Konsekvensutredning av Post- och telestyrelsens förslag till föreskrifter om vad som utgör en betydande incident för verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster

Post- och telestyrelsen (PTS) föreslår nya föreskrifter om vad som utgör en betydande incident enligt cybersäkerhetslagen (2025:1506).

De föreslagna reglerna kompletterar och förtydligar bestämmelsen i 2 kap. 5 § cybersäkerhetslagen för verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster (telekomområdet). Föreskrifterna ska tydliggöra vad som är en betydande incident inom telekomområdet enligt cybersäkerhetslagen.

Enligt cybersäkerhetslagen ska betydande incidenter rapporteras till Myndigheten för civilt försvar, som har fått bemyndigande att meddela föreskrifter om incidentrapportering enligt 2 kap. 5–8 §§.

De föreslagna föreskrifterna ersätter 17 kap. i de numera upphävda föreskrifterna (PTSFS 2022:11) om säkerhet i nät och tjänster.

De nya föreskrifterna föreslås börja gälla 15 oktober 2026.

Bilagor:
Tabell över bemyndigande och jämförelser
Omvärldsjämförelser

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

Innehåll

1. Inledning 7

2. Det aktuella problemet och den förändring som eftersträvas 8

2.1 Bakgrund 8

2.1.1 Andra EU-rättsakter av intresse 10

2.2 Det aktuella problemet och skälen för förslaget 12

2.2.1 Utgångspunkter 12

2.3 Nya utmaningar med cybersäkerhetslagen 17

2.3.1 Incidenter som kan orsaka skada 17

2.3.2 Incidenter med påverkan på verksamhetsutövarens ekonomi 18

2.3.3 Incidenter som har vållat betydande skada för annan 19

2.3.4 Harmonisering 19

2.4 Vilka som berörs av förslaget 20

2.4.1 Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster 20

2.5 Eftersträvad förändring 21

3. Konsekvenser som bedöms uppstå om inte någon åtgärd vidtas 22

3.1 Nollalternativet 22

4. De olika alternativen 24

4.1 Analys av alternativ för föreskrifternas utformning 24

4.2 Alternativ 1: Nya föreskrifter med samma innehåll som tidigare 24

4.2.1 Beskrivning 24

4.2.2 Fördelar, nackdelar och bedömning 24

4.3 Alternativ 2: Utgå från genomförandeförordningen och anpassa till det svenska telekomområdet 25

4.3.1 Beskrivning ... 25
4.3.2 Fördelar, nackdelar och bedömning ... 25
4.4 Alternativ 3: Utgå från Myndigheten för civilt försvars föreskrifter ... 26
4.4.1 Beskrivning ... 26
4.4.2 Fördelar, nackdelar och bedömning ... 26
4.5 Alternativ 4: Utgå från tidigare föreskrifter med nödvändiga tillägg ... 27
4.5.1 Beskrivning ... 27
4.5.2 Fördelar ... 27
4.5.3 Nackdelar ... 28
4.5.4 Bedömning ... 28
4.6 Alternativ 5: Helt nya föreskrifter ... 28
4.6.1 Beskrivning ... 28
4.6.2 Fördelar ... 29
4.6.3 Nackdelar ... 29
4.6.4 Bedömning ... 30

5. Det alternativ som bedöms lämpligast ... 30
5.1 Betydande incident enligt cybersäkerhetslagen ... 30
5.1.1 PTS valda alternativ - Alternativ 4: Utgå från tidigare föreskrifter med nödvändiga tillägg ... 30
5.1.2 Motivering av valet ... 31
5.1.3 Hantering av nackdelar ... 32
5.1.4 En betydande incident inom telekomområdet ... 32
5.2 Tidigare gällande definition av säkerhetsincident och kraven på övervakning och intern incidenthantering ... 35
5.3 Begreppen driftstörning och allriskperspektiv ... 35
5.3.1 Begreppet lagrade, överförda eller behandlade uppgifter ... 38
5.4 Betydande incident som har orsakat *allvarlig driftstörning* ... 39
5.4.1 En incident som har undergrävt tillgängligheten i nät, tjänster eller uppgifter (3 kap. 2 § 1 p) ... 39
5.4.2 En incident som har undergrävt tillgängligheten till minst 400 uthyrda passiva fiberförbindelser (3 kap. 2 § 2 p) ... 41

5.4.3 En incident som undergrävt riktigheten, autenticiteten eller konfidentialiteten i nät, tjänst eller uppgifter (3 kap. 2 § 3 p) *43*

5.4.4 En incident som är gränsöverskridande (3 kap. 2 § 4 p) *44*

5.4.5 En incident som påverkat tillgängligheten i 48 timmar (3 kap. 2 § 5 p) *45*

5.4.6 En incident som inträffat på grund av samma naturkatastrof (3 kap. 2 § 6 p) *47*

5.5 Betydande incident som orsakat ekonomisk skada för verksamhetsutövaren (3 kap. 3–5 §§) 49

5.6 Betydande incident som har påverkat andra fysiska eller juridiska personer 51

5.6.1 En betydande incident som vållat betydande skada för någon som tillhandahåller en viktig samhällsfunktion (3 kap. 6 § 1 p) *51*

5.6.2 Incidenter som har undergrävt verksamhetsutövarens medverkan till nödkommunikation eller medverkan till förmedling av viktiga meddelanden till allmänheten (3 kap. 6 § 2 och 3 p) *53*

5.6.3 En incident som orsakat dödsfall eller betydande skada på en fysisk persons hälsa (3 kap. 6 § 4 p) *56*

5.7 Riskbaserad bedömning - En incident eller ett identifierat betydande cyberhot eller betydande sårbarhet som *kan leda till* allvarlig driftstörning, ekonomisk skada för verksamhetsutövaren eller betydande skada för annan 57

5.7.1 En incident, betydande cyberhot eller betydande sårbarhet som bedöms sannolikt kunna utgöra en betydande incident enligt de föreslagna föreskrifterna (3 kap. 7 § 1 p) *58*

5.7.2 En incident som misstänks ha orsakats av skadlig handling och som sannolikt kan leda till allvarlig driftstörning (3 kap. 7 § 2 p) *59*

5.7.3 En incident i kritisk internationell, nationell eller regional infrastruktur (3 kap. 7 § 3 p) *60*

5.8 Återkommande incidenter (3 kap. 8 §) 64

6. Analys av förslaget 67

6.1 Beskrivning och beräkning av förslagets eller beslutets kostnader och intäkter för staten, kommuner, regioner, företag och andra enskilda 67

6.1.1 Allmänt om kostnader för cybersäkerhet *67*

6.1.2 Verksamhetsutövare som berörs av de föreslagna reglerna *70*

6.1.3 Vidtagna åtgärder i syfte att beräkna kostnaderna ... 72
6.1.4 Kostnader för berörda företag av de föreslagna incidentrapporteringsåtgärderna ... 74
6.2 Beskrivning och beräkning av andra relevanta konsekvenser ... 77
6.2.1 Påverkan på konkurrens och konkurrenskraft ... 78
6.2.2 Samhällsekonomiska nyttor ... 78
6.2.3 Sammanfattande bedömning av kostnader och nyttor ... 78
6.3 Redogörelse för vilka åtgärder som har vidtagits för att förslaget eller beslutet inte ska medföra mer långtgående kostnader eller begränsningar än vad som bedöms vara nödvändigt för att uppnå dess syfte ... 79
6.3.1 Utgångspunkter för proportionalitetsbedömningen ... 79
6.3.2 Är föreskrifterna nödvändiga för att uppnå syftet? ... 80
6.3.3 Är föreskrifterna utformade på ett sätt som minimerar onödiga kostnader och begränsningar? ... 80
6.3.4 Sammanfattande proportionalitetsbedömning ... 81
6.4 Beskrivning av hur och när konsekvenserna av förslaget eller beslutet kan utvärderas ... 81
6.4.1 Syfte med utvärderingen ... 81
6.4.2 Utvärderingsfrågor och indikatorer ... 82
6.4.3 Data, metod och tidplan ... 82
6.5 Ikraftträdande och informationsinsatser ... 82
6.5.1 Tidpunkt för ikraftträdande ... 82
6.5.2 Informationsinsatser ... 83

7. Bedömning av om förslaget eller beslutet inskränker den kommunala självstyrelsen ... 83

8. Bedömning av om förslaget eller beslutet överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen ... 84

8.1 Tillämpligt EU-rättsligt regelverk ... 84
8.2 Förhållandet mellan NIS2-direktivet och sektorsspecifik unionsrätt ... 84
8.3 Föreskrifternas förenlighet med EU-rätten ... 85

8.4 Bedömning av om föreskrifterna går utöver NIS2-direktivets miniminivå 85
8.5 Underrättelse för anmälan till Europeiska unionen 86
8.6 Sammanfattande EU-rättsbedömning 86

9. Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på 86

10. Kontaktpersoner 88

Bilaga 1 Jämförelsetabeller och bemyndiganden 89

Bilaga 2 Omvärldsjämförelser - EU-staters implementering av NIS2-direktivet med fokus på rapporteringströsklar inom telekomområdet 93

1. Inledning

Elektroniska kommunikationsnät och elektroniska kommunikationstjänster har en grundläggande betydelse för alla delar av det svenska samhället. Alla är beroende av fungerande och säkra elektroniska kommunikationer i såväl normalläge som i kris, höjd beredskap och krig.

Post- och telestyrelsen (PTS) är den myndighet som ansvarar för området säker elektronisk kommunikation i Sverige (nedan telekomområdet). Som en del av detta har PTS getts tillsynsansvar över bestämmelserna i cybersäkerhetslagen (2025:1506), över verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster (telekomverksamhetutövare eller verksamhetsutövare).

PTS är också den myndighet som har regeringens bemyndigande att meddela ytterligare föreskrifter om vad som utgör en betydande incident inom telekomområdet. Bemyndigandet finns i 37 § cybersäkerhetsförordningen (2025:1507). [1]

Regeringen har i propositionen till cybersäkerhetslagen (propositionen) angett att föreskrifter som meddelas enligt cybersäkerhetslagen förväntas utgöra en tydlig och konkret vägledning för incidentrapportering enligt lagen, något som också har efterfrågats av flera av regeringens remissinstanser. [2] Därför förtydligar de föreslagna föreskrifterna rapporteringskravet och sätter mätbara gränser för vad som utgör betydande incidenter inom telekomområdet enligt 2 kap. 5 § cybersäkerhetslagen.

Rapporteringsskyldigheten för betydande incidenter inom telekomområdet liksom för övriga sektorer som lyder under cybersäkerhetslagen stadgas i 2 kap. 5 § cybersäkerhetslagen och kommer att förtydligas i Myndigheten för civilt försvar (MCF) föreskrifter. Regler om säkerhetsarbete för telekomverksamhetsutövare kommer i andra föreskrifter från PTS. De föreskrifter som presenteras här tar endast sikte på att förtydliga och sätta mätbara gränser för betydande incidenter inom telekomområdet.

[1] PTS bemyndigande att meddela föreskrifter omfattar sektorerna digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster mellan företag, post- och budtjänster samt rymden. Denna konsekvensutredning omfattar endast telekomområdet.

[2] Prop. 2025/2026:28, *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag*, s. 117

2. Det aktuella problemet och den förändring som eftersträvas

2.1 Bakgrund

Den 15 januari 2026 trädde cybersäkerhetslagen i kraft. Lagen implementerar NIS2-direktivet [3] i svensk rätt. Lagen innehåller en detaljerad definition av betydande incidenter och krav på incidentrapportering av betydande incidenter för samtliga sektorer som omfattas av direktivet, inklusive telekomområdet. NIS2-direktivet ersatte också delar av den tidigare EU-regleringen på telekomområdet, den så kallade kodexen. [4] Kodexen definierade begreppet säkerhetsincident och låg till grund för rapporteringsreglerna för säkerhetsincidenter i lag (2022:482) om elektronisk kommunikation (LEK) och Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster, PTSFS 2022:11 (nedan de upphävda föreskrifterna).

NIS2-direktivet omfattar bland annat sektorn för digital infrastruktur, inom vilken telekomområdet ingår. Inom ramen för direktivet har EU-kommissionen antagit en genomförandeförordning (nedan genomförandeförordningen) [5] som i artikel 23.3 närmare fastställer i vilka fall en incident ska anses vara betydande för verksamhetsutövare inom sektorn digital infrastruktur. Telekomområdet undantogs dock medvetet från genomförandeförordningens tillämpningsområde. Skälet är att telekomområdet sedan länge har en etablerad nationell struktur för incidentrapportering och en tradition av nationell reglering, vilket ansågs motivera att området även fortsättningsvis hanteras nationellt.

När kodexens rapporteringsbestämmelser upphörde att gälla och ersattes av NIS2 direktivet innebar detta att vissa bestämmelser i 8 kap. LEK behövde upphävas. Eftersom PTS föreskrifter om incidentrapportering i PTSFS 2022:11 hade meddelats

[3] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555av 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 2-direktivet)

[4] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation.

[5] KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2024/2690 av den 17 oktober 2024 om fastställande av regler för tillämpningen av direktiv (EU) 2022/2555 vad gäller tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet och närmare angivelse av i vilka fall en incident ska anses vara betydande med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster

med stöd av de lagrum i LEK som upphävdes, försvann samtidigt PTS bemyndigande att meddela dessa föreskrifter med stöd av LEK.

Myndigheten för civilt försvar (MCF) har föreskriftsrätt enligt cybersäkerhetslagen för de sektorer där PTS inte är tillsynsmyndighet. MCF:s föreskrifter omfattar många olika sektorer med varierande förutsättningar och konsekvenser vid incidenter. Telekomområdet skiljer sig dock från dessa sektorer genom sin samhällsroll, sin tekniska struktur och sin långa erfarenhet av incidentrapportering.

NIS2-direktivet uttrycker dessutom i skäl 95 att befintlig praxis inom telekomområdet bör upprätthållas för att ta tillvara den kunskap och erfarenhet som byggts upp genom kodexens genomförande. Det är mot denna bakgrund PTS erhållit bemyndigande att reglera vad som utgör en betydande incident inom telekomområdet. MCF har dock bemyndigande att meddela föreskrifter om hur incidenter ska rapporteras och vilket innehåll rapporteringen ska ha, även för telekomområdet.

De nya överordnade regelverken, tillsammans med förändringar i samhället med markant ökande cybersäkerhetssårbarheter och exponeringar (så kallade CVE:er)[6] sedan de upphävda föreskrifterna trädde i kraft, har tydliggjort behovet av att uppdatera och precisera regleringen av incidentrapportering för verksamhetsutövare inom telekomområdet. Kommissionens mål är tydligt att öka rapportering av incidenter under NIS2-direktivet, inte bara incidenter som har skapat en skadeeffekt utan incidenter med potential att skapa en skadeeffekt ska rapporteras. [7] Det är även vad som har implementerats i cybersäkerhetslagen.

Syftet med de nya föreskrifterna är att införa tydliga och harmoniserade gränser för vad som utgör en betydande incident inom telekomområdet, i enlighet med cybersäkerhetslagens krav. Föreskrifterna ska säkerställa den nivå som eftersträvas i de överordnade regelverken och att säkerhetsnivån är lämplig i förhållande till riskerna och samhällets behov av säker elektronisk kommunikation.

Genom att de nya föreskrifterna bestämmer vilka incidenter som är betydande, och därigenom ska rapporteras till MCF enligt deras föreskrifter, kommer de nu aktuella bestämmelserna att i förlängningen ge MCF och PTS viktig information som kommer att kunna läggas till grund för PTS tillsyn av verksamhetsutövarnas säkerhetsarbete. De ska dessutom möjliggöra insamling av de uppgifter som årligen ska rapporteras till EU kommissionen och ENISA, samt säkerställa att PTS kan informera andra medlemsstater eller allmänheten när detta är motiverat. Slutligen ska föreskrifterna,

[6] NIST Limits CVE Enrichment After 263% Surge in Vulnerability Submissions, NIST Updates NVD Operations to Address Record CVE Growth | NIST

[7] NIS2-direktivet 2022/2555/EC, 2022, Schmitz-Berndt, 2023a; Schmitz-Berndt et al., 2022

enligt vad regeringen uttalade i propositionen, även utgöra tydlig och konkret vägledning för incidentrapporteringen enligt lagen.

I den fortsatta framställningen används begreppen ”kommunikationsnät” eller ”nät” synonymt med ”allmänt kommunikationsnät” enligt LEK, och ”kommunikationstjänst” eller ”tjänst” synonymt med ”elektronisk kommunikationstjänst” enligt LEK. Med NIS2-direktivet och cybersäkerhetslagen ersätts begreppet ”tillhandahållare” med ”verksamhetsutövare”, begreppet ”säkerhetsincident” ersätts med ”incident” och begreppet ”betydande incident” införs för att beskriva de incidenter som ska identifieras och sedan rapporteras till den centrala kontaktpunkten i landet, MCF.

I september 2025 gav regeringen PTS i uppdrag att förbereda föreskrifter om vad som utgör en betydande incident inom telekomområdet. Uppdraget innehöll ett uttryckligt krav på att genomförandeförordningens bestämmelser skulle beaktas.

PTS har samordnat föreskriftsarbetet med MCF för att uppnå en liknande struktur och systematik samt en enhetlig tolkning av centrala begrepp i cybersäkerhetslagen. Full överensstämmelse är dock varken möjlig eller lämplig, eftersom telekomområdet har andra förutsättningar, uppgifter och mognadsgrad än de övriga sjutton sektorer som omfattas av MCF:s reglering. PTS föreskrifter är därför anpassade till telekomsektorns specifika förhållanden, men bygger på samma grundläggande principer.

2.1.1 Andra EU-rättsakter av intresse

Samma dag som NIS-direktivet antogs, antogs Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, det så kallade CER-direktivet. CER-direktivet är ännu inte införlivat i svensk rätt. En lagrådsremiss väntas i närtid (från i maj 2026). I slutbetänkandet av utredningen om genomförande av NIS2- och CER-direktiven föreslår den särskilda utredaren att endast vissa begränsade delar av CER-direktivet ska gälla kritiska verksamhetsutövare inom sektorn digital infrastruktur.[8]

I korthet ställer CER-direktivet krav på motståndskraft i samhällsviktiga i samhällsviktiga tjänster. Medlemsstaterna ska enligt direktivet identifiera verksamhetsutövare som erbjuder samhällsviktiga tjänster inom de sektorer som pekas ut. Sektorerna är något färre än de sektorer som pekas ut i NIS2-direktivet och inkluderar digital infrastruktur inklusive telekomområdet. Av NIS2-direktivet följer också att alla verksamhetsutövare som pekas ut som kritiska enligt CER också är väsentliga verksamhetsutövare enligt NIS2. För de utpekade verksamhetsutövarna ska det gälla särskilda skyldigheter. De ska vidta åtgärder för att stärka sin

[8] *Motståndskraft i samhällsviktiga tjänster*, SOU 2024:64

motståndskraft och rapportera incidenter. Genom CER fastställs skyldigheter för kritiska entiteter som syftar till att stärka deras motståndskraft och förmåga att tillhandahålla samhällsviktiga tjänster. CER inför åtgärder för att skapa motståndskraft för såväl cyberrelaterade som fysiska aspekter.

Bakgrunden till CER är ökade utmaningar vilka behöver hanteras inom EU och också en önskan att säkerställa en närmare överenstämmelse med NIS-regelverket inom ett bredare fält av sektorer än tidigare. CER anses förenligt med och är tänkt att skapa synergier med NIS2 och ta itu med den ökade sammankopplingen mellan den fysiska och digitala världen.

Redan av artikel 8 i CER-direktivet följer emellertid att medlemsstaterna ska säkerställa att artikel 11 och kapitel III (krav om motståndskraft verksamhetsutövare), IV (bestämmelser om kritiska verksamhetsutövare av särskild europeisk betydelse) och VI (bestämmelser om tillsyn och efterlevnadskontroll) i direktivet inte ska vara tillämpliga på kritiska verksamhetsutövare inom bland annat sektorn digital infrastruktur.

Samtidigt presenterade kommissionen den 19 november 2025 ett förslag till en digital samlingsförordning, den så kallade *omnibus* som bland annat innefattar förslag på ett antal ändringar i rättsakter på datarättsområdet. Syftet med förslagen i omnibus är att harmonisera reglerna om artificiell intelligens (AI), cybersäkerhet och data, bland annat genom att säkerställa att de digitala regelverken uppfyller samma syften, och att minska kostnaderna för enskilda, företag samt den offentliga förvaltningen och öka konkurrenskraften för berörda företag.

Förslagen innebär bland annat att incidentrapportering enligt flera datarättsakter ska ske via en gemensam ingång eller portal för incidentrapportering. En gemensam kontaktpunkt föreslås som företagen kan använda för att uppfylla alla skyldigheter i fråga om incidentrapportering. För närvarande måste företag rapportera cybersäkerhetsincidenter enligt flera lagar, bland annat genom nationell implementering av NIS2-direktivet, den allmänna dataskyddsförordningen och genomförandeförordningen.

Utöver dessa presenterade kommissionen i januari 2026 ytterligare ett förslag, ett *cybersäkerhetspaket*,[9] som föreslår förändringar i NIS2-direktivet. Förslaget påverkar inte definitionen av vad som är en betydande incident enligt NIS2-direktivet, även om det föreslås att uppgifter om så kallade ransomware-angrepp ska identifieras och rapporteras. Förslaget är också att krav kring undervattensinfrastruktur ska omfatta såväl tillhandahållare av allmänna som icke-allmänna elektroniska

[9] Cybersäkerhetspaket; förändringar i EU:s cybersäkerhetsakt och i NIS 2-direktivet (Fakta-pm om EU-förslag 2025/26:FPM78 : COM(2026) 11) | Sveriges riksdag

kommunikationsnät. Även alla verksamhetsutövare som ansvarar för strategisk infrastruktur med både civil och militär användning (dubbla användningsområden) föreslås omfattas av direktivets tillämpningsområde.

PTS följer utvecklingen av förslagen.

2.2 Det aktuella problemet och skälen för förslaget

2.2.1 Utgångspunkter

De föreslagna föreskrifterna har sin grund i sammanlänkade behov.

Vi lever med en samhällsutveckling där cybersäkerhetssårbarheter och exponeringar, cyberattacker och hybridhot ökar för varje år.[10] Flera källor pekar på en samhällsutveckling med fortsatt ökning av både sårbarheter och exponeringen genom antalet attacker och dess komplexitet [11]. Utgångspunkten i skapandet av dessa föreskrifter är att bestämmelserna i kodexen och LEK har upphävts och att nya föreskrifter därför måste tas fram för att förtydliga vilka incidenter som inom telekomområdet ska vara betydande, med stöd av cybersäkerhetslagen och NIS2-direktivet, samt med beaktande av EU-kommissionens genomförandeförordning.

I och med cybersäkerhetslagens ikraftträdande har begreppet säkerhetsincident ersatts av begreppet *incident*. Dessutom har det nya begreppet *betydande incident* införts, vilket får anses motsvara de säkerhetsincidenter med betydande påverkan som tidigare skulle rapporteras till PTS. Uppgiften att ta emot incidentrapporter har flyttats från PTS till MCF. PTS uppgift vad gäller identifiering av incidenter har begränsats till att PTS ska föreskriva om vad som utgör en sådan betydande incident som ska anmälas till MCF för telekomområdet. När PTS nu tar fram nya föreskrifter utgår arbetet från de bestämmelser som gällde tidigare, men det krävs förtydliganden, begreppsdefinitioner och nya trösklar för att anpassa reglerna till de nya överordnade regelverken.

Det är nya och utvidgade krav som cybersäkerhetslagen och NIS2-direktivet ställer på incidenthantering och -rapportering jämfört med vad som gällde enligt LEK och kodexen. Det finns även behov av att skapa större tydlighet och detaljering jämfört med PTS tidigare regeln i 17 kap. 6 § i de upphävda föreskrifterna.

---

[10] NIST Limits CVE Enrichment After 263% Surge in Vulnerability SubmissionsNIST Updates NVD Operations to Address Record CVE Growth | NIST

[11] Se *Unveiling the Key Findings of the SANS Institute 2024 Cyber Threat Intelligence Survey,* Unveiling the Key Findings of the SANS Institute 2024 Cyber Threat Intelligence Survey | SANS Institute, och *Cybersecurity trends: Looking over the horizon*, 2022-03-10, Cybersecurity trends: Looking over the horizon | McKinsey

Med begreppet *incident* i 1 kap. 2 § 10 p i cybersäkerhetslagen avses en händelse som påverkar eller undergräver **tillgängligheten**, **autenticiteten**, **riktigheten** eller **konfidentialiteten** (nedan ofta säkerhetsaspekterna) hos uppgifter som lagras, överförs eller behandlas, eller hos de tjänster som tillhandahålls genom eller är åtkomliga via nätverks- och informationssystem. Begreppet incident omfattar alltså påverkan på samtliga dessa fyra säkerhetsaspekter i såväl lagrade, överförda eller behandlade uppgifter, som tjänster och nät.

Enligt 2 kap. 5 § 2 st cybersäkerhetslagen är en incident betydande om den har orsakat eller *kan orsaka* allvarlig driftstörning för den erbjudna tjänsten, eller ekonomisk skada för verksamhetsutövaren eller betydande skada för andra fysiska eller juridiska personer. Den erbjudna tjänsten är inte definierad i lagen eller i NIS2-direktivet. PTS utgår ifrån definitionen av nätverks- och informationssystem i 1 kap. 2 § 16 p i cybersäkerhetslagen och ifrån skrivningar i propositionen - och ser att regeringen har avsett att den erbjudna tjänsten inom telekomverksamhet omfattar såväl nät som tjänster och lagrade, överförda eller behandlade uppgifter.

Artikel 23 och skäl 101 i NIS2-direktivet anger även tydligt att incidenter som *kan orsaka* allvarliga störningar i tjänsterna eller ekonomiska förluster för den berörda entiteten eller påverka andra fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada ska identifieras som betydande.

Lagtexten i cybersäkerhetslagen ger dock ingen närmare vägledning om hur kriterierna för de olika typerna av betydande incidenterna ska tolkas. Definitionen är övergripande och lämnar ett betydande tolkningsutrymme, vilket innebär svårigheter för verksamhetsutövare eftersom de saknar stöd för att bedöma hur allvarlig en driftstörning måste vara, om incidenter i näten omfattas av definitionen av betydande incident, vilken nivå av ekonomisk skada som är relevant, vad som utgör betydande skada för andra samt hur potentiella konsekvenser ska värderas för att utgöra en betydande incident. Det saknas även vägledning om hur samtliga säkerhetsaspekter (tillgänglighet, riktighet, autenticitet och konfidentialitet) ska vägas in i bedömningen, och vilka lagrade, överförda eller behandlade uppgifter som ska kunna omfattas av en betydande incident. Regeringen har som angetts ovan i propositionen uttryckt en förväntan på tydlig och konkret vägledning i föreskrifter om vad som är en betydande incident inom telekomområdet, och har även tydliggjort att incidenter i näten omfattas av vad som kan utgöra en betydande incident. [12]

Tillsammans motiverar dessa skrivningar i de överordnade regelverken, oklarheterna i dessa och behoven det ger, en ny och mer detaljerad reglering som följer de överordnade regelverken och dessas syften, samt ger verksamhetsutövarna den

[12] Prop. 2025/2026:28, *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag,* s. 105 och 117.

konkreta vägledningen både genom definitioner och genom trösklar, för att kunna identifiera betydande incidenter enligt lagens begrepp.

2.2.1.1 Mängden incidenter då och nu

Regeringen bedömer i propositionen att rapporteringsskyldigheten för telekomområdet i allt väsentligt kommer att vara densamma sett till vilka *slags* incidenter som ska rapporteras. PTS tolkar detta som att samma grundläggande typer av incidenter fortsatt ska identifieras och hanteras, det vill säga händelser som haft en negativ påverkan på tillgänglighet, autenticitet, riktighet eller konfidentialitet i nät, tjänster och lagrade, överförda eller behandlade uppgifter, med tillägg i definitionen av betydande incident för händelser som på annat sätt har haft en betydande påverkan, till exempel genom att skapa ekonomisk skada för verksamhetsutövaren, genom att vålla betydande skada för andra än verksamhetsutövaren. Cybersäkerhetslagens definition av betydande incident innebär en högre detaljering än PTS nu upphävda föreskrifter om incidenthantering och -rapportering. Att det är *samma slags* incidenter är inte detsamma som att antalet incidenter som behöver identifieras som betydande kommer vara oförändrat. Tvärtom indikerar bland annat NIS2-direktivets och cybersäkerhetslagens nya fokus på sådana betydande incidenter som har lett till ekonomisk skada för verksamhetsutövaren, har vållat betydande skador för andra än verksamhetsutövaren eller som ännu inte har lett till skadeeffekter - men som potentiellt kan leda till det - att fler incidenter kommer att identifieras som betydande, och därmed i förlängningen behöver rapporteras till myndigheter. Detta betyder att även om regeringen beskriver att det i stort är samma slags incidenter som ska rapporteras, kommer antalet incidenter som ska identifieras som betydande incidenter enligt de överordnade regelverken att öka, vilket medför att rapporteringen kommer att öka.

PTS ser i årsstatistiken de senaste åren att mellan 20–35 säkerhetsincidenter årligen och totalt för hela telekomområdet har rapporterats till PTS. I telekomområdet finns ungefär 750 anmälda verksamhetsutövare. PTS gör antagandet att, i en jämförelse mellan mängden verksamhetsutövare och mängden säkerhetsincidenter med betydande påverkan på nät och tjänster under åren, att det finns ett stort mörkertal. Detta kan ha olika skäl, vilka utvecklas nedan i texten.

2.2.1.2 PTS tidigare reglering om incidenter

Tidigare var föreskrifterna om bedömningen av incidenters allvarlighetsgrad tydligare knuten till skyldigheten att rapportera incidenter, men nu är ansvaret och föreskriftsmandatet delat mellan PTS och MCF. I beskrivningen av de upphävda reglerna använder vi därför begreppen ”rapporteringsplikt” och

”rapporteringspliktiga incidenter” för att beskriva de typer av incidenter som motsvarar vad som nu benämns som betydande incidenter. PTS har haft regler för incidentrapportering sedan 2012.

Rapporteringsskyldigheten för säkerhetsincidenter enligt nu upphävda regler i LEK [13] omfattade liksom rapporteringsplikten i cybersäkerhetslagen skador eller negativ påverkan på tillgänglighet, riktighet, autenticitet och konfidentialitet i nät, tjänster och tjänster. Definitionen av säkerhetsincident i nu upphävda delar av LEK var denna:

”säkerhetsincident: en händelse med en faktisk negativ inverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster, eller på förmågan att motstå sådana händelser.”

Den legala definitionen av säkerhetsincident kombinerades med PTS regler om vilken övervakning och beredskap verksamhetsutövare inom telekomområdet skulle ha för att förebygga, upptäcka och åtgärda säkerhetsincidenter. Bland annat reglerade 12 kap 1 § vilken övervakning och beredskap som behövdes för att kunna förebygga, upptäcka och åtgärda säkerhetsincidenter, att system skulle finnas som larmade vid tillgänglighetsproblem och att verksamhetsutövaren skulle ha beredskap dygnet runt för att kunna hantera säkerhetsåtgärder.

Utöver 12 kap. 1 § fanns bestämmelsen i 17 kap. 5 § som tydliggjorde vilken negativ inverkan på tillgänglighet som krävdes för att rapporteringsplikt skulle inträda, medan säkerhetsaspekterna autenticitet, riktighet och konfidentialitet i nät, tjänster och uppgifter lämnades utan motsvarande konkreta kriterier som fanns för tillgänglighetsproblem och formulerades i bestämmelsen i 17 kap. 6 §.

Uppsamlingsbestämmelsen i 17 kap 6 §, var tänkt att fånga upp alla *övriga* säkerhetsincidenter med betydande påverkan på nätets eller tjänstens funktion eller på samhällsfunktioner, alltså sådana som föll utanför 17 kap 5 § och dess tillgänglighetsperspektiv.

I 17 kap. 3 § reglerades vad en incidentrapport skulle innehålla, bland annat uppgifter om hur tillgänglighet, autenticitet, riktighet eller konfidentialitet påverkats av incidenten, om samhällsviktiga funktioner påverkats samt om nödkommunikation begränsats.

