Försvarsdepartementet

Er referens: Fö2024/00496
Vår referens: 24-3029

PTS remissvar avseende delbetänkande Nya regler om cybersäkerhet (SOU 2024:18)

Sammanfattning

PTS delar både EU-kommissionens och utredningens bedömning att NIS2-direktivet och i förlängningen cybersäkerhetslagen är viktiga instrument för att uppnå en högre cybersäkerhetsnivå i samhället. Myndigheten bedriver redan nu ett viktigt arbete inom flera av de sektorer som föreslås ingå i den nya cybersäkerhetslagen. Att det bedrivs ett adekvat säkerhetsarbete inom de sektorer som PTS föreslås ansvara för är viktigt inte bara för dessa områden, utan har direkt inverkan på säkerheten i andra kritiska sektorer och på samhällets digitalisering i stort.

Av denna anledning anser PTS att det är mycket beklagligt att utredningens föreslagna anslag till myndigheten, tvärtemot behovet, medför en minskning och därmed sänkt ambitionsnivå för PTS tillsynsuppgifter. Den effekt som lagstiftaren vill uppnå med NIS2-direktivet och cybersäkerhetslagen – att öka cybersäkerheten i samhället – kan inte åstadkommas om myndighetens ambitionsnivå måste sänkas med anledning av lägre finansiering. PTS uppmanar därför lagstiftaren att säkerställa en rimlig och adekvat resurssättning i den fortsatta beredningen för att syftet med NIS2-direktivet ska kunna uppfyllas.

Givet att adekvat resurstilldelning säkerställs ser PTS positivt på att myndigheten föreslås få ett utökat tillsynsansvar, med nya och utökade sektorer. PTS har en lång erfarenhet av reglering och tillsyn av cybersäkerhetsfrågor och att utveckla och tillämpa regelverk i nya sektorer. Den kommande lagstiftningen förväntas innebära att cirka 1 100 aktörer som faller under regleringen kommer att falla under PTS tillsynsansvar. Av dessa utgörs drygt 700 aktörer av tillhandahållare som redan idag är anmälda till myndigheten enligt LEK. Enligt

Post- och telestyrelsen
Postadress: Box 6101, 102 32 Stockholm
Besöksadress: Hälsingegatan 38
Telefon: 08-678 55 00
E-post: pts@pts.se
www.pts.se

nuvarande reglering faller cirka 40–50 aktörer under PTS tillsynsansvar enligt NIS-lagen. Den föreslagna cybersäkerhetslagen innebär alltså en betydande utökning av PTS ansvarsområde.

PTS lämnar i detta remissvar ett flertal synpunkter och förslag på justeringar och förtydliganden i cybersäkerhetslagen och toppdomänlagen, men vill betona att de viktigaste förutsättningarna i det fortsatta lagstiftnings- och tillsynsarbetet för myndigheten är:

- **att PTS anslag förstärks i betydligt högre utsträckning än utredningens förslag**, så att myndigheten fortsatt ska kunna bedriva den tillsyn på området som redan sker och dessutom ta omhand ett utökat ansvar, och
- **att PTS får föreskriftsrätt** för riskhanteringsåtgärder samt för systematiskt och riskbaserat informationssäkerhetsarbete.

PTS bidrar gärna med kompetens och erfarenhet även i det fortsatta lagstiftningsarbetet.

Innehåll

PTS remissvar avseende delbetänkande Nya regler om cybersäkerhet (SOU 2024:18)..... 1

Sammanfattning..... 1

1. Introduktion..... 4

2. Synpunkter..... 7

2.1. Behov av ökad finansiering av PTS tillsynsverksamhet..... 7

2.2. PTS ansvar enligt cybersäkerhetslagen..... 8

2.3. Cybersäkerhetslagens relation till LEK..... 11

2.4. Cybersäkerhetslagens relation till eIDAS2-förordningen..... 15

2.5. PTS föreslår vissa ändringar i toppdomänlagen..... 17

2.6. Behov av avgränsning av begreppet leverantör av DNS-tjänster..... 21

2.7. Riskhanteringsåtgärder och incidenthantering..... 22

2.8. Administrativa sanktioner och andra ingripanden..... 24

2.9. Behov av förtydligande avseende verksamhetens omfattning..... 26

2.10. Rymdsektorns omfattning..... 26

2.11. Övriga synpunkter avseende författningsförslag cybersäkerhetslagen..... 27

2.12. Övriga synpunkter avseende författningsförslag toppdomänlagen..... 28

1. Introduktion

PTS har enligt 1 § förordningen (2007:951) med instruktion för Post- och telestyrelsen ett samlat ansvar inom postområdet och området för elektronisk kommunikation. Utifrån PTS ansvarsområde lämnar myndigheten i detta yttrande synpunkter på delbetänkandet *Nya regler om cybersäkerhet*, SOU 2024:18.

PTS ser positivt på att det införs en cybersäkerhetslag som, jämfört med nu gällande NIS-lag, bland annat omfattar fler sektorer och aktörer, innebär att kraven på berörda verksamhetsutövare utvidgas och tydliggörs samt att kraven kommer att gälla för verksamheterna i sin helhet. Införandet av cybersäkerhetslagen innebär ett viktigt steg mot ökad cyberresiliens, samtidigt som lagens tillämpningsområde håller sig väl inom NIS2-direktivets syfte och inte utsträcks till att omfatta andra områden som inte är avsedda att regleras genom en inremarknadsreglering från EU.

Enligt förslaget ska PTS vara tillsynsmyndighet för sektorerna digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster, post- och budtjänster samt rymden. PTS är sedan tidigare tillsynsmyndighet för digital infrastruktur samt för digitala tjänster, och ser positivt på förslaget om att utvidga myndighetens ansvarsområde. Föreslagna nya sektorer har en naturlig anknytning till PTS övriga områden och det finns goda skäl för att hålla samman dessa så att PTS får ett helhetsansvar för frågorna och ett övergripande ansvar för ett säkert och tryggt digitalt samhälle. Ansvaret bör hållas samman på en myndighet som tar helhetsansvar för att på bästa sätt uppnå digitaliseringen av samhället. För att PTS ska kunna bedriva det arbete som utredningen föreslår krävs dock ett väsentligt högre anslag än det som utredningen föreslår. Det är av största vikt att detta behov hörsammas för att syftet med NIS2-direktivet ska kunna uppfyllas.

PTS ser positivt på att det inom ramen för tillsynsuppdraget införs en möjlighet för tillsynsmyndigheterna att ålägga flera olika sanktioner samt att tillsynsmyndigheterna i varje enskilt fall ska avgöra om sanktionsavgift ska tas ut, snarare än att beslut om sanktionsavgift ska fattas undantagslöst vid konstaterad överträdelse.

Avseende föreskriftsrätten instämmer PTS i utredningens bedömning att närmare föreskrifter om riskhanteringsåtgärder samt systematiskt och riskbaserat informationssäkerhetsarbete ska tas fram av respektive tillsynsmyndighet. Detta gör sig särskilt gällande avseende tillhandahållare av allmänna elektroniska kommunikationsnät och tillhandahållare av allmänt tillgängliga kommunikationstjänster, där PTS ser stora fördelar med att även fortsättningsvis kunna dra nytta av sin långa erfarenhet av sektorn. Det medför även att det för sektorn anpassade regelverket, som främjar innovation, investeringar och konnektivitet, fortfarande kan ha ett harmoniserat fokus på säkerheten.

PTS har av pedagogiska skäl valt att lyfta fram de synpunkter som är mest angelägna enligt myndigheten och remissvaret följer därmed inte betänkandets ordning. Varje rubrik innehåller emellertid en referens till aktuellt avsnitt i betänkandet.

I remissvaret används följande förkortningar/begrepp.

CER	Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG
Cybersäkerhetslagen	(Förslag till) lagen om cybersäkerhet
Dataskyddsförordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
Delbetänkandet	Nya regler om cybersäkerhet (SOU 2024:18)
E-dataskyddsdirektivet	Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation)
eIDAS-förordningen	Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG
eIDAS2-förordningen	Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet
ENISA	Europeiska byrån för nät- och informationssäkerhet
FEK	Förordningen (2022:511) om elektronisk kommunikation
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IMY	Integritetsskyddsmyndigheten
LEK	Lagen (2022:482) om elektronisk kommunikation
NIS-direktivet	Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen

NIS2-direktivet	Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148
NIS-lagen	Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
PTS	Post- och telestyrelsen
Toppdomänlagen	Lagen (2006:24) om nationella toppdomäner för Sverige på internet

2. Synpunkter

2.1. Behov av ökad finansiering av PTS tillsynsverksamhet

PTS anslag behöver förstärkas med 22,5 miljoner kronor.

