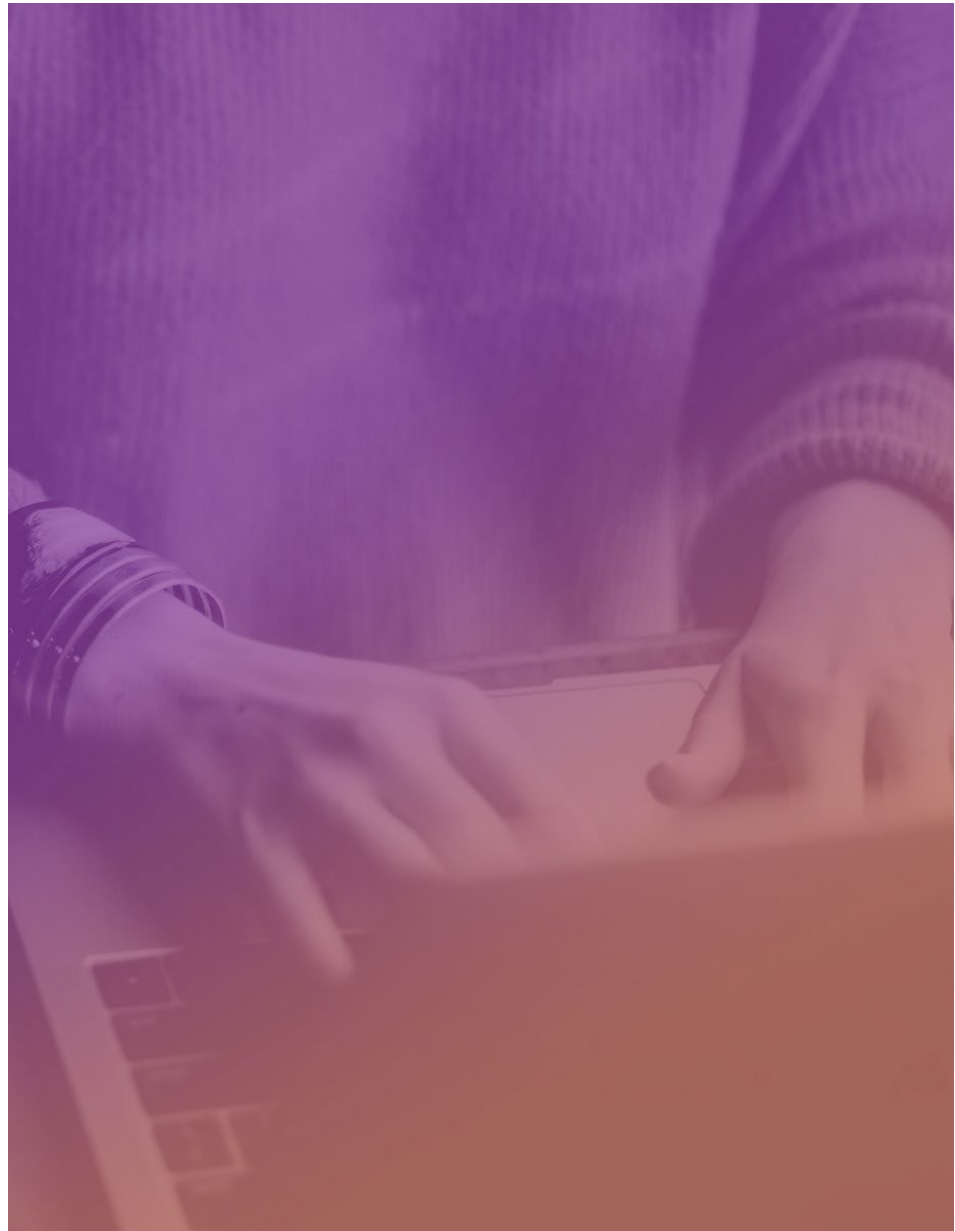


Remissammanställning

Föreskrifter om betydande incidenter inom telekomområdet



Vår referens: Diarienummer 25–19114

Innehåll

1.	Inledning.....	4
2.	Inkomna remissvar	4
3.	Övergripande synpunkter	6
3.1	Allmänt om de föreslagna föreskrifterna och behov av tydliga regler	6
3.1.1	Regler om rapporteringsplikt	7
3.1.2	Bedömning av vad som utgör en betydande incident.....	8
3.1.3	Nya arbetssätt för incidentidentifiering.....	9
3.1.4	Leverantörskedjor – vem ska bedöma en incident.....	10
3.1.5	Begreppet undergräver	11
3.1.6	Begreppet allvarlig driftstörning	12
3.1.7	Antalet rapporteringspliktiga incidenter	13
3.1.8	Nummeroberoende tjänster	14
3.2	Delat föreskriftsmandat mellan PTS och FRA.....	14
3.3	Regelinitiativ inom EU	15
3.4	Ikraftträdande för föreslagna föreskrifter.....	15
3.5	Regelrådets bedömning.....	16
3.6	Beaktande av Sveriges säkerhet vid tillämpning av cybersäkerhetslagen....	16
3.7	Kommerskollegiums bedömning	16
3.8	Synpunkter på alternativ som inte har föreslagits.....	16
4.	Närmare synpunkter på förslaget	17
4.1	Tillämpningsområde	17
4.1.1	Förhållandet till föreskrifter om rapporteringsskyldigheter	17

4.1.2	<i>Planerade arbeten blir planerade förändringar</i>	17
4.2	Ordförklaringar	19
4.2.1	<i>Avsaknad av definitioner</i>	19
4.2.2	<i>Frågor om definitioner</i>	20
4.3	Betydande incidenter.....	28
4.3.1	<i>En incident ska prövas mot samtliga tröskelvärden</i>	28
4.4	Allvarlig driftstörning	29
4.4.1	<i>Tillgänglighetsproblem enligt tabellbestämmelsen</i>	30
4.4.2	<i>Betydande incident i passiva fibernät</i>	35
4.4.3	<i>Betydande skada på riktighet, autenticitet eller konfidentialitet</i>	37
4.4.4	<i>Gränsöverskridande betydande incident</i>	39