Det bör i detta sammanhang framhållas att verksamhetsutövare formellt sett var skyldiga att identifiera även sådana säkerhetsincidenter som påverkade autenticitet,

[13] definitionen av säkerhetsincident som den såg ut i 1 kap. 7 § LEK

riktighet och konfidentialitet redan enligt LEK, eftersom skyldigheten följde direkt av lagen och inte enbart av PTS föreskrifter. Att sådana incidenter i praktiken sällan rapporterades bör ha varit en konsekvens av att PTS föreskrift i 17 kap 6 § inte angav några detaljerade trösklar för att avgöra vad som utgjorde en säkerhetsincident med de typerna av betydande påverkan på nät och tjänster. Föreskriften förtydligades dock genom utformningen av PTS rapporteringsblankett. Förslaget till föreskrifter innebär att det är samma slags incidenter som redan omfattades av LEK som omfattas nu. Det PTS nu gör är en nödvändig precisering av krav som redan följde av LEK och PTS upphävda föreskrifter – tillsammans med en nödvändig anpassning efter nu gällande överordnade regelverk, som ställer mer precisa krav.

2.2.1.3 Erfarenheter från PTS tidigare föreskrifter

Erfarenheterna från de upphävda föreskrifterna visar att bestämmelser med alltför abstrakta kriterier fungerar mindre väl i praktiken. Bestämmelsen i 17 kap. 5 §, med den så kallade tabellen, har innehållit tydliga tröskelvärden för tillgänglighetsincidenter sedan många år. Detta ledde till att den historiska rapporteringen till PTS i huvudsak omfattat incidenter som påverkat tillgängligheten i nät och tjänster. Regeln tillämpades relativt konsekvent och gav verksamhetsutövarna relativt goda förutsättningar att avgöra när rapportering skulle ske, men regeln innebar även otydligheter som nu behöver rättas till. Det var till exempel inte tydligt hur eller om säkerhetsincidenter i så kallade svarfibernät skulle rapporteras, och incidenter som innebar otillgänglighet till lagrade, överförda eller behandlade uppgifter omfattades heller inte av tabellen, trots att definitionen av säkerhetsincident enligt LEK gjorde det.

Bestämmelsen i 17 kap. 6 § fungerade inte heller tillfredställande. Den var för abstrakt genom att den saknade konkreta och mätbara kriterier, vilket innebar att verksamhetsutövare i princip sällan rapporterade incidenter enligt regeln. Införandet av det så kallade allriskperspektivet för säkerhetsincidenter, som alltså omfattade tre nya aspekter vid sidan av tillgänglighetsaspekten, var nytt med kodexen och det saknades praxis om sådana *övriga* säkerhetsincidenter som beskrivs i 17 kap. 6 § i de upphävda föreskrifterna. Detta ledde till att säkerhetsincidenter som påverkat autenticitet, riktighet och konfidentialitet eller som haft betydande påverkan på samhällsfunktioner - och som sannolikt borde ha rapporterats, inte rapporterades.

Erfarenheterna visar att verksamhetsutövare behöver konkreta och mätbara kriterier för att leva upp till kraven i de överordnade regelverken. Inte minst för att skapa en enhetlig tillämpning mellan alla verksamhetsutövare.

Konsekvensen av att den tidigare regleringen saknade tydliga trösklar var också att PTS i sin tillsynsverksamhet saknade en fullständig och tillförlitlig lägesbild över

säkerhetsincidenterna inom telekomområdet, något som efterfrågats av regeringen i bland annat ett regeringsuppdrag som gavs PTS i juni 2025.[14]

2.3 Nya utmaningar med cybersäkerhetslagen

Cybersäkerhetslagen innebär mer detaljering av begreppet betydande incident jämfört med tidigare reglering enligt LEK. Till skillnad från de delar som rör autenticitet, riktighet och konfidentialitet – där förslaget innebär en precisering av redan tidigare gällande skyldigheter att identifiera säkerhetsincidenter – utgör de nya inslagen i begreppet betydande incident enligt NIS2-direktivet och cybersäkerhetslagen andra bedömningspunkter för att avgöra om en incident utgör en betydande incident – det är bland annat de delar av begreppet betydande incident enligt cybersäkerhetslagen som omfattar påverkan på verksamhetsutövarens egen ekonomi, delvis andra aspekter av vållad betydande skada för andra och framhållandet i begreppet av sådana betydande incidenter som har potential att skapa skadeeffekter. I stor utsträckning omfattades de nu mer tydligt uttryckta aspekterna av betydande incidenter redan av LEK:s definition av säkerhetsincident. Bristen i den tidigare regleringen var att PTS inte tillhandahöll tillräckligt tydliga och detaljerade föreskrifter om vilka säkerhetsincidenter som hade betydande påverkan på när och tjänster.

2.3.1 Incidenter som *kan* orsaka skada

Verksamhetsutövarna ska inte, och skulle heller inte tidigare, i sitt arbete med att analysera och identifiera incidenter i sitt säkerhetsarbete endast bedöma om en incident faktiskt har orsakat skada, utan även om den *kan* göra det. Detta krav på bedömning av potentiell påverkan genom en incident är nu förtydligad i NIS2 och cybersäkerhetslagen i jämförelse med LEK. En säkerhetsincident enligt LEK var även sådana händelser som hade påverkat en verksamhetsutövares förmåga att upprätthålla sin säkerhetsförmåga. Ett exempel på en sådan säkerhetsincident som påverkat verksamhetsutövarens säkerhetsförmåga var enligt PTS uppfattning redan enligt LEK att verksamhetsutövaren fått intrång i sina system eller tjänster som påverkat verksamhetsutövarens förmåga att upprätthålla säkerheten.

För att identifiera och analysera betydande incidenter som *kan* orsaka skadeverkningar behöver verksamhetsutövaren sannolikt förfina sina bedömningar, trots den tidigare gällande definitionen enligt LEK. Sådana bedömningar behöver vägledning om hur framtida konsekvenser ska identifieras och värderas, och ställer

[14] *Uppdrag till Post- och telestyrelsen att stärka förmågan att förebygga och hantera incidenter som kan följa av aktörsdrivna hot i sektorn för elektronisk kommunikation*, Diarienummer: Fi2025/01205 (delvis) Fi2025/01426.

krav på verksamhetsutövarnas interna processer för incidenthantering. I propositionen skriver regeringen följande om detta:[15]

”En sådan inledande bedömning bör bland annat ta hänsyn till de drabbade nätverks- och informationssystemen, särskilt deras betydelse för tillhandahållandet av entitetens tjänster, allvaret i och de tekniska egenskaperna hos cyberhotet och eventuella underliggande sårbarheter som utnyttjas, samt entitetens erfarenhet av liknande incidenter. Indikatorer såsom i vilken utsträckning tjänstens funktion påverkas, hur länge incidenten pågår eller hur många tjänstemottagare som drabbas kan också, enligt skäl 101 [i NIS2], spela en viktig roll när man fastställer om tjänstens driftsstörning är allvarlig.”

I skäl 101 i NIS2 skrivs detta om vad sådana inledande bedömningar ska omfatta:

” En sådan inledande bedömning bör bland annat ta hänsyn till de drabbade nätverks- och informationssystemen, särskilt deras betydelse för tillhandahållandet av entitetens tjänster, allvaret i och de tekniska egenskaperna hos cyberhotet och eventuella underliggande sårbarheter som utnyttjas, samt entitetens erfarenhet av liknande incidenter. Indikatorer såsom i vilken utsträckning tjänstens funktion påverkas, hur länge incidenten pågår eller hur många tjänstemottagare som drabbas kan spela en viktig roll ”.

2.3.2 Incidenter med påverkan på verksamhetsutövarens ekonomi

Ekonomisk skada för verksamhetsutövaren införs som en ny del av definitionen av betydande incident i cybersäkerhetslagen. LEK saknade en motsvarande bedömningsdel om ekonomisk skada för verksamhetsutövaren. Verksamhetsutövare saknar därför erfarenhet av att bedöma incidenter utifrån detta kriterium. Det krävs nu tydliga kriterier för vad som avses med ekonomisk skada, vilken nivå av skada som är relevant och hur omfattningen ska bedömas och dokumenteras, för att rapporteringen ska bli enhetlig mellan verksamhetsutövare och för att skapa tydlighet samt underlätta för verksamhetsutövarna. Den kvantitativa tröskeln fanns inte uttryckligen i kodexen, inte i LEK och inte i PTS föreskrifter. Men PTS hade även utifrån de då gällande reglerna i LEK kunnat ha en tröskel om detta. Det är en tydlig och bra kvantitativ tröskel som indikerar betydande påverkan på nät, tjänster eller uppgifter.

[15] Prop. 2025/2026:28, *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag,* s. 102

2.3.3 Incidenter som har vållat betydande skada för annan

Betydande skada som vållats för andra genom en telekomincident införs också genom cybersäkerhetslagen. Detta innebär att verksamhetsutövare inte enbart ska beakta konsekvenser för den egna verksamheten, utan även för andra som har eller kan ha drabbats av incidenten hos verksamhetsutövaren. Denna rapporteringsgrund fanns delvis redan enligt kodexen, LEK och 17 kap. 6 § i PTS upphävda föreskrifter eftersom betydande påverkan på en samhällsfunktion skulle rapporteras som en säkerhetsincident.

För att underlätta för verksamhetsutövarna behövs nu tydligare föreskrifter och i vissa fall vägledning om vad som utgör sådana betydande incidenter som skadat andra.

2.3.4 Harmonisering

Eftersom ett tydligt syfte med NIS2-direktivet är att harmonisera reglerna inom sektorerna som omfattas av direktivet är det centralt att sträva efter detta gentemot såväl andra medlemsstaters tolkning av de överordnade reglerna i direktivet som nationellt. Det senare gäller inte minst gentemot de rapporteringsföreskrifter som MCF kommer att meddela för andra sektorer som lyder under cybersäkerhetslagen.

I arbetet att så långt som möjlighet harmonisera de svenska reglerna med andra medlemsstaters regler finns flera betydande utmaningar, bland annat att flera länder har ännu inte implementerat direktivet i nationell lag. [16] Andra länder har antagit lagstiftning, men har inte detaljerade regler på nivån motsvarande föreskrifter. Det är även en utmaning i harmoniseringshänseende att direktivet implementeras på vitt olika sätt, med olika nationella myndighetsstrukturer som har ansvar för olika sektorer eller för alla sektorer, se bilagan för omvärldsjämförelse.

Genomförandeförordningens utformning för övriga delar av sektorn för digital infrastruktur ger PTS viktig information om hur utmaningar med konkretiseringen av vad som utgör betydande incidenter för andra slags verksamheter kan hanteras. Förordningen utgör EU-kommissionens tolkning av NIS2-direktivets krav. Bland annat eftersom regeringen uttryckligen i ett tidigare regeringsuppdrag [17] meddelat att PTS ska beakta förordningen i sitt föreskriftsarbete, utgör även den en central referenspunkt för utformningen av tröskelvärden och kriterier även för telekomområdet.

[16] Irland, Spanien, Luxemburg, Frankrike och Nederländerna i mars 2026.

[17] Uppdrag den 4 september 2025 till Post- och telestyrelsen att förbereda genomförandet av NIS 2-direktivet (Fi 2025/01676), om att PTS skulle förbereda sig på att ta fram föreskrifter om vad som utgör betydande incidenter inom telekomområdet.

Samtidigt måste hänsyn tas till telekomområdets särskilda förutsättningar och den mångåriga nationella erfarenhet av incidentrapportering som motiverade att sektorn undantogs från genomförandeförordningens direkta tillämpningsområde.

2.4 Vilka som berörs av förslaget

De aktörer som berörs av regleringen är i första hand de verksamhetsutövare inom elektronisk kommunikation som omfattas av cybersäkerhetslagen, både stora operatörer och mindre aktörer. Mindre aktörer har ofta begränsade resurser och är särskilt känsliga för otydlig reglering, vilket ökar risken för underrapportering eller felaktiga bedömningar.

PTS påverkas direkt som tillsynsmyndighet, eftersom de föreslagna föreskrifterna skapar grund för tillsynsarbetet, skapar inblick i verksamhetsutövarnas säkerhetsarbete och ger möjligheten att upprätthålla en tillförlitlig lägesbild av incidenter inom området nationellt.

MCF berörs indirekt, eftersom de nu aktuella föreskrifterna från PTS kommer att utgöra grund för rapportering av incidenter till MCF enligt cybersäkerhetslagen.

Därutöver berörs andra myndigheter med cybersäkerhetsansvar, användare av elektroniska kommunikationsnät och tjänster, organisationer som tillhandahåller viktiga samhällsfunktioner, det svenska samhället i stort och den nationella cybersäkerheten, och i förlängningen även Enisa som ska ta emot aggregerade rapporter från MCF om betydande incidenter i Sverige.

2.4.1 Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster

Även verksamhetsutövare som är tillhandahållare av nummeroberoende interpersonella kommunikationstjänster, så kallade NOIK:ar, omfattas av NIS2-direktivet, cybersäkerhetslagen och de föreslagna föreskrifterna. I skäl 96 i NIS2-direktivet tydliggörs detta och skälen för det:

”Mot bakgrund av den ökande betydelsen av nummeroberoende interpersonella kommunikationstjänster enligt definitionen i direktiv (EU) 2018/1972 är det nödvändigt att säkerställa att sådana tjänster också omfattas av lämpliga säkerhetskrav med tanke på deras särskilda karaktär och ekonomiska betydelse. I takt med att attackytan fortsätter att växa blir nummeroberoende interpersonella kommunikationstjänster, såsom meddelandetjänster, utbredda attackvektorer. Inkräktare med uppsåt att vålla skada använder plattformar för att kommunicera och locka offer att öppna komprometterade webbsidor, vilket ökar sannolikheten för incidenter som involverar utnyttjande av personuppgifter och i förlängningen säkerhet i nätverks- och informationssystemen.”

2.5 Eftersträvad förändring

Enligt 37 § 2 cybersäkerhetsförordningen får PTS meddela ytterligare föreskrifter om vad som utgör en betydande incident inom telekomområdet.

Det finns behov av att förtydliga cybersäkerhetslagen definition av betydande incident för telekomområdet och att ersätta PTS tidigare regler i de upphävda föreskrifterna med regler som implementerar cybersäkerhetslagen.

PTS ser ett behov av att cybersäkerhetslagens nya och utvidgade begrepp *betydande incident* konkretiseras för att ge verksamhetsutövarna förutsättningar att fullgöra sina skyldigheter enligt den nya lagen och MCF:s rapporteringsföreskrifter.[18] Tydliga kriterier införs för påverkan bland annat på uppgifter, antagonistiska angrepp, ekonomisk skada, skada för andra fysiska eller juridiska personer och potentiell påverkan. Verksamhetsutövare ska genom föreskrifterna och i vissa fall vägledning ges stöd för hur bedömningen ska göras. Konkreta kriterier tas fram för samtliga fyra säkerhetsaspekter – tillgänglighet, autenticitet, riktighet och konfidentialitet – varav påverkan på de tre sistnämnda tidigare saknade detaljerad reglering i PTS upphävda föreskrifter. Förtydligandena avser också nät, tjänster och uppgifter. Vilka är begrepp som definieras i föreskrifterna.

Begreppet *betydande incident* förses i föreskrifterna med begreppsdefinitioner avsedda för identifiering av betydande incidenter samt konkreta och mätbara trösklar, i enlighet med de erfarenheter som visar att abstrakta bestämmelser inte fungerar i praktiken.

De nya föreskrifterna ska vidare ligga så långt i linje som möjligt med genomförandeförordningens bestämmelser för övriga delar av sektorn för digital infrastruktur samt med MCF:s föreskrifter för övriga sektorer. Detta är viktigt för att uppnå en ändamålsenlig harmonisering inom ramen för NIS2-direktivet och för att säkerställa en enhetlig tolkning av centrala begrepp i cybersäkerhetslagen på nationell nivå. Full överensstämmelse är varken möjlig eller lämplig med hänsyn till telekomområdets särskilda förutsättningar.

Sammantaget syftar föreskrifterna till att uppfylla regeringens förväntningar genom att precisera begreppet betydande incident för telekomområdet, säkerställa en konsekvent tillämpning mellan aktörer, stärka PTS lägesbild och tillsynsförmåga samt skapa rättssäkerhet och förutsägbarhet för de verksamhetsutövarna – allt inom

[18] MCF:s roll som gemensam nationell kontaktpunkt övergår till Nationellt cybersäkerhetscenter vid Försvarets Radioanstalt (FRA) den 1 juli 2026. PTS roll påverkas inte.

ramen för det EU-rättsliga regelverk som NIS2-direktivet och genomförandeförordningen utgör.

3. Konsekvenser som bedöms uppstå om inte någon åtgärd vidtas

3.1 Nollalternativet

Nollalternativet innebär att inga nya föreskrifter tas fram och att verksamhetsutövare inom telekomområdet enbart har cybersäkerhetslagens generellt hållna definition av begreppet betydande incident att förhålla sig till. Skyldigheten att rapportera betydande incidenter enligt lagen kvarstår i detta scenario, men utan för verksamhetsutövarna konkret vägledning om vilka incidenter som når upp till kriteriet betydande incident.

Till skillnad från övriga delar av sektorn för digital infrastruktur omfattas telekomområdet *inte* av EU-kommissionens genomförandeförordning, som fastställer konkreta tröskelvärden för incidentrapportering för övriga delar av sektorn. Detta innebär att verksamhetsutövare inom övriga delar av sektorn för digital infrastruktur har tillgång till tydlig och bindande EU-rättslig vägledning, medan telekomaktörerna i ett nollalternativ skulle stå utan motsvarande konkretisering – varken på EU-nivå eller nationell nivå. Den diskrepans som därmed skulle uppstå inom sektorn är problematisk, eftersom den riskerar att leda till en inkonsekvent rapportering och ojämlika förutsättningar för verksamhetsutövare som i övrigt verkar under liknande förhållanden. Genomförandeförordningen ger en modell för hur medlemsstater kan utforma nationella trösklar.

Trösklarna i genomförandeförordningen speglar NIS2-direktivets fokus på påverkan på tjänster och användare, *inte bara tekniska detaljer*. NIS2 och cybersäkerhetslagen innebär bland annat en skyldighet att rapportera betydande incidenter men innehåller inga praktiska riktlinjer för tröskelvärden – när en incident faktiskt ska rapporteras – vilket skapar osäkerhet hos verksamhetsutövare. Cybersäkerhetslagen behöver därför kompletteras med tröskelvärden för sektorn elektronisk kommunikation, så att operatörer och andra aktörer vet när en incident är rapporteringspliktig.

Erfarenheterna från PTS tidigare föreskrifter ger en tydlig bild av vad ett sådant scenario skulle innebära i praktiken. Uppsamlingsbestämmelsen i 17 kap. 6 § i de nu upphävda föreskrifterna var utformad på ett liknande abstrakt sätt och tillämpades sällan av verksamhetsutövarna.

Kostnaderna som nollalternativet för med sig för verksamhetsutövarna bedömer PTS som i vart fall uppgående till desamma som de nu föreslagna föreskrifterna innebär.

Detta eftersom en stor osäkerhet kring vilka incidenter som är betydande skulle medföra omfattande och onödiga analyser för verksamhetsutövarna. De kategorier av incidenter som anges nedan följer nämligen direkt av lagen, med undantag för kategorin återkommande incidenter.

Nollalternativet skulle även innebära att PTS inte uppfyller det mandat myndigheten har enligt cybersäkerhetsförordningen, och inte heller de förväntningar som regeringen har uttryckt på tydlighet i föreskrifter om betydande incidenter i propositionen. I propositionen berör regeringen att Telenor och Skatteverket, bland andra remissinstanser, har pekat på svårigheterna för en verksamhetsutövare att bedöma kraven i CSL om huruvida en omständighet kan orsaka en allvarlig driftsstörning eller ekonomisk skada, inte minst när det gäller att bedöma risken för potentiell skada för andra. Regeringen bedömer därför i propositionen att det finns ett behov av att den myndighet som regeringen bestämmer bör få meddela föreskrifter om incidentrapporteringen och konstaterar slutligen också att: ”*Föreskrifterna kommer enligt regeringens mening att utgöra sådan tydlig och konkret vägledning som Telenor efterfrågar*.” [19]

Att inte ta fram föreskrifter skulle således inte enbart försvåra PTS tillsynsansvar enligt cybersäkerhetslagen, utan även gå emot regeringens förväntningar på föreskrifter som dessa uttrycktes i propositionen och som framgår enligt mandatet till PTS i 37 § cybersäkerhetsförordningen att meddela ytterligare föreskrifter om vad som utgör en betydande incident enligt cybersäkerhetslagen.

Nollalternativet skulle vidare försvåra den samordning med MCF:s föreskrifter som är nödvändig för att säkerställa en enhetlig tolkning av centrala begrepp i cybersäkerhetslagen och uppnå en konsekvent systematik i det samlade regelverket för incidentrapportering på nationell nivå. MCF:s föreskrifter är avsedda att täcka de sektorer som omfattas av cybersäkerhetslagen, där PTS inte är tillsynsmyndighet. PTS nu föreslagna föreskrifter är avsedda att fungera som ett komplement anpassat till telekomområdets särskilda förutsättningar.

För verksamhetsutövarna skulle avsaknaden av tydliga kriterier skapa betydande osäkerhet kring vilka incidenter som ska rapporteras, vilket riskerar att leda till både under- och överrapportering samt till en inkonsekvent rapportering mellan olika aktörer. Mindre aktörer, som typiskt sett har sämre förutsättningar att hantera rättslig osäkerhet, skulle drabbas oproportionerligt hårt. För PTS skulle nollalternativet innebära en fortsatt ofullständig lägesbild över cybersäkerhetssituationen i sektorn, ökade resurser för tolkningsförfrågningar från verksamhetsutövarna och betydande svårigheter att bedriva en effektiv och rättssäker tillsyn, alternativt en stor mängd

[19] Prop. 2025/2026:28, *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag,* s. 117

oönskade rapporter. För samhället i stort riskerar bristande rapportering att försvaga den nationella cybersäkerheten och leda till att allvarliga incidenter eskalerar utan att upptäckas i tid.

Nollalternativet bedöms sammantaget inte vara förenligt med PTS tillsynsansvar, regeringens formulering i propositionen och det föreskriftsmandat som PTS erhållit genom cybersäkerhetsförordningen, behovet av harmonisering med genomförandeförordningen eller behovet av samordning med MCF:s föreskrifter. Det tjänar dock som en viktig referensram för bedömningen av de föreslagna föreskrifterna och de konsekvenser dessa förväntas ge upphov till jämfört med en situation utan sektorspecifik reglering.

4. De olika alternativen

4.1 Analys av alternativ för föreskrifternas utformning

Vid framtagandet av förslaget har PTS utrett och analyserat fem utformningsalternativ. Dessa alternativ beskriver olika möjliga sätt att strukturera föreskrifterna och sammanfattas nedan.

4.2 Alternativ 1: Nya föreskrifter med samma innehåll som tidigare

4.2.1 Beskrivning

Ett alternativ är att PTS meddelar nya föreskrifter med två paragrafer om vad som utgör en betydande incident inom telekomområdet med samma materiella innehåll som de bestämmelser som tidigare gällde enligt 17 kap. 5 § och 17 kap. 6 § i de upphävda föreskrifterna. Bestämmelsen i 17 kap. 6 § kan behållas som uppsamlingsregel, men kan förtydligas i syfte att klargöra vilka incidenter som omfattas.

4.2.2 Fördelar, nackdelar och bedömning

Alternativets främsta fördel är att verksamhetsutövarna är redan bekanta med regleringen, vilket minimerar behovet av anpassning och minskar den administrativa bördan vid övergången till nya regler. 17 kap. 6 § kan fortsatt fånga upp oförutsedda incidenttyper. Tydlighet kan skapas genom att konkreta kriterier införs inom ramen för 17 kap. 6 § för störningar av autenticitet, riktighet och konfidentialitet.

Men de tidigare föreskrifterna omfattar inte de nya överordnade regelverkens detaljering och inte alla delar av det nuvarande begreppet betydande incident enligt

cybersäkerhetslagen. 17 kap. 6 § har dessutom visat sig vara svår att tillämpa i praktiken, då aktörer sällan har rapporterat incidenter med stöd av bestämmelsen. Den tidigare regleringen delar inte heller den struktur och systematik som cybersäkerhetslagen och MCF:s föreskrifter för övriga sektorer bygger på, vilket försvårar en enhetlig tolkning av centrala begrepp i lagen och motverka den samordning som PTS och MCF eftersträvat.

Sammantaget skulle detta alternativ visserligen ge kontinuitet för verksamhetsutövarna genom att den gamla regelstrukturen med två paragrafer behålls, men det uppfyller inte de krav och förväntningar som följer av cybersäkerhetslagen, regeringens skrivningar i propositionen och det EU-rättsliga regelverket. Alternativet innebär vissa förbättringar jämfört med nollalternativet men åtgärdar inte problemet med otydlighet på ett tillräckligt sätt. Framför allt täcks inte cybersäkerhetslagens definition av betydande incident uttryckligen. Alternativet bedöms därför inte uppfylla regeringens förväntningar om att på ett tydligt och ändamålsenligt sätt precisera begreppet betydande incident inom telekomområdet. Det är därför inte ett genomförbart alternativ.

4.3 Alternativ 2: Utgå från genomförandeförordningen och anpassa till det svenska telekomområdet

4.3.1 Beskrivning

Ett alternativ är att PTS utformar föreskrifterna om betydande incidenter inom telekomområdet med EU-kommissionens genomförandeförordning som innehållsmässig, strukturell och språklig mall. Föreskrifterna skulle i så fall låna genomförandeförordningens uppbyggnad och formuleringar, men trösklarna skulle kunna anpassas till det svenska telekomområdets särskilda förutsättningar.

4.3.2 Fördelar, nackdelar och bedömning

Alternativets främsta styrka är att föreskrifterna uppnår en fullständig harmonisering med det EU-rättsliga regelverket, vilket underlättar jämförbarhet och enhetlighet inom NIS2-ramverket. Genomförandeförordningen utgör EU-kommissionens tolkning av rapporteringspliktens räckvidd inom NIS2, vilket ger föreskrifterna en tydlig EU-rättslig förankring. Föreskrifterna skulle inte gå utöver genomförandeförordningen genom att innehålla fler rapporteringskrav än vad förordningen föreskriver för de sektorer den omfattar.

Genomförandeförordningen är dock utformad för andra sektorer och undantog medvetet telekomområdet, bland annat med hänsyn till sektorns mångåriga erfarenhet av och upparbetade struktur för incidenthantering och rapportering.

Alternativet ger en god EU-rättslig förankring men beaktar inte det svenska telekomområdets särskilda förutsättningar och erfarenhet.

4.4 Alternativ 3: Utgå från Myndigheten för civilt försvars föreskrifter

4.4.1 Beskrivning

MCF:s föreskrifter är utformade för att definiera begreppet betydande incident för de sektorer som inte faller under PTS tillsynsmandat. MCF:s regler innehåller även incidentrapporteringskrav, vilket skulle falla utanför kopieringen.

4.4.2 Fördelar, nackdelar och bedömning

Alternativets främsta styrka är att föreskrifterna uppnår en hög grad av nationell samordning med MCF:s reglering av vad som är betydande incidenter för övriga sektorer, vilket underlättar en enhetlig tillämpning av cybersäkerhetslagen och en konsekvent tolkning av begreppet betydande incident. En gemensam struktur och begreppsapparat med MCF:s föreskrifter underlättar dessutom för verksamhetsutövare som kan bedriva verksamhet inom flera sektorer.

Mot dessa fördelar står flera betydande nackdelar. MCF:s föreskrifter är utformade för att täcka sjutton sektorer med mycket olika verksamheter, förutsättningar och mognadsgrad i cybersäkerhetsfrågor. En direkt kopiering riskerar därför att inte fullt ut fånga telekomområdets särskilda förutsättningar, samhällsbetydelse och den mångåriga nationella erfarenhet av incidentrapportering som motiverade att telekomområdet undantogs från genomförandeförordningens tillämpningsområde. En alltför nära koppling föreskrifterna emellan kan också försvåra möjligheten att i framtiden anpassa PTS föreskrifter till telekomområdets utveckling och särskilda behov utan att samtidigt avvika från den gemensamma strukturen. Regeringen har även givit PTS mandatet att skriva egna föreskrifter om betydande incidenter för telekomområdet.

PTS använder sig inte av begreppet ”sektorsverksamhet” i dessa föreskrifter som är det begrepp som MCF har valt. Med begreppet menar MCF ”*sådan verksamhet som omfattas av cybersäkerhetslagen*”. PTS kan inte använda sektorsverksamhet eftersom det är ett för övergripande begrepp för telekomområdet. Telekomområdet har sedan tidigt 2000-tal i stället hanterat incidenter i nät, tjänster och/eller uppgifter. Det är också så att definitionen av incident i cybersäkerhetslagen medför att PTS har behovet att tydligt definiera in de elektroniska kommunikationsnäten i var betydande incidenter kan inträffa för telekomområdet.

Alternativet ger god samordning nationellt med MCF:s föreskrifter, men beaktar inte telekomområdets särskilda förutsättningar och erfarenhet.

4.5 Alternativ 4: Utgå från tidigare föreskrifter med nödvändiga tillägg

4.5.1 Beskrivning

Detta alternativ innebär att 17 kap. 5 § i de upphävda föreskrifterna behålls med befintliga tröskelvärden och kompletteras med vissa tillägg.

Bestämmelsen i 17 kap. 6 § ersätts med flera separata och tydligt avgränsade paragrafer som var och en beskriver de incidenttyper som tidigare omfattades av den breda uppsamlingsbestämmelsen. Därutöver införs nya paragrafer som möter kraven i cybersäkerhetslagen på rapportering av ytterligare incidenttyper, bland annat incidenter som orsakat ekonomisk skada för verksamhetsutövaren, incidenter som medför betydande skada för andra fysiska eller juridiska personer samt andra incidenttyper som kan orsaka betydande skada.

Förslaget innehåller inte några allmänna råd. PTS avser i stället för allmänna råd att arbeta för att ta fram en mer levande och mer utförlig vägledning till föreskrifterna, än vad allmänna råd i en föreskrift kan skapa.

4.5.2 Fördelar

Alternativet ger tydlighet genom att varje incidenttyp definieras med konkreta och detaljerade kriterier, vilket innebär att aktörerna får klar vägledning om vilka incidenter som ska rapporteras. Kontinuiteten i regleringen av tillgänglighetsincidenter bibehålls genom att de befintliga tröskelvärdena i 17 kap. 5 § lämnas oförändrade med vissa tillägg.

Alternativet innebär en fullständig anpassning till lagens krav och täcker samtliga säkerhetsaspekter som omfattas av den nya lagstiftningen. Genom alternativet skapas ett regelverk som är helt i linje med cybersäkerhetslagens struktur och regeringens förväntningar. Tydligheten blir hög eftersom varje incidenttyp definieras med konkreta kriterier, vilket ger aktörerna en klar och förutsägbar vägledning om vad som ska rapporteras. Det minimerar även risken för feltolkningar och överrapportering eller underrapportering. Den ökade tydligheten stärker även rättssäkerheten genom att skapa stabila förutsättningar för tillsyn och sanktioner. Kontinuiteten bibehålls där det är möjligt genom att de befintliga tröskelvärdena i 17 kap. 5 § behålls och kompletteras med ett femte tröskelvärde för uthyrda passiva fiberförbindelser/svartfiberförbindelser och ett sjätte tröskelvärde för

glesbygdsområden, vilket innebär att omställningen för tillgänglighetsincidenter är begränsad.

4.5.3 **Nackdelar**

Regelverket blir mer omfattande och består av fler paragrafer än de upphävda föreskrifterna, vilket kan upplevas som tungrott. Det kräver utbildningsinsatser för att säkerställa korrekt tillämpning, något som kan vara särskilt utmanande för mindre aktörer. Alternativet innebär omställningskostnader, eftersom det kan vara resurskrävande att implementera och de löpande rapporteringskostnaderna ökar eftersom fler incidenttyper omfattas av rapporteringskrav. Detta är dock en direkt följd av lagstiftningen och NIS2-direktivet och därmed inte något som kan utelämnas ur föreskrifterna. Bristen på harmonisering av tröskelvärden kvarstår, eftersom 17 kap. 5 § inte anpassas till övriga EU-länder, vilket kan försvåra för aktörer med verksamhet i flera medlemsstater och leder till att incidenter som borde rapporteras inte kommer att göra det.