Relevant avsnitt i delbetänkandet: 12.6.7 Utredningens förslag – ekonomiska konsekvenser för tillsynsmyndigheterna och för Myndigheten för samhällsskydd och beredskap

Av utredningens förslag framgår att PTS bör ges ett förstärkt anslag för löpande kostnader med två miljoner kronor under 2025.

PTS vill inledningsvis föra fram att utredningens förslag på förstärkt anslag för 2025 kraftigt underskrider det behov av ökad finansiering som PTS har framfört i budgetunderlaget till regeringen för arbete med cybersäkerhetslagen under åren 2025–2027. Motsvarande behov har PTS även fört fram till utredningen både skriftligen och muntligen i samband med intervjun kring vad PTS ser att den nya cybersäkerhetslagen kommer att medföra för kostnader. PTS kan dock konstatera att de angivna siffrorna inte alls speglar de av PTS framförda kostnaderna.

PTS vidhåller fortsatt att myndigheten behöver förstärkning med sju årsarbetskrafter år 2025–2027 för att kunna omhänderta det utökade uppdraget.

Utöver detta behöver även de medarbetare (8,0 årsarbetskrafter), vars arbetsuppgifter idag är avgiftsfinansierade enligt LEK, övergå till att finansieras av förvaltningsanslaget.

Sammanfattningsvis ser PTS därmed ett behov av 15 årsarbetskrafter motsvarande 22,5 miljoner kronor. En tilldelning begränsad till två miljoner kronor skulle inte möjliggöra att bedriva den verksamhet som utredningen föreslår, ens med kraftigt sänkt ambitionsnivå jämfört med det arbete som PTS bedriver idag.

Bakgrund till PTS behov av förstärkt anslag

PTS föreslås få ansvar för fler sektorer än i nuläget och några av dessa är helt eller delvis nya för myndigheten. Detta kommer att innebära ett omfattande arbete för PTS. Den nya cybersäkerhetslagen innebär att PTS arbete med tillsyn, reglering, utredning och kartläggning inom NIS-området bedöms öka markant de närmaste åren.

Resursbehovet som finns idag och framöver är bl.a. hänförligt till det förberedande arbete som krävs; analys, utredning, samverkan i nationella och internationella arbetsgrupper, kommunikationsinsatser, marknadsanalys och att ta fram både nya och uppdaterade föreskrifter för PTS ansvarsområden.

För PTS del innebär cybersäkerhetslagen en stor ökning av antalet tillsynsobjekt, utökade tillsynsbefogenheter samt fler uppgifter inom reglering, vägledning och administration. PTS behöver ökad finansiering för att kunna avdela tillräckligt med resurser för arbetet med att utöva tillsyn över dessa. För närvarande faller ca 40-50 leverantörer under PTS tillsynsansvar enligt NIS-lagen. Den kommande lagstiftningen förväntas innebära att ca 1 100 aktörer faller under PTS tillsynsansvar, enligt den marknadsanalys som PTS genomfört. Drygt 700 aktörer av dessa utgörs av aktörer som idag är anmälda till PTS enligt LEK.

Konsekvenser av otillräcklig finansiering

Otillräcklig finansiering på området bedöms leda till svårigheter att kontrollera att de verksamhetsutövare som faller under PTS sektorsansvar vidtar adekvata riskhanteringsåtgärder, incidentrapporterar och bedriver ett systematiskt och riskbaserat säkerhetsarbete, samtidigt som PTS inte kan ge erforderlig vägledning i den omfattning som lagen ställer krav på. Utan adekvat tillskjutna medel kommer tillsynsarbetet att vara otillräcklig för att uppfylla kraven på tillsynsmyndigheterna i enlighet med cybersäkerhetslagen. Om regeringen vill att tillsynen över NIS2-direktivet ska leda till en hög cybersäkerhetsnivå, vilket ambitionerna på området cybersäkerhet i övrigt indikerar, behöver det följas upp med resurser.

PTS har upparbetad erfarenhet och bedriver tillsyn inom det idag avgiftsfinansierade området som rör säkerhet i nät och tjänster enligt LEK. Konsekvenserna av utebliven permanent finansiering för de befintliga 8,0 årsarbetskrafter som behöver bli anslagsfinansierade blir att PTS tappar väsentliga delar av det pågående arbete som rör säkerhet i nät och tjänster, där PTS har en redan upparbetad och idag aktiv roll som tillsynsmyndighet.

Eftersom sektorn digital infrastruktur påverkar alla delar av samhället kommer konsekvenserna av brister i riskhantering, incidentrapportering och det systematiska informationssäkerhetsarbetet inom denna sektor påverka andra verksamheter negativt. På motsvarande vis ger förbättrad säkerhet inom området elektroniska kommunikationer positiva spridningseffekter.

2.2. PTS ansvar enligt cybersäkerhetslagen

PTS bör ha föreskriftsrätt för riskhanteringsåtgärder samt systematiskt och riskbaserat informationssäkerhetsarbete.

Relevant avsnitt i delbetänkandet: 7.1 Övergripande lagreglering om riskhanteringsåtgärder

PTS instämmer i, och anser att det är av stor vikt, att närmare föreskrifter om riskhanteringsåtgärder samt systematiskt och riskbaserat informationssäkerhetsarbete ska tas fram av respektive tillsynsmyndighet i enlighet med de skäl som utredningen anger. PTS vill särskilt framhålla vikten av att PTS även fortsättningsvis ges föreskriftsrätt för riskhanteringsåtgärder samt systematiskt och riskbaserat informationssäkerhetsarbete avseende tillhandahållare av allmänna elektroniska kommunikationsnät och tillhandahållare av allmänt tillgängliga kommunikationstjänster. Detta eftersom PTS är expertmyndighet för dessa tillhandahållare och har lång erfarenhet av att reglera sektorn. Det finns en risk att upparbetad praxis och kunskap på området inte kan upprätthållas om en annan myndighet får föreskriftsrätt för telekomsektorn, som har speciella förutsättningar. Sektorn riskerar i så fall onödiga störningar genom att etablerade sektorsanpassade säkerhetskrav och rapporteringströsklar ändras. PTS möjlighet att bedriva en effektiv och ändamålsenlig tillsyn över cybersäkerheten i telekomsektorn riskerar att försämras om PTS tappar möjligheten att styra över när föreskrifterna ska uppdateras. I och med att kraven kan tänkas bli mer generella riskerar de även att bli mer urvattnade än gällande föreskrifter.

Vidare ifrågasätter PTS lämpligheten i att MSB ges i uppdrag att utarbeta en vägledning om riskhanteringsåtgärder till stöd för tillsynsmyndigheternas föreskriftsarbete. Om tillsynsmyndigheterna ska invänta MSB:s vägledning, vilken är tänkt att utgöra en viktig grund för likvärdiga föreskrifter, kommer detta innebära svårigheter för myndigheterna att färdigställa och besluta föreskrifter i tid. PTS har dessutom sedan tidigare föreskrifter[1] som gäller för aktörer som omfattas av NIS-lagen och LEK, som kommer behöva omarbetas inför ikraftträdandet av cybersäkerhetslagen. Att invänta MSB:s vägledning riskerar att försena de nya föreskrifternas ikraftträdande, vilket skulle innebära ett glapp i regleringen av de verksamhetsutövare som redan nu omfattas av PTS föreskrifter på området.

Om MSB ändå ska ta fram en sådan vägledning anser PTS att det är av vikt att MSB beaktar olika internationella riktlinjer och andra initiativ på området, även sådana initiativ som endast gäller vissa sektorer, t.ex. riktlinjer som har tagits fram av ENISA:s expertgrupp för säkerhet, European Competent Authorities for Secure Electronic Communications (ECASEC) för att säkerställa en harmonisering inom EU.

[1] Post- och telestyrelsens föreskrifter och allmänna råd om säkerhetsåtgärder för samhällsviktiga tjänster inom sektorn digital infrastruktur (PTSFS 2021:3), samt Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTSFS 2022:11).

Föreskrifter avseende incidentrapportering för tillhandahållare enligt LEK måste samverkas med PTS innan dessa beslutas.

Relevant avsnitt i delbetänkandet: 7.3 Incidentrapportering

PTS har idag föreskriftsrätt avseende incidentrapportering för tillhandahållare av allmänna elektroniska kommunikationsnät och tillhandahållare av allmänt tillgängliga kommunikationstjänster och har tagit fram föreskrifter med bl.a. tröskelbestämmelser som reglerar vilka incidenter och vilka uppgifter som ska rapporteras till PTS. För det fall PTS fortsättningsvis inte ges föreskriftsrätt avseende incidentrapportering, är det av mycket stor vikt att MSB (som föreslås få bemyndigandet istället) beaktar redan framtagna regler och rapporteringströsklar avseende incidentrapportering samt samverkar föreskrifterna med PTS innan dessa beslutas. Vidare är det viktigt att PTS får möjlighet att löpande samverka nödvändiga uppdateringar och ändringar av föreskrifter för incidentrapportering med MSB.