4.4.5	<i>Betydande incident på landsbygden</i>	41
4.5	Ekonomisk skada för verksamhetsutövaren.....	42
4.6	Betydande skada för annan än verksamhetsutövaren.....	44
4.6.1	<i>Betydande skada för en viktig samhällsfunktion</i>	44
4.6.2	<i>Betydande skada för nödkommunikation eller på VMA</i>	46
4.6.3	<i>Fysisk persons dödsfall, eller betydande skada på en fysisk persons hälsa</i>	53
4.7	Incidenter som alltid är betydande.....	53
4.7.1	<i>Det remitterade förslaget "identifierad risk för skadeeffekter" flyttas</i>	54
4.7.2	<i>Incidenter som alltid är betydande</i>	55
4.7.3	<i>Tillgänglighetsstörningar till följd av naturkatastrof</i>	56
4.7.4	<i>Intrång och angrepp</i>	58
4.7.5	<i>Betydande incident i central infrastruktur</i>	60
4.8	Återkommande incidenter	63
1.	Avslutning	64

Sammanställning och analys av inkomna remissvar avseende PTS förslag till nya föreskrifter om betydande incidenter inom telekomområdet

1. Inledning

Post- och telestyrelsen (PTS) har den 13 maj 2026 skickat ut ett förslag till nya föreskrifter om vad som utgör betydande incidenter enligt cybersäkerhetslagen (2025:1506) för verksamhetsutövare inom telekomområdet. Remisstiden gick ut den 12 juni 2026. PTS skickade ut förslaget och konsekvensutredning till totalt 234 mottagare, varav 197 verksamhetsutövare, 28 myndigheter och 9 organisationer.

Nedan sammanställs de huvudsakliga synpunkter som framförts i inkomna remissvar, tillsammans med PTS inställning till remissinstansernas synpunkter.

2. Inkomna remissvar

PTS har tagit emot svar från 37 remissinstanser. För att få ett tillräckligt underlag för bedömningar av vilka åtgärder som bör vidtas har PTS i vissa fall ställt kompletterande frågor till remissinstanserna. Remissvaren har i dessa fall kompletterats.

