Försvarsdepartementet
Rättssekretariatet
e-post: fo.remissvar@regeringskansliet.se
Kopia: visnja.raguz@regeringskansliet.se

Stockholm den 28 maj 2024

Remissvar över delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18), dnr Fö2024/00496

HI3G Access AB (”Tre”) har beretts tillfälle att lämna remissvar över rubricerat förslag, fortsättningsvis benämnt ”Förslaget”. Förslaget innebär ett införlivande av det så kallade NIS2-direktivet ((EU) 2022/2555) som rör säkerhet i nätverks- och informationssystem. Utredningen föreslår att detta huvudsakligen sker genom en ny lag om cybersäkerhet. Regleringen utvidgas till att omfatta fler verksamheter än tidigare, däribland telekomsektorn. NIS2-direktivet ersätter det tidigare NIS-direktivet från 2016, som genomfördes i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. NIS2-direktivet ersätter också bestämmelserna om säkerhet för nät och tjänster i art 40-41 i direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation, som genomfördes i svensk rätt genom lagen (2022:482) om elektronisk kommunikation 8 kap 1-4 §§.

Tre får med anledning av det remitterade Förslaget lämna följande allmänna och särskilda synpunkter.

1. Allmänna synpunkter

Utredningen har lyckats med att ta fram en enkelt utformad och begriplig lagstiftning som sätter utgångspunkterna för vad som krävs för att uppnå en hög cybersäkerhetsnivå i Sverige. Tre ser också att utredarens analys i viss utsträckning har resulterat i ett förslag som förenklar utformningen av kraven i NIS2-direktivet.

Förenkling välkomnas men ansträngningen att förenkla bör också ses i ljuset av den relativt brokiga floran av befintlig och kommande lagstiftning på informationssäkerhetsområdet. Under en relativt kort tidsperiod har det tillkommit en ny dataskyddsreglering (2018 dataskyddsförordning (EU) 2016/679) en ny säkerhetsskyddslag (2018:585) och en ny lag om elektronisk kommunikation (2022:482) där samtliga, inklusive ändringsregleringar, förordningar och föreskrifter, omfattar krav på säkerhet och skydd av information. Förändringstrycket har även fortsatt inom EU med nya säkerhetsregleringar på cybersäkerhetsområdet, som NIS2- och CER-direktiven utgör en del av, och som ingår i EU:s digitala agenda för 2030.[1] Därtill innebär det rådande säkerhetsläget att krav rörande Sveriges totalförsvar får allt större relevans för telekomsektorn.

En huvudförklaring till att lagkravens utformning på dessa områden väsentligen skiljer sig åt torde bero på bristande samordning på EU nivå [2] men också att nationell lagstiftning på säkerhetsområdet inte samordnas med EU lagstiftning samt att tillsynsmyndigheterna inte är samordnade utan endast svarar för ”sin” lagstiftning.

När nya regler som införlivar NIS2 och CER införs i svensk lagstiftning är det viktigt att lagstiftaren så långt som möjligt undviker fragmentering på informationssäkerhetsområdet och motverkar lagstiftningseffekter som innebär att företag förutsätts arbeta med flertalet processer och åtgärdsprogram för olika skyddsintressen men där ändamålet med åtgärderna överlappar varandra, dvs. skydda verksamheten, uppgifterna, tjänsterna och användarna. Tre anser därför att det är viktigt med en samordning och tydlighet i hur dessa regelverk ska förhålla sig till varandra samt att överlappande krav om säkerhet i största möjliga mån bör undvikas.

Regelverkens bestämmelser om säkerhetsåtgärder liknar varandra men skillnaderna i utformningen och bristande samordning kombinerat med höga sanktioner motverkar

[1] Även Cyber Security Act (2019), Cyber Resillience Act (förslag), e-Privacy regulation (förslag), AI act (2024) och Cyber Solidarity Act (förslag).

[2] Regelverkens relation till varandra brukar ofta uttryckas så ”detta direktiv X ska inte påverka förordning Y” eller att medlemsstaterna får göra undantag för entiter inom området för nationell säkerhet (se t.ex. NIS2 direktivet ingresspunkt 14 och 9) utan närmare reglering hur regelverken ska förhålla sig till varandra.

synergier som företagen annars skulle kunna ha stora fördelar av och som skulle effektivisera och förbättra säkerhetsarbetet [med skydd av personuppgifter, skydd av nät och tjänster, skydd av Sveriges säkerhet och totalförsvar].