PTS vill även framhålla vad som framgår av skäl 95 NIS2-direktivet, om vikten av att beakta befintliga nationella riktlinjer.

PTS ser även att det faktum att två olika myndigheter föreslås hantera incidenter (MSB som mottagare av rapporter och PTS som tillsynsmyndighet avseende rapporteringen) kan innebära vissa administrativa problem, t.ex. i samband med uppdateringar av ärendet, för det fall dessa incidenter inte hanteras i ett och samma ärendehanteringssystem.

PTS tillstyrker utredningens förslag att verksamhetsutövarens anmälan ska göras direkt till tillsynsmyndigheten.

Relevant avsnitt i delbetänkandet: 6.2 Register över väsentliga och viktiga verksamhetsutövare

PTS tillstyrker utredningens förslag att varje verksamhetsutövare ska anmäla sig till den tillsynsmyndighet vars sektor verksamheten faller under. Detta blir särskilt relevant för PTS med anledning av det tillsynsansvar som myndigheten redan har enligt LEK, över sådana aktörer som har anmälningsplikt enligt den lagen. Dessa verksamhetsutövare kommer fortsatt vara anmälningspliktiga enligt LEK, men behöver anmäla sig igen enligt cybersäkerhetslagen eftersom det delvis är nya uppgifter som ska samlas in. PTS anser att det är viktigt och lämpligt att myndigheten har ägandeskap över båda register för att enkelt kunna notera avvikelser, samt sköta kontakt med dessa verksamhetsutövare för att kunna erbjuda stöd.

Även vad gäller övriga verksamhetsutövare finns det anledning att låta registret skötas av tillsynsmyndigheten, såsom utredningen föreslår. Eftersom underlåtande att anmäla sig ska resultera i beslut om sanktioner, vilket sköts av tillsynsmyndigheten, är det lämpligt och rimligt att det är tillsynsmyndigheten som har kontroll över registret. Det är även tillsynsmyndigheterna som är bäst lämpade att stötta verksamhetsutövarna i sin bedömning av huruvida de är anmälningspliktiga eller inte, varför anmälningsförfarandet bör hanteras av tillsynsmyndigheterna.

2.3. Cybersäkerhetslagens relation till LEK

PTS möjlighet att meddela undantag från skyldigheten att vidta säkerhetsåtgärder och att rapportera incidenter, avseende tillhandahållare enligt LEK, bör föras över till cybersäkerhetslagen.

Relevant avsnitt i delbetänkandet: 7 Riskhantering och incidentrapportering

PTS har enligt 8 kap. 3 § LEK rätt att meddela föreskrifter om undantag från skyldigheten att vidta säkerhetsåtgärder respektive skyldigheten att rapportera incidenter till tillsynsmyndigheten. Cybersäkerhetslagen innehåller inte något sådant uttryckligt bemyndigande. PTS har i föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTSFS 2022:11) föreskrivit om undantag från vissa säkerhetsåtgärder. Det är viktigt att PTS även fortsättningsvis har motsvarande möjlighet för att garantera att en proportionalitetsbedömning av åtgärden alltid kan göras i varje enskilt fall.

Förbudet att påföra flera sanktionsavgifter för samma överträdelse bör gälla även i förhållande till LEK. Det kan även finnas behov av att harmonisera nivåerna på sanktionsavgifter enligt LEK med nivåerna enligt cybersäkerhetslagen.

Relevant avsnitt i delbetänkandet: 9.6.3 Hinder mot att ta ut sanktionsavgift

Artikel 35 NIS2-direktivet reglerar överträdelser som innebär personuppgiftsincidenter enligt EU:s dataskyddsförordning. Artikeln föreslås genomföras i 5 kap. 17 § andra stycket cybersäkerhetslagen.

E-dataskyddsdirektivet omnämns inte i artikel 35 NIS2-direktivet. Anledningen till det är troligtvis att det i e-dataskyddsdirektivet saknas explicita regler om sanktionsavgifter. Enligt svensk rätt ska dock sanktionsavgifter beslutas för överträdelser av bestämmelser i 8 kap. LEK som genomför e-dataskyddsdirektivet, se 12 kap. 1 § LEK. PTS anser därför att förbudet i 5

kap. 17 § andra stycket cybersäkerhetslagen om att påföra sanktionsavgifter inte bara ska gälla när IMY påfört sanktionsavgifter utan även när PTS påfört sanktionsavgifter enligt LEK.

PTS vill också lyfta frågan om det finns anledning att se över nivåerna för sanktionsavgifterna i LEK för överträdelser av bestämmelserna i 8 kap. LEK som genomför e-dataskyddsdirektivet så att de står i överensstämmelse med nivåerna i cybersäkerhetslagen. Om en sanktionsavgift ska utgå enligt LEK i första hand (i enlighet med PTS förslag ovan), blir avgiften lägre än om den skulle beslutas enligt cybersäkerhetslagen. PTS noterar att intervallet i LEK följer det intervall som gäller enligt nuvarande NIS-lag, se prop. 2021/22:136 s. 362.

Det bör framgå i förarbeten till cybersäkerhetslagen att proportionella riskhanteringsåtgärder ska ta hänsyn till teknik och kostnader (inte bara till risken).

Relevant avsnitt i delbetänkandet: 7.1.2 Riskhanteringsåtgärder

PTS anser att det är viktigt att även det resonemang som framgår av skäl 81 NIS2-direktivet, exempelvis kring *teknik och kostnader*, kommer till uttryck i förarbeten i samband med beskrivningen av faktorer som ska beaktas vid bedömningen av proportionella riskhanteringsåtgärder. I prop. 2021/22:136 s. 315, i samband med införandet av artikel 40.1 Kodexen i LEK anges t.ex. följande i samband med bedömningen av nivån på säkerhetsåtgärderna:

”I att åtgärderna ska säkerställa en lämplig nivå på säkerheten ligger bl.a. att de tekniska lösningar som är tillgängliga på marknaden vid varje given tidpunkt ska beaktas. Teknisk utveckling kan därför leda till att behovet av säkerhetsåtgärder förändras eller innebära nya möjligheter att vidta effektiva säkerhetsåtgärder. Kravet på att beakta den tekniska utvecklingen ligger i att säkerhetsåtgärderna ska ligga på en lämplig säkerhetsnivå (jfr prop. 2017/18:205 s. 41).”

Ordet ”riskanalys” i 3 kap. 1 § cybersäkerhetslagen bör utgå för att undvika missförstånd kring tillsynsmyndigheternas rätt att föreskriva om krav på dessa som en riskhanteringsåtgärd. Vidare riskerar användningen av ”riskanalys” att bidra till otydlighet kring när skyldigheten att vidta riskhanteringsåtgärder gäller.

Relevant avsnitt i delbetänkandet: 7.1.2 Riskhanteringsåtgärder

Enligt 3 kap. 1 § cybersäkerhetslagen ska verksamhetsutövaren vidta tekniska, driftsrelaterade och organisatoriska riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från ett

allriskperspektiv och en *riskanalys* och vara proportionella i förhållande till risken. Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om riskhanteringsåtgärder.

PTS anser visserligen att riskanalyser ska göras samt att de utgör ett mycket viktigt underlag för att kunna besluta hur risker ska hanteras och vilka riskhanteringsåtgärder som ska vidtas. PTS anser emellertid att riskanalyser i sig utgör en sådan riskhanteringsåtgärd som tillsynsmyndigheterna bör få föreskriva om. PTS har t.ex. sedan tidigare meddelat föreskrifter om riskanalyser (vad som ska analyseras samt när och hur detta ska göras) utifrån bemyndigandet i LEK och FEK att meddela föreskrifter om de säkerhetsåtgärder tillhandahållare av allmänna elektroniska kommunikationsnät och tillhandahållare av allmänt tillgängliga kommunikationstjänster är skyldiga att vidta. Om riskanalyser särskiljs från riskhanteringsåtgärderna blir det otydligt att tillsynsmyndigheten har ett bemyndigande i 3 kap. 1 § cybersäkerhetslagen att ta fram bestämmelser om riskanalyser.

PTS anser att det är viktigt att myndigheter kan ställa krav på riskhanteringsåtgärder i föreskrifter och vid tillsyn oavsett om verksamhetsutövaren har gjort någon riskanalys eller inte och oavsett utfallet av verksamhetsutövarens riskanalys, och föreslår därför att ordet ”riskanalys” utgår.