Följande företag, myndigheter och organisationer har lämnat synpunkter på PTS förslag till nya föreskrifter:

1. AC-net
2. Digimitt
3. Energimyndigheten
4. Finansinspektionen
5. Försvarets radioanstalt (FRA)
6. Försvarmakten
7. Google
8. Hi3G Access AB (Tre)
9. Integritetsskyddsmyndigheten
10. Kommerskollegium
11. Konkurrensverket
12. Konsumentverket
13. Krafringen Fiber AB
14. Läke medelsverket
15. Länsstyrelsen Norrbotten
16. Länsstyrelsen Västra Götaland
17. Länsstyrelsen Skåne
18. MittNät AB
19. Myndigheten för civilt försvar (MCF)
20. Myndigheten för delaktighet (MFD)
21. Netsam
22. OneMore Secure
23. Polismyndigheten
24. Regelrådet
25. Sinch
26. SOS Alarm
27. Stokab
28. Svenska kraftnät
29. Svenska stadsnätetsföreningen (SSNF)
30. Sveriges kommuner och regioner (SKR)
31. Säkerhetspolisen
32. Tele2 Sverige AB (Tele2)
33. Telenor Sverige AB (Telenor)
34. Telia Company AB (Telia)
35. Trafikverket
36. Transportstyrelsen
37. Vinnova

Följande remissinstanser (12) har inga synpunkter på, inget att invända mot, inget ytterligare att tillägga eller avstår från att lämna synpunkter på PTS förslag till nya föreskrifter:

Energimyndigheten, Finansinspektionen, FRA, Integritetsskyddsmyndigheten, Konkurrensverket, Konsumentverket, Länsstyrelsen Norrbotten, Länsstyrelsen Västra Götaland, Länsstyrelsen Skåne, Säkerhetspolisen, Transportstyrelsen och Vinnova.

Angående konsekvensutredningen framför Regelrådet i sitt yttrande att konsekvensutredningen är mycket väl genomförd och därmed uppfyller kraven i förordningen (2024:183) om konsekvensutredningar.

3. Övergripande synpunkter

3.1 Allmänt om de föreslagna föreskrifterna och behov av tydliga regler

Sammanfattning av synpunkter: Flera remissinstanser, däribland MCF, Försvarmakten, MFD, OneMore Secure och Tre, är övergripande positiva till föreskrifternas syfte och till att tröskelvärdena görs tydligare och mer förutsebara. Samtidigt framhåller flera remissinstanser, bland annat Digimitt, MittNät, Stadsnätetsföreningen, Telenor och Kraftringen, behovet av förtydliganden, avgränsningar och vägledning om hur bedömningen av vad som utgör en betydande incident ska göras och vad som ska ingå i en verksamhetsutövers kunskapsunderlag i en sådan bedömning. MCF, Transportstyrelsen, Försvarmakten och Tre ser positivt på harmonisering med MCF:s föreskrifter. AC-Net och SKR anser att konsekvensutredningen underskattar de administrativa kostnaderna för efterlevnad och eventuell tillsyn. Google efterfrågar en tydligare anpassning till nummeroberoende interpersonella kommunikationstjänster (NI-ICS). Polismyndigheten betonar vikten av informationsdelning och samverkan mellan berörda av incidenter. Tele2 och Telenor anser att förslaget riskerar att bli komplext, gå längre än vad som följer av lagstiftningen och medföra en ökad administrativ börda. MFD tillstyrker förslaget och framhåller betydelsen av robust elektronisk kommunikation för personer med funktionsnedsättning.

PTS kommentarer och åtgärder: *PTS har med anledning av synpunkterna justerat vissa delar av föreskrifterna. En omstrukturering har gjorts för att ge en tydligare och*

sammanhållen vägledning i föreskrifterna om vad som utgör betydande incidenter, vilka bedömningar som ska göras och vilket informationsunderlag som kan behövas.

Förändringarna innebär att ett nytt inledande kapitel 3 har skapats för att ge vägledning kring vad som utgör betydande incidenter och vilka bedömningar samt informationsunderlag som behövs för att veta vad som utgör betydande incidenter. Det är inte PTS avsikt att göra några materiella ändringar i föreskrifterna, bara att förtydliga och avgränsa bestämmelserna så att ursprungliga syftet med dem framgår.

Det innebär att det i stället är i kapitel 4 de olika kriterierna eller tröskelvärdena för vad som utgör betydande incidenter anges. Kapitel 4 är uppdelat i:

- allvarliga driftstörningar
- ekonomisk skada för verksamhetsutövaren
- betydande skada för annan än verksamhetsutövaren
- incidenter som alltid är betydande
- återkommande incidenter
- undantag vid planerade förändringar

Förändringarna rör sig i övrigt om språkliga förenklingar och om tydligare avgränsningar. Vilka närmare justeringar PTS har gjort framgår av efterföljande avsnitt om de enskilda bestämmelserna i denna sammanställning.

Flera remissinstanser har också efterfrågat exempel på hur reglerna ska tillämpas i praktiken. PTS kommer därför att ta fram frågor och svar, en så kallad FAQ, efter ikraftträdandet samt planerar också för en kommande vägledning som innehåller sådana förtydliganden och exempel.