När förslaget till cybersäkerhetslag nu ska ersätta bestämmelserna i LEK om säkerhet i nät och tjänster, till vilka ett anpassningsarbete nyligen har genomförts då bl.a. denna del i LEK ändrades så sent som sommaren 2022, är det utomordentligt viktigt att cybersäkerhetslagens efterföljande föreskrifter om bl.a. riskhanteringsåtgärder, ett systematiskt riskhanteringsarbete och incidentrapportering utformas nära och i överensstämmelse med de bestämmelser som redan gäller idag för telekomsektorn och som reglerar både informations-, och driftsäkerhet.

Förslaget ger emellertid MSB mandat att meddela föreskrifter om incidentrapportering. Eftersom PTS är expertmyndigheten på telekomområdet och har arbetat med säkerhet och incidentrapportering och anknytande föreskrifter under lång tid är det lämpligare och skulle ge bättre förutsättningar till anpassning av rapporteringskraven att PTS ha föreskriftsrätt även här.

Tre noterar att i det förlängda utredningsuppdraget[3], som ska redovisas till hösten, ska utredaren bl.a. ta ställning till och överväga om bestämmelserna i offentlighets- och sekretesslagen (2009:400) innebär ett tillräckligt skydd eller behöver stärkas. Idag gäller vid tillsyn av säkerhetsfrågor huvudsakligen en *svag sekretess*, t ex 15 kap 2 §, 18 kap 8 § och 30 kap 23 § enligt offentlighets- och sekretesslagen (2009:400), dvs. ett rakt skaderekvisit vilket innebär att inlämnande uppgifter som huvudregel är offentliga hos myndigheten. Eftersom Förslaget omfattar nya tillsynsbefogenheter och ställer ytterligare krav på verksamhetsutövare att lämna information, genomgå revisioner och säkerhetsskanningar som kan omfatta mycket känsliga uppgifter finns det ett behov av starkare och mer omfattande sekretesskydd för de uppgifter som tillsynsmyndigheten begär in, men också i sin tur delger andra myndigheter.

Vidare är det angeläget att verksamhetsutövarna ges en rimlig tid för anpassning till de nya reglerna, som i övrigt kommer att fyllas ut av föreskrifter och av EU kommissionen antagna genomförandeakter. Dessutom kvarstår utredningens förslag av övriga delar av uppdraget, avseende CER-direktivet m.m., som väntas i september med efterföljande remissbehandling, propositionsberedning samt framtagande av föreskrifter hos respektive tillsynsmyndighet. I

[3] Kommittéedir. 2024:3.

ljuset av det framstår ett ikraftträdandedatum per den 1 januari 2025 som alltför kort tid utan bör skjutas fram.

2. Särskilda synpunkter

1 kap. 2 § - uttryck i lagen

Uttrycken i Förslaget beskrivs på lite olika sätt, men kan med fördel göras mer enhetliga. T.ex. definieras uttrycket betydande cyberhot, medan definitionen av cyberhot så hänvisas till Cybersäkerhetsakten. Det finns i övrigt hänvisningar till nio olika rättsakter där uttrycken definieras. En annan systematik som valts är att skriva in definitionen direkt i lagtexten, som gjorts om incidentrapportering (avseende definitionen av betydande incidenter). Det hela blir en förhållandevis svårläst lagstiftning och Tre föredrar att uttryck i lagen anges på samma ställe, på ett enhetligt sätt och att definitionerna skrivs ut i klartext.

1 kap. 13 § - undantag för säkerhetskänslig verksamhet

Tre avstyrker Förslaget.

Enligt Förslaget ska lagen om cybersäkerhet inte vara tillämplig på verksamhetsutövare som bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen. Om verksamhetsutövaren bedriver säkerhetskänslig verksamhet till viss del så gäller lagen om cybersäkerhet för den övriga delen av verksamheten. Effekten kan då bli att den känsligaste delen av verksamheten, som är så pass samhällsviktig att den har bäring på den nationella säkerheten, inte omfattas av lagen om cybersäkerhet. Undantaget kan också innebära att två olika regelverk kan bli tillämpliga parallellt för samma verksamhet, t.ex. för ett och samma IT-system som stödjer såväl den säkerhetskänsliga verksamheten som övrig verksamhet.