4.5.4 **Bedömning**

Alternativet ger den mest heltäckande och systematiska anpassningen till cybersäkerhetslagen bland de alternativ som inte inkluderar harmoniserade tröskelvärden, samtidigt som det uppfyller regeringens förväntningar på ett tydligt och ändamålsenligt sätt. Det skapar maximal tydlighet för aktörerna och ger en robust grund för rapportering, tillsyn samt framtida utveckling. Nackdelarna i form av högre komplexitet och omställningskostnader bedöms dock kunna hanteras genom regelbunden uppföljning och utvärdering, beredskap att uppdatera föreskrifterna vid behov, kompletterande vägledningsmaterial för gränsfall samt en kontinuerlig dialog med aktörerna om nya hotbilder. Sammantaget bedöms alternativet vara det mest heltäckande och långsiktigt hållbara av de alternativ som inte inkluderar harmoniserade tröskelvärden.

4.6 **Alternativ 5: Helt nya föreskrifter**

4.6.1 **Beskrivning**

Detta alternativ innebär först och främst en mer genomgripande förändring av 17 kap. 5 § i de upphävda föreskrifterna. De fyra befintliga tröskelvärdena sänks och harmoniseras med motsvarande reglering i andra EU-länder. Det införs även tillägg med nya kvantitativa mätpunkter. Eventuellt tas tabellformen bort och ersätts med en annan form, utöver nytt innehåll och andra harmoniserade trösklar Vidare införs nya paragrafer med konkreta kriterier för incidenter som påverkar riktighet, autenticitet och konfidentialitet i nät, tjänster och lagrade, överförda eller behandlade uppgifter. Bestämmelsen i 17 kap. 6 § ersätts med flera separata och tydligt avgränsade

paragrafer som uppfyller cybersäkerhetslagens definition av betydande incidenter, bland annat incidenter som orsakar ekonomisk skada för verksamhetsutövaren, incidenter som medför betydande skada för andra fysiska eller juridiska personer samt andra incidenttyper som kan orsaka betydande skada. Alla regler ska så långt som det är möjligt harmoniseras med andra medlemsstaters motsvarande regler.

4.6.2 **Fördelar**

Alternativet omfattar samtliga fördelar som följer av Alternativ 4 och innebär dessutom en ytterligare harmonisering med andra EU-länder, och ett genomgripande arbete av hela föreskriften. Genom att tröskelvärdena i 17 kap. 5 § sänks till nivåer som motsvarar dem som tillämpas i flera andra medlemsstater underlättas tillämpningen för aktörer med verksamhet i flera länder, samtidigt som jämförbarheten mellan länder förbättras och förutsättningarna för gränsöverskridande samarbete stärks. Harmoniserade tröskelvärden stärker även EU-gemensam statistik och analys, vilket i sin tur kan förbättra det internationella cybersäkerhetssamarbetet och därigenom cybersäkerheten som sådan. Alternativet ökar regelverkets legitimitet genom att visa att Sverige strävar efter att ligga i linje med den nivå som tillämpas i andra medlemsstater, vilket minskar risken för kritik från EU-kommissionen och stärker förtroendet hos internationella aktörer. Skälet till att tröskelvärdena sänks är att flera andra EU-länder tillämpar betydligt lägre nivåer, vilket i praktiken innebär att svenska aktörer med verksamhet i andra länder redan rapporterar incidenter som inte behöver rapporteras i Sverige, och en harmonisering minskar denna inkonsekvens och skapar likvärdiga förutsättningar.

4.6.3 **Nackdelar**

Genom att tröskelvärdena i 17 kap. 5 § sänks bryts kontinuiteten även för tillgänglighetsincidenter, vilket innebär att verksamhetsutövarna behöver ställa om även på områden där de har etablerade rutiner och stor erfarenhet. Sänkta tröskelvärden innebär dessutom att fler tillgänglighetsincidenter kommer att rapporteras, vilket ökar både engångs- och löpande kostnader för aktörerna och innebär en större belastning på tillsynsmyndigheten. Ett försök till harmonisering innebär vidare i nuläget osäkerhet, eftersom det i dagsläget inte finns någon formell EU-standard för tröskelvärden och flera länder har ännu inte hunnit skapa regler på föreskriftsnivå och några har inte hunnit implementera NIS2-direktivet i nationell lag. Det finns därför en risk för att andra länder skapar andra nivåer, eller ändrar sina befintliga nivåer, vilket kan leda till att den svenska harmoniseringen blir kortvarig eller mindre ändamålsenlig. Alternativet är det mest kostsamma av samtliga, både vad gäller omställning och löpande rapportering och innebär den största resursökningen för tillsynsmyndigheten. Slutligen aktualiseras andra proportionalitetsfrågor, eftersom

det är oklart om sänkta tröskelvärden är motiverade utifrån svenska förhållanden eller om de riskerar att leda till överrapportering utan motsvarande nytta.

4.6.4 Bedömning

Alternativet innebär samma omfattande anpassning till cybersäkerhetslagen som Alternativ 4, men kompletteras med harmoniserade tröskelvärden som stärker det internationella samarbetet och ökar regelverkets legitimitet. Samtidigt innebär alternativet högre kostnader, större omställningsbehov och en tydlig brytning av kontinuiteten även för tillgänglighetsincidenter. Sammantaget framstår alternativet som attraktivt ur ett internationellt perspektiv, men innebär betydande ekonomiska och administrativa konsekvenser som i nuläget inte bedöms proportionerliga i förhållande till harmoniseringsvinsterna.

5. Det alternativ som bedöms lämpligast

5.1 Betydande incident enligt cybersäkerhetslagen

Betydande incidenter ska enligt 2 kap. 5–8 §§ cybersäkerhetslagen rapporteras av verksamhetsutövare. Av 1 kap. 6 § framgår att lagen gäller för verksamhetsutövare som i Sverige tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster och allmänt elektroniskt kommunikationsnät. Detta inkluderar även bland andra sådana verksamhetsutövare som tillhandahåller nummeroberoende elektroniska kommunikationstjänster, så kallade *NOIK:ar*.

5.1.1 PTS valda alternativ - Alternativ 4: Utgå från tidigare föreskrifter med nödvändiga tillägg

PTS har valt att gå vidare med alternativ 4. Detta innebär att bestämmelsen i 17 kap. 5 § om incidenter som undergrävt tillgänglighet behålls med sina befintliga tröskelvärden och kompletteras med ytterligare två mätvärden, som avser slutanvändare och uppgifter. Vidare införs nya paragrafer med konkreta kriterier för incidenter som påverkar autenticitet, riktighet och konfidentialitet i nät, tjänster eller uppgifter, såsom uppgifter definieras i förslaget till föreskrifter. Den tidigare uppsamlingsbestämmelsen i 17 kap. 6 § ersätts med flera separata och tydligt avgränsade paragrafer som var och en beskriver de incidenttyper som tidigare omfattades av den tidigare tröskellösa bestämmelsen. Därutöver införs nya paragrafer som möter definitionerna i cybersäkerhetslagen om incident och betydande incident som orsakar ekonomisk skada för verksamhetsutövaren, incidenter som medför betydande skada för andra fysiska eller juridiska personer samt incidenter som *kan* orsaka betydande skada.

Förslaget innehåller inte några allmänna råd. PTS avser i stället för allmänna råd att arbeta för att ta fram en mer levande och mer utförlig vägledning till föreskrifterna, än vad allmänna råd i en föreskrift kan skapa.

5.1.2 **Motivering av valet**

Efter en samlad bedömning av samtliga alternativ ovan bedömer PTS att Alternativ 4 är det mest lämpade för att uppfylla de krav och förväntningar som följer av cybersäkerhetslagen, regeringsuppdraget och det EU-rättsliga regelverket.

Alternativ 4 är det alternativ som på ett heltäckande sätt täcker samtliga delar som cybersäkerhetsgens definition av betydande incident omfattar, inklusive incidenter som rör autenticitet, riktighet, konfidentialitet, ekonomisk skada och potentiell påverkan, utan att samtidigt bryta kontinuiteten för tillgänglighetsincidenter på det sätt som Alternativ 5 gör. Alternativ 1 till 3 lämnar delar av lagens definition av betydande incidenter utan tydliga trösklar. Alternativ 4 är därmed det minst ingripande alternativet som ändå möter cybersäkerhetslagens krav.

Det tidigare givna regeringsuppdraget ställde uttryckligen krav på PTS att ta fram föreskrifter om vad som utgör betydande incidenter för telekomområdet och därvid också beakta genomförandeförordningens bestämmelser. Alternativ 4 uppfyller även detta krav genom att kombinera en heltäckande konkretisering av lagens begrepp, med beaktande av genomförandeförordningens trösklar, utan att för den skull låsa sig vid en direkt tillämpning av förordningens tröskelvärden på ett sätt som riskerar att skapa rättslig otydlighet om förhållandet till genomförandeförordningen.

Valet tar också tillvara de erfarenheter som gjorts under tidigare reglering.

Till skillnad från Alternativ 5 innebär Alternativ 4 att de befintliga tröskelvärdena i 17 kap. 5 § behålls oförändrade med två tillägg. Detta innebär att behovet av omställning för den del av regelverket som verksamhetsutövarna är mest förtrogna med hålls minimal. PTS bedömer att en harmonisering av tröskelvärdena med andra EU-länder, i enlighet med Alternativ 5, i nuläget inte är genomförbar, bland annat mot bakgrund av att det saknas enhetlig implementering av NIS2-direktivet mellan länderna och det saknas i många nationer regler på motsvarande nivå som PTS föreskrifter. Det saknas även en formell EU-standard för sådana tröskelvärden.

För verksamhetsutövarna innebär alternativet att rutiner för att identifiera och analysera betydande incidenter kan byggas upp på ett precist sätt, och med större förutsättningar för att minska skillnader i bedömningarna mellan verksamhetsutövare, vilket minskar både över- och underrapportering samt ger PTS ett mer komplett underlag för tillsyn, analys och uppföljning.

5.1.3 Hantering av nackdelar

PTS är medvetet om att Alternativ 4 innebär högre detaljering och för vissa verksamhetsutövare fler omställningsbehov än några av de övriga alternativen. Alternativ 4 består av fler paragrafer, vilket kan upplevas som detaljerat och kräver utbildningsinsatser för att säkerställa korrekt tillämpning, något som kan vara särskilt utmanande för mindre aktörer. Alternativet innebär också omställningskostnader för att implementeras i verksamhetsutövarens processer för incidenthantering, och de löpande incidenthanteringskostnaderna kan öka eftersom fler incidenter sannolikt kommer att identifieras som betydande incidenter. Slutligen kvarstår bristen på harmonisering av tröskelvärden, eftersom 17 kap. 5 § inte anpassas till övriga EU-länder, vilket kan försvåra för aktörer med verksamhet i flera medlemsstater.

Dessa nackdelar bedöms dock kunna hanteras på ett ändamålsenligt sätt. Två samrådsrundor har genomförts för att säkerställa att bestämmelserna är tydliga och praktiskt tillämpbara. Synpunkter från samråden har beaktats i utformningen av föreskrifterna. En större verksamhetsutövare har även använt de föreslagna föreskrifterna under en dryg månads tid, utan att problem eller överrapportering har inträffat. PTS avser att ta fram vägledning för att underlätta identifiering och analys av betydande incidenter enligt förslaget. PTS avser vidare att upprätthålla en kontinuerlig dialog med verksamhetsutövarna om tillämpningen och om behov av uppdateringar.

5.1.4 En betydande incident inom telekomområdet

I de föreslagna föreskrifterna anges gränser för när en incident ska anses vara betydande. Föreskrifter behövs eftersom det saknas sådana gränser i lagen och det inte heller ges någon vägledning i propositionen. I stället uttrycker regeringen en förväntan om att föreskrifter som meddelas med stöd av lagen kommer att utgöra en sådan tydlig och konkret vägledning som efterfrågats av flera instanser i remissförfarandet till lagen för att de ska kunna tillämpa lagen. Regeringen beskriver också att det är samma slags incidenter som omfattas av den nya överordnade regleringen som tidigare. Uttrycket samma slags incidenter som enligt LEK är en ram som enligt PTS avser incidenter påverkar nät, tjänster eller uppgifter, som kan leda till skadliga effekter men cybersäkerhetslagen inför även att betydande incidenter även är sådana incidenter som har skadat verksamhetsutövarens egen ekonomi och som har vållat betydande skada för andra fysiska och juridiska personer. Mot bakgrund av att den nya överordnade lagen och NIS2-direktivet både är vidare och mer detaljerade om vad som utgör en betydande incident, blir följden att även föreskrifter som skapas i syfte att utgöra tydlig och konkret vägledning för att efterleva lagen, blir mer detaljerade. Detaljeringen motsäger inte att det rör sig om samma slags incidenter som tidigare, utan följer förändringarna i de överordnade regelverken.

En incident är, som angetts ovan, enligt 2 kap. 5 § 2 st. cybersäkerhetslagen betydande om den har orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller om den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada. I begreppet den erbjudna tjänsten omfattas nät, tjänster och lagrade, överförda och behandlade uppgifter, vilka definieras i föreskrifterna. Regeringen utvecklar i propositionen hur **incidenter i näten** ingår i definitionen betydande incident: *”Regeringen anser visserligen, som framgår ovan, att det inte finns skäl att ge incidentbegreppet enligt den nya lagen samma innebörd som i LEK. En händelse som har fysisk påverkan på ett allmänt tillgängligt kommunikationsnät och som äventyrar tillgängligheten till exempelvis nät- eller slutkundstjänster bör dock anses utgöra en incident även enligt den nya lagen. En händelse som orsakar en kabelskada i ett sådant nät, som Stokab AB resonerar kring, kan därmed räknas som en incident. För att föranleda rapporteringsskyldighet krävs dock att även ovan angivna rekvisit för att incidenten ska räknas som en betydande incident är uppfyllda. När det gäller fysisk skada på ledningar för elektronisk kommunikation är det viktigt att tillsynsmyndigheten får underlag för att kunna kontrollera att det förebyggande arbetet mot oönskad påverkan på nätet bedrivs på ett lämpligt sätt med hänsyn till risken (jfr skäl 97 och 101). Att elektroniska kommunikationsnät fungerar på ett säkert sätt och med tillräcklig redundans är av mycket stor betydelse för bland annat totalförsvaret (jfr prop. 2024/25:34 s. 129 f.). Det rådande omvärldsläget innebär ökade risker i form av så kallade hybridhot mot nät och tjänster, där antagonistiska aktörer försöker påverka genom dolda sabotage som kan vara flera och samverkande. Mot den bakgrunden utgör information om fysiska skador på nät numera en viktigare del i operatörernas långsiktiga strategiska driftssäkerhetsarbete och i tillsynen. När det gäller ett ledningsbrott i ett elektroniskt kommunikationsnät kan en incident vara betydande även när den är sådan som typiskt sett medför allvarlig driftsstörning eller avbrott i ett nät eller en tjänst men som inte har gjort det i det enskilda fallet”*[20]

Lagens definition går att bryta ner i fyra typer av betydande incidenter. PTS har även med hänsyn tagen till genomförandeförordningen ett förslag på en femte typ som rör återkommande incidenter. Syftet med kategoriseringen är att skapa tydlighet och struktur, samt även att tydligt lyfta fram sådana betydande incidenter som *kan leda till* skadliga effekter, men som ännu inte har gjort det.

De fem typerna av betydande incidenter i PTS föreslagna föreskrifter är incidenter som skapat:

- allvarlig driftstörning i nät, tjänster eller lagrade, överförda eller uppgifter,
- ekonomisk skada för den berörda verksamhetsutövaren,

[20] Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag, sid. 105

- betydande skada för andra än verksamhetsutövaren,
- kan skapa allvarlig driftstörning, ekonomisk skada för den berörda verksamhetsutövaren eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada (Riskbaserad bedömning), samt
- återkommande incidenter.

En och samma incident kan vara betydande enligt flera olika regler samtidigt. Alla grunder ska bedömas av berörd verksamhetsutövare vid identifiering och analys av incidenten.

I verksamhetsutövares arbete med att identifiera och analysera betydande incidenter, kan det krävas även annan kompetens än att avläsa och återställa system eller avhjälpa fel i system, tjänster eller uppgifter. Sådan annan kompetens har behövts även för att följa de tidigare reglerna om säkerhetsincidenter enligt LEK och PTS nu upphävda föreskrifter.

Det krävs sannolikt för att identifiera vissa incidenter som betydande ett team av olika kompetenser för att göra en fullgod analys av om en incident har nått upp till några av cybersäkerhetslagens och de föreslagna trösklarna. Detta beror på cybersäkerhetslagens definition dels omfattar dels betydande incidenter som har eller kan skapa allvarliga driftstörningar, dels sådana som har skapat eller kan skapa ekonomisk skada för verksamhetsutövaren, eller har vållat betydande skada eller kan vålla betydande skada för andra fysiska och juridiska personer. Endast vid sådana incidenter som faktiskt nått upp till rent kvantitativa driftsmässiga trösklar, sådana som kan utläsas av systemövervakning och larm borde det vara tillräckligt att identifieringen görs av en ren teknisk kompetens. Analyserna som *krävs redan enligt cybersäkerhetslagens definition av betydande incidenter* – exempelvis identifierad ekonomisk skada, eller risk för ekonomisk skada eller betydande skador för andra kan i normalfallet inte göras endast utifrån tekniska systemuppgifter och larm.

Bedömningen av incidentens betydelse kan vänta tills att konsekvenserna eller de potentiella konsekvenserna av en incident står *rimligt klara*, men det går inte att prioritera ner när denna bedömning måste göras. Tidsfristerna enligt lag räknas från kännedom om incidenten enligt 2 kap. 5–6 §§ cybersäkerhetslagen. Det kan röra kännedom om omfattning, konsekvenser, risken för konsekvenser, eller orsaker. Det är värdefullt att påminna om att krav på riskbaserad bedömning av incidenter gällde redan enligt nu upphävda definitionen av säkerhetsincident enligt LEK och förtydligas nu genom NIS2-direktivet och cybersäkerhetslagen, samt nu ytterligare i dessa föreslagna föreskrifter. Det finns således inte möjlighet att avvakta med identifieringen av att en betydande incident har inträffat om viss kännedom har uppkommit i incidenthanteringsprocessen, särskilt inte eftersom det nu införs regler om riskbaserad bedömning eller med andra ord identifiering av incidenter som kan

leda till konsekvenser som gör att de är att bedöma som betydande enligt cybersäkerhetslagen.

Vad gäller rapporteringen av de betydande incidenterna gäller MCF:s föreskrifter om incidentrapportering.

5.2 Tidigare gällande definition av säkerhetsincident och kraven på övervakning och intern incidenthantering

Begreppet säkerhetsincident definierades i 1 kap 7 § LEK (före 15 januari 2026) som: ”*en händelse med en faktisk negativ inverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten, hos ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster, eller på förmågan att motstå sådana händelser*”

Sålunda var också varje händelse med en faktisk negativ inverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten en säkerhetsincident. Huruvida säkerhetsincidenten även var rapporteringspliktig till PTS framgick av 8 kap. 4 § LEK där det angavs att säkerhetsincidenter skulle rapporteras om de *haft en betydande påverkan på nät och tjänster*. Lagrummet förtydligades i 17 kap. 5 och 6 §§ i PTS upphävda föreskrifter.

I 12 och 13 kap. i de nu upphävda föreskrifterna reglerades ”övervakning och beredskap” respektive ”intern incidenthantering”. Av det 12 kap. framgick bland annat att: ”*Tillhandahållaren kontinuerligt skulle övervaka kommunikationstjänster och aktiva delar i kommunikationsnät för att kunna förebygga, upptäcka och åtgärda säkerhetsincidenter.*” PTS vill med detta påpeka att det redan sedan tidigare funnits krav på tillhandahållare att kunna upptäcka och åtgärda händelser med en negativ inverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten i nät, tjänster och uppgifter. Vidare följde av 13 kap. i de upphävda föreskrifterna bland annat att tillhandahållarna skulle säkerställa att säkerhetsincidenter rapporterades internt och att åtgärder vidtogs skyndsamt i anledning av säkerhetsincidenter.

5.3 Begreppen driftstörning och allriskperspektiv

Begreppet driftstörning omfattar, precis som i tidigare gällande regler i kodexen, LEK och PTS föreskrifter, mer än bara tillgänglighet i nät och tjänster. Begreppet driftstörning omfattar även nu samtliga relevanta säkerhetsaspekter, d.v.s. tillgänglighet, riktighet, autenticitet och konfidentialitet även för lagrade, överförda

eller behandlade uppgifter. Även allriskperspektivet enligt NIS2-direktivet och cybersäkerhetslagen omfattar dessa fyra säkerhetsaspekter, liksom även Kodexen och propositionen till LEK gjorde.

Det finns inte någon viktning i NIS2 eller cybersäkerhetslagen som signalerar att tillgängligheten av nät och tjänster skulle vara mer central än exempelvis konfidentialitet eller riktighet. Det finns dock en tydlig tradition inom telekomområdets incidenthantering som fokuserat på störningar och avbrott (alltså tillgänglighetsproblem) i nät och tjänster. Den traditionen har levt kvar sedan de ursprungliga incidentrapporteringsreglerna infördes i LEK genom en lagändring 2012, med följd därefter i PTS första föreskrifter om incidentrapportering för telekomområdet, som infördes samma år.[21]

PTS har i detta uppdrag genom att titta på tidigare faktisk incidentrapportering och genom svar inkomna i tidigt samråd kring de nu föreslagna föreskrifterna, insett att det även efter att kodexen implementerades i LEK, och PTS nu upphävda rapporteringsregler trädde i kraft, år 2022, har levt kvar en uppfattning om att begreppet driftstörning endast avser tillgänglighetsavbrott och störningar i tillgänglighet av nät och tjänster. Den gamla begreppsanvändningen av ordet driftstörning vidgades redan 2022 genom kodexen och LEK. Branschen har således haft fyra år på sig att komma till insikt om detta och förståelse måste nu skapas för att ordet inte längre omfattar endast tillgänglighetsproblem.

Att definitionen av säkerhetsincident omfattade såväl tillgänglighet som riktighet, konfidentialitet och autenticitet i kombination med de krav som ställdes på tillhandahållarnas säkerhetsarbete, bland annat i 12 och 13 kap. i de nu upphävda föreskrifterna innebar att verksamhetsutövare redan sedan flera år har haft en skyldighet att ha system och processer för att upptäcka, analysera och hantera incidenter med inverkan på samtliga fyra säkerhetsaspekter, inte bara tillgängligheten till nät, tjänster och uppgifter. Detta är något som är viktigt att ha i åtanke vid analysen av de kostnader som förslagen kan antas föranleda och de svar på kostnadsfrågor som PTS fått in.

Det är *betydande incidenter* som ska rapporteras enligt cybersäkerhetslagen. En betydande incident är enligt de förslagna föreskrifterna en incident som bland annat ha orsakat eller kan orsaka *allvarlig driftsstörning* i nät, tjänster eller uppgifter. Alla tre begreppen definieras i de föreslagna föreskrifterna.

Det är också utifrån omfattningen av alla fyra säkerhetsaspekterna viktigt att utröna vad begreppet driftstörning numer omfattar.

[21] lagen (2003:389) om elektronisk kommunikation, ändrad genom *Lag (2011:590)*, och PTSFS 2012:2

Begreppet *driftstörning* definieras inte i vare sig NIS2-direktivet, i propositionen eller i cybersäkerhetslagen. Däremot finns det skrivningar i den tidigare propositionen till LEK som hjälper till för att förstå vad ordet driftstörning omfattar sedan kodexen implementerades i svensk lag.

I propositionen till LEK när kodexen implementerades i Sverige år 2022 anges att: *”Enligt EU-direktivet ska säkerhetsincidenter som har haft en betydande påverkan på driften av nät och tjänster rapporteras. Det svenska uttrycket driften av nät och tjänster syftar i begränsad mening närmast på grundläggande teknisk funktion i nät och tjänster. Den engelska språkversionen använder i stället uttrycket ”operation of networks or services”. Detta uttryck – ”operation of network or services” bedöms alltså av regeringen omfatta även andra delar av verksamheten än den rent tekniska driften. Som framgår av avsnitt 17.1 omfattar EU-direktivets definition av säkerhet såväl tillgänglighet (driftsäkerhet) som riktighet, autenticitet och konfidentialitet. Mot denna bakgrund bör det anges i den nya lagen att den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst utan onödigt dröjsmål ska rapportera säkerhetsincidenter som har haft en betydande påverkan på nät och tjänster till tillsynsmyndigheten. Incidentens påverkan behöver alltså inte vara begränsad till tekniska driften som sådan.”*[22]

Begreppet driftstörning behöver därför tolkas och fyllas med innebörd som omfattar vad cybersäkerhetslagen benämner *allriskperspektivet*.

Begreppet driftstörning har som sagt en traditionell tolkning inom telekomområdet som allmänt avser enbart störningar i tillgängligheten i nät och tjänster. PTS upphävda driftsäkerhetsföreskrifter, som innehöll regler med fokus just på tillgängligheten i nät och tjänster, inklusive regler om rapportering av driftsäkerhetsincidenter (alltså incidenter som innebar avbrott i tillgängligheten i nät och tjänster) är upphävda sedan 2022, och ersattes med nya i enlighet med implementeringen av kodexen, men nu alltså även de upphävda, säkerhetsföreskrifter som redan då omfattade det gällande allriskperspektivet bland annat vad avser vad som utgör betydande incidenter.

[22] Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation s. 319–320.

5.3.1 Begreppet lagrade, överförda eller behandlade uppgifter

Vad gäller begreppet *lagrade, överförda eller behandlade uppgifter*, skapar PTS en definition av *uppgifter* som kan beröras av betydande incidenter enligt de föreslagna föreskrifterna.

Definitionen i reglerna syftar till att i varje regel kunna skriva *uppgifter*, och därmed skapa tydlighet kring *vilka slags uppgifter* som avses, utan att behöva upprepa orden *lagrade, överförda och behandlade*. Syftet är också att skapa tydlighet kring *vilket slags hantering* som omfattas av reglerna, och slutligen även att begränsa bort vissa slags uppgifter och hantering av dessa som i och för sig kan omfattas av cybersäkerhetslagens definitioner av just lagrade, överförda eller behandlade uppgifter. Både lagens definition av incident och definition av nätverks- och informationssystem innehåller begreppet *lagrade, överförda och behandlade uppgifter*. Samtidigt finns det sådana uppgifter som lagras, överförs eller behandlas hos verksamhetsutövarna som enligt PTS inte har en tillräckligt kopplad betydelse till näten och tjänsterna. Därför antar PTS att det behandlas sådana uppgifter hos verksamhetsutövarna som inte är relevanta att bedöma i förhållande till betydande incidenter. Det bör vara tillräckligt enligt PTS bedömning att skriva *uppgifter* i föreskrifterna, genom att samtidigt skapa en tydlig definition i föreskrifterna av vilken hantering och vilka uppgifter som kan beröras av en betydande incident inom telekomområdet. Definitionen i föreskrifterna är skapad med utgångspunkt både i cybersäkerhetslagens definition av incident och av nätverks- och informationssystem. I det föreslagna begreppet omfattas alltid såväl lagring, som överföring och en rad hanteringssätt som omfattas av ordet *behandling*. Dessa hanteringssätt är också inskrivna i definitionen. De är inte uttömmande, men avser att vara så tydliga som möjligt. Här är det viktigt att notera att utgångspunkten för föreskrifternas uppgiftsbegrepp är cybersäkerhetslagens definitioner av vilka uppgifter som åsyftas enligt lagen och NIS2. Begreppet har inte en utgångspunkt i tidigare bestämmelser i LEK, eller i annan regelgivning eller nationella regler som härstammar från e-privacydirektivet[23] eller genom Dataskyddsförordningen (EU) 2016/679[24], även om uppgiftsbegreppen har stora likheter. Det är inte endast sådana uppgifter som normalt sett kan omfattas av en integritetsincident enligt LEK. För enligt definitionen av nätverks- och informationssystem i 1 kap. 2 § 16 p cybersäkerhetslagen omfattas också sådana digitala uppgifter som lagras, behandlas, hämtas eller överförs med nät eller sammankopplade enheter för att nät, tjänster och uppgifter ska kunna användas, skyddas och underhållas. I de föreslagna föreskrifterna uttrycks detta i definitionen av uppgifter som:

[23] Direktiv 2002/58/EG (med ändringar 2009/136/EG)

[24] Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

”1. alla uppgifter som lagras, överförs eller behandlas i samband med tillhandahållande av ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst, inklusive en åtgärd eller kombination av åtgärder, oberoende av om de utförs automatiserat eller ej, såsom insamling, hämtning, registrering, organisering, strukturering, lagring, bearbetning, ändring, framtagning, läsning, användning, överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring av uppgifter, eller

2. alla uppgifter som stödjer eller möjliggör korrekt tillhandahållande av ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst”

5.4 Betydande incident som har orsakat *allvarlig driftstörning*

5.4.1 En incident som har undergrävt tillgängligheten i nät, tjänster eller uppgifter (3 kap. 2 § 1 p)

En tabell för störningar och avbrott i tillgängligheten motsvarande den som tidigare fanns i 17 kap. 5 § i de nu upphävda föreskrifterna bör även fortsättningsvis finnas.

Regeln motsvarar 17 kap. 5 § i de upphävda föreskrifterna.

Den upphävda regeln hade sin grund i LEK:s upphävda definition av säkerhetsincident och i rapporteringsplikten av säkerhetsincidenter med betydande påverkan, samt i kodexen Art. 40.2. a-d och tolkades genom Enisas vägledning. [25]

Förslaget har sin grund cybersäkerhetslagens definitioner av incident, betydande incident och nätverks- och informationssystem samt i Art. 23.3 a-b i NIS2-direktivet.

Förslaget motsvaras av regler i Art. 5a -12 a, 5b – 12b samt 8d och art. 3.3 a och b i genomförandeförordningen och även av 3 kap. 1 § 1–4 p i MCF:s föreskrifter om vad *som påverkat tillgängligheten och* utgör betydande incidenter.

Tabellen är etablerad på telekomområdet och ändamålsenlig. PTS har övervägt förändringar i tabellen eftersom myndigheten har noterat att de svenska trösklarna ligger högre än andra EU-länders. PTS har dock beslutat att inte ändra tabellen utöver de ändringar som är nödvändiga och som anges nedan. Skälen till detta är dels att PTS prioriterat att få föreskrifter om vad som utgör en betydande incident på plats så snart som möjligt, dels att det i skäl 95 i NIS2-direktivet anges att befintliga

[25] ENISA Technical Guideline on Incident Reporting under the EECC.pdf s. 21

nationella riktlinjer som har antagits för att införliva kodexens bestämmelser om säkerhetsåtgärder bör beaktas, när så är lämpligt och för att undvika onödiga störningar, för att ta fasta på den kunskap och kompetens som redan förvärvats inom ramen för kodexen avseende säkerhetsåtgärder och incidentunderrättelser. Ytterligare en anledning är att så långt som möjligt behålla den redan etablerade tabellen för att verksamhetsutövare till någon del ska kunna behålla befintliga rutiner och system.

Trots den avsikten är ett par förändringar av tabellen nödvändiga att göra för att införliva de nya gällande överordnade regelverken i föreskrifterna. PTS har i det syftet ändrat tabellen över tillgänglighetsproblem i två avseenden. Ändringarna består i att begreppet ”slutanvändare” läggs till i tabellen och att även tillgänglighetsproblem för uppgifter - vilket avser lagrade, överförda eller behandlade uppgifter enligt begreppsdefinitionen i föreskrifterna, också omfattas av denna regel.

Både användare och slutanvändare är begrepp som definieras i 1 kap. 7 § LEK där *användare definieras som* den som använder eller efterfrågar en allmänt tillgänglig elektronisk kommunikationstjänst, medan *slutanvändare* som en användare som inte tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst.

