer öka behovet av tillsynssamordning ytterligare.[22] MSB delar den bilden.

Med nuvarande förslag tillkommer fem nya tillsynsmyndigheter.[23] Samtliga 11 tillsynsmyndigheter ska bedriva tillsyn av alla delar av en aktörs verksamhet som inte omfattas av en annan tillsynsmyndighets tillsyn. Med flera nya sektorer och tillsynsmyndigheter, samt förslaget om överlappande föreskriftsmandat ökar komplexiteten avsevärt och förutsättningarna att uppnå effektiv och likvärdig tillsyn förändras därmed, samtidigt som ett mycket stort antal verksamhetsutövare nu kommer att omfattas i flera sektorer och behovet av likvärdighet ökar.

MSB vidhåller därför att det inte är rimligt att lämna tillsynssamordningen oförändrad. Särskilt inte då utredningen redan konstaterat att nuvarande samordningsform redan idag uppfattas som bristfällig av myndigheterna. Ett samordningsuppdrag kräver resurser och samverkan från alla ingående aktörer. Ett effektivt samordningsuppdrag i en komplex miljö blir därför möjligt först när det råder tydlighet om hur de nationella tillsynsmyndigheterna och samordningsmyndigheten ska bistå varandra. Ett sådant förtydligande bör, om utredningen inte anser att den bör framgå redan i författning, i vart fall förtydligas i tillsynsmyndigheternas och samordnarens regleringsbrev. Inte minst mot bakgrund av de skyndsamhetskrav som kan komma att uppstå vid gränsöverskridande verksamhet är det väsentligt att samordningsrutiner och åligganden är tydliga och förankrade.

Slutligen vill MSB framföra följande:

Av 13 § i förslaget till cybersäkerhetsförordning framgår att *”Om tillsyn över en verksamhetsutövare utövas av fler än en tillsynsmyndighet ska respektive tillsynsmyndighet inte utöva tillsyn gällande den del av verksamheten som anges som en annan tillsynsmyndighets tillsynsområde i 8 §.”* Enligt MSB:s bedömning innebär det att de delar av verksamhetens nätverk och informationssystem som inte hör till en NIS-sektor kan komma att tillsynas av flera berörda tillsynsmyndigheter.

Så som 2 § i förslaget är formulerad *” Tillsynsmyndigheten ska utöva tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs.”* förefaller det som att utredningen därmed menar att en tillsynsmyndighet som ska bedriva tillsyn i en sektor ska bedriva

[21] Se bland annat Utvärdering av resultatet av Sveriges implementering av NIS-direktivet, Myndigheten för samhällsskydd och beredskap, slutrapport 2022-12-20.
[22] Delbetänkandet sid 209.
[23] Dessa nya föreslagna tillsynsmyndigheter är Länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län (tillsyn för sektorn offentlig förvaltning) samt Läkemedelsverket (för del av hälso- och sjukvårdssektorn och del av sektorn tillverkning). IVO föreslås vara tillsynsmyndighet för sektorn hälso- och sjukvård istället för Socialstyrelsen.

tillsyn dels utifrån sina egna föreskrifter men även med andra NIS2-tillsynsmyndigheters föreskrifter som verksamhetsutövaren är ålagd att följa.[24]

En privat verksamhetsutövare som bedriver verksamhet både inom energi och transport skulle då få sina nätverk och informationssystem granskade av Energimyndigheten och Transportstyrelsen som båda ska basera sin tillsyn på den egna föreskriften men även på den andra myndighetens föreskrifter. Tillsynen över en region skulle i motsvarande situation kunna behöva samtidigt förhålla sig till åtminstone Transportstyrelsens, IVO:s och MSB:s föreskrifter.

Vissa verksamhetsutövare, som exempelvis kommunerna, kommer då att drabbas av multipel tillsyn av olika myndigheter i samma verksamhet. Organisationer kan även komma att bli sanktionerade på olika sätt.