Undantaget medför andra märkliga effekter. Det har att göra med att det är verksamhetsutövare som ska bedöma om verksamheten är av betydelse för Sveriges säkerhet och därmed omfattas av säkerhetsskyddslagen. I praktiken blir då effekten att det är verksamhetsutövaren som avgör om cybersäkerhetslagen eller säkerhetsskyddslagen är tillämplig eller ej och därmed vilka krav på åtgärder som gäller avseende incidentrapportering, former för tillsyn och ingripanden. T.ex. så finns det inte något krav på att rapportera betydande incidenter enligt 3 kap. i cybersäkerhetslagen om verksamheten

omfattas av säkerhetsskyddslagen, oaktat om incidenten utgör ett allvarligt cyberangrepp av betydelse för åtgärder såväl nationellt som internationellt. Problematiken ligger huvudsakligen i säkerhetsskyddslagens systematik.

Tre anser istället att alla samhällsviktiga verksamheter som utgångspunkt ska omfattas av lagen om cybersäkerhet men att lagstiftaren och förvaltningsmyndigheterna får, när så är nödvändigt och med hänsyn till skyddsintressets särart och behov av anpassningar, införa kompletterande bestämmelser för Sveriges säkerhet och kanske även Sveriges totalförsvar.

3 kap. 1 § - säkerhetsåtgärder

Bestämmelserna om säkerhetsåtgärder hanteras bara övergripande i Förslaget vilket förutsätter att kraven konkretiseras närmare i föreskrifter, och i avsaknad av detta kan inte konsekvenserna av alla delar av regleringen bedömas.

Tre tillstyrker Förslaget delvis men lämnar några förslag till förtydliganden.

Utgångspunkten för säkerhetskraven i LEK är att tillhandahållaren ska vidta åtgärder för att hantera risker som hotar säkerheten i nät och tjänster, dvs. i telekomverksamheten. Säkerhet i nät och tjänster är ett begrepp som följer av telekomdirektivet (”Kodexen” som införlivats i LEK). I utredningen görs en jämförelse av säkerhetsbegreppen i telekomdirektivet och NIS2-direktivet där utredningen bedömer att dessa två begrepp är likvärdiga.[4] Tre anser att det inte är alldeles tydligt i Förslaget om kraven omfattar nätverk- och informationssystem som tillhandahållaren använder för den samhällsviktiga tjänsten, ”NIS-tjänsten”, enbart eller om de träffar alla nätverk- och informationssystem som används i verksamheten, såsom t.ex. HR-system.[5] Det behöver alltså på ett tydligare sätt redogöras för om de åtgärder som ska vidtas även gäller nätverk och informationssystem som inte används, eller realiserar funktioner, i den samhällsviktiga verksamheten för att kunna avgöra räckvidden av den nya cybersäkerhetslagen. Om NIS2 utvidgar det riskbaserade säkerhetsarbetet bör detta också framgå av konsekvensanalysen i Förslaget.

Vidare så har bolaget några synpunkter på följande skrivning, i 3 kap. 1 § första stycket andra meningen, som kan uppfattas som något oklar.

[4] Förslaget s 318.

[5] Jämför enligt den nu gällande lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster som införlivar NIS direktivet (EU 2016/1148 NIS1) i svensk rätt där det framgår att leverantörer av samhällsviktiga tjänster ska vidta åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster (jml 11, 13 §§).

”*Åtgärderna ska utgå från ett allriskperspektiv och en riskanalys och vara proportionella i förhållande till risken. De ska utvärderas och särskilt innefatta följande*:” (här följer en uppräkning av riskhanteringsåtgärder som ska vidtas).