Kapacitetsbortfall är sedan länge definierat i PTS upphävda föreskrifter om incidenter. Definitionen överförs till de föreslagna föreskrifterna och formuleras för att även omfatta slutanvändare. Påverkan på slutanvändare ska bedömas i förhållande till kapacitetsbortfall och sammanhängande geografisk yta. Men uppgifter kan och ska *inte* bedömas i förhållande till kapacitetsbortfall eller i förhållande till sammanhängande geografisk yta. När det gäller påverkan på uppgifter är kapacitetsbortfall inte relevant.

Enligt de nu upphävda föreskrifterna omfattade tabellens gränsvärden användare, men inte slutanvändare. Detta har lett till svårigheter att avgöra storleken eller bedöma konsekvenserna i inrapporterade incidenter, dvs. hur många fysiska personer eller aktiva anslutningar som faktiskt har drabbats av ett avbrott eller en störning.

PTS mål att alla i Sverige ska ha tillgång till effektiva och säkra kommunikationstjänster. Även Europeiska unionens cybersäkerhetsbyrå (Enisa) och andra europeiska länder har samma fokus på slutanvändaren, eller närmare bestämt slutanvändartimmar, och inte i första hand avtalsparters eller organisationskunder. MCF ska även enligt 27 § cybersäkerhetsförordningen i enlighet med artikel 23.9 i NIS 2-direktivet, i den ursprungliga lydelsen, var tredje månad lämna in en sammanfattande rapport till Enisa som ska inkludera slutanvändartimmar - med

anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud. Tidigare hade PTS uppgiften att vidarerapportera till Enisa en gång årligen. Redan enligt tidigare vidarerapporteringsskyldighet skulle PTS bistå Enisa med uppgifter om hur många slutanvändare som hade drabbats av en inrapporterad säkerhetsincident enligt kodexen. Enisas tekniska vägledning för vidarerapportering enligt kodexen är nu under omarbetning från den version som gällde. Den nya vägledningen kommer att innehålla vad som ska rapporteras vidare.[26] För att MCF ska kunna fullgöra skyldighet som åligger myndigheten enligt NIS2-direktet krävs därför att ”slutanvändare” inkluderas i tabellen. Även i syfte att veta hur många som faktiskt kan uppskattas har drabbats av en incident är helt central information för tillsynsmyndigheten.

Av en rubrik i tabellen framgår att det ska göras en *uppskattning* av incidentens omfattning, bland annat med antal drabbade. PTS är medveten om att det för olika typer av nät och tjänster finns olika möjligheter att med säkerhet veta hur många slutanvändare som använder nät eller tjänster. Det är exempelvis lättare i det mobila nätet att veta detta. Regeln föreskriver av den anledningen att det är en uppskattning som ska göras av antalet slutanvändare. PTS avser att utveckla uppskattningsmetoder för olika typer av nät och tjänster i en kommande vägledning till de föreslagna föreskrifterna.

PTS bedömer att samtliga verksamhetsutövare berörs. Även svartfiberleverantörer ska bedöma om incidenter i deras nät är betydande incidenter enligt denna regel. Det gäller i de fall de i identifiering och analys av en incident har fått kännedom om gränsvärden enligt tabellen. Se dock avsnitt 5.4.2.1 nedan.

5.4.2 En incident som har undergrävt tillgängligheten till minst 400 uthyrda passiva fiberförbindelser (3 kap. 2 § 2 p)

Regeln består av en utbruten och förtydligad del av 17 kap. 5 § i de upphävda föreskrifterna och innebär en tydlig regel som direkt träffar de verksamhetsutövare som hyr ut passiva nät, så kallade svartfibernät.

Den upphävda regeln i 17 kap. 5 § hade sin grund i LEK:s upphävda definition av säkerhetsincident och i rapporteringsplikten av säkerhetsincidenter med betydande påverkan, samt i kodexen Art. 40.2 d

Förslaget har sin grund cybersäkerhetslagens definitioner av incident, betydande incident och nätverks- och informationssystem samt i Art. 23.3 a-b i NIS2-direktivet.

[26] ENISA Technical Guideline on Incident Reporting under the EECC.pdf

Förslaget motsvaras inte uttryckligen av regler i genomförandeförordningen. Den motsvaras av 3 kap. 1 § 1–4 p i MCF:s föreskrifter om vad *som påverkat tillgängligheten till nät* och utgör betydande incidenter.

Syftet är att skapa en tydlighet kring att även svartfibernätleverantörers incidenter kan nå upp till gränser för vad som utgör betydande incidenter. Det har tidigare rått en oklarhet och ett mörkertal kring incidenter i svartfibernäten. I det samråd som PTS har genomfört i arbetet med dessa föreskrifter framkom i dialog med en av de större verksamhetsutövarna som tillhandahåller passiva fiberförbindelser, så kallad svartfiber, att leverantörer av passiva fiberförbindelser inte kan eller i vart fall har mycket svårt att rapportera tillgänglighetsstörningar enligt tabellen i 3 kap. 2 § 1 p. i förslaget till föreskrifter. Detta eftersom de oftast saknar kännedom om användningen av fiberförbindelserna. När en fiberförbindelse skadas så att tillgängligheten påverkas blir verksamhetsutövaren dock i normalfallet kontaktad av kunden som hyr förbindelsen. På så sätt får även uthyraren kännedom om att tillgängligheten påverkats.

Denna regel utgör en precisering av gränsvärdena för incidenter som innebär att en incident som otillgängliggjort minst 400 uthyrda passiva fiberförbindelser ska anses vara betydande. Nivån i regeln har valts i samrådet och bedöms som lämplig för att träffa endast betydande påverkan.

PTS bedömer att endast några av de större svartfiberleverantörerna berörs, vilket innebär att endast några företag berörs av denna incidentrapporteringsåtgärd.

PTS vill här understryka att om en uthyrare av svartfiber får kännedom om omständigheter enligt tabellen i 3 kap. 2 § 1 p. i förslaget så ska en bedömning av om incidenten varit betydande enligt den regeln också göras.

PTS avser att följa upp den faktiska bördan efter att regleringen trätt i kraft och kommer vid behov att se över tröskelvärdet om uppföljningen visar att bördan är oproportionerligt stor.

5.4.3 En incident som undergrävt riktigheten, autenticiteten eller konfidentialiteten i nät, tjänst eller uppgifter (3 kap. 2 § 3 p)

Regeln motsvarar 17 kap. 6 § i de upphävda föreskrifterna, med tillägget att den omfattar otillgänglighet även av uppgifter och inför två tydliga kvantitativa gränser för antal drabbade.

Den upphävda regeln hade sin grund i LEK:s upphävda definition av säkerhetsincident och i rapporteringsplikten av säkerhetsincidenter med betydande påverkan, samt i kodexen Art. 40.2 a-e och tolkades genom Enisas vägledning om vad som bör omfattas. [27]

Förslaget har sin grund cybersäkerhetslagens definitioner av incident, betydande incident och nätverks- och informationssystem samt i Art. 23.3 a-b i NIS2-direktivet.

Förslaget motsvaras av regler i Art. 5c, 6c, 7d) – 12d) i genomförandeförordningen och även av 3 kap. 1 § 3 p och 6 § 1 p MCF:s föreskrifter om incidentrapportering m.m. och den information som ska skyddas och trösklar för vad som utgör betydande incidenter.

Den tidigare regeln i 17 kap 6 § i de upphävda föreskrifterna och den rapporteringsplikt som tidigare gällde enligt 8 kap. 3 § LEK. omfattade säkerhetsincidenter med betydande påverkan på nät och tjänster, men inte direkt på uppgifter. Den nu föreslagna regeln omfattar negativ påverkan på nät, tjänster *och* uppgifter. Regeln är således inte ny, dock införs två tydliga gränser jämfört med 17 kap. 6 § i de upphävda föreskrifterna som tydliggör att det är vid 500 drabbade slutanvändare och vid 20 drabbade organisationskunder som en allvarlig driftstörning av detta slag uppstår.

PTS har vid bestämmandet av tröskelns nivå utgått från MCF:s motsvarande tröskel, vilken även den omfattar 500 drabbade, med tillägget om organisationskunder för att bättre spegla hur avtalsförhållanden och användandeser ut i telekomområdet. Användningen av gränsen 500 är alltså avsedd att skapa harmonisering av regler om vad som utgör betydande incidenter inom landet för alla sektorer som omfattas av cybersäkerhetslagen.

Regeln kommer att innebära att vissa stora integritetsincidenter hos tjänstetillhandahållare ska rapporteras också som betydande incidenter. Detta är inte ett nytt förhållande. Den tidigare gällande regleringen innebar även den att tillräckligt

[27] ENISA Technical Guideline on Incident Reporting under the EECC.pdf s. 21

stora incidenter med uppgifter som påverkade nät eller tjänster negativt rapporterades som både integritetsincidenter och säkerhetsincidenter. Dubbelrapporteringskravet kvarstår.

PTS avser även att förtydliga hur antal slutanvändare kan uppskattas av verksamhetsutövare i en kommande vägledning.

Alla företag berörs.

5.4.4 En incident som är gränsöverskridande (3 kap. 2 § 4 p)

Regeln som uttryckligen har gränsöverskridande skadeeffekt som tröskel för vad som är en betydande incident är ny. Gränsöverskridande incidenter har dock redan tidigare omfattas av kodexen och Enisas tolkning av kodexens kvalitativa trösklar för säkerhetsincidenter. I omvärldsjämförelsen kan PTS se att flera andra länder redan har en motsvarande regel.

Den upphävda regeln i 17 kap. 6 § i de tidigare föreskrifterna hade sin grund i LEK:s upphävda definition av säkerhetsincident och i rapporteringsplikten av säkerhetsincidenter med betydande påverkan, samt i kodexen Art. 40.2 c och d samt 3 stycket och tolkades genom Enisas vägledning om vad som bör omfattas av *geografisk omfattning*, varvid gränsöverskridande skadeeffekter var en sådan kvalitativ bedömningströskel som Enisa angav som lämplig för att avgöra om en incident var en säkerhetsincident med betydande påverkan på nät och tjänster [28].

Den föreslagna regeln har sin grund i, utöver de tidigare gällande kraven utifrån kodexen och Enisas tolkning, i cybersäkerhetslagens definitioner av incident, betydande incident och nätverks- och informationssystem samt skrivningar i NIS2-direktivets art. 23.1 och 23.4 a. I art. 23.1 anges att varje medlemsstat ska säkerställa att verksamhetsutövare bland annat rapporterar information som gör det möjligt att fastställa incidenters eventuella gränsöverskridande verkningar. Artikel 23.4 a i sin tur anger att det i den tidiga varningen för att ska anges om den betydande incidenten kan ha gränsöverskridande verkningar.

I MCF:s föreskrifter finns regler om vad en upplysning enligt cybersäkerhetslagen ska innehålla, vilket inkluderar om incidenten är gränsöverskridande. Genomförandeförordningens regler om vad som utgör betydande incidenter har gränsöverskridande omfattning.

[28] ENISA Technical Guideline on Incident Reporting under the EECC.pdf s. 17

PTS bedömer att det bör röra sig om relativt få betydande incidenter av detta slag, mot bakgrund dels av att regeln inte träffar de flesta incidenter, dels att rapporteringsplikt ofta torde infalla på grund av att rapporteringsplikt inträder genom annan regel. Regeln träffar skador på sådana delar av verksamhetsutövarens nät som förbinder Sverige med andra länder och incidenter i tjänster som tillhandahålls gränsöverskridande, och uppfattningen är att det är en viktig faktor för tillsynsmyndigheten att kunna följa. Bedömningen grundar sig i det alltmer nationsgränsöverskridande användandet av nät och tjänster, samt på ökande risker och hot i vår omvärld.

PTS avser att följa upp den faktiska bördan efter att regleringen trätt i kraft och kommer vid behov att se över om uppföljningen visar att bördan är oproportionerligt stor.

5.4.5 En incident som påverkat tillgängligheten i 48 timmar (3 kap. 2 § 5 p)

En ny 48-timmarsregel skapas för att fånga upp incidenter med landsbygds- och glesbygdsstörningar, där få alternativ finns till elektronisk kommunikation. Det har under åren när elektroniska kommunikationer har blivit allt viktigare för alla användare och för samhällets funktionalitet, också blivit tydligare att avsides kommuner och byar har drabbats hårt när deras elektroniska kommunikationer inte fungerar. Det har skrivits åtskilliga artiklar och samhällsdebatterats kring ett bristande fokus på säker elektronisk kommunikation för dessa områden. I dagsläget har PTS inte en helt klar bild av hur stor problematiken med denna ojämlikhet är. En ny regel kommer att innebära med kunskap om bortfall av tillgång till elektroniska kommunikationer över hela landet, inklusive avsides bygder och glesbygdsområden. Detta motsvarar även NIS2-direktivets syften.

Regeln utgör en ny lägre tröskel som ligger i linje med regeln i 17 kap. 5 § i de upphävda föreskrifterna. 17 kap. 5 § hade sin grund i LEK:s upphävda definition av säkerhetsincident och i rapporteringsplikten av säkerhetsincidenter med betydande påverkan, samt i kodexen Art. 40.2 c-e och en tolkning genom Enisas vägledning om vad som bör omfattas av *geografisk omfattning*, varvid *avlägsna eller rurala områden* var en sådan kvalitativ bedömningströskel som Enisa angav som lämplig för att avgöra om en incident var en säkerhetsincident med betydande påverkan på nät och tjänster [29].

Förslaget har sin grund cybersäkerhetslagens definitioner av incident, betydande incident och nätverks- och informationssystem samt i Art. 23.3 b i NIS2-direktivet

[29] ENISA Technical Guideline on Incident Reporting under the EECC.pdf s. 17

Motsvarande regel saknas i genomförandeförordningen och hos MCF.

Bristande tillgång till de elektroniska kommunikationerna har långt större betydelse för slutanvändare på dessa platser eftersom det oftast saknas redundans som kan ta över bortfall i funktionalitet. Detta leder till att landsbygds- och glesbygdsområden som tappar tillgången till elektroniska kommunikationer under störningar och avbrott är avskurna från övriga samhällets kommunikationer. Det blir en omfattande och påtaglig påverkan i dessa områden vid tillgänglighetsstörningar, även om antalet personer som drabbas kan vara få.

Det finns även studier som påpekar att fokus på glesbygd och områden där en enda operatör kan vara kritisk för kommunikation och samhällsfunktioner bör finnas vid skapande av regler som grundar vad som sedan ska rapporteras till myndigheter.[30]

Den föreslagna regeln innebär att en störning eller ett avbrott av tillgången till elektroniska kommunikationer i landsbygds- eller glesbygdskommun som varar längre än 48 timmar och som faktiskt drabbar minst 100 slutanvändare betraktas som en betydande incident.

Syftet med 48-timmarsregeln är att fånga upp incidenter i delar av landet där det finns få andra sätt att kommunicera om telekommunikationen går ner för en tjänsteleverantör. Regeln är avsedd att träffa tillgänglighetsproblem för relativt få slutanvändare längre bort från storstadsregionerna, där det tar längre tid att åtgärda ett fel. Det tar längre tid att reparera mer avsides problem i nät och tjänster, och det beror ofta på logistik och långa transportsträckor av tekniska komponenter som behövs för att laga felen.

Alla driftsstörningar eller - avbrott som pågår längre än 48 timmar och som drabbar 100 eller fler användare ska med den föreslagna regeln anses utgöra en betydande driftstörning – alldeles oavsett i vilket geografiskt område som en sådan störning uppstår. PTS har vid utformningen av tröskelvärdet beaktat synpunkter från aktörer om att ett lågt satt tröskelvärde riskerar att medföra en oproportionerligt stor rapporteringsbörda. PTS delar bedömningen att rapporteringsplikten bör träffa störningar av verklig betydelse för slutanvändarna.

[30] Boddy, Sara (2024). *Case study: The decision-support framework and NIS2, CER, and DORA incident reporting obligations*, samt Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive | Journal of Cybersecurity | Oxford Academic https://jyx.jyu.fi/bitstreams/5ed12901-092a-42f7-8857-84c43303eba0/download

Tröskelvärdet om 48 timmar och 100 användare har valts för att uppnå denna balans. En störning som pågår längre än 48 timmar och samtidigt drabbar 100 eller fler användare bedöms typiskt sett indikera en allvarlig påverkan på tillgängligheten som motiverar rapportering. Båda villkoren måste vara uppfyllda samtidigt för att rapporteringsplikt ska uppstå, vilket begränsar rapporteringsplikten till störningar av faktisk betydelse.

PTS bedömer att tröskelvärdet är proportionerligt i förhållande till syftet med regleringen. Bedömningen grundar sig på att störningar av denna varaktighet och omfattning erfarenhetsmässigt är ovanliga i nät med välutvecklad redundans och god tillgång till reservkomponenter. Den faktiska rapporteringsbördan bedöms därför bli begränsad för de flesta aktörer. Tröskelvärdet gäller dock utan undantag oavsett geografiskt område eller nätets utbyggnadsgrad – det är de faktiska förhållandena vid varje enskild störning som avgör om rapporteringsplikt uppstår.

PTS avser att följa upp den faktiska bördan efter att regleringen trätt i kraft och kommer vid behov att se över tröskelvärden om uppföljningen visar att bördan är oproportionerligt stor.

PTS bedömer att alla verksamhetsutövare berörs av denna utveckling av det redan befintliga kravet

5.4.6 En incident som inträffat på grund av samma naturkatastrof (3 kap. 2 § 6 p)

Regeln sätter ett gränsvärde för när en incident ska anses vara betydande och av typen allvarlig driftstörning hos en verksamhetsutövare när flera telekomverksamhetsutövare har drabbats av incidenter till följd av samma naturkatastrof. Det är inte nödvändigt att något annat tröskelvärde i föreskrifterna har uppnåtts, men det är nödvändigt att verksamhetsutövaren själv, samt en till verksamhetsutövare, har drabbats av en incident. Regeln presumerar påverkan i form av allvarlig driftstörning när flera drabbas av samma naturkatastrof. Naturkatastrof definieras även i 2 kap. för att förtydliga vad som avses med ordet i dessa föreskrifter.

Regeln är ny men omfattades av Art 40.2 e i kodexen tolkad genom Enisas vägledning om hur geografisk spridning skulle bedömas och om incidents påverkade tillgängligheten och det fanns gränsöverskridande skadeeffekter. [31] Men den saknades i de upphävda föreskrifterna.

[31] ENISA Technical Guideline on Incident Reporting under the EECC.pdf s. 21

Förslaget har sin grund cybersäkerhetslagens definitioner av incident, betydande incident och nätverks- och informationssystem samt i Art. 23.3 a-b i NIS2-direktivet.

Förslaget är en presumtionsregel för allvarlig driftstörning och saknar motsvarighet i genomförandeförordningen och i MCF:s föreskrifter om incidentrapportering m.m. och den information som ska skyddas och trösklar för vad som utgör betydande incidenter.

Angivandet av gränsen om att incidenter ska ha drabbat *två eller flera verksamhetsutövare* inom telekomområdet utgör grunden för presumtionen om allvarlig driftstörning hos de verksamhetsutövare som har drabbats. Regelvärdena är tänkta att förenkla analysen och identifieringen av betydande incidenter av detta slag.

Begreppet naturkatastrof är situationsberoende och ska tolkas i sitt sammanhang. Det kan omfatta till exempel jordbävningar, översvämningar, stormar eller skred som orsakar eller har orsakat omfattande mänskliga, materiella eller miljömässiga skador.

Under de senaste två decennierna har Sverige drabbats av flera sådana naturkatastrofer som regeln är avsedd att omfatta. Det har rört naturkatastrofer, främst i form av stormar, skogsbränder och översvämningar. Bland stormarna är Gudrun år 2005, Per år 2007 och Johannes 2025 omfattande, med stora skador på infrastruktur i framför allt södra Sverige. Även skogsbränder har orsakat allvarliga konsekvenser. Västmanlandsbranden 2014 var den största skogsbranden i modern svensk historia, och sommaren 2018 drabbades landet av ett flertal mycket omfattande bränder som tillsammans omfattade omkring 25 000 hektar skog och ledde till evakueringar i flera län. Sverige har också återkommande drabbats av stora översvämningar, bland annat i Värmland, Dalarna och södra Norrland under åren 2000 och 2001, samt i Västra Götaland 2006. Under senare år har betydande översvämningar inträffat bland annat 2021 i östra Götaland och Svealand samt 2024 i delar av Skåne och Östergötland. Därtill förekommer ras och skred, bland andra Stenungsundsskredet och skredet i Åretrakten, Jämtlands län under 2025.

Angivandet i regeln av *visst geografiskt område* som ska omfatta *minst en kommun* avser att begränsa antalet incidenter som behöver identifieras enligt denna regel. Även ordet *naturkatastrof* begränsar antalet incidenter som behöver identifieras enligt denna regel. Det är alltså inte tillräckligt att det rört sig om ett mindre omfattande naturfenomen. Minst en del av en kommun ska ha berörts av störningar eller risker för störningar. Omfattas flera kommuner ska endast en incident identifieras av samma verksamhetsutövare. Kommunerna eller regionerna behöver inte vara geografiska grannar, dock ska det röra sig om samma naturkatastrof.

Det är inte möjligt att bygga en automatiserad process kring rapporteringsregeln. Regeln bygger på kännedom och bedömning av incidenter som *inte* kan utläsas ur verksamhetsutövarens egna IT-system och övervakning. Information når i stället verksamhetsutövaren på skilda sätt, bland annat genom information inom nationella telesamverkansgruppen (NTSG), från kunder eller tillsynsmyndighet, eller kunskap om extremväder genom SMHI:s vädervarningar, regionala eller nationella nödlägen eller sabotage som har utförts gentemot flera telekomverksamhetsutövare.

Det bör röra sig om få incidenter som når upp till tröskeln enligt denna regel mot bakgrund dels av att det inträffar ett begränsat antal naturkatastrofer som påverkar två eller flera telekomverksamhetsutövare. Regeln kommer sannolikt i huvudsak att aktualiseras vid tillgänglighetsstörningar och den innebär att flera verksamhetsutövare ska rapportera om samma externa händelse, det vill säga naturkatastrofen, och hur den har haft negativ påverkan på nät, tjänster och uppgifter hos var och en av verksamhetsutövarna som identifierat att de har drabbats av samma naturkatastrof.

I omvärldsjämförelsen har PTS sett att bland andra Spanien och Irland har infört motsvarande regler.

Samtliga slags verksamhetsutövare bör enligt PTS bedömning kunna beröras.

5.5 Betydande incident som orsakat ekonomisk skada för verksamhetsutövaren (3 kap. 3–5 §§)

Regeln är ny och följer uttryckligen av 2 kap. 5 § cybersäkerhetslagen. Lagen anger inte en beloppsmässig tröskel. Därför behövs en regel på föreskriftsnivå som definierar ett tröskelvärde. Förslaget har sin grund cybersäkerhetslagens definitioner av incident, betydande incident och nätverks- och informationssystem samt i Art. 23.3 a i NIS2-direktivet.

Förslaget motsvaras av regler i Art. 2.1 i genomförandeförordningen och även av 3 kap. 3–5 §§ MCF:s föreskrifter om incidentrapportering m.m. och den information som ska skyddas och trösklar för vad som utgör betydande incidenter. Art. 40.2 e i kodexen angav visserligen att påverkan på ekonomisk verksamhet skulle bedömas för att fastställa hur betydande påverkan en säkerhetsincident hade. Men det fanns inte något i kodexen eller i Enisas vägledning som indikerade att påverkan på ekonomin skulle röra verksamhetsutövarens egen enligt kodexen.

Det som behöver regleras av PTS i föreskrifter är dels hur stor skadan ska vara för att den ska anses utgöra en betydande incident, dels hur beräkningen av skadans storlek ska göras.

Hur stor skadan ska vara anges i 3 § i förslaget. Till skillnad mot MCF har PTS valt att ange ett nominellt belopp, fem miljoner kronor, i stället för att ange en procentsats av verksamhetsutövarens omsättning. Detta för att motverka att regeln blir oskäligt betungande för mindre verksamhetsutövare, vilket också påpekandes av en sådan i de intervjuer som PTS genomförde i anslutning till samrådet.

Sättet att beräkna den ekonomiska skadan anges i 4 § i förslaget, medan det i 5 § anges att skadan ska uppskattas om den inte kan fastställas.

PTS gör bedömningen att omfattningen av de ekonomiska skadorna inte alltid helt kan klargöras inom en kort tid från inträffad händelse. Detta kan i sin tur få till följd att sådana uppgifter måste tillföras bedömningen senare, när de blir kända. Bedömningen av om en incident varit betydande på grund av ekonomisk skada kan därför ta längre tid än bedömningen av vissa andra betydande incidenter.

En incident som orsakat ekonomisk skada ska anses vara betydande när verksamhetsutövaren har tillräckligt med information om kostnaderna för att bedöma att incidenten ger en slutlig ekonomisk skada för tillhandahållare som överstiger de aktuella gränserna i regeln. Det är tillräckligt att en ekonomiskskada enligt regeln kan uppskattas ha uppstått för att incidenten ska anses vara betydande.

Den ekonomiska skadan som ska bedömas är inte knuten till vem som i slutändan ska bära kostnaden. Det vill säga oavsett om det finns ett försäkringsbolag eller en ansvarig underleverantör utgör skadan en betydande incident om den överskrider gränserna i regeln.

Vissa aktörer har i det samråd som genomförts i arbetet med reglerna pekat på svårigheten i att beräkna indirekta kostnader, sådana som inte direkt är en del av den egna verksamheten och som kan falla ut senare. PTS ser att de kostnader som aktören kan se som utmanande eventuellt är beräknande av ”uteblivna intäkter till följd av oplanerade produktionsbortfall”, och ”uteblivna intäkter till följd av minskad konkurrenskraft”. Här vill PTS poängtera att förslaget ger verksamhetsutövaren möjlighet att uppskatta dessa belopp om denne vid tidpunkten för fastställandet inte kan fastställa skadans exakta omfattning.

Samtliga verksamhetsutövare bör enligt PTS bedömning kunna beröras.

5.6 Betydande incident som har påverkat andra fysiska eller juridiska personer

5.6.1 En betydande incident som vållat betydande skada för någon som tillhandahåller en viktig samhällsfunktion (3 kap. 6 § 1 p)

Regeln är inte ny, men har nu preciserats. Bestämmelsen genomför krav som följer av NIS2-direktivet och cybersäkerhetslagen, och förtydligar nu den liknande rapporteringsplikt som tidigare gällde enligt PTS upphävda föreskrift, LEK och kodexen. En liknande regel finns även i MCF:s föreskrifter för de sektorer som MCF reglerar.

Regeln motsvarar 17 kap. 6 § i de upphävda föreskrifterna, med nytt tydligt angivande av trösklar för vad som utgör betydande påverkan och att det är *viktiga* samhällsfunktioner som ska ha påverkats.

Den upphävda regeln hade sin grund i LEK:s upphävda definition av säkerhetsincident och i rapporteringsplikten av säkerhetsincidenter med betydande påverkan, samt i kodexen Art. 40.2 e och tolkades genom Enisas vägledning om vad som borde utgöra kvalitativa trösklar för att bedöma om en samhällsfunktion hade drabbats genom en säkerhetsincident. Vilket enligt Enisas tolkning var *påverkan på kontinuiteten i samhällsviktiga tjänster eller kritiska sektorer/verksamhetsutövare. påverkan under särskilt kritiska dagar, såsom valdagar eller dagar för folkomröstningar, påverkan på samhällsviktiga funktioner (t.ex. departement, statliga myndigheter m.m.)* [32]

Förslaget har sin grund cybersäkerhetslagens definitioner av incident, betydande incident och nätverks- och informationssystem samt i Art. 23.3 a-b i NIS2-direktivet.

Förslaget motsvaras av 3 kap. 6 § 3 p MCF:s föreskrifter om incidentrapportering m.m. och den information som ska skyddas och trösklar för vad som utgör betydande incidenter. Motsvarande regel saknas i genomförandeförordningen.

PTS har som uppdrag att granska cybersäkerhetsarbetet hos telekomoperatörerna och 1 kap. 1 § cybersäkerhetslagen stadgar att syftet med lagen är att uppnå en hög nivå av cybersäkerhet i samhället. De erbjudna näten och tjänsterna inom telekomområdet är ofta helt avgörande för att tillhandahålla flera, om inte alla, viktiga samhällsfunktioner, och telekomområdet har därför en alldeles särskild roll för att skapa en hög nivå av cybersäkerhet i hela samhället. Det finns därmed ett starkt

[32] ENISA Technical Guideline on Incident Reporting under the EECC.pdf s. 21

samhällsintresse av att PTS erhåller information om incidenter inom tillsynsområdet som påverkar dessa viktiga samhällsfunktioner, i enlighet med de krav som följer av NIS2-direktivet och cybersäkerhetslagen.

Den tidigare bestämmelsen i 17 kap. 6 § i de upphävda föreskrifterna stadgade att en säkerhetsincident skulle rapporteras om den haft betydande påverkan på funktioner i samhället, utan krav på att den drabbade funktionen skulle klassificeras som *viktig* samhällsfunktion – det var tillräckligt att den drabbade var en *samhällsfunktion*, och utan tydliga kriterier för när påverkan skulle anses vara tillräckligt betydande. Avsaknaden av tydliga trösklar har i praktiken lett till underrapportering, tillsynsproblem och rättsosäkerhet. PTS och verksamhetsutövarna har löpande behövt hantera frågor om huruvida en specifik händelse ska rapporteras som en säkerhetsincident, om incidenter har haft betydande påverkan på en samhällsfunktion och frågor om hur telekomverksamhetsutövare ska ta till sig information som inte härrör ur övervakning och larm från de egna systemen för att kunna leva upp till regler i de överordnade regelverken. Information om en incident hos telekomverksamhetsutövaren enligt denna regel kan inte enbart härröra från verksamhetsutövarens tekniska information om funktionaliteten i nätet eller tjänsterna. Yttre information är och har varit nödvändig för att kunna identifiera incidenter även enligt de upphävda föreskrifterna.

Verksamhetsutövare har efterlyst tydligare föreskrifter och tydligare vägledning om vad som gäller vid denna typ av påverkan på samhällsfunktioner. Kundkännedom om att kunden tillhandahåller en viktig samhällsfunktion krävs för att kunna identifiera denna typ av betydande incident.

Den föreslagna bestämmelsen kräver att den drabbade funktionen klassificeras som *viktig* i enlighet med MCF:s lista över viktiga samhällsfunktioner. Regeln innehåller alltså en högre tröskel än den tidigare upphävda bestämmelsen, och färre situationer än tidigare bör omfattas genom tillägget *viktig.* De nu detaljerade trösklarna i regeln förväntas leda till ökad förutsebarhet för verksamhetsutövarna i deras bedömning av om en incident ska bedömas vara betydande, minskad tillsyn till följd av färre tolkningsfrågor samt, utgöra ett bättre underlag för tillsyn av cybersäkerhetsarbetet inom telekomområdet.

Den nya bestämmelsen syftar till att åtgärda otydlighet och tolkningsproblemen genom att införa konkreta kriterier för när en incident hos telekomverksamhetsutövaren ska identifieras som betydande till följd av att incidenten har påverkat en organisation eller kund som tillhandahåller en viktig samhällsfunktion i Sverige. Det krävs också att incidenten har pågått minst sex timmar samt att minst ett av de alternativa kriterierna i punkt b i–iv är uppfyllt.

Kravet på att tjänsten används av en kund som tillhandahåller en viktig samhällsfunktion avgränsar mängden betydande incidenter till de fall där incidenten kan ha samhällskritiska konsekvenser. Sextimmarsgränsen enligt regelns punkt a säkerställer att kortvariga störningar inte utgör en betydande incident, vilket begränsar den administrativa bördan för verksamhetsutövarna. PTS har harmoniserat sextimmarsgränsen med MCF:s motsvarande gränsvärde för de sektorer som MCF reglerar, vilket minskar den administrativa bördan för verksamhetsutövare som omfattas av flera regelverk.

De icke-kumulativa alternativa kriterierna enligt regelns punkt b i–iv utgör omständigheter som syftar till att förenkla bedömningen i tydliga situationer och minskar behovet av komplexa proportionalitetsbedömningar. PTS avser även att förtydliga hur de olika gränsvärdena i regeln kan uppskattas av verksamhetsutövare i en kommande vägledning.

PTS avser även att följa upp den faktiska bördan efter att regleringen trätt i kraft och kommer vid behov att se över tröskelvärden om uppföljningen visar att trösklarna inte varit funktionella eller att bördan för verksamhetsutövarna är oproportionerligt stor.