När det gäller allmän tillämpbarhet har PTS följande kommentarer:

3.1.1 Regler om rapporteringsplikt

Polismyndigheten och Netsam har framfört att föreskrifterna inte innehåller några bestämmelser som tydliggör rapporteringsplikten.

PTS kommentar: Rapporteringsplikten som är knuten till att identifiera betydande incidenter regleras inte av PTS, utan av FRA. Betydande incidenter ska rapporteras till Nationellt cybersäkerhetscenter (NCSC) vid FRA. Inrapporterade incidenter som misstänks ha sin grund i brottslig handling ska vidare rapporteras till Polismyndigheten. Tidpunkter för rapportering av identifierade betydande incidenter regleras i cybersäkerhetslagen (2025:1506) och hur rapporteringen ska gå till och vad den ska innehålla regleras i föreskrifter meddelade av FRA (MCFFS 2026:8): Upplýsing om en betydande incident ska lämnas så snart det kan ske, dock senast inom 24 timmar efter att incidenten identifierats som betydande. Incidentanmälan ska sedan lämnas

så snart det kan ske, dock senast 72 timmar efter att verksamhetsutövaren har identifierat incidenten som betydande. Slutrapport ska slutligen lämnas senast en månad efter incidentanmälan eller en månad efter att incidenten har hanterats (2 kap. MCFFS 2026:8).

3.1.2 Bedömning av vad som utgör en betydande incident

Sammanfattning av synpunkter: Flera remissinstanser har ställt återkommande frågor om hur identifieringen av betydande incidenter ska göras, vilket informationsunderlag som får läggas till grund för bedömningen och hur sannolikhets- och riskbedömningar ska genomföras. Frågor om bedömningsmetodik återkommer både i synpunkter på den generella bestämmelsen i förslagets 3 kap. 1 § och på flera av de enskilda tröskelbestämmelserna. Tre anser dessutom att betydande incidenter som har orsakat skadeeffekter och sådana som kan orsaka skadeeffekter bör behandlas samlat. Flera remissinstanser efterfrågar även ytterligare vägledning och praktiska exempel för att skapa en mer enhetlig tillämpning av föreskrifterna.

PTS kommentarer och åtgärder: PTS konstaterar att remissvaren visar ett tydligt behov av att förtydliga hur identifieringen och bedömningen av vad som utgör betydande incidenter ska göras samt vilket underlag som behövs i bedömningen.

Mot denna bakgrund har föreskrifterna omstrukturerats. Bestämmelser om bedömning, informationsunderlag och identifiering av vad som utgör betydande incidenter har samlats i kapitel 3. Enskilda bedömningsregler som i förslaget låg i tröskelbestämmelserna har flyttats till kapitel 3. Syftet är att skapa gemensamma bedömningsregler för vad som utgör betydande incidenter som gäller för samtliga bestämmelser i föreskrifterna och därigenom underlätta en enhetlig och förutsebar tillämpning.

I nya 3 kap. 1 § tydliggörs att bedömningen ska utgå från den information som verksamhetsutövaren faktiskt har tillgång till, har fått kännedom om eller rimligen kan inhämta. Bestämmelsen tydliggör även liksom i förslaget att bedömningen ska göras utifrån samtliga relevanta bestämmelser i föreskrifterna.

Verksamhetsutövaren ska enligt 3 kap 1 § tredje stycket, om det inte går att ange exakt, uppskatta hur stora effekterna av en incident är. PTS har dock förståelse för att det inte alltid kan göras en relevant uppskattning. Det kan till exempel för vissa aktörer i leverantörskedjorna vara svårt att veta hur många slutanvändare som har drabbats av en incident. Därför är bestämmelsen om uppskattningar formulerad med viss flexibilitet. Verksamhetsutövaren ska göra en uppskattning utifrån det underlag denne har eller rimligen kan inhämta enligt 3 kap 1 § första stycket. Finns inte någon kunskap, inga rimliga kontakter att ta eller andra kontroller att göra, till exempel av information på hemsidor hos partners i leverantörskedjan, kan det betyda att

verksamhetsutövaren inte kan, och därför inte ska, göra en uppskattning. Utgångspunkten är dock att verksamhetsutövaren ska försöka göra en uppskattning.