Bestämmelsen går att uppfatta så att hela den obligatoriska listan av åtgärder (punkterna 1-9) ska grunda sig på en riskanalys och proportionalitetsbedömning. Det finns anledning att ifrågasätta om åtgärder för incidenthantering, åtkomstkontroll, tillgångsförvaltning och möjligen kontinuitetshantering ska utgå ifrån en riskanalys och grunda sig på en proportionalitetsbedömning. NIS2 direktivet art 21 är inte riktigt utformad på det sättet. I stället föreslår Tre att andra meningen kan utformas enligt följande:

”Åtgärderna ska vara proportionella i förhållande till risken. Informationssäkerhetsarbetet och de åtgärder som vidtas ska utvärderas. Informationssäkerhetsarbetet ska åtminstone omfatta:”

Härefter finns det anledning och peka på utformningen av punkterna 5 och 7 som skiljer sig från övriga punkter genom att åtgärderna gäller ”strategier” för säkerhetsarbetet med kryptering, åtkomst och tillgångsförvaltning medan övriga punkter om åtgärder anges som ”säkerhet” (i leveranskedjan, vid förvärv, personal, kommunikation). Bemyndigandet att meddela föreskrifter i punkterna 5 och 7 skulle då anses vara avgränsat till strategier (eller handlingsplaner) på dessa områden. Avses något ytterligare eller annat behöver det förtydligas.

I punkt 6 ska åtgärder vidtas avseende *personalsäkerhet*. Kravet är en nyhet i förhållande till LEK eller PTS föreskrifter. Vad detta krav syftar på framgår varken av NIS2 direktivet eller i Förslaget utan behöver beskrivas närmare. Säkerhetsskyddslagens bestämmelser om personalsäkerhet är inte tillämpliga för verksamhet som inte omfattas av säkerhetsskyddet samtidigt som t.ex. CER-direktivets bestämmelser om personalsäkerhet ser ut att undanta utpekade kritiska entiteter inom digital infrastruktur (jml. CER direktivet art 8, 13.1 e). Förutsätter punkt 6 i Förslaget åtgärder om bakgrundskontroller och behandling av integritetskänsliga uppgifter bör det finnas ett lagstöd för behandlingen samt även vilka personalkategorier som bestämmelsen syftar på.

En ytterligare synpunkt gäller utformningen av punkten 8 ”*säkrade lösningar för kommunikation”.* Uttrycket ”säkrade lösningar..” torde syfta på säkra lösningar och vilka åtgärder, tex förbindelsekryptering, som ska utvärderas för att motsvara kravet. Eftersom den obligatoriska listan gäller säkerhet i olika avseenden vore det konsekvent och något tydligare att ange säkerhet även här, dvs säkerhet vid kommunikation.

3 kap. 2 § - krav på systematiskt och riskbaserat säkerhetsarbete

Tre tillstyrker Förslaget.

Eftersom 2 § handlar om det övergripande säkerhetsarbetet och metoderna för det så vore det lämpligare att inleda kapitlet med denna bestämmelse. Även bestämmelsen om utbildning i 3 § är en mer övergripande åtgärd som borde placeras i kapitlets inledning.

När det gäller tillämpning av standarder så anges i utredningen att ”Enligt artikel 21.1 andra stycket ska relevanta europeiska och internationella standarder beaktas i tillämpliga fall. Även av artikel 25.1 följer att medlemsstaterna, utan att föreskriva eller gynna användningen av viss teknik, ska uppmuntra användningen av europeiska och internationella standarder och tekniska specifikationer av relevans för säkerheten i nätverks- och informationssystem. Innebörden bör vara att medlemsstaterna inte kan uppställa krav om standarder. Med hänsyn härtill menar utredningen att det inte är möjligt att i lag föreskriva att standarder ska beaktas utan detta får uppmuntras på andra och frivilliga sätt.” [6]

Det är motsvarande skrivning som finns i NIS 1 direktivet (EU 2016/1148) art 19.1 med den skillnaden att i angivna åtgärder för digitala tjänster så ska hänsyn tas till efterlevnaden av internationella standarder (se NIS 1 art 16.1 e). [7]

Är det inte så att ett systematiskt och riskbaserat säkerhetsarbete i grunden utgör ett krav på ett ledningssystem för informationssäkerhet och att denna metod baseras på standardserien ISO/IEC 27000 ? Med den bedömning som utredaren gör beträffande tillämpning av standarder så innebär det att NIS 2 direktivet inte ger stöd för att nationellt införa krav på att följa en viss standard enligt motsvarande reglering som ovan. Tre anser därför att krav på vad ett systematiskt och riskbaserat informationssäkerhetsarbete innebär behöver närmare beskrivas eller uttolkas i föreskrifter.

[6] Förslaget s 193.