Samtliga verksamhetsutövare berörs av regeln enligt PTS bedömning.

5.6.2 Incidenter som har undergrävt verksamhetsutövarens medverkan till nödkommunikation eller medverkan till förmedling av viktiga meddelanden till allmänheten (3 kap. 6 § 2 och 3 p)

Identifiering av incidenter med negativ påverkan på nödkommunikation och viktiga meddelanden till allmänheten (VMA) är inte nya krav, men kraven på identifiering av sådana betydande incidenter förtydligas nu och bryts ut i två olika regler. Rapporteringsplikten fanns sedan tidigare genom 17 kap. 3 och 6 §§ i de upphävda föreskrifterna.

PTS har kunnat konstatera att rapporteringen enligt de tidigare gällande rapporteringsreglerna om påverkan på nödkommunikation inte fungerade på eftersträvat sätt, ur kodexens perspektiv eller Enisas perspektiv, eller den svenska lagstiftarens perspektiv, och att detta kan ha lett till mörkertal. Underrapportering kan bero på att verksamhetsutövare har lutat sig mot nödroamingfunktionalitet.

I 3 kap. 6 § 2 och 3 p. införs därför två regler om identifiering av betydande incidenter i de fall när telekomverksamhetsutövarens inte kan genomföra sin medverkan till nödkommunikation eller VMA.[33]

[33] PTS har utöver detta även föreskrifter (2022:3) om förmedling av nödsamtal och tillhandahållande av lokaliseringsuppgifter till samhällets alarmeringstjänst, ändrade genom föreskrifterna (2024:1).

De upphävda reglerna i 17 kap. 3 § 7 p och 10 p samt 17 kap. 6 § i de tidigare föreskrifterna hade sin grund i LEK:s upphävda definition av säkerhetsincident och i rapporteringsplikten av säkerhetsincidenter med betydande påverkan, samt i kodexen Art. 40.2 c och d samt 3 stycket Art. 108 och 109.

Artikel 108 i kodexen implementerades genom lagregeln i 8 kap. 1 § om säkerhetsåtgärder, 7 kap. 35 § och 7 kap. 36 § i LEK. 8 kap. 1 § LEK är nu upphävd och flyttad till cybersäkerhetslagen. Art. 40 tolkades genom Enisas vägledning om vad som bör omfattas av påverkan på samhällets funktioner där *påverkan på tillgång till 112 eller nationella nödnummer och påverkan på publika varningssystem* var sådana kvalitativa bedömningströsklar som Enisa angav som lämplig för att avgöra om en incident var en säkerhetsincident med betydande påverkan på nät och tjänster [34]. PTS tillhandahöll också en blankett för rapportering av säkerhetsincidenter. I blanketten fanns vägledning om att en incident som stört 112 eller VMA var en sådan incident som skulle rapporteras enligt 17 kap 6 §.

De två föreslagna reglerna har sin grund i, utöver de tidigare gällande kraven utifrån kodexen och Enisas tolkning, i cybersäkerhetslagens definitioner av incident, betydande incident och nätverks- och informationssystem samt skrivningar i NIS2-direktivets art. 23.3 b och skäl 95.

Av 2 kap. 3 § cybersäkerhetslagen framgår även att verksamhetsutövaren ska vidta säkerhetsåtgärder för att skydda de nätverks- och informationssystem som används i verksamheten eller för att tillhandahålla dess tjänster och systemens fysiska miljö mot incidenter. Verksamhetsutövare inom telekomområdet är enligt ovan skyldiga att medverka till nödkommunikation och utsändning av VMA. De funktioner och system som krävs för att uppfylla dessa skyldigheter utgör därmed en del av den tjänst som ska skyddas enligt 2 kap. 3 § cybersäkerhetslagen. En störning som påverkar 112 eller VMA kan därför indikera brister i verksamhetsutövarens säkerhetsåtgärder, exempelvis riskbedömning, redundans, testning eller kontinuitetshantering eftersom tjänstens funktion inte har upprätthållits i en av dess mest samhällskritiska delar. Tillsynsmyndigheten ska enligt 4 kap. 1 § cybersäkerhetslagen ingripa om en verksamhetsutövare åsidosätter skyldigheterna. För att kunna ingripa behövs en regel, likt de förra incidentrapporteringsreglerna, som kan fånga upp ifall medverkanskraven inte har efterlevts.

Motsvarande regler saknas i genomförandeförordningen och i MCF:s föreskrifter.

[34] ENISA Technical Guideline on Incident Reporting under the EECC.pdf s. 21

Verksamhetsutövare inom telekomområdet hade innan cybersäkerhetslagen trädde i kraft, och har fortfarande, skyldighet att medverka till att förmedla och lämna uppgifter i nödkommunikation samt skyldighet att medverka till att förmedla (VMA) enligt LEK. Reglerna i LEK följer av artikel 108 och 109 i kodexen. Dessa artiklar har inte upphävts genom NIS2-direktivet. Enligt artikel 108 ska medlemsstaterna säkerställa att tillhandahållare av talkommunikationstjänster vidtar alla nödvändiga åtgärder för att säkerställa en oavbruten tillgång till alarmeringstjänster och oavbruten utsändning av varningar till allmänheten. Telekomverksamhetsutövares medverkan till nödkommunikation och VMA är helt nödvändig och utan deras medverkan till förmedling och uppgiftslämnande finns vare sig förutsättningar för nödkommunikation eller VMA till slutanvändares mobiltelefoner. Telekomområdets nödvändighet gör att det behöver finnas regler för att identifiera sådana incidenter specifikt för området. Eftersom varken genomförandeförordningen eller MCF:s motsvarande föreskrifter reglerar telekomområdet saknas motsvarande regler där.

En incident ska identifieras som betydande om den har undergrävt verksamhetsutövarens medverkan till förmedling av nödkommunikation eller vidarebefordran av lokaliseringsuppgifter. En incident ska bedömas vara betydande om den har eller får antas ha hindrat eller försvårat tillhandahållarens medverkan till förmedling eller uppgiftslämnande till nödkommunikation. Hit hör fall där det kunnat konstateras att en hjälpsökandes nödkommunikation inte kunnat förmedlas, men också fall där det utifrån en sammantagen bedömning av antalet berörda slutanvändare, den geografiska ytan, tiden incidenten pågått och andra omständigheter är rimligt att anta att medverkan eller förmedlingen av nödkommunikation i praktiken har försvårats. Regeln träffar de verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller *nummerbaserade* elektroniska kommunikationstjänster enligt 7 kap. 35 § LEK. Regeln omfattar därmed inte NOIK:ar.

En incident ska även identifieras som betydande om den har, eller får antas ha, inneburit att tillgången till, eller riktigheten, autenticiteten eller konfidentialiteten i VMA-meddelanden har undergrävts. Regeln träffar de verksamhetsutövare som tillhandahåller *mobilnummerbaserad* elektronisk kommunikationstjänst.

En händelse där VMA har begärts, men verksamhetsutövarens medverkan eller förmedling av VMA inte har fungerat, och VMA har därför inte kunnat nå ut till de avsedda mottagarna ska anses utgöra en betydande incident. För att efterleva bestämmelsen att rapportera incidenter måste verksamhetsutvecklaren kunna upptäcka dem, åtminstone i efterhand. Verksamhetsutövaren måste alltså säkerställa att denne får tillräcklig kännedom, dels om huruvida utsändning begärts, dels om huruvida verksamhetsutövaren lyckats i sin medverkan till förmedling, för att kunna

efterleva sina skyldigheter. Vid upprepade utsändningar inträder skyldigheten om inte någon av utsändningarna lyckats.

PTS avser att följa upp den faktiska bördan efter att regleringen trätt i kraft och kommer vid behov att se över tröskelvärden om uppföljningen visar att bördan är oproportionerligt stor.

De verksamhetsutövare som berörs är gruppen nummerbaserade interpersonella kommunikationstjänster. Dessa var (2024) 146 st. Inom mobiltelefoni finns 70 företag och inom fast telefoni finns 107 företag, samt 31 företag som är verksamma inom både mobiltelefoni och fast telefoni). Av dessa 146 är 10 stora, 6 medelstora, 34 små och 96 mikroföretag.

5.6.3 En incident som orsakat dödsfall eller betydande skada på en fysisk persons hälsa (3 kap. 6 § 4 p)

Regeln är ny. I Enisas vägledning anges förvisso att en kvalitativ tröskel kunde vara *hög risk för förlust av människoliv*, för sådana säkerhetsincidenter som anses ha skapat betydande påverkan för samhällsfunktioner enligt Art 40.2 e i kodexen.

Incidenter som har påverkat fysiska personer genom att vålla dem betydande skada är uttryckligen betydande enligt 2 kap. 5 § cybersäkerhetslagen.

Förslaget har sin grund cybersäkerhetslagens definitioner av incident, betydande incident samt i Art. 23.3 a-b i NIS2-direktivet. Förslaget motsvaras av regler i Art. 3 c och d i genomförandeförordningen och även av 3 kap. 6 § 3 p b och c i MCF:s föreskrifter om incidentrapportering m.m. och den information som ska skyddas och trösklar för vad som utgör betydande incidenter.

Det saknas i 2 kap. 5 § cybersäkerhetslagen en närmare precisering av vad som är en sådan betydande skada för en fysisk person att en incident ska anses vara betydande. Vad som är en vållad betydande skada genom en telekomincident för en fysisk person behöver således definieras. Den föreslagna regeln är formulerad såsom i kommissionens genomförandeförordning, förutom att PTS har lagt samman de två reglerna i genomförandeförordningen till en enda regeln som omfattar både dödsfall och betydande skada på en fysisk persons hälsa.

Det går att förutse att det är ett mycket litet antal incidenter som kommer att rapporteras enligt denna regel, men trots det behöver den finnas för att förtydliga lagens krav på rapportering av en betydande incident som har påverkat fysiska

personer genom att vålla dem betydande skada. Det finns knappast någon mer betydande skada än ett dödsfall för en fysisk person.

Ett exempel på när en händelse kan utgöra en betydande incident enligt denna regel är att verksamhetsutövaren har vetskap om att elektroniska kommunikationsmöjligheter har upphört helt i ett område och att någon samtidigt har dött inom det området, som inte haft några möjligheter att kommunicera sin nödsituation. Indikationer från media, kunder, slutanvändare eller myndigheter kan leda till att verksamhetsutövaren behöver avgöra om en incident ska rapporteras. Det ska finnas en koppling till störningen i den erbjudna tjänsten och händelsen som lett till dödsfallet/skadan.

PTS har kännedom idag om två incidenter under en gången femårs-period med två olika personer som hamnat i en akut nödsituation och dött samtidigt som det var ett avbrott i deras tillgång till elektroniska kommunikationer. Dessa två personer kunde inte, eller svårligen, nå nödkommunikation i sina respektive situationer. Dessa händelser ser PTS skulle ha behövt rapporteras enligt denna nya regel.

Vid båda dessa incidenter skrev media flera artiklar om händelserna med dödsfallen och avbrottet i möjligheterna till kommunikation. Det finns dock inte någon möjlighet att avgöra huruvida personer som saknat möjligheter att kommunicera sin nödsituation skulle ha överlevt om de hade haft sin vanliga tillgång till elektronisk kommunikation, för att till exempel larma 112.

Samtliga verksamhetsutövare berörs av regeln enligt PTS bedömning.

5.7 Riskbaserad bedömning - En incident eller ett identifierat betydande cyberhot eller betydande sårbarhet som *kan leda till* allvarlig driftstörning, ekonomisk skada för verksamhetsutövaren eller betydande skada för annan

Regelkategorin om incidenter, identifierat betydande cyberhot eller betydande sårbarhet som kan leda till allvarlig driftstörning, ekonomisk skada för verksamhetsutövaren eller betydande skada för annan följer av 2 kap 5 § cybersäkerhetslagen. Det är en fråga om att identifiera dessa händelser som incidenter genom initiala incidentanalyser och att sätta gränsvärden för vad som ska identifieras som betydande incidenter utan att skadeeffekter har inträtt ännu.

I skäl 101 i NIS2-direktivet står följande: *”I detta direktiv fastställs en flerstegsstrategi för rapportering av betydande incidenter för att hitta rätt balans mellan, å ena sidan, snabb rapportering som bidrar till att begränsa den potentiella spridningen av betydande incidenter och gör det möjligt för väsentliga och viktiga entiteter att söka bistånd och, å andra sidan, ingående rapportering som drar värdefulla lärdomar av*

enskilda incidenter och med tiden förbättrar cyberresiliensen hos enskilda entiteter och hela sektorer. I detta avseende bör detta direktiv omfatta rapportering av incidenter som, baserat på en första bedömning som utförts av den berörda entiteten, kan orsaka allvarliga störningar i tjänsterna eller ekonomiska förluster för den berörda entiteten eller påverka andra fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada. En sådan inledande bedömning bör bland annat ta hänsyn till de drabbade nätverks- och informationssystemen, särskilt deras betydelse för tillhandahållandet av entitetens tjänster, allvaret i och de tekniska egenskaperna hos cyberhotet och eventuella underliggande sårbarheter som utnyttjas, samt entitetens erfarenhet av liknande incidenter. Indikatorer såsom i vilken utsträckning tjänstens funktion påverkas, hur länge incidenten pågår eller hur många tjänstemottagare som drabbas kan spela en viktig roll när man fastställer om tjänstens driftsstörning är allvarlig."

PTS har därför skapat tre olika regler i syfte att definiera cybersäkerhetslagens definition av betydande incidenter när en skadeeffekt inte ännu har inträtt och i syfte att respektera NIS2-direktivets skäl 101.

PTS har valt att lyfta fram dessa incidenttyper i en paragraf med underpunkter för att skapa en högre medvetenhet om den tidiga analys som krävs enligt skäl 101 för att identifiera incidenter som ännu inte lett till skada eller påverkan, men som ändå kan utgöra betydande incidenter av olika skäl.

5.7.1 En incident, betydande cyberhot eller betydande sårbarhet som bedöms sannolikt kunna utgöra en betydande incident enligt de föreslagna föreskrifterna (3 kap. 7 § 1 p)

Redan definitionen av säkerhetsincident i nu upphävda delar av 1 kap. 7 § LEK omfattade sådana incidenter som påverkade verksamhetsutövarens säkerhetsförmåga negativt. Det saknades dock uttrycklig föreskrift i PTS nu upphävda föreskrifter för den typen av säkerhetsincidenter, då en skadlig påverkan på verksamhetsutövarens säkerhetsförmåga inte ansågs nå upp till en betydande påverkan på nät och tjänster.

Regeln är att anse som ny enligt PTS bedömning, även om den omfattats av tidigare gällande definition av vad som var en säkerhetsincident enligt LEK.

Förslaget har sin grund cybersäkerhetslagens definitioner av incident, betydande incident och nätverks- och informationssystem samt i Art. 23.3 a-b i NIS2-direktivet.

Samtliga trösklar i genomförandeförordningen omfattar incidenter som ”kan” leda till skadeeffekter, men har i genomförandeförordningen lagts i samma regel där skadeeffekter redan har inträffat och därför kan bedömas.

PTS och MCF har i stället lagt betydande incidenter som ”kan” leda till skada som egna tydligare regler. MCF har en regelstruktur där tre olika bestämmelser för risker för allvarlig driftstörning, ekonomisk skada respektive betydande skada för annan upprepas i 3 kap. 2, 4 och 7 §§. PTS har i stället skapat en regel för dessa tre scenarier.

Kostnader genom denna regel förväntas uppstå för verksamhetsutövare, trots att LEK:s definition omfattade en skadad säkerhetsförmåga och trots att utrymme fanns i PTS tidigare formulär för att rapportera även sådana säkerhetsincidenter som endast hade påverkat verksamhetsutövarens säkerhetsförmåga.

PTS avser att följa upp den faktiska bördan efter att regleringen trätt i kraft och kommer vid behov att se över tröskelvärden om uppföljningen visar att bördan är oproportionerligt stor.

Samtliga verksamhetsutövare berörs av regeln enligt PTS bedömning.

5.7.2 En incident som misstänks ha orsakats av skadlig handling och som sannolikt kan leda till allvarlig driftstörning (3 kap. 7 § 2 p)

Den föreslagna regeln rör incidenter som har orsakats av obehöriga intrång, som ännu inte har lett till en allvarlig driftstörning, men som bedöms kunna leda till en allvarlig driftstörning enligt reglerna i 3 kap. 2 § för allvarliga driftstörningar.

Redan definitionen av säkerhetsincident i nu upphävda delar av 1 kap. 7 § LEK omfattade sådana incidenter som påverkade verksamhetsutövarens säkerhetsförmåga negativt. Det saknades dock uttrycklig rapporteringsskyldighet för den typen av säkerhetsincidenter, då en skadlig påverkan på verksamhetsutövarens säkerhetsförmåga inte ansågs nå upp till en betydande påverkan på nät och tjänster. Regeln är därför att anse som ny enligt PTS bedömning, även om den omfattats av tidigare gällande definition av vad som var en säkerhetsincident.

Förslaget har sin grund cybersäkerhetslagens definitioner av incident, betydande incident och nätverks- och informationssystem samt i Art. 23.3 a-b i NIS2-direktivet.

Regeln finns i motsvarande form i Art. 3.1 e) och Art. 7c-9c. 3 kap. 2 § 1 p genomförandeförordningen. Regeln återfinns även i MCF:s regel i 3 kap. 2 § 1 p.

En incident enligt den föreslagna regeln blir betydande om ett intrång har konstaterats i verksamhetsutövarens nät, tjänster eller uppgifter och verksamhetsutövaren också gör analysen att detta intrång kan leda till en allvarlig driftstörning.

Det är den enda regeln som föreslås som enbart syftar till bedömning av *orsaken* till en incident. En vetenskaplig artikel publicerad Journal of Cyber security redogör bland annat för de ökande cyberhoten och intrången som är grunden för den riskbaserade bedömningen som krävs enligt NIS2-direktivet av vad som är betydande incidenter. [35]

Regeln uttrycker inte något om specifika risker för att företagshemligheter extraheras av någon obehörig. En sådan uttrycklig regel finns i art. 3.1 b genomförandeförordningen. PTS har bedömt att den nu föreslagna regeln är tillräcklig även för risken att företagshemligheter extraheras, och inför därför inte en uttrycklig bestämmelse som täcker läckta företagshemligheter.

Enligt svar i samrådet med branschen i arbetet med de nya reglerna bedöms regeln av de verksamhetsutövarna kunna leda till ett fåtal incidenter varje år.

Samtliga verksamhetsutövare berörs av regeln enligt PTS bedömning.

5.7.3 En incident i kritisk internationell, nationell eller regional infrastruktur (3 kap. 7 § 3 p)

NIS2-direktivet, cybersäkerhetslagen och genomförandeförordningen identifierar incidenter som betydande om de kan leda till betydande störning, innebär allvarlig och konkret risk, påverkar redundans eller säkerhetsnivå även om tjänsten ännu fungerar.

Regeln är ny.

Förslaget har sin grund cybersäkerhetslagens definitioner av incident, betydande incident samt i Art. 23.1 och 23.3 i NIS2-direktivet och skäl 97, samt i skrivningar i propositionen. Motsvarande förslag finns inte i genomförandeförordningen eller i MCF:s föreskrifter.

En ny regel föreslås för att identifiera sådana incidenter som påverkat kritisk infrastruktur negativt som betydande. Det rör sig om incidenter i viss utpekad kritisk

[35] Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive | Journal of Cybersecurity | Oxford Academic

internationell, nationell och regional infrastruktur som medför nedsatt stabilitet, motståndskraft eller förmåga att skydda tillgänglighet, riktighet, autenticitet eller konfidentialitet. Till regeln knyts två definitioner – Kritisk internationell infrastruktur och kritisk nationell eller regional infrastruktur. Det är den enda föreslagna regeln som har som mätpunkt var i nätet en incident har inträffat. Regeln omfattar även incidenter i vissa redundanta lösningar.

I skäl 97 i NIS2-direktivet står det att *”Den inre marknaden är mer beroende av ett fungerande internet än någonsin. Tjänster från nästan alla väsentliga och viktiga entiteter är beroende av tjänster som tillhandahålls via internet. För att säkerställa ett smidigt tillhandahållande av tjänster som levereras av väsentliga och viktiga entiteter är det viktigt att alla tillhandahållare av allmänna elektroniska kommunikationsnät har infört lämpliga riskhanteringsåtgärder för cybersäkerhet och rapporterar betydande incidenter i samband med dessa. Medlemsstaterna bör säkerställa att säkerheten i de allmänna elektroniska kommunikationsnäten upprätthålls och att deras vitala säkerhetsintressen skyddas mot sabotage och spionage. Eftersom internationell konnektivitet förstärker och påskyndar en konkurrenskraftig digitalisering av unionen och dess ekonomi bör incidenter som påverkar undervattenskablar rapporteras.”*

I propositionen till CSL[36] står det att: ”*När det gäller ett ledningsbrott i ett elektroniskt kommunikationsnät kan en incident vara betydande även när den är sådan som typiskt sett medför allvarlig driftsstörning eller avbrott i ett nät eller en tjänst men som inte har gjort det i det enskilda fallet. Huruvida en driftsstörning är att se som allvarlig kan vara beroende av omfattningen av ett kapacitetsbortfall eller hur många aktiva anslutningar eller hur stort område som påverkats av incidenten. Även en störning eller risk för störning som skulle kunna vålla betydande skada i form av påverkan på redundans eller viktiga samhällsfunktioner kvalificerar som en betydande incident.”*

Förbindelser som binder samman Sverige med andra länder såsom sjökablar, markförlagda gränsöverskridande fiberstråk, internationella transportnät och interregionala transportnät utgör centrala beroenden för samhällsviktig kommunikation. De har i NIS2 och i BEREC:s analyser en särskild riskprofil eftersom de kan sakna fullvärdig redundans, de är attraktiva mål för antagonistiska aktörer, de kan orsaka gränsöverskridande störningar, de är beroenden i leveranskedjan som verksamhetsutövaren inte alltid kontrollerar fullt ut.

De ovanstående analyserna och uttalandena i NIS2-direktivet, i propositionen och hos BEREC, och kunskapen om inträffade incidenter i sjökablarna i Östersjön och den ändrade hotbilden mot kommunikationsnät och tjänster, betyder sammantaget att

[36] Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag, sid. 105

föreskrifterna om vad som utgör en betydande incident specifikt för telekomområdet bör ha en regel även för dessa situationer.

En incident som inträffar i kritisk internationell eller kritisk nationell eller regional infrastruktur som *medför försämring av* nätets stabilitet och motståndskraft eller dess förmåga att skydda nät, tjänster eller uppgifters konfidentialitet, riktighet, autenticitet och tillgänglighet – ska bedömas som en betydande incident enligt förslaget.

Skillnaden mellan de två definierade begreppen i föreskrifterna är att den internationella även omfattar redundant infrastruktur och knutpunkter. Detta beror på att de överordnade regelverken och dess syften tydligt pekar på behovet av att fånga upp sådana incidenter som *kan påverka* internationell konnektivitet och sådana som påverkar internationella undervattenskablar, men utan att trafiken har störts. Behovet av regeln grundas även i att regeringen skriver i propositionen att en risk för störning som skulle kunna vålla betydande skada i form av påverkan på redundans eller viktiga samhällsfunktioner kvalificerar som en betydande incident.

Den nya regeln är inte kopplad till hur många slutanvändare som påverkas vid problem, utan i stället att problemen uppstår i dessa centrala delar av näthierarkin utifrån hur olika nätägare har byggt sina nät. Händelsen ska alltså ha inträffat i dessa kritiska förbindelser i näten, för att utgöra en betydande incident enligt de föreslagna föreskrifterna. Utöver det ska skadan bedömas. Rekvisitet skadat i regeln definieras genom att skadan är ett delvis eller helt bortfall som försämrar nätets stabilitet, robusthet, motståndskraft eller resiliens eller dess förmåga att skydda nätets, tjänsternas eller uppgifternas konfidentialitet, riktighet, autenticitet och tillgänglighet. En bedömning behöver göras efter att en verksamhetsutövare har mottagit ett larm om händelsen har försämrat nätets stabilitet, robusthet, motståndskraft eller resiliens eller förmågan att skydda nätets, tjänsternas eller uppgifternas konfidentialitet, riktighet, autenticitet och tillgänglighet.

Exempel: En redundant fiber i en internationell kritisk infrastruktur som kapas men där tjänsten fortsätter fungera – är ett typiskt fall av ”försämrad motståndskraft” som ska rapporteras. Detta innebär att vi kommer att få incidenter rapporterade om exempelvis en sjökabel i Östersjön, eller annan förbindelse som går mellan Sverige och ett annat land bryts eller blir oriktig.

En aktör har svarat i samrådet i arbetet med reglerna att regeln kan komma att leda till identifiering av ett stort antal incidenter som betydande per år, medan en annan aktör sagt att regeln kan innebära några få identifierade betydande incidenter per år.

PTS avser att följa upp den faktiska bördan efter att regleringen trätt i kraft och kommer vid behov att se över tröskelvärden om uppföljningen visar att bördan är oproportionerligt stor.

Endast nätägare berörs eftersom regeln enbart omfattar nät, inte tjänster. Det har inte betydelse för identifieringen av en betydande incident enligt denna regel om några användare eller slutanvändare har upplevt störningar.

5.7.3.1 Om begreppen för kritisk infrastruktur

En kritisk förbindelse är en fysisk eller logisk överföringsväg (till exempel fibersträcka, våglängd, länk, tunnel, virtuell förbindelse eller interconnect) mellan knutpunkter/noder, datacenter, molnresurser eller andra infrastrukturelement, vars bortfall eller störning kan medföra betydande negativ påverkan på tillgänglighet, riktighet, autenticitet eller konfidentialitet för nät eller tjänster på internationell, nationell eller regional nivå. Skador i de kritiska förbindelserna kan orsaka trafikstopp, isolering av noder eller annan betydande påverkan på nätets eller tjänstens tillgänglighet, redundans, riktighet, autenticitet eller konfidentialitet. Den utgör alltså en överföringsväg där störningar får oproportionerligt stor effekt på funktionalitet eller samhällsviktig kommunikation.

En kritisk knutpunkt eller nod är en fysisk eller logisk funktion, plats, punkt eller resurs i infrastrukturen i ett elektroniskt kommunikationsnät eller en tillhörande tjänsteplattform (inklusive datacenter- och molnresurser där fel kan medföra betydande systemisk, negativ påverkan på nätets, tjänstens eller uppgifters tillgänglighet, redundans, autenticitet eller konfidentialitet på internationell, nationell eller regional nivå. Kritiska knutpunkter eller noder omfattar alltså sådana komponenter som utgör centrala beroenden i kedjan för signalering, styrning, routing, autentisering, adresshantering, lagring eller säkerhetsfunktioner, inklusive funktioner som tillhandahålls via moln- eller tredjepartsleverantörer enligt NIS2 och genomförandeförordningen.

Kritisk internationell infrastruktur är enligt förslaget till föreskrifter infrastruktur, förbindelser och knutpunkter inklusive redundant infrastruktur och knutpunkter, som utgör centrala delar av ett allmänt elektroniskt kommunikationsnät och vars funktion har avgörande betydelse för nät och tjänster mellan Sverige och ett annat land.

Kritiska internationella förbindelser kännetecknas av att de utgör centrala kapacitets- eller redundansbärare, knyter samman kritiska knutpunkter/noder eller utgör väsentliga beroenden mot externa leverantörer, moln- och datacenterkopplingar samt leveranskedjeberoenden enligt NIS2.

Kritisk nationell eller regional infrastruktur är enligt förslaget infrastruktur, förbindelser och knutpunkter exklusive redundant infrastruktur och knutpunkter, som utgör centrala delar av ett allmänt elektroniskt kommunikationsnät och vars funktion har avgörande betydelse för nät och tjänster nationellt eller (inter)regionalt i Sverige.

Det krävs således två saker för att infrastrukturen ska omfattas av denna regel. Det är *dels* att infrastrukturen utgör centrala delar av ett allmänt elektroniskt kommunikationsnät, dels att funktionen *har avgörande betydelse* för nät och tjänster antingen internationellt eller nationellt eller regionalt inom landet

5.8 Återkommande incidenter (3 kap. 8 §)

Regeln är ny. Det fanns visserligen visst stöd för en sådan här regel redan genom Art 40.2 d och e i kodexen, men en tolkning av kvalitativa gränsvärden enligt Enisas vägledning om sådana incidenter som upprepar sig saknades.

Förslaget har sin grund cybersäkerhetslagens definitioner av incident, betydande incident och nätverks- och informationssystem samt i Art. 23.3 a-b i NIS2-direktivet.

Regeln finns i motsvarande form i Art. 4 a-c och i skäl 40 i genomförandeförordningen. Regeln återfinns även i MCF:s regel i 3 kap. 6 §

Cybersäkerhetslagen innehåller inte något uttryckligt om att återkommande incidenter bör ses som betydande incidenter. Inte heller nämns den typen av betydande incident i propositionen.

Vissa telekomverksamhetsutövare har redan kravet på sig att identifiera återkommande incidenter för de delar av sin verksamhet som omfattas av genomförandeförordningen, medan andra inte omfattas av kraven i genomförandeförordningen. MCF har också valt att införa motsvarande krav i sina föreskrifter för övriga sektorer som lyder under cybersäkerhetslagen. ENISA kräver in information kvartalsvis från medlemsstaterna om återupprepade incidenter.

Mot bakgrund av att regeln finns både i genomförandeförordningen och i MCF:s föreskrifter om vad som är en betydande incident för övriga sektorer under cybersäkerhetslagen är det enligt PTS uppfattning rimligt med ett motsvarande krav för telekomområdet. PTS ser också erfarenhetsmässigt att det finns ett behov av kunskapen som skapas genom regeln.

Syftet med regeln är att identifiera incidenter som har inträffat upprepat, och är sådana som indikerar att verksamhetsutövaren inte ännu har åtgärdat risken på ett tillräckligt sätt i sitt säkerhetsarbete för att en händelse ska upprepa sig från den första incidenten. Regeln är ett nytt verktyg för att upptäcka om någon verksamhetsutövare inte lever upp till säkerhetsreglerna i cybersäkerhetslagen och

PTS kommande säkerhetsföreskrifter. Identifiering av betydande incidenter enligt regeln kan avslöja sårbarheter och för låg säkerhet om incidenter upprepar sig.

För att en betydande incident enligt denna bestämmelse ska föreligga krävs att alla tre olika faktorer a, b och c är uppfyllda.

Om samma slags incident återkommer ska en (1) betydande incident anses ha uppstått. Den betydande incidenten innehåller därmed olika tidpunkter för de upprepade händelserna.

Det är först vid verksamhetsutövarens kännedom om de faktorer som beskrivs i paragrafen möjlighet att identifiera en upprepad incident uppstår. Bedömningen av om de återkommande incidenterna utgör en betydande incident ska göras när verksamhetsutövaren fått viss kännedom om de faktorer som beskrivs i paragrafen. Faktorerna utgör bedömningar i den berörda verksamhetsutövarens analyser av incidenter.

PTS har i förslaget valt att byta ut begreppet grundorsak till ordet orsak. Grundorsaker är definierade av ENISA och denna typ av orsak ligger på en för övergripande nivå för att kunna definiera vad som är återkommande.[37] Det finns viss översättningsproblematik från engelska till svenska kring begreppen root cause och grundorsak. I stället för grundorsak ska verksamhetsutövare inom telekom bedöma om incidenterna indikerar samma orsak, sårbarhet, bristande säkerhetsåtgärder, rutiner eller redundanta lösning. Anpassningen är gjord för att bättre passa kunskap och säkerhetsarbete inom telekomområdet. Vad gäller kravet om att incidenterna tillsammans sannolikt beror på samma orsak, sårbarhet, bristande säkerhetsåtgärder, rutiner eller inträffar i samma redundanta lösning, kan följande sägas. Det är i första hand verksamhetsutövarens egen analys som ska ligga till grund för bedömningen. Även annan information än verksamhetsutövarens interna data kan vara aktuell att lägga in i bedömningen.