Förslag:

10. Ge MSB i uppgift att stå för samlad metodik samt uppföljning av utförd tillsyn, bland annat genom Cybersäkerhetskollen.

11. Ge tillsynsmyndigheterna i uppgift att, om inte särskilda skäl talar emot, aktivt bidra till samordning när det gäller planering, metodik och uppföljning.

9. Fördjupa konsekvensanalysen

Enligt utredningens förslag bör regeringen för år 2025 ge MSB ett förstärkt anslag med två miljoner kronor för löpande kostnader avseende NIS2.

MSB fick möjlighet att under korta tidsförhållanden göra en kostnadsuppskattning. Myndigheten bedömer att en mer fullödig analys behöver göras men kan redan nu konstatera att det förstärkta anslag med två miljoner kronor som utredningen föreslår inte är tillräckligt för att hantera de kostnadsökningar som föranleds av NIS2-direktivets implementering.

Förslag:

12. Fördjupa konsekvensanalysen ytterligare.

10. Övriga synpunkter - koppla NIS2 och CER-regleringen mot beredskapssystemet

Det har inte ingått i utredningens uppdrag att närmare analysera hur NIS2-regleringen ska implementeras i svensk rätt för att kunna stärka pågående arbete med utveckling av krisberedskap och totalförsvar.

När ett så omfattande regelverk som NIS2- och CER-direktiven implementeras i svensk rätt med så många praktiska kopplingar till ett aktivt och prioriterat arbete att stärka beredskapsarbetet och totalförsvaret är det enligt MSB:s uppfattning av central vikt att

[24] I delbetänkandet sid 225 redogörs för tillsynsmyndighetens uppdrag och några undantag eller begränsningar till vilka föreskrifter som ska ligga till grund för tillsyn görs inte. Frågan adresseras inte heller i delbetänkandet sid 242 som rör när verksamhetsutövare står under tillsyn av flera myndigheter.

relationen och rollfördelningen mellan dessa båda system hanteras samlat. Detta särskilt eftersom de som kommer att omfattas av NIS2- och CER-regleringarna är viktiga aktörer i beredskapssystemet.

Kravställning, incidentrapportering och tillsyn enligt NIS2- och CER-regleringarna kommer enligt MSB:s uppfattning kunna stärka Sveriges motståndskraft vid alla typer av störningar. För att kunna koppla de behov av förmågehöjning som identifieras i beredskapssektorerna till de möjligheter att kravställa och bygga lägesbild som NIS2- och CER-regleringarna innebär behöver det finnas strukturella och organisatoriska kopplingar mellan Sveriges beredskapssystem och NIS2- och CER-regleringarna. Exempelvis behöver enligt MSB:s bedömning utpekade tillsynsmyndigheter aktivt delta i den samverkan som nu byggs upp inom beredskapssystemet. Flertalet, men inte alla, av de utpekade tillsynsmyndigheterna deltar i respektive beredskapssektor. MSB ser en stor risk att synergier går förlorade om inte samtliga NIS-tillsynsmyndigheter deltar i motsvarande beredskapssektors arbete.

Förslag:

13. Inkludera en bilaga om relationen mellan NIS2- och CER-regleringarna respektive beredskapssystemet i kommande proposition.

14. Regeringen bör utnämna de NIS-tillsynsmyndigheter som idag inte ingår i en beredskapssektor, exempelvis IVO, till beredskapsmyndigheter enligt beredskapsförordningen och placera dem i en beredskapssektor (för IVO i beredskapssektorn Hälsa, vård och omsorg).

I detta ärende har generaldirektör Charlotte Petri Gornitzka beslutat. Johan Turell har varit föredragande. I den slutliga handläggningen har också avdelningschefen Åke Holmgren deltagit.

Charlotte Petri Gornitzka Johan Turell

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240 Fax: 010-240 56 00
registrator@msb.se www.msb.se
Org.nr: 202100-5984