[7] Jämför de föreskrifter som MSB har meddelat med stöd av nuvarande NIS-lag så anges att ”varje leverantör ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 om ledningssystem för informationssäkerhet eller motsvarande.” (MSBFS 2018:8, § 5).

3 kap. 4 § - betydande incident

Även om Förslaget följer NIS2-direktivet är definitionen betydande incident svårtolkad. En incident ska rapporteras om den:

- orsakat eller kan orsaka allvarlig driftsstörning,
- orsakat eller kan orsaka ekonomisk skada för verksamhetsutövaren eller
- har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada

Genom att betydande incidenter också ska omfatta händelser som kan orsaka driftstörning och eller skada ska bedömningarna, som Tre uppfattar denna definition, omfatta hypotetiska scenarios. Rapporteringsskyldigheten måste bygga på principen att det går att snabbt och relativt enkelt förstå och fastställa om rapportering ska ske samt vad som ska rapporteras relaterat till incidentens effekt, t.ex. genom angivna kriterier eller tröskelvärden. Bestämmelsen måste vara förutsägbar och föreskrifter behöver tydliggöra inte bara tröskelvärden för konstaterad påverkan eller skada utan även beskriva rapporteringspliktiga händelser som ”kan” orsaka driftstörning eller skada.

Utan erforderliga förtydliganden av begreppet betydande incident kommer incident-rapporteringen leda till bl.a. betungande och kostsam administration och ta onödig fokus från de åtgärder som snabbt behöver vidtas i samband med en incident. Vidare är det inte rimligt att utfärda t.ex. en sanktionsavgift om reglerna är otydliga eller lämnar stort tolkningsutrymme om en verksamhetsutövare missbedömt innebörden av begreppet samt att detta avses vara särskilt graverande (jfr 5 kap. 5 § punkten 2 i Förslaget).

Definitionen av betydande incident i Förslaget (NIS2) skiljer sig från definitionen i LEK (och angivna tröskelvärden som regleras i PTS föreskrifter). Rapporteringen i LEK syftar huvudsakligen på driftsrelaterade incidenter med syfte på avbrottets eller störningens påverkan på antalet användare, dess varaktighet eller påverkat geografiskt område eller om en viss kritisk tjänst påverkats t.ex. nödkommunikation eller annan betydande samhällspåverkan. I nuvarande bestämmelser finns inte något krav på att rapportera händelser som vållat skada för verksamhetsutövaren eller vållat betydande materiell eller immateriell skada för ”andra personer” utan sådana händelser måste förtydligas vad som avses. Tre anser att vad som är rapporteringspliktigt behöver på föreskriftsnivå anpassas till telekomsektorn och de rapporteringskrav som idag gäller enligt PTS föreskrifter. Då Förslaget innebär att det är MSB som fått föreskriftsrätt avseende vad som utgör en ”betydande incident” måste tillämpningen av detta på elektroniska kommunikationsnät och tjänster

samordnas noggrant med PTS. Alternativet är att PTS ges även en sådan föreskriftsrätt för sektorn digital infrastruktur.

3 kap. 5 § - varning

Bestämmelsens andra meningen är något oklar i sin utformning; ”*Det ska anges om att det finns misstanke om incidenten orsakats uppsåtligen och om incidenten kan ha gränsöverskridande effekter*”. Bestämmelsen kan det ge uppfattningen av att underrättelse alltid ska innehålla den informationen.

Ett förslag är att skriva på följande sätt. ”*Vid misstanke om att incidenten orsakats uppsåtligen eller om incidenten kan ha gränsöverskridande effekter ska det anges i underrättelsen*.”

3 kap. 6 § - incidentanmälan

Bestämmelsen beskriver tidpunkten för incidentanmälan och vad den ska innehålla. Bland annat ska anmälan innehålla ”förekomsten av angreppsindikatorer”, ett begrepp som inte förklaras närmare i Förslaget. Om det finns en vedertagen teknisk definition, alternativt om termen relaterar till viss typ av teknisk bevisning eller data, bör det anges i motiven eller tydliggöras i föreskrifter.