Vad gäller uttrycket ”samma redundanta lösning” omfattar bedömningen ifall olika skador på *samma* redundanta lösning har inträffat inom sex månaders tid. Det behöver inte röra *exakt samma* typ av skada, orsak, sårbarhet eller brister i säkerhetsåtgärder eller rutiner. Det är i stället viktigt för bedömningen om *samma* redundanta lösning, tillgång eller förbindelse *upprepat skadas* på exakt samma ställe, men orsakerna kan vara olika.

Sammantagen skada måste dock alltid uppgå till minst fem miljoner kronor för att incidenten ska anses vara en betydande incident enligt denna regel.

[37] ENISA Technical Guideline on Incident Reporting under the EECC.pdf s.26 (Human errors, system failures natural phenomena, malicious actions, third party failures

Vad gäller c) det vill säga att incidenterna bedömda tillsammans kan leda till en skada eller kostnad på minst fem miljoner kronor kan följande sägas: En tröskel avseende ekonomisk skada/kostnad innebär att verksamhetsutövaren inte behöver identifiera incidenter under tröskeln och därmed kommer små händelser inte att behöva rendera någon bedömning av om incidenten var betydande. Det är inte nödvändigt att den ekonomiska kostnaden för den upprepade incidenten slutligen ska bäras av just den berörda verksamhetsutövaren för att rapporteringsplikt ska inträda. Det relevanta är att verksamhetsutövarens bedömning av att incidenterna tillsammans, uppskattas leda till ekonomiska skador på minst fem miljoner kronor. Om skadan ska bäras exempelvis av en underleverantör eller ett försäkringsbolag har inte relevans. De ekonomiska skadorna eller kostnaderna efter upprepade incidenter ska uppskattas, och behöver inte avgöras slutligen, annars identifieras incidenten för långt efter att de sammanlänkade händelserna har inträffat - eftersom den ekonomiska skadan av upprepade incidenter tar tid att bedöma slutligen.

Angående en återkommande fråga om incidenter med avgrävda/skadade kablar ska anses omfattas av regeln kan följande sägas: om det är på exakt samma plats eller med exakt samma omständigheter som händelsen upprepar sig ska det som hänt identifieras som en upprepad incident. Det krävs alltså då att samma sak sker på samma plats och av liknande orsak, inom sex månader och att det kostar mer än fem miljoner kronor att laga detta. Det kan till exempel finnas kabeldragningar på utsatta platser, som upprepat behöver lagas på samma ställe, men av olika skäl. Eller samma slags angrepp på samma ställe som upprepas. Incidenter vid sådana platser kvalificerar som upprepade incidenter.

PTS avser att utveckla mer kring begrepp och vad som ska vara gemensamt för incidenterna i en vägledning.

Av de som har svarat så har endast en uppgett att regeln kommer leda till några nya incidenter.

Samtliga verksamhetsutövare berörs av regeln enligt PTS bedömning.

6. Analys av förslaget

6.1 Beskrivning och beräkning av förslagets eller beslutets kostnader och intäkter för staten, kommuner, regioner, företag och andra enskilda

6.1.1 Allmänt om kostnader för cybersäkerhet

Regeringen konstaterar i propositionen att ”Det är många faktorer som påverkar kostnaderna för exempelvis incidenthantering, som ingår i lagens krav på säkerhetsåtgärder, såsom störningens art och omfattning, dess konsekvenser för kontinuiteten samt hur snabbt verksamhetsutövaren återhämtar sig från incidenten. En betydande incident kan orsaka både direkta utrednings- och reparationskostnader och indirekta kostnader på grund av exempelvis avbrott i verksamheten eller ett skadat anseende.”

Kostnadsanalysen i propositionen är generell och innehåller inga kostnadsberäkningar. Regeringen konstaterar bland annat att det inte går att presentera en mer exakt och för samtliga företag relevant uppskattning av kostnaderna kopplade till införandet av den nya lagen, men att flera av förslagen inte heller bör innebära några beaktansvärda kostnader. Förslagen kan dock innebära ökade kostnader och kommer att innebära administrativa bördor för enskilda verksamhetsutövare. Det kan konstateras att förslagen i allt väsentligt är nödvändiga för att genomföra NIS 2-direktivet i Sverige.

Detta innebär att PTS saknar kännedom om vad kostnaderna är för nollalternativet, det vill säga att inte meddela några föreskrifter. I propositionen anges att EU-kommissionen uppskattat att utgifterna för de företag som omfattas av NIS2-regelverket kommer att öka med 22 procent under de första åren efter införandet av de nya reglerna. För företag som omfattas av NIS-direktivet uppskattas utgifterna öka med 12 procent. Verksamhetsutövare inom telekomområdet har inte i egenskap av telekomverksamhetsutövare omfattats av NIS-direktivet, men väl av kodexen med snarlika regler. PTS bedömer av den anledningen att utgiftsökningen snarare blir i paritet med den som gäller för företag som sedan tidigare omfattats av NIS-direktivet. Samtidigt understryker kommissionen att det också kan bli fråga om besparingar för berörda företag med hänvisning till att kostnaderna för att hantera cybersäkerhetsincidenter kommer att minska. Detta avser de totala kostnaderna för samtliga åtgärder enligt direktivet.

Regeringen anger vidare i propositionen att det i propositionen som avser genomförandet av NIS2-direktivet i Finland anges att kostnaderna för hanteringen av cybersäkerhetsrisker för ett företag som omfattas av tillämpningsområdet för den

finländska cybersäkerhetslagen uppskattas uppgå till ca 0,2–0,8 procent av den årliga omsättningen med den miniminivå som den finska lagen kräver, om man jämför med en nivå där företaget inte tidigare vidtagit några åtgärder för att hantera sådana risker. Det betonades att bedömningarna är förenade med betydande osäkerhet när det gäller skillnaderna mellan olika företag. Den finska utredningen anger enligt regeringen dessutom att verksamhetsutövarens arbete med att rapportera det som har identifierats som betydande incidenter endast kommer att medföra smärre kostnader för aktörerna.

De kostnadsmässiga och andra konsekvenser som följer av denna reglering bör bedömas utifrån ett helhetsperspektiv tillsammans med de krav som följer av cybersäkerhetslagen, PTS föreskrifter om säkerhetsåtgärder som utfärdas i enlighet med cybersäkerhetsförordningen och MCF:s föreskrifter om rapportering av betydande incidenter. Bedömningen av vad som utgör en betydande incident är en länk mellan verksamhetsutövarnas säkerhetsarbete enligt PTS föreskrifter och skyldigheten att rapportera betydande incidenter enligt MCF:s föreskrifter. De kostnader som uppstår specifikt för tröskelföreskrifterna är hänförliga till bedömningen av vad som utgör en betydande incident.

Tillsammans med PTS kommande föreskrifter om säkerhetsåtgärder kommer samhället på sikt att minska sin risk för att drabbas av incidenter och därmed kunna erbjuda mer stabila leveranser samt höja sin konkurrenskraft.

För de verksamhetsutövare som inte redan bedriver ett systematiskt och riskbaserat arbete idag kan krav i föreskrifterna om vad som utgör en betydande incident initialt ge ökade kostnader. Detta är dock inte en kostnad som följer av de föreslagna föreskrifterna eftersom kraven följer redan av cybersäkerhetslagen och tidigare av LEK. De flesta verksamhetsutövare bedöms därför redan idag arbeta med cybersäkerhet och har interna regler, arbetssätt och system för att upptäcka och hantera incidenter i sina nätverk och informationssystem. Därtill är det idag en självklarhet att en verksamhetsutövare har kostnader för att skydda sina nätverk och informationssystem. I denna kostnad ingår utgifter för system och annat tekniskt stöd för att bedriva verksamheten samt personalkostnader för att upprätthålla en säker informationsbehandling.

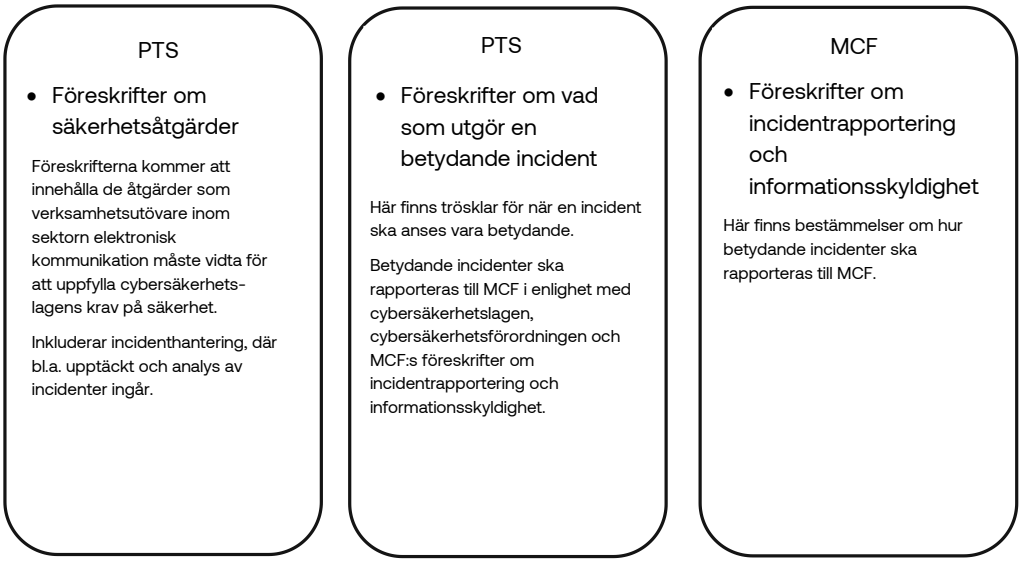
Med den snabba utveckling som sker på AI-området kan det förväntas att användningen av AI inom en snar framtid kommer att innebära stora kostnadsbesparingar vad gäller arbetet med att bedöma om en incident är betydande. Verksamhetsutövare kommer sannolikt att snabbt och till en låg kostnad med hjälp av AI hämta nödvändig information från sin incidenthantering och stämma av denna mot kriterierna för vad som utgör en betydande incident.

MCF har i sin konsekvensutredning för föreskrifter om rapportering och vad som utgör en betydande incident för alla sektorer utom de som faller under PTS tillsynsansvar funnit att tidsåtgången för efterlevnaden av myndighetens föreskrifter om incidentrapportering och informationsskyldighet uppskattas inte överstiga sammanlagt en halv dag per rapporterad betydande incident. MCF anger att förutsättningen är att nödvändiga vägledningar och systemstöd finns att tillgå samt att interna regler och arbetssätt har etablerats i enlighet med MCF:s föreskrifter om säkerhetsåtgärder och utbildning.

Det är vidare värt att återigen påpeka att regler för identifieringen av vad som är en betydande incident, såväl som rapportering av sådana, följer direkt av cybersäkerhetslagen. Kostnader för rutiner, system och processer uppstår således även helt utan föreskrifter för att kunna möta lagens krav. Det är därmed inte kostnader som tillkommer med anledning av det nu remitterade förslaget till föreskrifter.

I skärningspunkten mellan föreskrifter om säkerhetsåtgärder och vad som utgör en betydande incident, som meddelas av PTS, samt rapportering av betydande incidenter, som meddelas av MCF uppstår kostnader för verksamhetsutövare inom telekomområdet. Kostnader vad avser säkerhetsåtgärder för att identifiera och analysera incidenter, kostnader för att specifikt bedöma om en incident utgör en betydande incident enligt dessa föreskrifter och också kostnader för själva rapporteringen enligt MCF:s föreskrifter därom. Kostnadsbiten för att identifiera om incidenten är betydande är enligt PTS bedömning en liten del av den totala kostnaden för cybersäkerhet och incidenthantering.

Delat föreskriftsansvar enligt cybersäkerhetslagen mellan PTS och MCF för sektorn elektronisk kommunikation



Figur 1 beskriver de tre sammanflätade föreskriftsansvaren

6.1.2 Verksamhetsutövare som berörs av de föreslagna reglerna

Som angetts ovan är det tillhandahållare av allmänna elektroniska kommunikationsnät och allmänt tillgängliga kommunikationstjänster som omfattas av de föreslagna föreskrifterna. Dessa utgörs dels av de företag som är anmäla till PTS enligt LEK idag, dels de NOIK:ar som tidigare inte omfattats av anmälningsplikten, men som nu gör det enligt CSL. Eftersom den anmälningstjänst som MCF svarar för där verksamhetsutövare ska anmäla sig enligt cybersäkerhetslagen i uppstartsfasen under våren 2026 har haft problem med tillgängligheten till tjänsten, saknar PTS dock idag exakt kännedom om anmälda.

PTS fann vid en genomgång gjord i oktober 2025 att antalet anmälda aktörer enligt LEK vid tidpunkten var 651 st, rensat för bolag som baserat på omsättning och antal anställda bedömdes inte bedriva någon verksamhet. PTS saknar exakt kunskap om hur många NOIK:ar som kommer omfattas av reglerna, men bedömer att det totalt bör röra sig om under 700 verksamhetsutövare som kommer att omfattas av de föreslagna föreskrifterna.

Samtliga dessa ovan nämnda verksamhetsutövare har omfattats av skyldigheten att rapportera säkerhetsincidenter enligt de tidigare gällande reglerna i LEK och de nu upphävda föreskrifterna.

PTS har för sina interna analysändamål delat in företagen efter vilken typ av verksamhet företagen har. Dessa är nätägare, tjänsteleverantörer, hybrid (både nät och tjänst) samt övrig/oklar enligt nedan

Nätägare

Aktören äger och driver fysisk infrastruktur (fiber, våglängder, svartfiber, accessnät). Typexempel; Lokala stadsnät, nätbolag, kommunala nätägare.

Antal nätägare uppdelat på bolagsstorlek

Nätägare				
Mikro		Små	Medel	Stora
Mikro enmansföretag med mindre än 2 miljoner SEK i intäkter	Mikro övriga			
25	74	42	17	2

Tjänstetillhandahållare

Aktören tillhandahåller elektroniska kommunikationstjänster till slutkund, men äger normalt inte nätet. Typexempel; ISP:er, mobiloperatörer, tjänsteplattformar.

Antal tjänsteleverantörer uppdelat på bolagsstorlek

Tjänsteleverantör				
Mikro		Små	Medel	Stora
Mikro enmansföretag med mindre än 2 miljoner SEK i intäkter	Mikro övriga			
59	78	46	22	3

Hybrider

Aktören är både nätägare och tjänsteleverantör – äger nät och säljer tjänster via det. Typexempel; Större leverantörer av mobiltelefoni och bredband, större regionala bolag.

Antal hybrid uppdelat på bolagsstorlek

Hybrid				
Mikro		Små	Medel	Stora
Mikro enmansföretag med mindre än 2 miljoner SEK i intäkter	Mikro övriga			
6	34	22	12	8

Övriga/oklara

Aktören har otydlig eller blandad profil, t.ex. endast datakommunikationstjänster eller samtrafik utan slutkundstjänster. Typexempel; Tekniska grossister, mellanoperatörer, specialnät.

Antal övriga/oklara uppdelat på bolagsstorlek

Övrig/oklar				
Mikro		Små	Medel	Stora
Mikro enmansföretag med mindre än 2 miljoner SEK i intäkter	Mikro övriga			
119	40	31	7	4

6.1.3 Vidtagna åtgärder i syfte att beräkna kostnaderna

PTS har genomfört ett samråd med ett tiotal utvalda verksamhetsutövare och branschorganisationer, där synpunkter har lämnats på regelförslaget. Med samrådet bifogades en frågeenkät med frågor avseende de förslag som skiljer sig från vad som gällde enligt de nu upphävda föreskrifterna. I frågorna gavs de svarande möjlighet att ange vilka kostnader som de föreslagna föreskrifterna skulle medföra, dels i kronor, dels i timmar, initialt och årligen. Tyvärr var svarsfrekvensen mycket låg,

endast ett fåtal aktörer svarade på enkäten och de inrapporterade kostnaderna skiljer sig avsevärt åt mellan svaren, vilket gör det svårbedömt såväl att avgöra rimligheten i de olika kostnadsuppgifterna som att med antaganden beräkna ett faktiskt representativt genomsnittsvärde

Eftersom svaren var få och varierande valde PTS att gå ut med enkäten, justerad efter synpunkter på förslagen i samrådet, till en bredare krets om ca 150 verksamhetsutövare. Urvalet på 150 verksamhetsutövare gjordes baserat på PTS tidigare erfarenheter av liknande undersökningar i syfte att representera de olika typföretag som beskrivits ovan. Sett till myndighetens tidigare erfarenheter bedömdes att urvalet skulle medföra en tillräckligt hög svarsfrekvens för att innebära tillförlitligt underlag för kostnadsbedömningar. PTS genomförde efter det andra utskicket av kostnadsfrågor även några intervjuer med ett fåtal mindre verksamhetsutövare i syfte att försöka komplettera svaren.

Dessvärre var svarsfrekvensen mycket låg även på det andra utskicket av enkät. Endast ett fåtal svar har inkommit och endast från större verksamhetsutövare. Av de inkomna svaren kan PTS som angetts ovan konstatera att uppskattningarna skiljer sig avsevärt åt. Vissa uppskattningar förefaller enligt PTS bedömningar vara väl tilltagna. En del svar har varit så anmärkningsvärt höga att de enligt PTS bedömning framstår som orealistiska. Alternativt kan det förhålla sig så att de verksamhetsutövare som uppskattat kostnader i det högre intervallet inte sedan tidigare vidtar de säkerhets- och incidenthanteringsåtgärder som de varit ålagda redan enligt LEK och de nu upphävda föreskrifterna. Det har även vid PTS analys av vissa av svaren blivit tydligt för PTS att den svarande har svårt att bryta ut kostnader hänförliga till de tre olika föreskrifter som beskrivits ovan under avsnitt 6.1.1 och bilden där. Det vill säga kostnader för utveckling av system och larm för identifiering av incidenter och nya kostnader för nya rapporteringsregler i cybersäkerhetslagen har tagits upp som en kostnad föranledd av förslaget om föreskrifter om vad som utgör en betydande incident. Som angetts ovan innebär cybersäkerhetslagens definition av begreppet betydande incident sådan nödvändig identifiering av incidenter som inte kan genomföras enbart genom övervakning eller automatiserade system. Det är därför inte möjligt för verksamhetsutövare att endast bygga upp sin process för bedömning av betydande incidenter kring övervakning och larm i systemen. Det är även uppenbart att de nya rapporteringskraven i cybersäkerhetslagen, med nya tidsramar och en ny kontaktpunkt, MCF, samt MCF:s ytterligare föreskrifter kring rapporteringsplikten, även är kostnadsdrivande.

PTS har med ledning av data från enkäter och intervjuer försökt att med egna antaganden göra beräkningar för respektive föreslagen regel. Dock medförde den stora osäkerhet som beskrivits ovan att beräkningarna behäftades med så stor osäkerhet att de bedömdes sakna tillförlitlighet.

Som referens kan i sammanhanget nämnas att PTS i konsekvensutredningen av de nu upphävda föreskrifterna fann att dessa skulle medföra totala kostnader för de då 513 företagen till ca 51 miljoner kronor i engångskostnader och ca 90 miljoner kronor i årliga kostnader. Dessa kostnader avsåg alltså samtliga åtgärder enligt de upphävda föreskrifterna innefattande bland annat säkerhetsåtgärder, redundans, bedömning av rapporteringsplikt och själva rapporteringen.

6.1.4 Kostnader för berörda företag av de föreslagna incidentrapporteringsåtgärderna

Regeringen bedömer i propositionen att när det gäller skyldigheten att rapportera betydande incidenter så bör kostnaderna hänförliga till denna skyldighet bli begränsade. Regeringens bedömning delas av PTS utifrån det som beskrivs nedan.

6.1.4.1 Engångskostnader vid införandet

De nya föreskrifterna kommer att kräva att verksamhetsutövarna anpassar sina interna processer och rutiner samt utbildning av personal. Detta är en engångskostnad som uppstår i samband med att föreskrifterna träder i kraft. Anpassningsbehovet varierar beroende på verksamhetsutövarens storlek, befintliga processer och mognadsgrad i cybersäkerhetsfrågor.

För stora operatörer med etablerade processer för incidenthantering är förhoppningen att anpassningskostnaderna ska vara begränsade, eftersom dessa aktörer typiskt sett redan har system och rutiner på plats som kan anpassas till de nya kriterierna. Den huvudsakliga kostnaden för dessa aktörer avser uppdatering av befintliga processer och utbildning av berörd personal. För mindre aktörer kan anpassningskostnaderna vara proportionerligt sett större.

6.1.4.2 Löpande kostnader

De löpande kostnaderna för verksamhetsutövarna består huvudsakligen av den tid och de resurser som krävs för att bedöma om en incident är betydande enligt kriterierna i de föreslagna föreskrifterna. Det kan också vara aktuellt med exempelvis årligt återkommande utbildning. Kostnaden per tillfälle för incidenter avseende störningar i tillgängligheten i 3 kap. 2 § i förslaget bedöms vara jämförbar med kostnaden för att rapportera en tillgänglighetsincident enligt tidigare föreskrifter. I de fall det rör sig om rapportering enligt regler som motsvarar de som gällde enligt de nu upphävda föreskrifterna rör det sig heller inte om några nya, tillkommande kostnader.

Kostnader för bedömning av genuint nya incidenttyper – ekonomisk skada, potentiell påverkan, skada för andra och upprepade incidenter – bedöms vara högre per rapporteringstillfälle, eftersom bedömningen av dessa kräver mer komplex analys och dokumentation, som inte kan komma från ren systemövervakning och larm.

Något som även bekräftas av de enkätsvar och svar i samrådet som inkommit till myndigheten. PTS estimerar att bedömningen av om en sådan incident är *betydande eller inte* kommer att ta i genomsnitt en halv arbetsdag i anspråk. Några incidenter är av enklare karaktär och kommer därför att ta kortare tid i anspråk, medan några är mer komplexa och kräver bedömningar utifrån flera parametrar och informationsbedömningar. De senare kan komma att ta något längre tid i anspråk.

Estimatet om en halv dag har PTS först formulerat och sedan stämt av genom konsultationer med cybersäkerhetsexperter och tekniker med erfarenhet hos verksamhetsutövare inom telekomområdet. Estimatet är efter detta kontrollerat mot, och visade sig motsvara, vad MCF kommit fram till är en rimlig tidsåtgång för efterlevnaden av myndighetens föreskrifter om incidentrapportering och informationsskyldighet. I MCF:s uppskattade tidsåtgång inkluderas även tiden för själva rapporteringsförfarandet och informationslämnande till mottagare. PTS estimat är därmed till och med något högre än vad MCF estimerat tidsåtgången till vad gäller själva bedömningen av om en incident är betydande. Detta beror på att verksamheten inom telekomområdet i detta avseende bedöms vara något mer komplex på grund av sin bärande roll för all slags elektronisk kommunikation och därmed bärande för de flesta, om inte alla, sektorers verksamhet inom NIS-området, och också på att telekomområdet är en nytt NIS-område, till skillnad från andra sektorer som MCF har estimerat tidsåtgången för.

Utifrån uppskattningen att bedömningen av om en incident är betydande kommer att ta i genomsnitt en halv dag kan kostnaden per incident beräknas till drygt 2 500 kronor. För att beräkna kostnaden har PTS utgått från lönen på 55 500 kronor i månaden för en IT-säkerhetsspecialist 2024[38] och en normal arbetstid på 160 timmar/månad. Eftersom lönekostnaden för en arbetsgivare består av mer än lönen så har vi räknat upp lönen med Tillväxtverkets faktor 1,84 som fångar OH-kostnader, arbetsgivaravgifter och semesterersättning[39]. Som angetts ovan kan de mest komplexa incidenterna komma att kräva ett team av olika kompetenser. PTS anser dock att den stora merparten av arbetet kommer att kunna utföras av IT-säkerhetsspecialister, varför det enligt myndighetens bedömning blir rättvisande att utgå från dessas löneförhållanden.

Det är viktigt att komma ihåg att beräkningarna är grova uppskattningar som baseras på bristfälliga data. I de enkäter som skickades ut ombads även de svarande att uppskatta hur många incidenter per år som skulle bedömas som betydande enligt förslaget till föreskrifter. Även här varierade svaren i så stor utsträckning att det inte varit möjligt för PTS att uppskatta detta. Vissa svarande angav att en föreslagen regel

[38] SCB

[39] Ekonomiska effekter av nya regler – så beräknar du företagens kostnader

skulle leda till noll nya incidenter, medan en annan kunde uppskatta antalet till stora volymer. Förslaget bör dock enligt PTS bedömningar leda till att fler incidenter än vad som tidigare bedömts som rapporteringspliktiga säkerhetsincidenter enligt LEK nu ska bedömas som betydande incidenter enligt cybersäkerhetslagen. Detta faller sig naturligt genom definitionerna och skälen i NIS2-direktivet och genom reglerna i cybersäkerhetslagen. En av de svarande i det tidiga samrådet har också sedan i början av april 2026 använt sig av de förslagna föreskrifterna för att identifiera betydande incidenter, något som under ca en månad medfört att *en* incident har identifierats av den verksamhetsutövaren som en betydande incident. Det är inte möjligt att uttala hur många fler incidenter som kommer att identifieras som betydande genom de föreslagna föreskrifterna. PTS har möjlighet att utvärdera om det finns behov av höjda eller ändrade trösklar om någon regel visar sig leda till stora volymer av incidenter som det inte finns behov av att staten hanterar. Detta är noga övervägt redan nu, men det innebär i sig inte några hinder för en kommande utvärdering.

6.1.4.3 Differentierad analys: stora och små aktörer

För mindre aktörer kan de nya föreskrifterna medföra en proportionerligt sett större administrativ börda i vissa fall. PTS har försökt att beakta detta i utformningen av föreskrifterna genom att säkerställa att kriterierna är tydliga och konkreta, vilket minimerar behovet av komplexa bedömningar och minskar risken för osäkerhet och feltolkning. Som angetts ovan har detta även särskilt beaktats vid valet av en beloppsmässig gräns för ekonomisk skada. Tydliga och konkreta kriterier är i detta avseende inte enbart ett krav på god normgivning, utan också ett aktivt verktyg för att begränsa den regulatoriska bördan för mindre aktörer.

6.1.4.4 Offentligfinansiella effekter

På grund av att bolagen kommer får ökade kostnader till följd av de nya reglerna så kommer också deras vinster att minska. Eftersom arbetstimmarna ökar så kommer statens intäkter från arbetsgivaravgifterna att öka, vilket också innebär att avgifterna till ålderspensionssystemet påverkas positivt. Även intäkterna från statlig inkomstskatt och kommunala skatteintäkter påverkas positivt. Om de har varit arbetslösa och haft a-kassa blir effekten större jämfört med om de har arbetat. Eftersom förslaget bedöms leda till begränsade kostnader för företagen bedöms dock de offentligfinansiella effekterna som små.

6.1.4.5 Kostnader och intäkter för staten – PTS

De nya föreskrifterna medför även kostnader för PTS som tillsynsmyndighet. Dessa avser framför allt resurser för att hantera den förväntade ökningen av inkomna incidentrapporter samt utbildning och vägledning till verksamhetsutövarna i samband med att föreskrifterna träder i kraft. Som angetts ovan uppskattas dock ökningen av inkomna rapporter vara begränsad. Effekterna på PTS kostnader bedöms därför vara försumbar.

Mot dessa kostnader ska ställas de betydande nyttor som de nya föreskrifterna förväntas ge PTS i form av en mer fullständig och tillförlitlig lägesbild över cybersäkerhetssituationen i sektorn, förbättrade förutsättningar för en effektiv och rättssäker tillsyn samt minskade resurser för tolkningsförfrågningar från verksamhetsutövarna på sikt. En mer heltäckande rapportering förbättrar även PTS förmåga att identifiera mönster, trender och systemrisker, vilket stärker myndighetens möjligheter att förebygga och hantera allvarliga incidenter.

6.2 Beskrivning och beräkning av andra relevanta konsekvenser

De nya föreskrifterna förväntas stärka cybersäkerheten inom telekomområdet genom en mer heltäckande och konsekvent incidentrapportering. En fullständigare lägesbild ger PTS och andra berörda myndigheter bättre förutsättningar att identifiera och hantera systemrisker och hotbilder, vilket i förlängningen stärker samhällets motståndskraft mot cyberattacker och andra säkerhetsincidenter. Detta är en konsekvens av särskild betydelse mot bakgrund av telekomområdets centrala roll för samhällets funktioner och för totalförsvaret.

För verksamhetsutövarna innebär de nya föreskrifterna ökad rättssäkerhet och förutsägbarhet. Tydliga och konkreta kriterier minskar risken för att aktörer oavsiktligt underlåter att rapportera rapporteringspliktiga incidenter, vilket i sin tur minskar risken för tillsynsåtgärder och sanktioner. Detta är en positiv konsekvens som delvis kompenserar för de ökade administrativa kostnaderna.

De nya föreskrifterna kan även ha positiva konsekvenser för konkurrensförhållandena inom telekomområdet, i den mån de säkerställer att samtliga aktörer – oavsett storlek – tillämpar samma rapporteringskriterier. En inkonsekvent tillämpning av rapporteringsskyldigheten, där vissa aktörer rapporterar mer än andra, kan snedvrida konkurrensen och skapa ojämlika förutsättningar. Tydliga och enhetliga kriterier motverkar detta.

6.2.1 Påverkan på konkurrens och konkurrenskraft

Förslagen är utformade för att vara teknikneutrala och så tydliga som möjligt för att inte betunga små företag onödigt mycket. Det blir tyvärr ändå emellanåt som vissa företagstyper och storlekar drabbas förhållandevis mer av vissa incidentrapporteringskrav.

Den grupp företag som är hybrider kommer att möta samtliga nya eller modifierade/förtydligade krav, men de flesta kraven kommer träffa samtliga företag varför PTS bedömer att de olika typgrupperna inte kommer drabbas orimligt olika.

Vissa enmansföretag som PTS talat med har exempelvis inte utryckt någon oro med hänvisning till att de är så kallade MVNO (en virtuell mobiloperatör som saknar eget nät) hos en stor operatör, som bistår med mycket kopplat till incidenter. Andra mikroföretag har dock oroat sig över otydligheter gällande tolkningar av föreskrifterna. PTS har som angetts sökt motverka detta genom tydliga föreskrifter och avser att ytterligare underlätta detta med hjälp av en kommande vägledning.

Ett proaktivt incidentarbete är liksom ett proaktivt säkerhetsarbete nödvändigt för telekomområdet och samhället i stort, vilket kostnader måste vägas mot.

6.2.2 Samhällsekonomiska nyttor

Utöver de direkta kostnaderna och intäkterna för enskilda aktörer och myndigheter medför de nya föreskrifterna samhällsekonomiska nyttor som bör beaktas i den samlade bedömningen. En mer heltäckande incidentrapportering, vari PTS föreskrifter om vad som utgör en betydande incident ingår, stärker den nationella cybersäkerheten genom att möjliggöra tidigare upptäckt och hantering av allvarliga incidenter, minska risken för att incidenter eskalerar och får bredare samhällspåverkan, samt förbättrar förutsättningarna för samordning mellan PTS, MCF och andra myndigheter med cybersäkerhetsansvar. Dessa nyttor är svåra att kvantifiera i monetära termer, men är reella och betydande. Kostnaden för en allvarlig cyberincident som inte rapporteras i tid och därför eskalerar kan vara mångfalt större än de administrativa kostnader som de nya föreskrifterna medför för verksamhetsutövarna.

6.2.3 Sammanfattande bedömning av kostnader och nyttor

De nya föreskrifterna medför kostnader för verksamhetsutövarna i form av engångskostnader för anpassning samt löpande (årliga) kostnader för bedömning av betydande incidenter. Den stora merparten av kostnader kommer emellertid direkt från rapporteringsskyldigheten som följer av cybersäkerhetslagen och den definition av betydande incident som framgår av lagen. En del av kostnaderna avser även fullgörandet av skyldigheter som redan existerade enligt LEK men som i praktiken

förefaller inte ha fullgjorts. PTS har i utformningen av föreskrifterna strävat efter att minimera den regulatoriska bördan genom att utforma tydliga och konkreta kriterier som underlättar bedömningen för verksamhetsutövarna, och genom att ligga i linje med genomförandeförordningen och MCF:s föreskrifter för att undvika onödig fragmentering av regelverket. Mot kostnaderna ska ställas de betydande nyttor som föreskrifterna förväntas ge i form av stärkt cybersäkerhet, förbättrad tillsyn och ökad rättssäkerhet för verksamhetsutövarna. Den samlade bedömningen är att nyttorna av de föreslagna föreskrifterna klart överstiger kostnaderna.