PTS vill lyfta frågan om leverantörer av internetknutpunkter fortsatt ska anses vara tillhandahållare av allmänna elektroniska kommunikationsnät enligt LEK, och därmed omfattas av en annan beräkningsmodell än vad som anges i NIS2-direktivet för leverantörer av internetknutpunkter. PTS anser att så borde vara fallet, men anser att detta i så fall bör tydliggöras i cybersäkerhetslagen eller förarbeten till denna, för att undvika förvirring.

Relevant avsnitt i delbetänkandet: 4 Beskrivning av de nya sektorerna

Enligt bilaga 1, sektor 8 Digital infrastruktur, NIS2-direktivet, ingår leverantörer av internetknutpunkter som en typ av entitet i regelverkets tillämpningsområde. Utredningen nämner inte denna typ av leverantör i delbetänkandet, varken i författningsförslagen eller i analysdelen. Anledningen kan tänkas vara att leverantörer av internetknutpunkter inte är en ny typ av verksamhetsutövare, jämfört med NIS-direktivet, utan ingick redan i det ursprungliga regelverket under sektorn digital infrastruktur[2]. Under avsnitt 4, Beskrivning av de nya sektorerna, anges i delbetänkandet att endast ”de nya sektorer, delsektorer och typer av verksamhetsutövare som omfattas av NIS2-direktivets tillämpningsområde” kommer

[2] Bilaga 2, sektor 7 Digital infrastruktur, NIS-direktivet.

beskrivas i kapitlet (s. 103). Läsaren hänvisas till SOU 2017:36, *Informationssäkerhet för samhällsviktiga och digitala tjänster*, s. 65 ff., för en beskrivning av de gamla sektorerna.

I SOU 2017:36, s. 83, anges följande:

”Inom sektorn digital infrastruktur ska bestämmelserna i NIS-direktivet tillämpas på enheten internetknutpunkter. Internetknutpunkter som flera aktörer kan ansluta sig till anses i svensk rätt som ett allmänt kommunikationsnät och omfattas av 5 kap. 6 b och c §§ lagen (2003:389) om elektronisk kommunikation (LEK)”

När NIS-direktivet implementerades i svensk rätt föll internetknutpunkter utanför NIS-lagens tillämpningsområde, genom undantaget i 5 § NIS-lagen som slog fast att lagen inte gäller för företag som tillhandahåller allmänna elektroniska kommunikationsnät enligt LEK. Vidare tydliggörs detta undantag i MSB:s föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2024:4), 9 kap. 1 §, där endast registreringsenheter för toppdomäner och DNS-tjänster räknas upp som samhällsviktiga tjänster under sektorn digital infrastruktur, och inte internetknutpunkter.

Enligt NIS2-direktivet ska både leverantörer av internetknutpunkter och tillhandahållare av allmänna elektroniska kommunikationsnät ingå i regelverkets tillämpningsområde. PTS noterar dock att leverantörer av internetknutpunkter är en sådan verksamhetsutövare som faller under huvudregeln för beräkning av huruvida en entitet är viktig eller väsentlig enligt NIS2-direktivet (*väsentlig* om den överstiger trösklarna för medelstora företag, artikel 3.1 a, NIS2-direktivet; *viktig* om den understiger trösklarna, artikel 3.2, NIS2-direktivet), medan en tillhandahållare av allmänna elektroniska kommunikationsnät är väsentlig redan som medelstort företag (artikel 3.1 c). Detta innebär att om den svenska implementeringen av NIS2-direktivet följer tidigare resonemang om internetknutpunkter, så kommer även internetknutpunkter utgöra väsentliga verksamhetsutövare om de är medelstora företag. De kommer även utgöra viktiga verksamheter om de är små- eller mikroföretag, istället för att falla utanför tillämpningsområdet helt, se artikel 2.2 a (i), NIS2-direktivet.

Eftersom NIS2-direktivet fastställer minimiharmonisering (artikel 5 NIS2-direktivet) föreligger det visserligen inget hinder för Sverige att implementera NIS2-direktivet på så sätt att även internetknutpunkter utgör väsentliga verksamhetsutövare som medelstora företag (och viktiga verksamheter som små- och mikroföretag), genom att de ingår i kategorin tillhandahållare av allmänna elektroniska kommunikationsnät. PTS vill dock lyfta denna fråga eftersom det faktum att internetknutpunkter inte omnämns i delbetänkandet förefaller vara en kvarleva från implementeringen av NIS-direktivet, där man genom 5 § NIS-lagen helt uteslöt operatörer som omfattades av kraven i kraven i 8 kap. 1 och 3 §§ LEK.

Om utredningen anser att internetknutpunkter fortsatt ska regleras som tillhandahållare av elektroniska kommunikationsnät så anser PTS att resonemang om detta bör stå med i förarbetena till cybersäkerhetslagen, och det bör tydligt fastställas att så är fallet, för att undvika förvirring. PTS ser anledning att behålla den nuvarande ordningen, där internetknutpunkter faller under kategorin tillhandahållare av allmänna elektroniska kommunikationsnät, eftersom dessa aktörer redan är anmälda enligt LEK.

PTS efterfrågar en analys av möjligheten att behålla nuvarande regler i LEK.

Relevant avsnitt i delbetänkandet: 11.2 Bestämmelserna i LEK, kodexen och NIS2

PTS kan inte se att utredningen har gjort någon analys av om NIS2-direktivet delvis skulle kunna genomföras genom att ha kvar bestämmelserna i LEK. Enligt PTS finns det vissa fördelar med att behålla bestämmelserna i 8 kap. 1-4 §§ LEK eftersom de problem som lyfts ovan då inte skulle uppstå. Vidare finns det enligt PTS en stor fördel med att regelverket för telekomsektorn fortsatt är sammanhållet i en lag som på ett tydligt sätt pekar ut PTS som ansvarig för tillsyn, främjande och inte minst reglering genom föreskrifter. Det skulle även troligtvis innebära en minskad administrativ börda för både sektorn och PTS.

2.4. Cybersäkerhetslagens relation till eIDAS2-förordningen

PTS vill uppmärksamma lagstiftaren på att det inom kort kan finnas behov av att ompröva bedömningen att ingen myndighet som undantas i sin helhet tillhandahåller en betrodd tjänst.

Relevant avsnitt i delbetänkandet: 5.5.4 Undantag för offentliga verksamhetsutövare

Statliga myndigheter som till övervägande del bedriver säkerhetskänslig eller brottsbekämpande verksamhet kommer enligt utredningens förslag inte omfattas av cybersäkerhetslagen. Av artikel 2.9 NIS2-direktivet framgår dock att verksamhetsutövare som agerar som tillhandahållare av betrodda tjänster inte kan undantas från lagens tillämpningsområde. Utredningen har bedömt att ingen myndighet som undantas i sin helhet är tillhandahållare av en betrodd tjänst. PTS håller med om att så kan vara fallet nu, men i och med den reviderade versionen av eIDAS-förordningen som träder i kraft i maj 2024 tillkommer nya betrodda tjänster. Som exempel kan nämnas elektroniska attributsintyg eller validering av sådana intyg. Med de nya tjänsterna kan fler myndigheter komma att bli tillhandahållare av betrodda tjänster. Detta kan även innefatta myndigheter som bedriver säkerhetskänslig eller brottsbekämpande verksamhet.

Incidentrapporteringsbestämmelserna enligt cybersäkerhetslagen överlappar motsvarande bestämmelser i eIDAS-förordningen. Detta motverkar syftet med att överföra vissa delar av eIDAS-förordningen till NIS2-direktivet. PTS efterfrågar ett förtydligande i denna del.

Relevant avsnitt i delbetänkandet: 7.3 Incidentrapportering

Av skäl 92 NIS2-direktivet framgår att tanken med övergången från eIDAS-förordningen till NIS2-direktivet har varit att rationalisera de skyldigheter som åläggs bland annat tillhandahållare av betrodda tjänster och att kunna möjliggöra för såväl tillhandahållare som tillsynsmyndigheter att dra nytta av den rättsliga ram som inrättas genom NIS2-direktivet, inbegripet utnämning av en CSIRT-enhet med ansvar för risk- och incidenthantering. Man vill alltså underlätta bland annat för tillhandahållare genom att bland annat göra incidentrapporteringen enhetlig för fler verksamhetsutövare.

PTS vill göra lagstiftaren uppmärksam på att tillhandahållare av betrodda tjänster är skyldiga att rapportera incidenter även enligt eIDAS-förordningen, som offentliggjordes i en reviderad version i april 2024. Enligt det förslag till incidentrapporteringsbestämmelse som följer av eIDAS2-förordningen ska tillhandahållare av betrodda tjänster rapportera alla säkerhetsincidenter eller störningar vid tillhandahållandet av tjänsten eller genomförandet av de åtgärder som avser registrerings- och anslutningsförfaranden för en tjänst, förfarandemässiga eller administrativa kontroller som krävs för att tillhandahålla betrodda tjänster samt förvaltning och genomförande av betrodda tjänster när dessa har en betydande inverkan på den tillhandahållna betrodda tjänsten eller de personuppgifter som lagras däri, utan onödigt dröjsmål och under alla omständigheter inom 24 timmar från säkerhetsincidenten eller störningen.