Samtidigt som incidentanmälan skickas in ska kunder som kan antas påverkas av den betydande incidenten informeras. Kunder ska även informeras om betydande cyberhot. För att kunna efterleva kravet behöver det klargöras i föreskrifter eller vägledning vad informationen till kunder ska innehålla och på vilket sätt kunderna ska informeras. Kan det t. ex. ske via en öppen kanal, t.ex. en webbsida, eller innebär kravet att det behöver säkerställas att informationen kommer berörd till del? Ett säkerställande innebär behandling av personuppgifter och systemkontroller samt identifiering av påverkade kunder, t.ex. om incidenten eller cyberhotet berör ett visst geografiskt område. Om informationen behöver riktas till de som påverkas kan det bli fråga om behandling av lokaliseringsuppgifter vilket är mycket känslig information. Behandlingen av trafikuppgifter och lokaliseringsuppgifter regleras i LEK och får behandlas endast för de i LEK angivna ändamålen. Det torde saknas lagstöd i LEK för denna typ av behandlingar.

Definitionen av betydande cyberhot är svårläst och det går inte att enkelt avgöra eller bedöma vilka omständigheter eller förekomster som aktualiserar informationskravet. Ett betydande cyberhot är ett hot ”som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en verksamhetsutövares nätverks- och informationssystem eller användarna av verksamhetsutövarens tjänster genom att vålla betydande materiell eller immateriell skada.” Av denna definition går det inte att dra några slutsatser om vilka händelser eller scenarios som aktualiserar informationskravet.

I anslutning till det så vill Tre särskilt framhålla riskerna med sådan information och behovet av en restriktiv/återhållsam tillämpning. Information, som nu förväntas komma från flertalet sektorer (el, telekom, banktjänster, swish, post, flyg- och kollektivtrafik, sociala medier, m.m.) som kunder har en relation till kan dels skapa onödig oro försåvitt kunden inte själv kan påverka situationen eller hotet som föranleder informationen dels kan informationen öppna vägar för t.ex. nätfiske (phishing) och andra bedrägerier.[8]

Tre anser att det i föreskrifter, i vägledning eller på annat sätt behöver anges hur informationsplikten kan fullgöras.

Angående kravet att underrätta, så avser det påverkade *kunder*. Kund definieras inte, men framförallt i telekomsektorn blir det viktigt att förstå vem som ska underrättas, dvs. om det med kund avses abonnent eller om även användare avses (jfr LEK 1 kap 7 §). Det behöver förtydligas.

4 kap. 8-9 §§ - säkerhetsrevision och säkerhetskanningar

I LEK (8 kap. 2 §) finns sedan tidigare en bestämmelse om säkerhetsgranskning som får utföras på verksamhetsutövarens bekostnad, om det finns särskilda skäl till en sådan granskning. Vad som nu införs är ytterligare bestämmelse om regelbundna säkerhetsrevisioner av väsentliga verksamhetsutövare. Utökade tillsynsbefogenheter får trots allt inte vara betungande för verksamhetsutövaren eller stå i strid med proportionalitetsprincipen. Det framgår inte av bestämmelsen med vilken frekvens eller hur omfattande dessa säkerhetsrevisioner får göras. Det bör finnas en möjlighet för verksamhetsutövaren att påverka vald tidpunkt för revision eller skanning, eftersom åtgärderna annars skulle kunna orsaka betydande olägenhet om vald tidpunkt krockar med

[8] Se bl.a. ENISAs vägledning *Cyber Threats Outreach in Telecom*, 2022 s 24, https://www.enisa.europa.eu/publications/cyber-threats-outreach-in-telecom.

annat omfattande i verksamheten pågående IT- eller revisionsarbete. Tre anser därför, vilket får anses stå i överensstämmelse med nämnda proportionalitetsprincip, att åtgärderna inte får vålla större kostnad eller olägenhet än vad som är nödvändigt och inte i onödan hämmar verksamhetsutövarens affärsverksamhet, jfr NIS2 direktivet ingresspunkt 123. Det bör framgå av lagtexten som en princip för tillsynsverksamheten.

I 30 § (och i art 11 NIS2) förslaget till förordning till cybersäkerhetslagen framgår att CSIRT (MSB) får utföra proaktiva skanningar i syfte att upptäcka sårbarheter, m.m. Det är inte tydligt för Tre varför två myndigheter, PTS och MSB, ska ha befogenheter att utföra skanningar för till synes samma syfte. I det ena fallet ska skanningen ske i samarbete med verksamhetsutövaren i det andra fallet får det ske utan samarbete. Det förklaras inte närmare i utredningen ändamålet med 30 § och vad MSB ska använda skanningsresultatet till.