6.3 Redogörelse för vilka åtgärder som har vidtagits för att förslaget eller beslutet inte ska medföra mer långtgående kostnader eller begränsningar än vad som bedöms vara nödvändigt för att uppnå dess syfte

Ett tidigt samråd har genomförts och kostnadsfrågor skickats ut. Möten med de aktörer som anmält intresse för samrådsmöten och diskussioner har genomförts. Förslaget till föreskrifter har efter synpunkter och dialog i det tidiga samrådet justerats. Dialogen har med intresserade verksamhetsutövare fortsatt fram till färdigställandet av förslaget och konsekvensutredning

PTS har som angetts ovan även skickat ut kostnadsenkäten till ett större urval samt genomför kompletterande intervjuer med ett antal verksamhetsutövare. Även efter detta har förslaget till föreskrifter justerats i syfte att inte vara mer långtgående än nödvändigt. Bland annat har justeringar gjorts för att inte reglerna ska drabba små företag på ett oproportionerligt hårt sätt och för att uppnå regelförenkling.

Vid en europeisk omvärldsjämförelse har PTS kunnat konstatera att trösklarna avseende påverkan på tillgänglighet som förut fanns i 17 kap. 5 § i de nu upphävda föreskrifterna ligger betydligt högre än motsvarande regler i bland annat Finland, Danmark och Spanien. De tidigare gällande reglerna om bristande tillgänglighet förts över i stort sett oförändrade till det nu aktuella förslaget Trots att en harmonisering hade varit förenlig med NIS2-direktivets syfte har PTS för närvarande beslutat att inte sänka trösklarna avseende påverkan på tillgänglighet för att förslaget inte ska medföra för långtgående kostnader för verksamhetsutövarna.

6.3.1 Utgångspunkter för proportionalitetsbedömningen

Proportionalitetsbedömningen tar sin utgångspunkt i det syfte som de föreslagna föreskrifterna ska uppfylla, nämligen att precisera begreppet *betydande incident* för telekomområdet på ett sätt som ger verksamhetsutövarna konkret vägledning, säkerställer en konsekvent rapportering mellan aktörer och ger PTS de verktyg som krävs för en effektiv tillsyn. Bedömningen görs i förhållande till nollalternativet, det vill

säga en situation där verksamhetsutövarna enbart har cybersäkerhetslagens generella definition att förhålla sig till.

En central utgångspunkt är att åtgärder som vidtas av det offentliga ska vara samhällsekonomiskt motiverade, proportionerliga och kostnadseffektiva. Det innebär att föreskrifterna ska utformas så att de inte medför mer långtgående kostnader och begränsningar för berörda aktörer än vad som är nödvändigt för att uppnå syftet. Proportionalitetsbedömningen fokuserar särskilt på de delar av föreskrifterna som innebär genuint nya krav, nämligen rapportering av ekonomisk skada, potentiell påverkan och skada för andra, eftersom dessa utgör reella utvidgningar av rapporteringsskyldigheten jämfört med vad som gällde enligt LEK.

6.3.2 Är föreskrifterna nödvändiga för att uppnå syftet?

Frågan om föreskrifternas nödvändighet besvaras i hög grad av den analys som gjorts av nollalternativet och av erfarenheterna från tidigare reglering. Erfarenheterna från de nu upphävda föreskrifterna visar entydigt att abstrakta bestämmelser utan konkreta kriterier inte ger tillräcklig vägledning och att verksamhetsutövare behöver tydliga och mätbara tröskelvärden för att kunna rapportera konsekvent. En situation där verksamhetsutövarna enbart har cybersäkerhetslagens generella definition att förhålla sig till skulle antingen leda till samma utfall som 17 kapitlet 6 § i de nu upphävda föreskrifterna, det vill säga att bestämmelsen i praktiken inte tillämpas, eller en betydande överrapportering enligt 2 kap. 5 § i cybersäkerhetslagen eftersom verksamhetsutövarna utan föreskrifter själva skulle tvingas avgöra vad som är en betydande incident. Svar på regeringens remiss av förslaget på cybersäkerhetslag från telekomområdets verksamhetsutövare visade också ett tydligt behov av de förtydliganden och den detaljnivå som föreskrifterna nu ger.

Föreskrifterna är vidare nödvändiga för att uppfylla det uppdrag som regeringen gav PTS i september 2025 och för att möta de förväntningar som regeringen uttryckligen angett i propositionen till cybersäkerhetslagen. Slutligen är föreskrifterna nödvändiga för att säkerställa att PTS föreskrifter ligger i linje med genomförandeförordningen och MCF:s föreskrifter för övriga sektorer, och för att undvika den omotiverade asymmetri som annars skulle uppstå inom sektorn för digital infrastruktur.

6.3.3 Är föreskrifterna utformade på ett sätt som minimerar onödiga kostnader och begränsningar?

En grundläggande princip i utformningen av de nya föreskrifterna är att konkreta och tydliga kriterier inte enbart är ett krav på god normgivning, utan också ett aktivt verktyg för att begränsa den regulatoriska bördan för verksamhetsutövarna. Tydliga tröskelvärden och mätbara kriterier minskar osäkerhet, och behovet av komplexa

bedömningar vid varje inträffad incident, reducerar risken för feltolkningar, icke enhetlig tillämpning samt minskar behovet av tolkningsförfrågningar till PTS.

PTS har i utformningen av föreskrifterna strävat efter att ligga i linje med genomförandeförordningens bestämmelser och MCF:s föreskrifter, vilket säkerställer att telekomaktörerna inte åläggs krav som går utöver vad som gäller för jämförbara aktörer. En total linjering är inte möjlig på grund av telekomområdets särskilda vikt och långa tradition av nationell reglering.

PTS har vidare särskilt beaktat de förutsättningar som gäller för mindre verksamhetsutövare och utformat föreskrifterna med ambitionen att kriterierna ska vara enkla att tillämpa även för aktörer utan specialiserad kompetens inom cybersäkerhet. Som angetts ovan har de mindre verksamhetsutövarnas ekonomi särskilt beaktats vid valet av en beloppsmässig gräns för ekonomisk skada. PTS har även avstått ifrån att göra skärpningar i tabellen i 3 kap. 2 § i förslaget, som vid en internationell överblick skulle kunna medföra en ökad harmonisering. De nya föreskrifterna är slutligen begränsade till att precisera vad som ska anses utgöra en betydande incident enligt cybersäkerhetslagen och att konkretisera de säkerhetsdimensioner som redan gällde av LEK, utan att införa krav som går utöver vad cybersäkerhetslagen och NIS2-direktivet kräver.

6.3.4 Sammanfattande proportionalitetsbedömning

De föreslagna föreskrifterna bedöms sammantaget vara proportionerliga i förhållande till det syfte de ska uppfylla. De är nödvändiga för att komplettera lagen och därmed ge verksamhetsutövarna den konkreta vägledning de behöver, för att möta regeringens förväntningar och för att skapa tillräcklig harmonisering med genomförandeförordningen och MCF:s föreskrifter. De är utformade på ett sätt som minimerar onödiga kostnader och begränsningar, och de genuint nya krav som föreskrifterna inför är en direkt och nödvändig följd av cybersäkerhetslagens utvidgade definition av *betydande incident* och av de krav som NIS2-direktivet ställer på Sverige som medlemsstat i EU.

6.4 Beskrivning av hur och när konsekvenserna av förslaget eller beslutet kan utvärderas

6.4.1 Syfte med utvärderingen

En utvärdering av de nya föreskrifternas effekter bör ha två överlappande syften. Det första är ett kontrollerande syfte, nämligen att bedöma om föreskrifterna har lett till den vägledning som behövs och om en tillräcklig harmonisering har uppnåtts. Det andra är ett lärande syfte, nämligen att identifiera eventuella brister eller oavsedda konsekvenser i föreskrifternas utformning och ge underlag för framtida justeringar.

Som nämnts ovan pågår också harmoniserings- och förenklingsåtgärder på EU-nivå. Resultatet av dessa initiativ kommer att behöva beaktas och kan eventuellt medföra behov av ändring av föreskrifterna.

6.4.2 Utvärderingsfrågor och indikatorer

Utvärderingen bör försöka besvara följande huvudsakliga frågor. Utgör föreskrifterna den konkreta vägledning som har efterfrågats och eftersträvats? Har de nya föreskrifterna lett till en ökad rapportering av incidenter som rör autenticitet, riktighet och konfidentialitet eller betydande skada för andra viktiga samhällsfunktioner jämfört med perioden under de nu upphävda föreskrifterna? Tillämpas de nya trösklarna i definitionen av betydande incident – ekonomisk skada, potentiell påverkan och skada för andra – av verksamhetsutövarna på ett konsekvent och ändamålsenligt sätt? Har föreskrifterna lett till en mer enhetlig rapportering mellan olika aktörer? Har föreskrifterna medfört en oproportionerlig administrativ börda för verksamhetsutövarna, särskilt för mindre aktörer? Har föreskrifterna uppnått tillräcklig harmoniseringsnivå jämfört med andra länder?

6.4.3 Data, metod och tidplan

Utvärderingen bör i första hand baseras på statistik över inkomna incidentrapporter uppdelat på rapporteringsgrund, incidenttyp, aktörsstorlek och tidsperiod, kompletterat med kvalitativ information från tillsynsarbetet och från dialog med berörda verksamhetsutövare, andra svenska myndigheter och andra utländska regulatoriska myndigheter. Jämförelser med MCF:s erfarenheter från tillämpningen av motsvarande föreskrifter för övriga sektorer bör också göras.

Regeringen anger i propositionen att en utvärdering av konsekvenserna av lagstiftningen bör ske tre år efter lagens i ikraftträdande. PTS bedömer att en utvärdering av föreskrifterna inte bör ske före utvärdering av lagen, om inte särskilda skäl påkallar det. PTS kommer därför att kontinuerligt övervaka vilken typ av incidenter och mängden betydande incidenter inom telekomområdet, samt även löpande stämma av med andra regulatoriska myndigheter inom EU i syfte att följa harmoniseringsåtgärder. Utvärderingen bör genomföras i samråd med MCF om möjligt

6.5 Ikraftträdande och informationsinsatser

6.5.1 Tidpunkt för ikraftträdande

Tidpunkten för ikraftträdande påverkas av flera rättsliga och praktiska faktorer. Cybersäkerhetslagen trädde i kraft den 15 januari 2026 och PTSFS 2022:11 upphävdes samtidigt, vilket innebär att telekomområdet sedan dess enbart

har cybersäkerhetslagens generella definition att förhålla sig till. Det finns därför ett starkt skäl att de nya föreskrifterna träder i kraft så snart som möjligt.

Det planerade datumet för ikraftträdandet av dessa föreskrifter är den 15 oktober 2026. MCF:s motsvarande föreskrifter som även inkluderar rapporteringsregler ska enligt uppgift från MCF träda i kraft den 1 juli 2026. Eftersom remissen går ut till branschen i maj 2026 och de föreslagna föreskrifterna planeras att träda i kraft i oktober 2026 bedömer PTS att verksamhetsutövarna har god tid på sig (fem månader) att anpassa sin verksamhet efter de föreslagna reglerna. PTS bedömer att de föreslagna föreskrifterna ligger i linje med cybersäkerhetslagens överordnade definition av betydande incident, MCF:s föreskrifter om vad som utgör betydande incidenter, genomförandeförordningens gränser för vad som utgör betydande incidenter samt LEK:s upphävda definitioner och rapporteringsplikt enligt LEK och PTS nu upphävda föreskrifter.

6.5.2 **Informationsinsatser**

Cybersäkerhetslagen innebär vissa förändringar av rapporteringsskyldigheten jämfört med LEK och de nu upphävda föreskrifterna och verksamhetsutövarna behöver inte enbart känna till de nya kriterierna utan också förstå hur de ska tillämpas i praktiken. PTS planerar att genomföra följande informationsinsatser i samband med att föreskrifterna träder i kraft.

En vägledning, som kontinuerligt kan uppdateras, på PTS webbplats med en samlad beskrivning av de nya kriterierna, praktiska exempel och svar på vanliga frågor, utformad för att kunna användas av verksamhetsutövare utan specialiserad juridisk kompetens. Riktade informationsinsatser till berörda där de nya föreskrifterna presenteras och verksamhetsutövarna ges möjlighet att ställa frågor. Samordning med MCF:s informationsinsatser för övriga sektorer, för att säkerställa en konsekvent kommunikation om de delar av regelverket som är gemensamma. Löpande tillgänglighet för tolkningsförfrågningar från verksamhetsutövarna under en inledande period efter ikraftträdandet.

Informationsinsatserna bedöms kunna genomföras inom PTS befintliga anslag men kräver prioritering av resurser under perioden närmast före och efter ikraftträdandet.

7. Bedömning av om förslaget eller beslutet inskränker den kommunala självstyrelsen

Det är vanligt förekommande att kommuner, oftast genom kommunala bolag, tillhandahåller allmänna elektroniska kommunikationsnät. Dessa kommer i tillämpliga fall att omfattas av de föreslagna föreskrifterna.

PTS bedömer att detta inte inskränker den kommunala självstyrelsen.

8. Bedömning av om förslaget eller beslutet överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen

8.1 Tillämpligt EU-rättsligt regelverk

Sverige har en skyldighet att implementera NIS2-direktivet. De föreslagna föreskrifterna har sin grund i cybersäkerhetslagen, som genomför NIS2-direktivet i svensk rätt. NIS2-direktivet innebär en utvidgning och skärpning av kraven på cybersäkerhet och incidentrapportering för verksamhetsutövare inom ett brett spektrum av samhällsviktiga sektorer, däribland telekomområdet som ligger i sektorn för digital infrastruktur.

Utöver direktivet är EU-kommissionens genomförandeförordning om tröskelvärden för incidentrapportering för sektorn för digital infrastruktur (som inte omfattar telekomområdet) samt Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation (kodexen) två källor som PTS ska ta hänsyn till i utarbetandet av dessa föreskrifter.

Skäl 95 i NIS2-direktivet anger att befintliga nationella riktlinjer som antagits för att införliva bestämmelserna i artiklarna 40 och 41 i direktiv (EU) 2018/1972 bör beaktas vid införlivandet av NIS2-direktivet för att ta fasta på den kunskap och kompetens som redan förvärvats inom ramen för direktiv (EU) 2018/1972 avseende säkerhetsåtgärder och incidentunderrättelser. Det ska göras när så är lämpligt och för att undvika onödiga störningar.

8.2 Förhållandet mellan NIS2-direktivet och sektorsspecifik unionsrätt

En central fråga i EU-rättsbedömningen är hur NIS2-direktivet förhåller sig till sektorsspecifik unionsrätt avseende incidentrapportering för telekomområdet. Enligt

artikel 4 i NIS2-direktivet gäller direktivet som lex generalis i förhållande till sektorsspecifik unionsrätt som ställer krav på cybersäkerhet eller incidentrapportering. Om sektorsspecifik unionsrätt kräver att väsentliga eller viktiga entiteter vidtar cybersäkerhetsåtgärder eller anmäler incidenter, och om dessa krav är minst lika stränga som de krav som fastställs i NIS2-direktivet, ska de relevanta bestämmelserna i NIS2-direktivet inte tillämpas på dessa entiteter. Förhållandet mellan NIS2-direktivet och sektorsspecifik unionsrätt behöver därför analyseras noggrant för att fastställa vilket regelverk som är primärt tillämpligt för telekomområdet.

8.3 Föreskrifternas förenlighet med EU-rätten

PTS gör bedömningen att de föreslagna föreskrifterna överensstämmer med de skyldigheter som följer av Sveriges anslutning till EU. De föreslagna föreskrifterna har utformats i enlighet med bestämmelser som följer av NIS2-direktivet och genomförandeförordningen.

De föreslagna föreskrifterna syftar till att precisera begreppet *betydande incident* för telekomområdet inom ramen för det handlingsutrymme som cybersäkerhetslagen och NIS2-direktivet ger PTS som tillsynsmyndighet. Föreskrifterna är utformade med utgångspunkt i cybersäkerhetslagens definition av *betydande incident* i 2 kap. 5 § 2 st., som i sin tur genomför NIS2-direktivets definition i artikel 23.

Föreskrifterna inför inte några rapporteringsgrunder eller krav som inte redan framgår av cybersäkerhetslagen eller NIS2-direktivet, med undantag för rapporteringen av återkommande incidenter som härstammar från genomförandeförordningen, och bedöms inte ge upphov till hinder mot den fria rörligheten på den inre marknaden.

I de delar där PTS föreskrifter avviker från genomförandeförordningens tröskelvärden för övriga delar av sektorn för digital infrastruktur är detta motiverat av telekomområdets särskilda förhållanden och den mångåriga nationella erfarenhet av incidentrapportering som motiverade att sektorn undantogs från genomförandeförordningens direkta tillämpningsområde.

8.4 Bedömning av om föreskrifterna går utöver NIS2-direktivets miniminivå

PTS bedömning är att de föreslagna föreskrifterna ligger i linje med NIS2-direktivets miniminivå och i linje med genomförandeförordningens tröskelvärden för jämförbara aktörer inom sektorn för digital infrastruktur.

Föreskrifterna inför inte rapporteringsgrunder eller krav som saknar stöd i NIS2-direktivet eller cybersäkerhetslagen. I den mån föreskrifterna avviker från

genomförandeförordningens tröskelvärden är detta motiverat genom skäl 95 i NIS2-direktivet och telekomområdets särskilda förhållanden. Det innebär att föreskrifterna inte går utöver NIS2-direktivets miniminivå.

8.5 Underrättelse för anmälan till Europeiska unionen

Av 6 § förordningen (1994:2029) om tekniska regler framgår att en myndighet som avser fatta beslut om en teknisk regel i god tid ska underrätta Kommerskollegium om det förslag som den har utarbetat. Av 1 § samma förordning framgår att bestämmelserna i förordningen ansluter till Sveriges internationella förpliktelser enligt bland annat Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (anmälningsdirektivet).

PTS bedömer att föreskrifterna inte ställer krav på säkerhetsåtgärder för informationssamhällets tjänster, eftersom kraven rör tillhandahållande av elektroniska kommunikationsnät och tjänster, som främst möjliggör e-tjänster i ett senare led. En eventuell påverkan på informationssamhällets tjänster blir därmed endast indirekt och PTS gör bedömningen att någon anmälan enligt anmälningsdirektivet inte behöver göras eftersom de aktuella föreskrifterna inte utgör sådana tekniska regler som ska anmälas. Någon underrättelse till Kommerskollegium ska därför enligt PTS bedömning inte ska göras.

8.6 Sammanfattande EU-rättsbedömning

De föreslagna föreskrifterna är förenliga med Sveriges skyldigheter som EU-medlem. Föreskrifterna genomför cybersäkerhetslagens krav på incidentrapportering för telekomområdet inom ramen för det handlingsutrymme som NIS2-direktivet ger medlemsstaterna, och är utformade med beaktande av genomförandeförordningens tröskelvärden för övriga delar av sektorn för digital infrastruktur. Föreskrifterna går inte utöver NIS2-direktivets miniminivå och bedöms inte ge upphov till hinder mot den fria rörligheten på den inre marknaden. De är inte anmälningspliktiga enligt anmälningsdirektivet.

9. Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

PTS beslutanderätt grundar sig på följande bemyndiganden.

NIS2-direktivet implementeras i Sverige genom cybersäkerhetslagen (2025:1506) och cybersäkerhetsförordningen (2025:1507).

Det framgår av 7 § cybersäkerhetsförordningen att PTS är tillsynsmyndighet för sektorn för digital infrastruktur, inom vilken elektronisk kommunikation/telekomområdet omfattas som en del

Enligt 37 § cybersäkerhetsförordningen får PTS för sina tillsynsområden, med undantag rörande Länsstyrelserna, meddela ytterligare föreskrifter om vad som utgör en betydande incident enligt 2 kap 5 § cybersäkerhetslagen. Samma gäller för rätten att meddela föreskrifter om informationsskyldighet enligt 2 kap. 9 och 10 §§ samma lag.

Föreskriftsmandatet för PTS om vad som utgör en betydande incident enligt 2 kap. 5 § samt föreskrifter om informationsskyldighet enligt 2 kap. 9 och 10 §§ cybersäkerhetslagen omfattar sektorerna Digital infrastruktur, Digitala leverantörer, Post- och budtjänster och Rymden. Kommissionens genomförandeförordning gäller dock redan för verksamhetsutövare inom sektorerna digital infrastruktur och digitala leverantörer, dock inte för elektroniska kommunikationer/telekomområdet. PTS föreskriftsmandat om vad om utgör en betydande incident omfattar således sektorerna som PTS har inom sitt tillsynsområde, med undantag för Länsstyrelserna - men inte de sektorer som redan omfattas av genomförandeförordningen.

Det är skäl 95 i NIS2-direktivet som särskilt anger att medlemsstaterna kan utse de nationella regleringsmyndigheterna till behöriga myndigheter för elektronisk kommunikation enligt direktiv (EU) 2018/1972 (kodexen) för att säkerställa att nuvarande praxis upprätthålls och för att ta fasta på den kunskap och erfarenhet som förvärvats som en följd av genomförandet av det direktivet.

Det är skrivningen i skäl 95 i NIS2-direktivet, telekomområdets särprägel som bärare av funktionalitet av de flesta andra sektorers verksamhet som omfattas av NIS2 och CSL, lång tid och erfarenhet av nationella säkerhets- och incidentrapporteringsreglering samt den relativt nyliga implementeringen av kodexen som ligger bakom att regeringen tilldelat PTS mandatet att särreglera vad som utgör en betydande incident för telekomområdet.

I bilagan i denna konsekvensutredning anges vilka bemyndiganden som har använts som stöd för att meddela respektive bestämmelser i de föreslagna föreskrifterna. I bilagan finns även en jämförelsetabell över förhållandena mellan de föreslagna reglerna och tidigare och nu gällande överordnade regelverk, EU-kommissionens genomförandeförordning och MCF:s motsvarande rapporteringsregler.

10. Kontaktpersoner

Therese Braathen, Mats Jönsson och Erica Nyström

Bilaga 1 Jämförelsetabeller och bemyndiganden

PTS får skriva föreskriver enligt 37 § cybersäkerhetsförordningen (2026:1507) enligt följande:

37 § Post- och telestyrelsen får för sina tillsynsområden, med undantag för 8 § 1, meddela

1. ytterligare föreskrifter om säkerhetsåtgärder enligt 2 kap. 3 § cybersäkerhetslagen (2025:1506),

2. ytterligare föreskrifter om vad som utgör en betydande incident enligt 2 kap. 5 § samma lag,

3. föreskrifter om informationsskyldighet enligt 2 kap. 9 och 10 §§ samma lag

Bemyndigandet till PTS i 37 § 2 p. cybersäkerhetsförordnigen grundar arbetet med detta förslag till föreskrifter. Observera undantaget för länsstyrelserna i 37 § jämfört med 8 § cybersäkerhetsförordningen. PTS är tillsynsmyndighet över länsstyrelserna men saknar bemyndigande att skriva föreskrifter för det tillsynsområdet.

PTS gör jämförelser i nedanstående tabell mellan:

- De nya föreskrifterna om vad som utgör betydande incidenter
- bemyndigande
- PTS tidigare gällande rapporteringsföreskrifter
- Kodexen och Enisas technical guidelines for incident reporting under the EECC (Enisas vägledning), vad avser Enisas tolkning av kodexens trösklar
- NIS2-direktivet
- genomförandeförordningen och
- MCF:s motsvarande trösklar för betydande incidenter för de övriga sjutton sektorer som lyder under cybersäkerhetslagen.

Jämförelsetabell: De nya föreskrifterna, bemyndiganden, tidigare gällande rapporteringsföreskrifter, kodexen (EECC) och Enisas vägledning, NIS2-direktivet,

genomförandeförordningen samt Myndigheten för civilt försvars motsvarande föreskriftsregler.

Föreskriften	**Bemyndigande**	**PTSFS 2022:11**	**Kodexen och Enisas vägledning**	**NIS2-direktivet**	**Genomförandeförordningen**	**Motsvarande regel i MCFFS 2026:6****
3 kap. 2 § 1p Undergrävd tillgänglighet i nät, tjänster och uppgifter	2 kap. 5 § CSL* och 37 § CSF*	17 kap. 5 § med tillägg	Art. 40.2 a till d	Art. 23.3 a-b	Art. 5a) -12 a), 5b) – 12b), 8 d och art. 3.3 a och b	3 kap. 1 § 1–4 p
3 kap. 2 § 2p Undergrävt tillgänglighet för svartfiber	2 kap. 5 § CSL och 37 § CSF	17 kap. 5 § förtydligad	Art. 40.2 d	Art. 23.3 a-b	Art. 5a) -12 a) och 5b) – 12b) samt 8 d	3 kap. 1 § 1–4 p
3 kap. 2 § 3p Undergrävd riktighet, autenticitet eller konfidentialitet i nät, tjänster eller uppgifter	2 kap. 5 § CSL och 37 § CSF	17 kap. 6 §	Art. 40.2 a och d	Art. 23.3 a-b	Art. 5c, 6c, 7d) – 12d)	3 kap. 1 § 3 p och 6 § 1 p
3 kap. 2 § 4p Gränsöverskridande incident	2 kap. 5 § CSL och 37 § CSF	17 kap. 6 §	Art. 40 2p. c och d samt Art 40.2 3 st. samt Enisas vägledning s. 17	Art. 23.1	-	-
3 kap. 2 § 5p Incident i landsbygds- eller glesbygdskommun	2 kap. 5 § CSL och 37 § CSF	17 kap. 5 § men med lägre tröskel	Art. 40.2 e samt Enisas vägledning s. 21	Art. 23.3 b	-	-
3 kap. 2 § 6p Incident vid samma naturkatstrof	2 kap. 5 § CSF och 37 § CSF	Delvis både 17 kap. 5 och 6 §§ förtydligad	Art 40.2 e samt Enisas vägledning	Art. 23.3 a-b	-	-

3 kap. 3 – 5 §§ Ekonomisk skada för verksamhetsutövaren	2 kap. 5 § CSL och 37 § CSF	-	-	Art. 23.3 a	Art. 2.1 a	3 kap. 3–5 §§
3 kap. 6 § 1p Betydande skada på viktig samhällsfunktion efter telekom-incident	2 kap. 5 § CSL och 37 § CSF	17 kap. 6 § med mer definierad tröskel	Art 40.2 e samt Enisas vägledning	Art. 23.3 a-b	-	3 kap. 6 § 3 p
3 kap. 6 § 2p Undergrävd TRAK*** i verksamhetsutövarens medverkan till nödkommun-ikation	2 kap. 5 § CSL och 37 § CSF	17 kap 3 § 7 p och 10 p och 17 kap. 6 §§ men förtydligad	Art. 40.2 e samt Enisas vägledning s. 21	Art. 23.3 b	-	-
3 kap. 6 § 3p Undergrävd TRAK*** i verksamhetsutövarens medverkan till VMA	2 kap. 5 § CSL och 37 § CSF	17 kap 3 § 7 p och 10 p och 17 kap. 6 §§ men förtydligad §	Art. 40.2 e samt Enisas vägledning s. 21	Art. 23.3 b	-	-
3 kap. 6 § 4p Dödsfall eller betydande skada på någons hälsa	2 kap. 5 § CSL och 37 § CSF, samt propositionen s. 105	-	-	Art. 23.3 a-b	Art. 3 c och d	3 kap. 6 § 3 p b och c
3 kap. 7 § 1p **Risk för** allvarlig driftstörning, ekonomisk skada, eller betydande skada för annan	2 kap. 5 § CSL och 37 § CSF	Definitionen av säkerhetsincident i 1 kap. 7 § LEK (upphä	Definition i kodexen och LEK av säkerhets-incident	Art. 23.3 a-b	Samtliga tröskelvärden i genomförandeförordningen omfattar ”kan” få effekt.	3 kap. 2, 4, 7 §§. MCF har tre olika bestämmelser för risker för allvarlig driftstörning, ekonomisk skada

		vd del) **				respektive betydande skada för annan.
3 kap. 7 § 2p Konstaterat eller misstänkt intrång som **kan orsaka** allvarlig driftstörning	2 kap. 5 § CSL och 37 § CSF	Definitionen av säkerhets-incident i 1 kap. 7 § LEK **** (upp-hävd)	Definition i kodexen och LEK av säkerhetsincident och kodexen art. 40.2 d	Art. 233 a-b	Art. 3.1 e och art. 7c-9c.	3 kap. 2 § 1 p
3 kap. 7 § 3p Incident i kritisk internationell, nationell och regional infrastruktur som medför nedsatt stabilitet, motståndskraft eller förmåga att skydda TRAK	2 kap. 5 § CSL och 37 § CSF, samt propositionen s. 105	-	Art 40.2 3 st	Art. 23.1 och 23.3	-	-
3 kap. 8 § återkommande incidenter	2 kap. 5 § CSL och 37 § CSF	-	Art 40 2p d och e	Art. 233 a-b	Art. 4 och skäl 40	3 kap. 6 §

* CSL och CSF = cybersäkerhetslagen och cybersäkerhetsförordningen

** MCFFS 2026:6 = Myndigheten för civilt försvars föreskrifter om betydande incidenter och informationsskyldighet för väsentliga och viktiga verksamhetsutövare

***TRAK= tillgänglighet, riktighet, autenticitet och konfidentialitet

**** Tillhandahållarens förmåga att motstå händelser som undergräver tillgängligheten, äktheten, riktigheten eller konfidentialiteten hos näten eller tjänsterna, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via era elektroniska kommunikationsnät eller elektroniska kommunikationstjänster, eller på er förmåga att motstå sådana händelser (enligt den tidigare definitionen av säkerhetsincident i 1 kap 7 § LEK).

Bilaga 2. Omvärldsjämförelser - EU-staters implementering av NIS2-direktivet med fokus på rapporteringströsklar inom telekomområdet

En utblick över vad andra EU-länder, redan innan hade, eller nu har skapat, för att definiera rapporteringströsklar under NIS2-direktivet och kodexen. Jämförelsen har endast fokus på telekomområdet.

Generellt kan sägas att det är tidigt att göra harmoniseringsjämförelser mellan olika länder för att det råder ännu både ett oklart regleringsläge och praxisläge för de flesta medlemsstater enligt NIS2-direktivet. Det gör att utblicken om rapporteringströsklar sannolikt kommer att förändra sig över tid (den här bilagan skrivs under våren 2026).

I den här bilagan gör PTS, trots oklarheterna som fortfarande råder, ändå ett försök att beskriva situationen med rapporteringsregler för telekomområdet, runt om i EU-länderna

NIS2-direktivet

Ett helt centralt syfte med NIS2-direktivet är att skapa en högre gemensam cybersäkerhetsnivå i och mellan EU-länderna för att skapa en förbättrad funktion i den inre marknaden. Det var i huvudsak både samhällsutvecklingen och bristande harmonisering efter införande av NIS-direktivet, i de olika länderna som var ett av skälen till att NIS-direktivet byttes ut till NIS2-direktivet.

Det finns generellt, och även nu efter att NIS-direktivet bytt ut med NIS2-direktivet, skilda sätt att genomföra alla de olika nationella implementeringarna av NIS2-direktivet.

I det som avses häri - att i regelgivning definiera vad som utgör betydande incidenter enligt NIS2-direktivet - finns i huvudsak fyra nationella metoder som PTS har identifierat i arbetet med föreskrifter om vad som utgör betydande incidenter inom telekomområdet (rapporteringströsklar):

Det ena är att den nationella lag som implementerar direktivet anses tillräcklig och det saknas kompletterande sekundära regler, till exempel myndighetsföreskrifter.

Alternativt har vissa länder ännu inte beslutat om sådana sekundära regler till den nationella lagen ska införas.

Det andra är att det skapas sekundära regler till den nationella NIS2-lagen – genom rapporteringsföreskrifter som gäller för alla sektorer under NIS2-direktivet, alltså inklusive telekomsektorn.

Det tredje är att bryta ut till exempel telekomområdet och skapa enskilda rapporteringsföreskrifter på sekundär regelgivningsnivå - specifikt för telekomområdet - för att avgöra vad som utgör betydande incidenter inom telekom – genom att skapa rapproteringströsklar i föreskrifter endast för telekom. Det är den metod som svenska PTS har valt.