PTS bedömer att denna bestämmelse överlappar de bestämmelser om incidentrapportering som följer av förslaget till cybersäkerhetslagen, främst utifrån skrivningen ”åtgärder rörande förvaltning och genomförande av tjänster” som PTS anser är generellt uttryckt. PTS efterfrågar därför att det ska tydliggöras under vilket regelverk som tillhandahållare av betrodda tjänster ska rapportera in incidenter vid avsaknad av en genomförandeakt från Kommissionen.

2.5. PTS föreslår vissa ändringar i toppdomänlagen

PTS anser att definitionen av *domänadministratör* i toppdomänlagen bör spegla definitionen av *registreringsenhet för toppdomän* i cybersäkerhetslagen, genom att även den förstnämnda definitionen innefattar ett krav på att *ha delegerats* en specifik

toppdomän. Detta för att undvika tolkningssvårigheter avseende vilka aktörer, och i vilken roll, som omfattas av toppdomänlagen.

Relevant avsnitt i delbetänkandet: 6.3 Domännamnsregistreringsuppgifter

PTS instämmer i utredningens bedömning att det är lämpligt med en sammanhållen lagstiftning för toppdomäner, och att artikel 28 NIS2-direktivet därmed bör införlivas i toppdomänlagen.

PTS instämmer däremot inte i alla delar i utredningens resonemang på s. 186 och 187 avseende artikel 28 NIS2-direktivet och den bedömning som görs av definitionen i artikel 6.21 samt resonemanget som förs kring toppdomänen .nu, och den slutsats som utredningen drar baserat på det förda resonemanget. PTS bemöter inte enskilda delar av utredningens resonemang utan utvecklar istället nedan sin egen syn på sakförhållandena kring det som utredningen tar upp på nämnda sidor.

Bestämmelserna i artikel 28 NIS2-direktivet riktar sig till både registreringsenheter och enheter som tillhandahåller domännamnsregistreringstjänster. Utifrån beskrivningen av definitionen i artikel 6.21 NIS2-direktivet menar PTS att en registreringsenhet är en s.k. registry, dvs. en enhet som i nuvarande toppdomänlag benämns som domänadministratör. En viktig aspekt i definitionen är att en registreringsenhet har delegerats en specifik toppdomän, och alltså inte bara ansvarar för administrationen av toppdomänen. PTS anser därför inte att utredningens ansats att tillämpa en förenklad version av definitionen i artikel 6.21 för registreringsenhet är lämplig, dvs. att i toppdomänlagen definiera domänadministratör som den som ansvarar för administrationen av en toppdomän utan att det samtidigt i förarbetena till lagen tydliggörs att det innefattar att ha delegerats toppdomänen. PTS noterar också i sammanhanget att utredningen i sitt förslag till cybersäkerhetslagen har med den viktiga aspekten om delegering i definitionen av registreringsenhet. PTS föreslår därmed att definitionen av domänadministratör får följande lydelse ”*den som har delegerats en toppdomän och som ansvarar för administrationen och den tekniska driften av toppdomänen*”.

Att inte tydliggöra vilken typ av aktör som avses med domänadministratör skulle enligt PTS mening riskera att skapa osäkerhet och tolkningssvårigheter om vilka aktörer, och i vilken roll, som omfattas av toppdomänlagens bestämmelser. I propositionen (2004/05:175) till nuvarande toppdomänlag framgår det tydligt i förarbetena och författningskommentarerna att domänadministratör motsvarar begreppet registry, alltså den aktör som har delegerats toppdomänen.

Vidare, utifrån beskrivningen av definitionen i artikel 6.22 NIS2-direktivet menar PTS att en enhet som tillhandahåller domännamnsregistreringstjänster är en s.k. registrar, dvs. en aktör

som har avtal med en eller flera registreringsenheter för att sälja domännamn under en aktuell toppdomän som registreringsenheten har delegerats.

Internetstiftelsen har av ICANN (IANA-funktionen) delegerats toppdomänen .se och är således registreringsenhet (domänadministratör enligt toppdomänlagen) för den toppdomänen. Internetstiftelsen har i sin tur avtal med ett flertal enheter som tillhandahåller domännamnsregistreringstjänster (registrarer) som säljer domännamn under .se.

Vad gäller toppdomänen .nu så har inte Internetstiftelsen delegerats den toppdomänen, och är därmed enligt PTS mening inte en registreringsenhet för .nu. Den organisation som har delegerats .nu är IUSN Foundation. Internetstiftelsens roll avseende .nu är att på uppdrag av IUSN Foundation sköta drift och administration av .nu. Internetstiftelsen säljer inte heller själv domännamn under .nu, men på motsvarande sätt som för .se finns ett flertal enheter som tillhandahåller domännamnsregistreringstjänster (registrarer) som säljer domännamn under .nu.

Internetstiftelsen är således enligt PTS bedömning vare sig registreringsenhet (registry) eller en enhet som tillhandahåller domännamnsregistreringstjänster (registrar) för .nu. Internetstiftelsens verksamhet avseende .nu torde därmed enligt PTS uppfattning inte omfattas av artikel 28 NIS2-direktivet utifrån beskrivningen av definitionerna i artikel 6.21 och 6.22. De aktörer som enligt PTS uppfattning omfattas av artikel 28 avseende toppdomänen .nu är de enheter som tillhandahåller domännamnsregistreringstjänster (registrarer) som säljer domännamn under .nu. PTS noterar dock att utredningen, såsom framgår på s. 188, gjort bedömningen att enheter som tillhandahåller domännamnsregistreringstjänster (registrarer) inte ska omfattas av den kommande toppdomänlagen. Om lagstiftaren ändå väljer att låta den kommande toppdomänlagen omfatta enheter som tillhandahåller domännamnsregistreringstjänster (registrarer) så utgår PTS ifrån att lagstiftningen blir generell, dvs. att den kommer att gälla alla sådana enheter, med andra ord inte bara de som säljer .nu-domännamn utan också de som säljer domännamn under andra toppdomäner.

Ett annat scenario där toppdomänen .nu skulle omfattas av artikel 28 NIS2-direktivet är om IUSN-Foundation (som har delegerats .nu) skulle etablera ett huvudsakligt etableringsställe i Sverige, och då blir det IUSN-Foundation såsom registreringsenhet för .nu som bestämmelserna i artikel 28 riktar sig mot.

Att det är två olika saker att å ena sidan ha delegerats en toppdomän å andra sidan att enbart sköta administrationen av toppdomänen på uppdrag av den som har delegerats toppdomänen framgår också i Södertörns tingsrätts dom den 14 mars 2024 i mål T 17546-23, där följande citat är hämtat ”*Det skiljer sig åt huruvida det är den av IANA utsedde ccTLD*

Managern som också administrerar och förvaltar toppdomänen, eller om själva administrationen och förvaltningen utförs av en tredje part på uppdrag av den som är ccTLD Manager. Just denna fråga är av central betydelse i målet.".

PTS noterar utredningens ambition, genom att t.ex. föreslå en förenklad version av definitionen i artikel 6.21 NIS2-direktivet för registreringsenhet, att .nu ska omfattas av kraven i artikel 28 och kommande toppdomänlag. Som nämnts ovan delar PTS inte den ansatsen om det inte kompletteras med ett tydliggörande i kommande proposition om vilken roll den aktuella aktören ska ha avseende .nu för att omfattas av kommande toppdomänlag. PTS har ovan redogjort för på vilka sätt myndigheten anser att .nu kan omfattas.

Om lagstiftaren ändå bedömer det lämpligt att toppdomänen .nu ska omfattas i kommande toppdomänlag genom den verksamhet som Internetstiftelsen bedriver avseende .nu, vilket då inte är som registreringsenhet utan endast genom att administrera .nu genom avtal med den aktör som har delegerats .nu, så utgår PTS ifrån att det i så fall blir lagstiftarens mening att det ska gälla även andra toppdomäner än bara .nu där en aktör enbart sköter administrationen av toppdomänen. PTS menar att det i så fall bör tydliggöras i kommande proposition att toppdomänlagen också omfattar aktörer med sitt huvudsakliga etableringsställe i Sverige som via avtal med en registreringsenhet sköter administrationen av registreringsenhetens toppdomän. Lagstiftningen bör alltså utformas mer generellt och inte enbart peka ut en specifik toppdomän.

PTS föreslår att ytterligare tillägg görs i toppdomänlagen för att artikel 28 NIS2-direktivet till fullo ska anses implementerat i svensk rätt.