PTS inför även 3 kap. 2 § som tydliggör att betydande incidenter kan bestå av tre olika typer av händelser:

1. händelser som medför påverkan eller konsekvenser enligt föreskrifterna,
2. betydande cyberhot eller betydande sårbarheter som innebär en risk som sannolikt kan orsaka, bidra till eller möjliggöra påverkan eller konsekvenser enligt föreskrifterna, och
3. annan upptäckt risk eller händelse som sannolikt kan orsaka, bidra till eller möjliggöra påverkan eller konsekvenser enligt föreskrifterna.

PTS bedömer att denna struktur är tydligare och mer rättssäker än alternativet att slå samman samtliga incidenttyper som har orsakat eller kan orsaka skadeeffekter i samma bestämmelser. Den valda lösningen skapar en tydligare systematik än i förslaget och gör det lättare att förstå att även händelser, betydande cyberhot och betydande sårbarheter är betydande incidenter om de innebär tillräckligt höga risker för skadeeffekter enligt föreskrifterna.

För att ytterligare stödja tillämpningen av föreskrifterna avser PTS att publicera FAQ och vägledning. I takt med att PTS bedriver tillsyn kommer även sådana beslut att kunna ligga till grund för ytterligare vägledning.

3.1.3 Nya arbetssätt för incidentidentifiering

Sammanfattning av synpunkter: OneMore Secure, SKR, Tele2 och Telenor har framhållit att föreskrifterna innehåller bestämmelser som kräver kvalificerade bedömningar snarare än enbart teknisk mätning. Remissinstanserna framhåller att detta innebär mer komplexa bedömningar, större behov av olika kompetenser och en ökad arbetsinsats jämfört med tidigare. Telenor betonar särskilt att incidentrapporteringen inte får inverka negativt på verksamhetsutövarens arbete med att avhjälpa incidenter.

PTS kommentarer och åtgärder: PTS har förståelse för synpunkten att incidenthantering och återställning måste prioriteras under ett pågående incidentförlopp. Avsikten är inte att identifiering av betydande incidenter ska fördröja åtgärder för att begränsa eller avhjälpa en incident.

PTS konstaterar samtidigt att NIS2-direktivet och definitionerna av incident, betydande incident och betydande cyberhot i cybersäkerhetslagen innebär att alla betydande incidenter inte längre kan identifieras enbart genom teknisk övervakning av nät och tjänster. Det överordnade regelverket omfattar även händelser som orsakar ekonomisk skada, betydande skada för andra eller risker för sådana

konsekvenser. Detta innebär att bedömningen i vissa fall måste grundas på annan information än traditionell teknisk drift- och övervakningsdata.

PTS bedömer därför att verksamhetsutövare kan behöva involvera ytterligare kompetenser i arbetet med att identifiera betydande incidenter och att nya organisatoriska rutiner krävs. Bedömningen behöver inte nödvändigtvis göras av den personal som ansvarar för den dagliga nätövervakningen eller tekniska driften. Även intern information av annat slag än monitoreringsdata samt extern information från exempelvis kunder, myndigheter eller andra källor behöver beaktas för att ha förmåga att bedöma eller identifiera om det har inträffat en betydande incident enligt cybersäkerhetslagen.

Utvecklingen är inte heller helt ny. Redan genom de ändringar av rapporteringsreglerna som genomfördes 2022 till följd av den så kallade kodexen¹ och ändringar i lagen (2022:482) om elektronisk kommunikation (LEK) utvidgades bedömningsunderlaget till att omfatta fler omständigheter än enbart tillgängligheten i nät och tjänster.

PTS bedömer att den föreslagna incidentidentifieringen ligger i linje med cybersäkerhetslagens syfte att uppnå en hög cybersäkerhetsnivå och med NIS2-direktivets betoning av tidig identifiering och rapportering av betydande incidenter. I likhet med den vägledning som tagits fram till MCFFS 2026:8 ska kravet förstås som att verksamhetsutövaren skyndsamt ska påbörja processen för att bedöma om en incident är betydande, inte att en slutlig bedömning måste vara färdigställd i realtid.

PTS bedömer sammantaget att kraven på kvalificerade bedömningar och användning av relevanta informationskällor är proportionerliga och nödvändiga för att säkerställa korrekta bedömningar enligt cybersäkerhetslagen och de föreslagna föreskrifterna.

3.1.4 Leverantörskedjor – vem ska bedöma en incident

Några remissinstanser har väckt frågan om vilken eller vilka verksamhetsutövare i en leverantörskedja som ska göra bedömningen av om en betydande incident har inträffat.