5 kap. 1 § p 2 och 12 § –anmälningsskyldighet och sanktionsavgift

Tre avstyrker Förslaget.

Tre noterar att bestämmelsen om anmälningsskyldighet i NIS2-direktivets art 3.4 inte är avgiftssanktionsgrundad enligt art 34. Förslaget innebär en väsentlig förändring mot vad NIS2 direktivet föreskriver och bör inte införas. Någon närmare motivering varför sanktioner bedömts nödvändig framgår inte av Förslaget. I utredningsuppdraget framgår i övrigt att om förslag lämnas som går utöver EU-direktivens krav, ska utredaren särskilt motivera varför dessa är nödvändiga. [9]

5 kap. 1 § p 4 och 12 § – utbildning och sanktionsavgift

Tre avstyrker Förslaget.

Tre noterar att bestämmelsen om utbildning i NIS2-direktivets art 20 inte är inte avgiftssanktionsgrundad enligt art 34. Förslaget innebär en väsentlig förändring mot vad NIS2 direktivet föreskriver och bör inte införas.

[9] Jml Komm.dir 2023:30 s 20

5 kap. 2 §

Punkterna 2 och 3 hänvisar till fel bestämmelser.

5 kap. 12 § - sanktionsavgift

Tre ser positivt på att tillsynsmyndigheten får avstå från att meddela sanktionsavgift snarare än att det är en skyldighet om brister upptäcks, såsom är fallet idag med strikt ansvar i LEK 12 kap 1 § och i NIS-lagen 29 §.

5 kap. 17 § - Hinder mot att ta ut sanktionsavgift

Tre tillstyrker förslaget men har synpunkter på att bestämmelsen inte är reciprok.

Av bestämmelsens andra stycke framgår att en sanktionsavgift får inte beslutas för samma överträdelse som lett till att verksamhetsutövaren har påförts en sanktionsavgift enligt Allmänna dataskyddsförordningen.

Bestämmelsen reglerar förhållandet i ena riktningen dvs. sanktioner beslutade med stöd av cybersäkerhetslagen men det saknas motsvarande bestämmelse om dubbelprövning enligt dataskyddsförordningen. Dubbelprövningsförbudet blir då i viss mån illusoriskt eftersom det beror på vilken myndighet som först påför sanktionsavgift för bristande säkerhet.

På samma sätt bör dubbelprövningsförbudet även gälla sanktionsavgift för samma överträdelse som lett till sanktionsavgift enligt LEK 9 kap om behandling av trafikuppgifter samt integritetsskydd.

Förordning om cybersäkerhet - 15 § tillsynsmyndighetens och Integritetsskyddsmyndighetens (IMY) samarbete - rapportering av personuppgiftsincidenter enligt dataskyddsförordningen

Bestämmelsen i andra stycket innebär att tillsynsmyndigheten ska informera IMY om personuppgiftsincidenter som upptäcks vid tillsyn. Enligt nuvarande ordning är det den personuppgiftsansvarige som ska bedöma om en händelse utgör en personuppgiftsincident

och om den ska anmälas till IMY enligt dataskyddsförordningen (art 33). Tre ser inget skäl till att ändra nuvarande ordning.

LEK:s (e-dataskyddsdirektivets) bestämmelser om rapportering av integritetsincidenter preciserar vad som gäller vid rapportering till PTS och får i detta avseende anses gälla före dataskyddsförordningens bestämmelser om rapportering av personuppgiftsincidenter enligt principen om *lex specialis*. Incidenter som är rapporteringspliktiga enligt LEK, och ska rapporteras till PTS, ska således inte samtidigt rapporteras till IMY.[10] Om PTS vid en tillsyn enligt LEK (om bl.a. skydd av uppgifter som behandlas vid tillhandahållandet av elektroniska kommunikationstjänster) upptäcker omständigheter som skulle kunna utgöra en personuppgiftsincident ska denna enligt nuvarande reglering och principen om lex specialis inte rapporteras till IMY. PTS bör således inte informera om incidenter som upptäcks vid tillsyn till IMY.

Stockholm som ovan

Carl-Johan Broman Josefine Jonsson

[10] Se bl.a. uttalanden från EDPB i yttrandet 5/2019 s 14-16, https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_sv.pdf