Relevant avsnitt i delbetänkandet: 6.3 Domännamnsregistreringsuppgifter

Enligt artikel 28.1 NIS2-direktivet ska medlemsstaterna ålägga registreringsenheter för toppdomäner och enheter som tillhandahåller domännamnsregistreringstjänster att samla in och upprätthålla korrekta och fullständiga registreringsuppgifter för domännamn i en särskild databas. För registreringsenheter för toppdomäner föreslås implementeringar genom ändringar i toppdomänlagen. För enheter som tillhandahåller domännamnsregistreringstjänster saknas dock en fullständig implementering i svensk lag.

Enheter som tillhandahåller domännamnsregistreringstjänster nämns visserligen i 1 kap. 6 § cybersäkerhetslagen som en gränsöverskridande verksamhetsutövare, samt i 7 § där det anges att de omfattas oavsett storlek. I 7 § hänvisas dock till 4 §, som i sin tur hänvisar till bilaga 1 eller 2 i NIS2-direktivet där enheter som tillhandahåller domännamnsregistreringstjänster inte finns med. Frågor som uppkommer är exempelvis (1)

vilken myndighet som dessa leverantörer ska anmäla sig till eftersom de inte ingår i en sektor, (2) vilken myndighet som ansvarar för förteckning över leverantörerna och (3) om leverantörerna över huvud taget ska anmäla sig när de varken finns uppräknade i bilaga 1 eller bilaga 2 i NIS2-direktivet och inte heller omfattas av toppdomänlagen.

Anledningen till att tillhandahållare av domännamnsregistreringstjänster omfattas av NIS2-direktivet framgår bl.a. av skäl 109. Det framgår där att domännamnsystemets säkerhet, stabilitet och resiliens säkerställs genom att upprätthålla korrekta och fullständiga databaser med registreringsuppgifter för domännamn (WHOIS-data). Även tillhandahållare av domännamnsregistreringstjänster anges som en leverantör för detta ändamål. I skäl 110 anges också att tillhandahållare av domännamnsregistreringstjänster bör vara skyldiga att möjliggöra för legitima åtkomstsökande att få laglig åtkomst till specifika domännamnsregistreringsuppgifter som är nödvändiga för åtkomstbegärans syfte, i enlighet med unionsrätten och nationell rätt. Inget av dessa skäl implementeras för tillhandahållare av domännamnsregistreringstjänster, varken i cybersäkerhetslagen eller toppdomänlagen, eftersom toppdomänlagen enligt utredningen endast ska omfatta registreringsenheter.

För att följa NIS2-direktivet fullt ut skulle toppdomänlagen enligt PTS behöva kompletteras så att även enheter som tillhandahåller domännamnsregistreringstjänster omfattas av toppdomänlagen, och därmed åläggs att samla in information om innehavaren till ett domännamn i en särskild databas, på samma sätt som gäller för registreringsenheter i toppdomänlagen, och att lämna ut domännamnsregistreringsdata till legitima åtkomstsökande.

En komplettering av toppdomänlagen med enheter för domännamnsregistreringstjänster innebär att förutom avseende lagens tillämpningsområde behöver ytterligare ändringar göras i toppdomänlagen, såsom i 2, 6 och 11 §§. PTS har inte i samband med detta remissvar analyserat vilka exakta ändringar som är lämpliga att göra i dessa, och eventuellt andra, paragrafer.

Att komplettera toppdomänlagen med enheter för domännamnsregistreringstjänster bedömer PTS som lämpligt eftersom det kommer uppstå situationer där registreringsenheten för en viss toppdomän är etablerad utanför EU, samtidigt som tillhandahållaren av domännamnsregistreringstjänsten (registraren) kan ha huvudsakligt etableringsställe i Sverige. Det finns t.ex. idag i Sverige ett flertal enheter som tillhandahåller domännamnsregistreringstjänster som säljer domännamn under .com, .org, .tv m.fl. Om dessa enheter inte skulle omfattas av Sveriges genomförande av NIS2-direktivet skulle det kunna innebära att Sverige inte ställer samma krav på vissa domäner som andra medlemsländer avseende korrekthet och riktighet på domännamnsregistreringsuppgifter.

Som nämns ovan blir det ett problem att en enhet som tillhandahåller domännamnsregistreringstjänster som finns i Sverige kan undkomma kravet på att lämna ut uppgifter om en domännamnsinnehavare för sådana domännamn. Rättigheten för myndigheter (svenska och i annat EU land) att enligt artikel 28 NIS2-direktivet begära ut uppgifter om en domännamnsinnehavare för sådana domäner åsidosätts därmed. Det är dessutom enheter som tillhandahåller domännamnsregistreringstjänster som har avtal och kontakt med kunderna som köper domäner och som därför lättare kan ställa krav och säkerställa att den information man samlar in är korrekt och fullständig.

2.6. Behov av avgränsning av begreppet *leverantör av DNS-tjänster*

PTS anser att en avgränsning av begreppet *leverantör av DNS-tjänster* bör tydliggöras i kommande förarbeten till cybersäkerhetslagen för att säkerställa att lagens tillämpningsområde inte blir oproportionerligt brett.

Relevant avsnitt i delbetänkandet: 4.5 Digital infrastruktur

Enligt NIS2-direktivet ska leverantörer av DNS-tjänster omfattas av regelverket oavsett storlek (artikel 2.2 a (iii)), som väsentlig entitet (artikel 3.1 b). Det finns dock vissa undantag, som kan utläsas ur direktivet.[3]

Utöver dessa undantag bör en avgränsning göras för sådana företag som inte *tillhandahåller* en DNS-tjänst, men som innehar en auktoritativ namnserver för *egna* domäner (egna webbplatser hos stora företag kan tänkas inbegripa sådana). Sådana företag bör enligt PTS falla utanför NIS2-direktivets tillämpningsområde utifrån en tolkning av begreppen ”leverantör” och ”tillhandahålla”.

Trots att dessa namnservrar skulle kunna beskrivas som allmänt tillgängliga, så torde det inte röra sig om en *tjänst* som *tillhandahålls*[4], utan snarare om ett verktyg som organisationen

[3] Två exempel: En privatperson som tillhandahåller rekursiva DNS-tjänster endast till familjemedlemmar tillhandahåller inte *allmänna* rekursiva tjänster (på eng. ”*publicly available*), enligt artikel 6.20 a, och faller därmed utanför NIS2-direktivets tillämpningsområde. Denna tolkning har fått stöd av EU-kommissionen genom ett Q&A-dokument som cirkulerats till medlemsländer, baserat på frågor som dykt upp inom ramen för arbetet med olika länders NIS2-implementering. EU-kommissionen har även förtydligat att en DNS-resolver (rekursiv DNS), som tillhandahålls av en internetleverantör uteslutande för att tillhandahålla internetåtkomsten, ska betraktas som en del av internetåtkomsten. Detta eftersom DNS-resolvern installeras automatiskt när uppkopplingen aktiveras och internetåtkomsten skulle vara oanvändbar för den genomsnittliga internetslutanvändaren utan den. I dessa fall ska DNS-resolvern därför kategoriseras som en elektronisk kommunikationstjänst. Detta stöds även av BEREC Guidelines on the Implementation of the Open Internet Regulation, s. 24.

[4] Jämför artikel 3.1 b och artikel 6.20, NIS2-direktivet.

använder inom ramen för sin egen verksamhet. I det fall det finns organisationer som för egen del innehar egna auktoritativa DNS:er/namnservrar, bör dessa alltså falla utanför NIS2-direktivets tillämpningsområde så länge dessa inte marknadsförs och tillhandahålls som tjänster till tredje man.

PTS har lyft denna fråga inom ramen för de NIS-expertgrupper som myndigheten deltar i på EU-nivå. PTS har där kommunicerat ovanstående tolkning, att organisationer som endast innehar auktoritativa DNS:er för sina egna domäner bör falla utanför NIS2-direktivets tillämpningsområde, och fått medhåll från flera andra experter som deltagit. Ingen expert har uttryckt motsatt syn på tillämpningsområdet.

Konsekvensen av att inte göra den föreslagna avgränsningen skulle kunna innebära att upp mot 25 000 verksamhetsutövare faller in under begreppet *leverantör av DNS-tjänst* enligt artikel 6.20 NIS2-direktivet. Med den avgränsning som PTS föreslår torde siffran vara närmare 100. PTS kan inte se att syftet med NIS2-direktivet är att reglera samtliga företag som innehar egna domännamnservrar, och rekommenderar att denna avgränsning tydliggörs inom ramen för den svenska implementeringen av NIS2-direktivet.

2.7. Riskhanteringsåtgärder och incidenthantering

Det uttryckliga kravet att bedriva systematiskt och riskbaserat informationssäkerhetsarbete bör utgå eftersom detta krav redan framgår av en annan bestämmelse. Om detta krav kvarstår bör bestämmelsen omfattas av ingripande- och sanktionsmöjligheter.