PTS kommentar: PTS vill förtydliga att samtliga berörda verksamhetsutövare ska göra en självständig bedömning av om en betydande incident har inträffat. En och samma händelse kan därför vara en betydande incident för flera verksamhetsutövare i en leveranskedja av nät, tjänster eller uppgifter. En verksamhetsutövare kan inte utgå från att en leverantör, kund, tillhandahållare av slutkundstjänster eller samhällsviktig kund övertar ansvaret för bedömningen av om en incident är betydande. Detta

¹ EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation.

betyder att samma händelse ska bedömas av samtliga verksamhetsutövare som har drabbats, utifrån hur incidenten har påverkat den egna driften, de egna kunderna, slutanvändarna osv. Observera att "driften" inkluderar tillgänglighet, riktighet, autenticitet och konfidentialitet i nät, tjänster och uppgifter. Verksamhetsutövarna har alla olika perspektiv av händelser, betydande cyberhot, betydande sårbarheter, incidenter och dess skadeeffekter och tillsammans bildar informationen en helhetsbild av incidenten i hela leverantörskedjan. Det finns ett tydligt fokus på säkerhet i leverantörskedjan i både NIS2-direktivet och cybersäkerhetslagen. Något som inte går att uppfylla utan kunskapsöverföring genom leverantörskedjan.

Detta innebär inte någon egentlig förändring i förhållande till tidigare reglering om rapportering av säkerhetsincidenter, men PTS vill förtydliga att detta ansvar har gällt sedan tidigare och alltså gäller.

3.1.5 Begreppet undergräver

Flera remissinstanser har haft synpunkter på användningen av ordet undergräver som beskrivande ord för all slags negativ påverkan på tillgänglighet, riktighet, autenticitet eller konfidentialitet i föreskrifterna. Remissinstanserna föreslår alternativa formuleringar som är lättare att förstå.

PTS kommentar och åtgärd: Ordet undergräver är det ord som används i cybersäkerhetslagens definition av begreppet incident (1 kap. 2 § 10). En incident definieras där som en händelse som **undergräver** tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem. Uttrycket "undergrävd tillgänglighet" ersätter på så vis det tidigare använda begreppet "störningar och avbrott" i nät och tjänster.

Det är det engelska ordet **compromise** i definitionerna för säkerhet i nätverks- och informationssystem, incident och tillbud i NIS2-direktivet som har översatts till det svenska ordet undergräver.

PTS bedömer att det är viktigt att använda samma terminologi som i överordnade regelverk. Att ersätta ordet med ett annat, förvisso kanske bättre ord, skulle kunna skapa oklarheter om vad som avses med en incident enligt cybersäkerhetslagen och om vad som är säkerhet i nätverks- och informationssystem enligt NIS2-direktivet.

Enligt Svenska Akademiens ordböcker är synonymerna till att undergräva att förstöra, förhindra och underminera.

Synpunkterna på begreppet undergrävd föranleder därför ingen ändring.

3.1.6 Begreppet allvarlig driftstörning

Tre och Tele2 önskar att betydande incidenter som anses vara en allvarlig driftstörning endast ska omfatta händelser som påverkat tillgängligheten till nät och tjänster negativt.

PTS kommentar: *PTS konstaterar angående begreppet allvarlig driftstörning att begreppet driftstörning omfattar, precis som i tidigare gällande regler i kodexen, LEK och PTS nu upphävda föreskrifter, mer än bara tillgänglighet i nät och tjänster. Begreppet driftstörning omfattar samtliga relevanta säkerhetsaspekter, d.v.s. tillgänglighet, riktighet, autenticitet och konfidentialitet i nät och tjänster – och utöver det även för lagrade, överförda eller behandlade uppgifter. 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 i nät, tjänster eller lagrade, överförda eller behandlade uppgifter. Det finns dock en tydlig tradition inom telekområdets incidenthantering som tidigare enbart har fokuserat på störningar och avbrott, alltså på tillgänglighetsproblem, i nät och tjänster. Den traditionen har levt kvar sedan de ursprungliga incidentrapporteringsreglerna infördes i LEK genom en lagändring 2012, med följd därefter även i PTS första föreskrifter om incidentrapportering för telekområdet, som infördes samma år. Den gamla begreppsanvändningen av ordet driftstörning vidgades redan 2022 genom kodexen och LEK. Branschen har haft flera år på sig att anpassa sin tillämpning till denna förändring. Begreppet driftstörning kan därför inte längre förstås som begränsat till enbart tillgänglighetsproblem.*

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.”²

3.1.7 Antalet rapporteringspliktiga incidenter

Tele2 och Telenor har uppfattat att regeringen i propositionen till cybersäkerhetslagen har bedömt att antalet identifierade rapporteringspliktiga incidenter inte ska öka med cybersäkerhetslagens krav och definitioner. Polismyndigheten å andra sidan lyfter fram att föreskrifterna antas kunna öka de berörda myndigheternas samlade kännedom om allvarliga telekomincidenter, vilket är positivt.