Det fjärde är att både behålla de tidigare gällande nationella rapporteringsreglerna som skapats under den nationella implementeringen av kodexen, och parallellt skapa nya rapporteringsregler enligt den nationella implementeringen av NIS2-direktivet. Det skapar en situation med två olika rapporteringskrav, åtminstone i en övergångsperiod.

Länder som ännu *inte* implementerat NIS2-direktivet i nationell lag per den 26 mars 2026

Enligt EUR-lex är det Irland, Spanien, Luxemburg, Frankrike och Nederländerna som inte har lagstiftning på plats.[40] Dessa länder har dock redan rapporteringströsklar på plats för telekom. Dessa är baserade på nationell implementering av kodexen.

För att jämföra med dessa länder används häri deras rapporteringströsklar enligt den nationella implementeringen av kodexen. Det har uttryckligen i NIS2-direktivet beskrivits att vad som gällde enligt kodexen för telekomverksamhetsutövare, ska fortsätta att gälla. Det är i vart fall inte åsyftat någon minskning av kraven.

En jämförelse av olika länders implementerade krav enligt kodexen är intressant utifrån att de nya rapporteringsreglerna inte ska sänka kraven och också vara mer harmoniserade. Det innebär att om vi kan se att andra länders rapporteringskrav utifrån kraven i kodexen redan omfattar det vi nu föreslår i de kommande rapporteringsreglerna enligt cybersäkerhetslagen – är de nya kraven i utkastet på föreskrifter om vad som utgör betydande incidenter för telekomverksamhetsutövare i Sverige inte för höga, utan ligger inom ramen för NIS2-direktivet.

[40] Direktiv - 2022/2555 - SV - EUR-Lex

Länder med rapporteringströsklar enligt kodexen

Spanien har ännu inte implementerat NIS2 i nationell lag, men stramar nu åt sina rapporteringströsklar för telekom enligt den implementerade kodexen. [41]

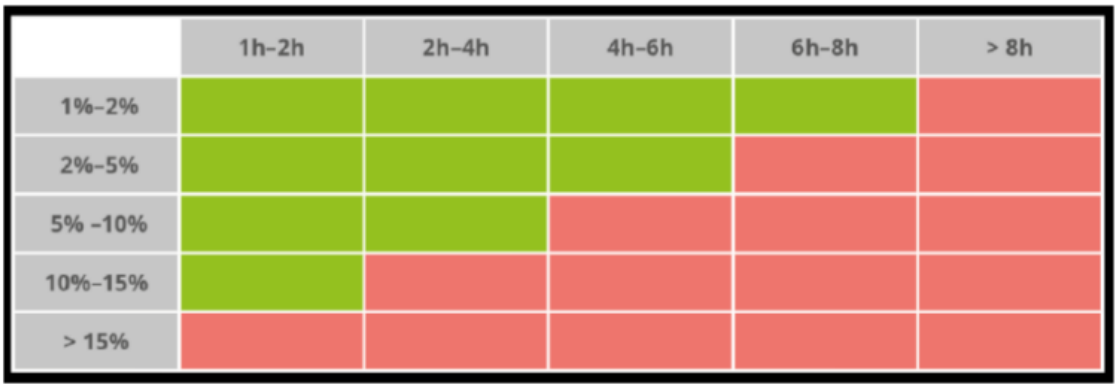
Rapporteringsströsklar i urval för avbrott eller minskad kvalitet på telekomtjänsten (tillgänglighetsproblem):

- 10 000 drabbade uppkopplingar (lineas) under mer än en timme (significant)
- Färre än 10 000 drabbade lineas under mindre än en timme om incidenten inträffat under tiden kl. 07 till midnatt (less significant).
- Båda typerna ska rapporteras som en säkerhetsincident.
- 10 000 drabbade användare vid broadcast transmission service under mer än en timma (significant).
- Färre än 10 000 drabbade användare under mindre än en timma (less significant).
- Båda typerna ska rapporteras.
- Avbrott eller kvalitetsbrist för 10 % av användarna på någon ö eller i de spanska enklaverna i Afrika (Ceuta och Melilla) oavsett tidslängd.
- störningar på nödkommunikation eller VMA oberoende av hur många uppkopplingar som störts.
- incident som drabbar flera operatörer på grund av naturkatastrof eller strömavbrott (avsett antal drabbade lineas eller användare. Det viktiga är att flera operatörer drabbas).
- incident som definieras av den regulatoriska myndigheten som att den har stört ekonomin eller samhället.

Irland har ännu inte implementerat NIS2 i nationell lag. Rapporteringströsklarna nedanför gäller enligt den nationella implementeringen av kodexen.

[41] Cullen International. Proposed Spanish decree on network security and resilience, FLTEES20260001 - 11 Jan. 2026 - Carmen Mateas

Den andel av tjänstens nationella slutanvändarbas som påverkas och varaktigheten av säkerhetsincidenten.



	1h–2h	2h–4h	4h–6h	6h–8h	> 8h
1%–2%					
2%–5%					
5% –10%					
10%–15%					
> 15%					

Figure 2: Thresholds, based on National User Base and Incident Duration[46]

§§ Leverantörer måste också rapportera varje säkerhetsincident som uppgår till eller överstiger en miljon (1 000 000) användartimmar har inträffat eller pågår.

§§ Leverantörer måste också rapportera varje säkerhetsincident som påverkar 1 % eller mer av den nationella slutanvändarbasen och som påverkar tjänstens konfidentialitet, integritet eller autenticitet.

§§ Tydliga regler för att räkna ut verksamhetsutövarens nationella slutanvändarbas för olika slags verksamhetsutövare (fiber, mobil, NI-ICS med fler)

§§ ”Stormrapportering: när Met Éireann utlyser en storm eller utfärdar en orange eller röd vädervarning kommer ComReg att informera de leverantörer som är registrerade i e-licensieringsportalen för incidentrapportering, med ytterligare detaljer och den rapporteringsmall eller metod som ska användas.

Länk:<https://www.comreg.ie/media/2024/04/ComReg-2423-D0824.pdf> (ComReg Decision D08/24.)

Rapporteringströsklarna är under revidering, men *utan* anpassning till NIS2 eller CER-direktiven. Länk: <https://www.comreg.ie/publication/network-incident-reporting-processes-review-and-subsequent-revision-of-comreg-decision-instrument-d08-24-consultation>

Observera: PTS har inte hittat några rapporteringsregler för störningar av nödkommunikationer eller varningar till allmänheten

Luxemburg har ännu inte implementerat NIS2 i nationell lag. Rapporteringströsklarna enligt den nationella implementeringen av kodexen gäller enligt nedan.

En säkerhetsincident anses ha haft en betydande påverkan på driften av nätverk eller tjänster om minst en av följande situationer har inträffat:

a) Mellan 1 och 2 procent av användarna påverkades i minst 3 timmar
b) mellan 2 och 5 procent av användarna påverkades i minst 2 timmar
c) mellan 5 och 10 procent av användarna påverkades i minst en timme
d) 10 procent eller mer av användarna påverkades oavsett varaktighet
e) händelsen har påverkat äktheten, integriteten eller konfidentialiteten hos (i) näten, (ii) tjänsterna, (iii) de data som lagrats, behandlats, överförs eller omvandlas eller (iv) de relaterade tjänster som erbjuds av den berörda operatören via ett nätverk eller en tjänst tillhörande operatören, förutsatt att denna påverkan på äkthet, integritet eller sekretess har påverkat mer än 50 slutanvändare i Luxemburg
f) Händelsen har skapat en risk för allmän säkerhet eller har lett till dödsfall
g) Händelsen påverkade larmsystem
h) händelsen påverkade tillgången till nödvändiga tjänster enligt definitionen i bilagan till lagen av den 28 maj 2019 om införandet av Europaparlamentets och rådets direktiv (EU) 2016/1148 från 6 juli 2016 om åtgärder för en hög gemensam säkerhetsnivå för nätverks- och informationssystem i hela Europeiska unionen samt ändring 1° den ändrade lagen av den 20 april 2009 inrättandet av Statens informationsteknologiska centrum och 2° lagen av den 23 juli 2016 som inrättar en högkommission för nationellt skydd
i) Händelsen var potentiellt kopplad till dagar med avgörande händelser, såsom bland annat valdagen eller ett statsbesök
j) Händelsen påverkade viktiga funktioner för företaget, såsom bland annat ett ministerium eller en administration;
k) Händelsen har påverkat nyckelpersoner såsom bland andra statschefer, regeringschefer, parlamentariker, ministrar, ambassadörer och i allmänhet fysiska personer som innehar eller har anförtrotts en viktig offentlig funktion;
l) Händelsen fick internationell betydelse;
m) Händelsen orsakade materiella skador på minst 50 000 euro för användaren, trots att användaren vidtagit alla nödvändiga åtgärder enligt konstens regler för att undvika eller minska skadorna som orsakades av händelsen;
n) Händelsen påverkade räddningstjänstens funktion

Länk: Règlement ILR/N23/3, Art 1:
https://legilux.public.lu/eli/etat/leg/rilr/2023/07/20/a447/jo

Finland arbetar nu med ändringar av rapporteringsföreskriften 66 A/2019 som gäller för telekom. De nu gällande rapporteringströsklarna i 66A/2019 är de som summeras här. I nuläget räcker det med att telekombolagen incidentrapporterar antingen enligt 66A/2019 eller enligt de nya cybersäkerhetslagen.

De finska rapporteringsreglerna har skiljer på informationssäkerhetsincidenter (vilka rapporteras enligt EU-förordning 611/2013) och funktionalitetsincidenter (eventuellt samma sak som säkerhetsincidenter enligt kodexen).

Landet klassificerar funktionalitetsincidenterna (eventuellt samma som säkerhetsincidenter enligt kodexen) i kategorier A-D.

Alla incidenter i kategori A-C är rapporteringspliktiga.

Eventuellt omfattar reglerna om funktionalitetsincidenter endast problem med tillgängligheten av nät och tjänster. Det vill säga de omfattar inte problem med tillgängligheten av lagrade, överförda eller behandlade uppgifter, och inte problem med riktighet, autenticitet eller konfidentialitet för nät, tjänster eller uppgifter.

Observera: Det är oklart i översättningen om användare avser slutanvändare, så som i de fysiska personer eller maskiner som använder tjänsterna - eller användare, så som företagskunder och liknande.

§§ Störningar i möjligheten att ringa 112

- störningar i överföring av nödsamtal
- störningar i prioriterad trafik
- störningar i funktioner som krävs för att nödsamtal ska fungera

§§ Kategori A: Störningen förhindrar

1. driften av en allmän telefonitjänst för ≥ 100 000 användare, eller
2. driften av en telefonitjänst i ett sammanhängande geografiskt område på ≥ 60 000 km² och driftstörningen påverkar ≥ 25 000 användare, eller
3. driften av en internetåtkomsttjänst för ≥ 200 000 användare, eller
4. driften av en internetåtkomsttjänst i ett sammanhängande geografiskt område på ≥ 60 000 km² och driftstörningen påverkar ≥ 25 000 användare, eller

5. driften av en SMS-tjänst för ≥ 200 000 användare, eller
6. driften av en e-posttjänst för ≥ 500 000 användare, eller
7. driften av ≥ 500 basstationer i ett mobilnät i ett sammanhängande geografiskt område.

§§ Kategori B: Störningen förhindrar

1. driften av en allmän telefonitjänst för ≥ 10 000 användare, eller
2. driften av en telefonitjänst i ett sammanhängande geografiskt område på ≥ 20 000 km^2, eller
3. driften av en internetåtkomsttjänst för ≥ 50 000 användare, eller
4. driften av en internetåtkomsttjänst i ett sammanhängande geografiskt område på ≥ 20 000 km^2, eller
5. driften av en SMS-tjänst för ≥ 50 000 användare, eller
6. driften av en e-posttjänst för ≥ 200 000 användare, eller
7. driften av en annan kommunikationstjänst för ≥ 200 000 användare, eller
8. driften av ≥ 100 basstationer i ett mobilnät i ett sammanhängande geografiskt område.

§§ Kategori C: Störningen förhindrar

1. driften av en allmän telefonitjänst för ≥ 1 000 användare, eller
2. driften av en internetåtkomsttjänst för ≥ 1 000 användare, eller
3. driften av en SMS-tjänst för ≥ 1 000 användare, eller
4. driften av en e-posttjänst för ≥ 50 000 användare, eller
5. driften av en annan kommunikationstjänst för ≥ 50 000 användare, eller
6. driften av ≥ 10 basstationer i ett mobilnät i ett sammanhängande geografiskt område.

§§ Störningar med allvarlighetsgrad A, B eller C

Störningar med allvarlighetsgrad A, B eller C som har varat under en sammanhängande period om minst 30 minuter ska anmälas till Transport- och kommunikationsverket.

Om en funktionsstörning med allvarlighetsgrad A, B, C eller D orsakas av en Denial-of-Service-attack får teleoperatören alternativt uppfylla sin anmälningsskyldighet enligt 1 mom. genom att använda Transport- och kommunikationsverkets DDoS-anmälningsgränssnitt.

När en säkerhetsincident som påverkat tillgängligheten enligt kategori A-C ska rapporten innehålla uppgift om den estimerade längden på störningen och den estimerade påverkan på nödkommunikation.

Länk: EN_M66A.pdf

Länder som endast har en nationell lag som implementerar NIS2-direktivet, utan sekundär regelgivning om rapporteringströsklar i dagsläget

Slovenien Det saknas rapporteringströsklar. Det finns en nationell lag som implementerar NIS2-direktivet och den gäller för alla NIS2-sektorer.

Länk: https://pisrs.si/pregledPredpisa?id=ZAKO8934

Österrike Det saknas rapporteringströsklar. Det finns en nationell lag som implementerar NIS2 och den gäller för alla NIS2-sektorer. Om trösklar ska införas i sekundär reglering till lagen kommer de sannolikt att omfatta alla arton NIS2-sektorerna och sannolikt även telekomområdet.

Länder med rapporteringströsklar för alla sektorer under NIS2

Kroatien har rapporteringströsklar i den nationella lagen som implementerar NIS2-direktivet. Lagen omfattar alla arton sektorer som träffas av NIS2, inklusive telekom. Landet kommer inte att skapa särskilda regler för telekomområdet.

Trösklar

§§ (1) Incidenter som orsakar eller kan orsaka allvarlig driftstörning i tjänsterna är incidenter:

- som negativt påverkar tjänstens tillgänglighet eller försämrar tjänstens kvalitet, eller
- som negativt påverkar eller kan negativt påverka äkthet, integritet eller konfidentialitet hos lagrade, överförda eller behandlade data eller tjänster.

§§ (2) En incident ska anses negativt påverka tjänstens tillgänglighet eller försämra tjänstens kvalitet om minst ett av följande tröskelvärden uppnås:

- minst 20 % av tjänstemottagarna kunde inte få tillgång till tjänsten under minst en timme
- minst 1 % av tjänstemottagarna kunde inte få tillgång till tjänsten under minst åtta timmar, förutsatt att 1 % motsvarar minst 100 tjänstemottagare
- tillgång till tjänsten var inte möjlig under en timme eller mer, och verksamhetsutövaren inte kan fastställa hur många tjänstemottagare som saknade tillgång under perioden
- minst 30 % av tjänstemottagarna kunde tillfälligt inte få tillgång till tjänsten eller kunde inte använda tjänsten funktionellt på grund av försämrad tjänstekvalitet, om de tillfälliga avbrotten eller funktionsnedsättningarna varade totalt minst en timme under en fyratimmarsperiod
- tillgång till tjänsten i ett sjukhus, en flygplats, ett flygbolag, en bankanläggning med datacenter, en polisverksamhet, en aktiv vattenpumpstation och kontrollcentral, en anläggning tillhörande en elektronisk kommunikationsoperatör, en anläggning tillhörande en säkerhets- eller underrättelsemyndighet, en professionell brandkår eller en aktör som identifierats som kritisk enligt lagstiftning om kritisk infrastruktur, var inte möjlig under minst en timme
- tillgång till flygtrafikledningstjänsten var inte möjlig, oavsett avbrottets längd och antalet berörda mottagare

- tillgång till tjänster som används av Försvarsministeriet, de väpnade styrkorna, civila försvarsplaneringsmyndigheter eller juridiska personer av särskild betydelse för försvaret, var inte möjlig under minst en timme
- tillgång till 112-centralens tjänster eller andra räddningstjänster var inte möjlig, oavsett avbrottets längd och antalet berörda mottagare
- tillgång till tjänsten i minst ett län eller en stad som är länets säte var inte möjlig under minst en timme.

§§ (3) En incident ska anses negativt påverka eller kunna negativt påverka äkthet, integritet eller konfidentialitet hos lagrade, överförda eller behandlade data eller tjänster om minst ett av följande tröskelvärden uppnås:

- obehörig person har fått tillgång till kritiska delar av verksamhetsutövarens nätverk och informationssystem eller kritiska data, eller förutsättningar har uppstått som möjliggör sådan åtkomst
- obehörig person har konfigurerat verksamhetsutövarens kritiska nätverk och informationssystem, eller förutsättningar har uppstått som möjliggör sådan konfigurering
- incidenten har skapat omständigheter som hindrar behörig person från att konfigurera det kritiska nätverket och informationssystemet
- konfigureringen av verksamhetsutövarens kritiska nätverk och informationssystem har ändrats, kompletterats eller på annat sätt gjorts otillförlitlig utan behörighet, eller kritiska data har tagits bort, ändrats, kompletterats eller på annat sätt gjorts otillförlitliga utan behörighet
- verksamhetsutövarens kritiska nätverk och informationssystem och/eller andra nätverk och informationssystem som kan påverka de kritiska systemen utför uppgifter som avviker från etablerade rutiner eller kontrollramverk, särskilt om systemen utför uppgifter de inte är avsedda för eller inte utför nödvändiga uppgifter som de är avsedda att utföra.

§§(4) Om verksamhetsutövaren inte har klassificerat kritikaliteten hos sina nätverk och informationssystem, inte identifierat kritiska data eller inte kan identifiera vilka kritiska system eller data som påverkats av incidenten, ska alla system och data anses vara kritiska.

§§ (1) En incident ska anses orsaka eller kunna orsaka ekonomisk förlust för en verksamhetsutövare om minst ett av följande tröskelvärden uppnås:

- om intäktsbortfall eller kostnader orsakade av incidenten, eller summan av dessa, uppgår till 100 000 euro eller minst 5 % av verksamhetsutövarens totala årliga rörelseintäkter, beroende på vilket som är lägre
- om tillgång till tjänsten inte var möjlig under minst en timme för tjänstemottagare som genererade intäkter på 100 000 euro föregående år eller minst 5 % av verksamhetsutövarens totala årliga rörelseintäkter, beroende på vilket som är lägre
- om incidenten orsakat skada på verksamhetsutövarens anseende.

(2) Med total årlig rörelseintäkt avses verksamhetsutövarens totala rörelseintäkter enligt föregående års bokslut, oavsett om verksamheten även omfattar andra tjänster eller aktiviteter utanför bilaga I och II till lagen.

(3) Med intäkter avses alla intäkter på årsbasis, oavsett om de genereras genom ordinarie verksamhet eller genom verksamhet utanför ordinarie drift.

(4) Med kostnader avses alla kostnader som uppstår till följd av åtgärder för att begränsa, hantera eller återhämta sig från en incident, inklusive åtgärder för att återställa normal drift. Detta inkluderar inte avtalsvite eller annan ersättning som verksamhetsutövaren måste betala på grund av avtalsbrott orsakat av incidenten.

(5) En incident ska anses ha orsakat anseendeskada om minst ett av följande tröskelvärden uppnås:

- en public service-medieaktör rapporterade om incidenten
- incidenten ledde till att minst 1 % av tjänstemottagarna inkom med klagomål, stämningar eller andra krav.

§§ (1) En incident ska anses ha påverkat eller kunna påverka andra fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada om incidenten resulterade i:

- dödsfall eller kroppsskada som krävde sjukhusvård eller behandling
- total förstörelse eller betydande skada på egendom som tillhör andra personer
- avbrott eller betydande begränsning av verksamheten hos andra personer
- förlust eller kompromettering av personuppgifter eller känsliga uppgifter som tillhör andra personer.

(2) Med andra fysiska och juridiska personer avses tjänstemottagare till en väsentlig eller viktig enhet, samt alla andra som lidit skada enligt punkt 1.

§§ Incidenter som var för sig inte uppfyller kriterierna för en betydande incident enligt artiklarna 59–61 ska ändå anses vara en betydande incident om:

- de inträffat minst två gånger under en sexmånadersperiod
- de har samma grundorsak
- de tillsammans uppfyller minst ett av kriterierna i artiklarna 59–61.

§§ Avbrott i tjänsteleverans eller försämrad tjänstekvalitet på grund av planerat rutinunderhåll av nätverk och informationssystem hos väsentliga eller viktiga enheter ska inte anses vara en betydande incident enligt artiklarna 59–62.

Länk till artikel 59–63 som rör incidentrapporteringströsklar:
https://ncsc.hr/UserDocsImages/ostalo/Regulation_on_Cybersecurity.pdf?vel=1041993

Länder med kvarvarande rapporteringströsklar enligt kodexen, som har implementerat NIS2 men inte är klara över om de ska skapa andra trösklar än de som gällde under kodexen

Bulgarien har nyligen implementerat NIS2 i Bulgarian Cybersecurity Act. Just nu analyserar de förändringarna, och har inte tydliga planer på att byta ut rapporteringströsklarna enligt kodexen. Trösklarna finns här på sid 4-5 (art 21-24) och sid. 27 (Annex 2 till art. 22-23). Länk:
https://crc.bg/files/Pravna/Pravila_minimalni_iziskvania.pdf

Rumänien har implementerat NIS2 till lag Government Emergency Ordinance No. 155/2024. Länk: https://legislatie.just.ro/public/DetaliiDocument/293121).

I dagsläget saknas sekundär regelgivning med rapporteringströsklar för alla sektorer.

Sannolikt kommer den regulatoriska myndigheten för telekomområdet konsulteras I arbetet med sådana trösklar. Fram till att det finns några nya regler gäller de trösklar som gällde enligt kodexen och uttolkades i Technical Guideline on Incident Reporting under the EECC.

Länder med särskilda rapporteringströsklar för telekomområdet enligt NIS2

Danmark har särskilda rapporteringströsklar enligt NIS2 för telekomområdet i sekundär regelgivning i Executive Order no. 1069, 7–11 §§. Föreskrifterna innehåller trösklar för vad som utgör betydande incidenter inom telekom och är ett komplement till de bredare trösklarna för alla sektorer under NIS2.

- De använder begreppet ”slutbruger”.
- De har en punkt för tillgänglighet §7.1 och en för RAK § 7.2
- De använder ”brugertimer” som trösklar men det är egentligen samma sak som slutanvändare * antal timmar nere
- De använder mätning på slutanvändare och slutanvändatimmar
- De har med vållad betydande skada för viktiga samhällsfunktioner/särskilda organisationer. Det är försvar, polisen, och särskilda händelser
- De har rapporteringsplikt för om tjänster till ett eller flera länder än Danmark är inte möjlig
- Och om 50 % av kapaciteten hos en operatör är påverkad eller en ö med fler än 1500 personer.

Anmälan till Cybersäkerhetscentralen vid säkerhetsincidenter i Danmark:

§ 7. Leverantörer av NI-ICS -tjänster och allmänt tillgängliga elektroniska kommunikationsnät och kommunikationstjänster ska underrätta centrumet för IT-säkerhet om säkerhetsincidenter som har haft en väsentlig inverkan på driften av nät eller tjänster i form av skador på tillgänglighet till dessa nät och tjänster, lagrade eller överförda eller behandlade data eller tillhörande tjänster som erbjuds av eller är tillgängliga via dessa nät eller tjänster. Jfr 8 §.

(2) Leverantörer av NI-ICS -tjänster och allmänt tillgängliga elektroniska kommunikationsnät och kommunikationstjänster ska underrätta centrumet för cybersäkerhet om säkerhetsincidenter som har haft en väsentlig inverkan på driften av nät eller tjänster i form av en händelse som har haft en faktisk negativ inverkan på nätens och tjänsternas förmåga att motstå åtgärder som är skadliga för konfidentialiteten, riktigheten eller autenticiteten hos dessa nät och tjänster, lagrade,

överförda eller bearbetade uppgifter eller relaterade tjänster som erbjuds av eller är tillgängliga via dessa nätverk eller tjänster, Jfr 9 §.

(3) Anmälningsskyldigheten enligt (1) och (2) uppstår när leverantören får kännedom om att säkerhetsincidenten har haft en väsentlig inverkan på driften av nät eller tjänster (Jfr 8 § eller 9 §. Anmälan ska göras utan onödigt dröjsmål genom den gemensamma digitala lösningen för rapportering till offentliga myndigheter om www.virk.dk.

§ 8. En väsentlig påverkan på driften av nät eller tjänster i form av skada på tillgängligheten enligt 7 § (1), föreligger när berörda användartimmar överstiger något av de gränsvärden som nämns nedan, jfr punkterna 1)-6), jfr dock 5). Påverkade användartimmar avser varaktigheten för säkerhetsincidenten multiplicerat med antalet slutanvändare som påverkas av säkerhetsincidenten.

1) För mobiltelefoni, 35 000 användartimmar.

2) För fast telefoni, 10 000 användartimmar.

3) För internetåtkomst, 10 000 användartimmar.

4) För televisions- och radiosändning av rikstäckande public service-tv och radio, 55 000 användartimmar.

5) För NI-ICS -tjänster, 50 000 användartimmar.

6) För övriga tjänster som inte omfattas av 1) -5), 5 000 användartimmar.

(2) Om säkerhetsincidentens varaktighet inte kan kvantifieras i enlighet med 8 (1) ska konsekvenserna anses vara väsentlig för driften av nät eller tjänster när antalet berörda slutanvändare överstiger ett av följande gränsvärden:

1) För mobiltelefoni, 35 000 slutanvändare.

2) För fast telefoni, 10 000 slutanvändare.

3) För internetåtkomst, 10 000 slutanvändare.

4) För televisions- och radiosändningar av rikstäckande public service-tv och radio, 55 000 slutanvändare.

5) För NI-ICS -tjänster, 50 000 slutanvändare.

6) För övriga tjänster som inte omfattas av 1) -5), 5 000 slutanvändare.

(3) Om antalet berörda slutanvändare inte kan kvantifieras med säkerhet måste leverantörerna göra en kvalificerad uppskattning när de beräknar det.

(4) Inverkan på driften av nät eller tjänster anses också vara väsentlig, om inte annat följer av (5), om

1) Mer än 200 slutanvändare vid försvar, polis eller räddningspersonal har drabbats.

2) Nät och tjänster för nödsituationer eller exceptionella situationer har påverkats på regional eller nationell tjänstenivå.

3) Trafik via nät och tjänster till ett eller flera andra länder än Danmark är inte möjlig.

(4) Mer än 50 % av kapaciteten hos en leverantör av allmänt tillgängliga elektroniska kommunikationsnät och kommunikationstjänster på en ö utan brygga med mer än 1 500 invånare har påverkats.

(5) Oavsett vad som anges i (1) och (4) föreligger inte någon väsentlig inverkan på driften av nät eller tjänster om säkerhetsincidenten varar mindre än en timme.

§ 9. En väsentlig inverkan på driften av nät eller tjänster enligt 7 § (2), föreligger när säkerhetsincidenten i fråga har drabbat mer än 1 000 slutanvändare.

Slutanvändare: en användare av elektroniska kommunikationsnät och kommunikationstjänster som inte på kommersiell grund gör dessa nät och tjänster tillgängliga för andra.

Nödsituationer och andra exceptionella situationer: allvarliga olyckor, katastrofer eller tillbud för vilka det kan bli nödvändigt att vidta särskilda åtgärder som rör nät och tjänster för att upprätthålla samhällets funktion.

Länk: https://www.retsinformation.dk/eli/lta/2025/1069

Tyskland har implementerat NIS2 i nationell lag. Det finns särskilda rapporteringströsklar för energisektorn och för telekomsektorn. Telekomsektorn täcks också av en annan nationell lag (Telecommunications act) vid sidan av den lag som implementerat NIS2.

Verksamhetsutövare inom telekomområdet måste efter implementeringen av NIS2 rapportera incidenter både till den regulatoriska myndigheten för telekom och den nationella myndigheten för cybersäkerhet. Den tyska regulatoriska myndigheten för telekomområdet har specifika incidentrapporteringsregler för telekomområdet i ”section 168 Telecommunications Act (TKG)”.

Länk till rapporteringskonceptet och rapporteringsformuläret:

EntwurfMeldekonzept168TKG.pdf

Sicherheitsvorfall §168 TKG

Grekland har implementerat NIS2-dorektivet och har en myndighetsstruktur med nära samarbete inom just telekomområdet mellan å ena sidan myndigheten för säkra elektroniska kommunikationer, posttjänster och personuppgifter och å andra sidan den nationella cybersäkerhetsmyndigheten.

Myndigheten för säkra elektroniska kommunikationer ska nu uppdatera sina rapporteringströsklar, som i dagsläget rör konfidentialitetsbrister, så att de följer NIS2-direktivet och den nationella cybersäkerhetslagen. De nya rapporteringströsklarna kommer att omfatta brister i konfidentialitet, integritet och tillgänglighet i nätverks- och informationssystem inom telekom. De upphävda trösklarna om konfidentialitetsbrister kommer att utgöra modellen för det arbetet. Länk: https://adae.gov.gr/images/nomothetiko-plaisio/FEK-2024-Tefxos_B-00551_29_01_2024.pdf

Utanför EU

Norge kommer att implementera NIS2-direktivet trots att de inte är medlemmar i EU. Implementeringen kommer att gälla även för telekomområdet, med grund i EES-avtalet.

Redan nu finns rapporteringsregler för att rapportera tillgänglighetsproblem för telekomverksamhetsutövare. Det är följande:

§§ Tillhandahållare ska omedelbart, och senast inom en halvtimme efter att tillhandahållaren fått kännedom om en säkerhetshändelse som har medfört ett väsentligt avbrott i tillgängligheten i elektroniska kommunikationsnät eller elektronisk kommunikationstjänst, underrätta Nasjonal kommunikasjonsmyndighet.

§§ Tillhandahållaren ska omedelbart efter att tillhandahållaren fått kännedom om en säkerhetshändelse som kan medföra ett väsentligt avbrott i tillgängligheten i elektroniska kommunikationsnät eller elektronisk kommunikationstjänst, underrätta Nasjonal kommunikasjonsmyndighet.

§§ Följande händelser ska alltid rapporteras:

a. instabilitet eller bortfall av mer än **hälften av kunderna eller basstationerna** i en **kommun**

b. instabilitet eller bortfall av mer än **hälften av kunderna eller basstationerna** i **tätorter** med fler än **20 000 invånare**

c. instabilitet eller bortfall av mer **än tio procent av kunderna eller basstationerna** på **nationell nivå**

d. instabilitet eller bortfall för **användare med ansvar för liv och hälsa**, eller i situationer som innebär **hög risk för förlust av liv och hälsa**.

Länk till Varsling och rapporterig o hendelser i ekomnett + vejledning

https://nkom.no/sikkerhet-og-beredskap/varsling-og-rapportering-om-hendelser-i-ekomnett

Norge har även föreskriftsregler för att rapportera integritetsincidenter i samma föreskrift.

§§ Kommissionens förordning (EU) nr 611/2013 om åtgärder som ska tillämpas vid rapportering av brott mot personuppgiftssäkerheten, jämförd med Europaparlamentets och rådets direktiv 2002/58/EG om dataskydd för elektronisk kommunikation, gäller som föreskrift med de anpassningar som följer av bilaga XI, protokoll 1 till avtalet och avtalet i övrigt.

Länk till den norska ekomföreskriften (se § 2-8)
https://lovdata.no/dokument/SF/forskrift/2024-12-20-3410/KAPITTEL_2#KAPITTEL_2

Sverige

Se föreslagna föreskrifter för telekomverksamhetutövare och trösklar för betydande incidenter enligt MCF:s föreskrifter för de övriga sektorer som lyder under NIS2-direktivet (exklusive de i sektorn för digital infrastruktur som redan omfattas av Kommissionens Genomförandeförordning).