Relevant avsnitt i delbetänkandet: 7.1.3 Systematiskt informationssäkerhetsarbete

PTS anser att kravet att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete utgör organisatoriska riskhanteringsåtgärder som följer av artikel 21 NIS2-direktivet. Enligt PTS följer därmed kravet på ett riskbaserat och systematiskt informationssäkerhetsarbete redan av 3 kap. 1 § cybersäkerhetslagen och den föreslagna bestämmelsen 3 kap. 2 § cybersäkerhetslagen bör därmed utgå för att undvika dubbelreglering. PTS anser att exempelvis genomförande av riskanalyser utgör en sådan organisatorisk riskhanteringsåtgärd som verksamhetsutövare behöver vidta i enlighet med artikel 21 NIS2-direktivet och 3 kap. 1 § cybersäkerhetslagen.

Om utredningens förslag behålls oförändrat ser PTS att utmaningar kan uppstå i samband med framtagande av närmare föreskriftskrav. Den överlappning som till viss del föreligger mellan 3 kap. 1 § och 3 kap. 2 § cybersäkerhetslagen riskerar att medföra att det blir svårt att fastställa vilka föreskriftskrav som ska hänföras till respektive bestämmelse i

cybersäkerhetslagen. Även om PTS enligt förslaget ges föreskriftsrätt för båda paragraferna, anser PTS att det är olyckligt att tillsynsmyndighetens ingripande- och sanktionsmöjligheter skiljer sig åt beroende på om det handlar om bristande efterlevnad av 1 § eller 2 §.

PTS noterar vidare att det saknas ingripande- och sanktionsmöjligheter vid brister i det riskbaserade och systematiska informationssäkerhetsarbetet (3 kap. 2 § cybersäkerhetslagen). Detta innebär en diskrepans jämfört med PTS nuvarande ingripande- och sanktionsmöjligheter i LEK för motsvarande brister. Genom den tillsyn som PTS har bedrivit under åren och genom inrapporterade incidenter, har det framkommit att det ofta brister i det riskbaserade och systematiska informationssäkerhetsarbetet. För det fall 3 kap. 2 § behålls som en separat bestämmelse anser PTS att det är mycket viktigt att bestämmelsen omfattas av de ingripandemöjligheter som följer av 5 kap. cybersäkerhetslagen. Utredningens förslag skulle i annat fall innebära att tillsynsmyndighetens möjligheter att ingripa i samband med brister i det riskbaserade och systematiska informationssäkerhetsarbetet begränsas, jämfört med idag.

Se även skäl 95 i NIS2-direktivet där vikten av att ta fasta på den kunskap och kompetens som redan förvärvats inom Kodexen, inom ramen för säkerhetsåtgärder och incidentrapporter, framhålls.

Definition av *incidenthantering* bör införas i cybersäkerhetslagen.

Relevant avsnitt i delbetänkandet: 7.1.2 Riskhanteringsåtgärder

I artikel 6.8 NIS2-direktivet finns en definition av *incidenthantering*. PTS anser att denna definition bör införas i cybersäkerhetslagen alternativt att begreppets innebörd redogörs för i förarbeten och att det tydliggörs att begreppet även innefattar åtgärder och förfaranden som syftar till att förebygga och upptäcka incidenter. Detta skulle tydliggöra vilka närmare riskhanteringsåtgärder som avses i 3 kap. 1 § punkten 1 cybersäkerhetslagen.

PTS föreslår att kravet på att information till användare vid betydande cyberhot bryts ut till en egen separat bestämmelse för att inte stå i strid med artikel 23.2 NIS2-direktivet.

Relevant avsnitt i delbetänkandet: 1.1 Förslag till lag om cybersäkerhet

Den nu föreslagna författningslösningen i 3 kap. 6 § fjärde stycket cybersäkerhetslagen är otydlig och delvis missvisande. PTS anser att det är viktigt att kravet omformuleras, för att inte stå i strid med kravet i artikel 23.2 NIS2-direktivet. Av den artikeln framgår att kravet tar sikte på att informera användare om eventuella åtgärder eller avhjälpande arrangemang som

dessa kan vidta. Information om själva hotet ska endast ske "när så är lämpligt". Det kan i vissa fall vara olämpligt att informera kunderna om själva hotet. I vissa fall är det bättre att informationen endast innehåller förslag på eventuella åtgärder eller avhjälpande arrangemang.

Bestämmelsen bör förslagsvis formuleras så här:

”Verksamhetsutövaren ska utan onödigt dröjsmål informera användare som kan antas påverkas av ett betydande cyberhot om eventuella skydds- eller motåtgärder dessa kan vidta och, om det är lämpligt, om själva hotet.”

Cybersäkerhetslagen behöver möjliggöra för tillsynsmyndigheten att ålägga verksamhetsutövaren att informera allmänheten om betydande incidenter.

Relevant avsnitt i delbetänkandet: 11.2.8 Informera allmänheten om incidenter

PTS kan inte se att utredningen har föreslagit en motsvarande möjlighet i cybersäkerhetslagen för tillsynsmyndigheten som i dag följer av 8 kap. 3 § andra stycket LEK. PTS håller därmed inte med om att 8 kap. 3 § andra stycket LEK direkt motsvaras av utredningens föreslagna reglering. PTS anser heller inte att det är tydligt hur artikel 23.7 NIS2-direktivet har implementerats i cybersäkerhetslagen.

2.8. Administrativa sanktioner och andra ingripanden

Det finns behov av klargörande kring sanktionsmöjligheter vid information till användare om betydande cyberhot.

Relevant avsnitt i delbetänkandet: 11.2.9 Informera om betydande cyberhot

Tillsynsmyndigheterna föreslås, som en sanktion, kunna förelägga verksamhetsutövare att informera användare om betydande cyberhot och det anges i delbetänkandet att en liknande bestämmelse finns i 8 kap. 4 § LEK. Enligt den angivna paragrafen i LEK har tillhandahållarna en lagreglerad skyldighet att informera påverkade användare utan att myndigheten först beslutar detta i ett föreläggande. I 3 kap. 6 § cybersäkerhetslagen finns en liknande bestämmelse som i LEK med krav på att informera kunder som kan antas påverkas av betydande cyberhot inom en viss angiven tid. För en ökad tydlighet bör förhållandet mellan sanktionen att informera användare och kravet på verksamhetsutövaren att informera kunder utvecklas i kommande lagstiftningsarbete.

Enligt förslaget kan skyldigheten leda till samtliga föreslagna sanktioner inklusive sanktionsavgift men PTS anser att detta inte framgår tydligt av uppräkningen i 5 kap. 1 § cybersäkerhetslagen. I uppräkningen över situationer när ingripande ska ske begränsas bestämmelserna i 3 kap. 6 § cybersäkerhetslagen till incidentrapportering. Enligt PTS tolkning avser kravet i 3 kap. 6 § fjärde stycket cybersäkerhetslagen snarare krav på information till kunder och borde därmed inte kunna leda till samtliga föreslagna sanktioner. Mot bakgrund av att en överträdelse av 8 kap. 4 § LEK (som föreslås upphävas) kan bli föremål för sanktionsavgifter enligt 12 kap. 1 § LEK, medför förslaget en skillnad mellan LEK och cybersäkerhetslagen avseende vilka sanktioner som kan bli aktuella i denna situation.

PTS har svårt att bedöma konsekvenserna av att möjligheten att inhämta upplysningar från andra aktörer försvinner.

Relevant avsnitt i delbetänkandet: 11.2.10 Ingripanden, sanktioner och vissa tillsynsåtgärder

Så som utredningen noterat i delbetänkandet följer av 11 kap. 3 § andra stycket LEK en möjlighet för PTS att förelägga andra aktörer än den aktuella tillhandahållaren att lämna upplysningar eller handlingar. Av laglydelsen framgår att ett sådant föreläggande kan meddelas om de uppgifter som lämnas av tillhandahållaren inte är tillräckliga, och av förarbeten till LEK (prop. 2021/22:136 s. 515 och 516) framgår att en grundläggande förutsättning är att uppgifterna behövs för tillsynen och att tillräckliga uppgifter inte kan fås av den som omfattas av lagen. PTS har svårt att bedöma konsekvenserna av denna förlorade möjlighet. PTS har inom ramen för sitt tillsynsuppdrag ännu inte meddelat något sådant föreläggande, men möjligheten till detta infördes också relativt nyligen.