PTS kommentar: PTS delar inte den tolkning som Tele2 och Telenor gör av regeringens uttalande i propositionen. Cybersäkerhetslagen innebär ett bredare och mer detaljerat ramverk för identifiering av betydande incidenter. Bland annat omfattas incidenter som har skadat verksamhetsutövarens säkerhetsförmåga och som kan leda till skadeeffekter, incidenter som orsakat ekonomisk skada för verksamhetsutövaren samt incidenter som vållat betydande skada för andra.

Definitionerna av incident och betydande incident i cybersäkerhetslagen, tillsammans med genomförandeförordningens regler och FRA:s föreskrifter om betydande incidenter, utgör PTS utgångspunkter för dessa föreskrifter.

Det regeringen bedömer i propositionen är att rapporteringsskyldigheten inom telekomområdet i allt väsentligt kommer att avse samma slags incidenter som tidigare. Det rör sig om samma grundläggande kategorier av säkerhetshändelser som LEK från 2022 omfattade, det vill säga händelser som påverkar tillgänglighet, riktighet, autenticitet eller konfidentialitet i nät, tjänster och uppgifter, och även skador på samhällsfunktioner. Det är nu efter cybersäkerhetslagens ikraftträdande ännu tydligare att incidenter, betydande cyberhot och betydande sårbarheter som vållat betydande skador för andra än verksamhetsutövaren ska bedömas.

Att samma slags incidenter omfattas innebär dock inte att antalet incidenter som identifieras som betydande kommer att vara oförändrat. Tvärtom bedömer PTS att fler incidenter nu kommer att identifieras som betydande. Detta följer bland annat av att ekonomiska skadeverkningar, betydande skador för andra och incidenter som ännu inte har lett till skadeeffekter men som kan göra det omfattas av regelverket. Detta kan i sin tur medföra att fler incidenter behöver rapporteras till myndigheter.

PTS bedömer därför att föreskrifterna inte behöver ändras med anledning av dessa synpunkter.

² Prop. 2021/22:136 s. 319–320.

3.1.8 Nummeroberoende tjänster

Google har föreslagit att tröskelvärdena skulle gynnas av att skilja på regler mellan traditionella elektroniska kommunikationsnät och mjukvarudrivna NI-ICS. En sådan anpassning av tröskelvärden specifikt för NI-ICS skulle göra det möjligt för PTS att mer effektivt fokusera på incidenter i kritisk infrastruktur, samtidigt som onödiga administrativa bördor undviks för både myndigheten och leverantörer av digitala tjänster.

PTS kommentar: Föreskrifterna utgår inte från den tekniska lösningen eller antal användare eller slutanvändare som en verksamhetsutövare har, utan ifrån näten, tjänsterna och uppgifternas tillgänglighet, riktighet, autenticitet och konfidentialitet, och påverkan på främst slutanvändare, användare och viktiga samhällsfunktioner, inte från den tekniska lösningen. Användandet av NI-ICS ökar och användningsområdet förändras över tid. NI-ICS utgör redan i dag en integrerad del av den elektroniska kommunikationsinfrastrukturen. Särskilda eller högre tröskelvärden för NI-ICS skulle riskera att skapa ojämlikhet och bristande jämförbarhet i rapporteringen samt försvåra för tillsyn.

PTS delar mot den bakgrunden inte uppfattningen att tröskelvärdena bör skilja mellan mer traditionella elektroniska kommunikationsnät eller tjänster och NI-ICS. PTS inför därför inte särskilda trösklar för NI-ICS.