PTS ser emellertid att det kan finnas situationer, i samband med tillsyn kring säkerhetsåtgärder eller för att kunna följa marknads- och tjänsteutveckling hos flera närliggande aktörer, där möjligheten att inhämta upplysningar från närliggande företag kan vara till hjälp för PTS. Det kan exempelvis underlätta vid bedömningen av hur en tillsynsinsats fortsatt ska avgränsas. Upplysningar från andra företag inom sektorn eller företag i nära anknutna sektorer, kan vara till hjälp för att fastställa orsaken till en inträffad incident, vilka brister i säkerhetsåtgärder som föreligger samt vilken aktör som bör vidta ytterligare åtgärder.

2.9. Behov av förtydligande avseende verksamhetens omfattning

PTS efterfrågar ett förtydligande avseende tillämpningen av cybersäkerhetslagen i de situationer då en verksamhetsutövare tillhandahåller tjänster som klassificeras som både väsentliga och viktiga, alternativt faller under flera olika sektorer.

Relevant avsnitt i delbetänkandet: 5.2.2 Verksamhetsutövare

Under avsnitt 5.2.2 framhåller utredningen att hela verksamheten ska omfattas av regleringen, även om ett företag skulle bedriva annan verksamhet som inte tas upp i bilaga 1 eller 2 (s. 125). PTS delar denna tolkning av direktivet, men vill påpeka att det inte tydliggörs vad konsekvensen blir om en verksamhetsutövare tillhandahåller olika tjänster som innebär att verksamheten både är viktig och väsentlig. PTS anser att denna situation måste innebära att verksamheten blir väsentlig i sin helhet, och uppmanar lagstiftaren att klargöra detta i lagtext eller förarbeten för att undvika förvirring.

Under 8.4.7, Samordning och informationsutbyte, förklarar utredningen vad konsekvensen blir för en verksamhetsutövare som står under tillsyn av flera myndigheter (s. 242). PTS vill dock lyfta frågan om vad konsekvensen blir om en verksamhet har en verksamhetsdel som ska tillsynas av en tillsynsmyndighet, en annan del som ska tillsynas av en annan tillsynsmyndighet, och en tredje del som inte omfattas av NIS2-direktivet alls. Frågan uppstår då hur denna tredje del omfattas av regelverket och vilken tillsynsmyndighet som i sådana fall ska ansvara för denna del. PTS föreslår att detta förtydligas för att undvika förvirring.

2.10. Rymdsektorns omfattning

PTS föreslår tillägg i definitionen av rymdsektorn för att klargöra dess omfattning.

Relevant avsnitt i delbetänkandet: 4.8. Rymden

I NIS2-direktivet definieras rymdsektorn enligt tabellen i bilaga 1. Delbetänkandet påpekar att NIS2-direktivet inte ger någon ytterligare vägledning om vilka rymdbaserade tjänster som omfattas. Vad som nämns är satellitkommunikation, positionerings- och tidstjänster samt jordobservation.

PTS bedömer att det är otydligt huruvida rymdsektorn omfattar *tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster* eller inte. Enligt tabellen i bilaga 1 i NIS2-direktivet omfattas tillhandahållare av både *allmänna elektroniska kommunikationsnät* och *allmänt tillgängliga elektroniska kommunikationstjänster* av sektorn *Digital infrastruktur*. Dock är endast *tillhandahållare av allmänna elektroniska kommunikationsnät* explicit undantagen från rymdsektorn. Eftersom ingen begränsning av sektorn *Digital infrastruktur*s

omfattning av entiteten *allmänt tillgängliga elektroniska kommunikationstjänster* anges i NIS2-direktivet, tolkar PTS det som att denna entitet helt faller inom sektorn *Digital infrastruktur* och därför inte omfattas av rymdsektorn.

Med en sådan tolkning, skulle det vara bättre att tydliggöra rymdsektorn med följande fetstilta tillägg:

”Operatörer av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter och som stöder tillhandahållandet av rymdbaserade tjänster, undantaget tillhandahållare av allmänna elektroniska kommunikationsnät ***och tillhandahållare av allmänna elektroniska kommunikationstjänster****.”*

2.11. Övriga synpunkter avseende författningsförslag cybersäkerhetslagen

Relevant avsnitt i delbetänkandet: 1.1 Förslag till lag om cybersäkerhet

I tillägg till ovan lämnade synpunkter vill PTS framföra nedan förslag för att förtydliga cybersäkerhetslagen.

- En redaktionell ändring behövs i 1 kap. 2 § punkten 33, där ordet ”leverantör” upprepas en andra gång i definitionen.
- I 1 kap. 2 § punkten 9 definieras *domännamnsregistreringstjänster* som en verksamhetsutövare. PTS ställer sig frågande till varför en *tjänst* definieras som en *verksamhetsutövare*, och föreslår att denna definition istället ska beskriva begreppet ***enhet som tillhandahåller*** *domännamnsregistreringstjänster,* alternativt att begreppet domännamnsregistreringstjänster ska definieras som ”**de tjänster som tillhandahålls av** registrar eller en annan verksamhetsutövare som verkar som ombud eller återförsäljare av domännamn”.
- I 1 kap. 4 § förefaller det saknas ett ”om” framför punkten 2 och framför punkten 3. Dessa undantag bör skrivas i sin helhet som ”om inte annat följer av…”. Det ”om” som följer av huvudsatsen (”Denna lag gäller för enskilda verksamhetsutövare om”) är istället kopplad till det som kommer efter undantagen. Bestämmelsen ska alltså kunna läsas som ”Denna lag gäller för enskilda verksamhetsutövare om, om inte annat följer av 5 och 6 §§, verksamheten är etablerad i Sverige…”.
- I 1 kap. 6 § tredje stycket bör följande (fetstilta) tilläggas: ”För gränsöverskridande verksamhetsutövare krävs det i stället för etablering **i Sverige**, att Sverige är huvudsakligt etableringsställe eller att företrädaren är etablerad i Sverige för att

verksamhetsutövaren ska omfattas av lagen” för att förtydliga vad som här avses med ”etablering”.

2.12. Övriga synpunkter avseende författningsförslag toppdomänlagen

Relevant avsnitt i delbetänkandet: 1.2 Förslag till lag om ändring i lagen (2006:24) om nationella toppdomäner för Sverige på internet

Lagens tillämpningsområde

PTS bedömning är att en toppdomän i sig inte är ett fysiskt objekt som har ett huvudsakligt etableringsställe, och menar att det i 1 § bör framgå att det huvudsakliga etableringsstället är knutet till domänadministratören. Vidare bör beskrivningen av lagens tillämpningsområde innefatta att lagen även omfattar enheter som tillhandahåller domännamnsregistreringstjänster, om lagstiftaren instämmer med PTS resonemang ovan om att dessa enheter bör omfattas. PTS föreslår därför att 1 § får följande lydelse ”*Denna lag gäller teknisk drift av toppdomäner på internet där domänadministratören har sitt huvudsakliga etableringsställe i Sverige. Den gäller även enheter som tillhandahåller domännamnsregistreringstjänster som har sitt huvudsakliga etableringsställe i Sverige. Vidare omfattar […] toppdomäner*”.

Definitioner

PTS har följande synpunkter på enskilda definitioner i 2 §.

Domännamnssystemet: PTS anser att definitionen, som utredningen valt att behålla från nuvarande toppdomänlag, bör ändras, dels för att domännamnssystemet inte används för att tilldela domännamn, dels för att det är oklart vad som avses med befordringsändamål. PTS anser det lämpligt att definitionen får samma lydelse som den kommer att ha i cybersäkerhetslagen.

Borttagen definition av nationell toppdomän: Definitionen av nationell toppdomän har utgått. PTS vill dock i sammanhanget uppmärksamma lagstiftaren på att begreppet nationell toppdomän används i 14 § nuvarande toppdomänlag, och utredningen föreslår ingen ändring av den paragrafen. Med tanke på att 14 § handlar om förhållanden då Sverige är i krig eller krigsfara är utredningens bedömning eventuellt att just den paragrafen ska gälla enbart för nationella toppdomäner. Om begreppet nationell toppdomän ska finnas med i 14 § anser PTS att en definition av nationell toppdomän bör finnas med i 2 §, i syfte att undvika oklarheter om vad som då i 14 § avses med nationell toppdomän. Om lagstiftaren väljer att ha med en definition av nationell toppdomän i 2 § föreslår PTS att den får följande lydelse ”*toppdomän*

som betecknar en nation, region eller annan geografisk beteckning av nationellt intresse”, vilket är den något utvidgade definition som PTS föreslog i sin rapport till regeringen i mars 2015 (PTS-ER-2015:13).

Detta yttrande har beslutats av ställföreträdande generaldirektören Catarina Wretman. I ärendets slutliga handläggning har även avdelningschefen Patrik Bystedt, verksjuristen Sofie Sandell, juristen Nicole Masur och juristen Anna Söyland (föredragande) deltagit. Vid föredragningen närvarade chefsjuristen Karolina Asp och kommunikationschefen Fredrik Kapper.