3.2 Delat föreskriftsmandat mellan PTS och FRA

Trafikverket har uttryckt oro för verksamhetsutövare som kan omfattas av FRA:s föreskrifter om rapportering av betydande incidenter (MCFFS 2026:8³) i en roll, men samtidigt omfattas av dessa föreskrifter i egenskap av verksamhetsutövare inom telekomsektorn. Trafikverket framhåller att analysen av vilket regelverk som ska tillämpas riskerar att ta fokus från den operativa incidenthanteringen. Trafikverket har vidare anförts att myndigheten har få mottagare av telekomtjänster och att de mer generella kriterierna i MCFFS 2026:8 därför är enklare att tillämpa. Mot denna bakgrund efterfrågar Trafikverket ett enkelt och tydligt stöd för att verksamhetsutövare ska kunna rapportera betydande incidenter enligt rätt regelverk.

PTS kommentar: Enligt PTS kännedom medger det incidentrapporteringsverktyg som används av FRA och Nationellt cybersäkerhetscenter (NCSC) att verksamhetsutövare kan ange vilken eller vilka föreskrifter som en betydande incident omfattas av. Det är

³ Vid ikraftträdandet av cybersäkerhetslagen och cybersäkerhetsförordningen var det MCF som hade rätt att meddela föreskrifter om rapporteringen. Den föreskriftsrätten övergick den 1 juli 2026 till FRA i samband med övergången av NCSC.

således möjligt att markera flera regelverk samtidigt och därigenom få de följdfrågor som är relevanta enligt respektive föreskrift.

För verksamhetsutövare som bedriver verksamhet inom flera sektorer enligt cybersäkerhetslagen innebär regelverket dock att en inledande bedömning behöver göras av i vilken roll eller vilka roller verksamhetsutövaren har drabbats av den betydande incidenten. Verksamhetsutövaren behöver därför först fastställa inom vilken eller vilka verksamheter som incidenten har inträffat i och vilket eller vilka regelverk som därmed är tillämpliga. Om incidenten exempelvis endast har inträffat i ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst som verksamhetsutövaren tillhandahåller ska bedömningen göras utifrån de sektorsspecifika regler som gäller för telekomsektorn. Den betydande incidenten kan också beröra andra verksamheter som verksamhetsutövaren bedriver och som omfattas av cybersäkerhetslagen. Det är då viktigt att verksamhetsutövaren identifierar om flera sektorsspecifika regler aktualiseras.

3.3 Regelinitiativ inom EU

Inga synpunkter har kommit in.

PTS kommentar: PTS bedömer att nu föreliggande och eventuella kommande regelinitiativ inom EU för närvarande inte påverkar vilka verksamhetsutövare som omfattas av föreskrifterna eller kriterierna för identifiering av betydande incidenter inom telekomområdet. Om framtida förändringar i EU-regelverk skulle motivera justeringar av föreskrifterna får sådana övervägas i ett senare skede. Detta påverkar dock inte behovet av föreskrifterna i nuläget.

3.4 Ikraftträdande för föreslagna föreskrifter

Inga synpunkter har kommit in.

PTS kommentar: Föreskrifterna kompletterar och förtydligar skyldigheter enligt cybersäkerhetslagen, som trädde i kraft i januari 2026, och syftar till att säkerställa en lagelig och enhetlig identifiering av betydande incidenter inom telekomområdet. Föreskrifterna om rapportering av betydande incidenter (MCFFS 2026:8) trädde i kraft den 1 juli 2026. För att det samlade regelverket ska kunna tillämpas på avsett sätt bedömer PTS att dessa föreskrifter bör träda i kraft den 16 oktober 2026.

3.5 Regelrådets bedömning

Regelrådet finner att PTS konsekvensutredning uppfyller kraven i förordningen (2024:183) om konsekvensutredningar. Se regelrådets bedömning i deras ärende, RR 2026-119.

3.6 Beaktande av Sveriges säkerhet vid tillämpning av cybersäkerhetslagen

Inga synpunkter har kommit in.

3.7 Kommerskollegiums bedömning

Kommerskollegium delar PTS bedömning att förslaget inte behöver anmälas till kollegiet enligt förordning (1994:2029) om tekniska regler eftersom det inte utgör tekniska föreskrifter och inte heller enligt förordning (2009:1078) om tjänster på den inre marknaden eftersom förslaget omfattas av undantaget för elektroniska kommunikationstjänster.

3.8 Synpunkter på alternativ som inte har föreslagits

Telenor har efterlyst en mer harmoniserad implementering jämfört med Danmark och Finland samt en mer minimalistisk reglering.

PTS kommentar: *PTS delar inte uppfattningen att de föreslagna svenska föreskrifterna avviker i någon avgörande utsträckning från motsvarande reglering i de nordiska länder som redan har genomfört NIS2-regelverket i specifika föreskrifter för telekomområdet. I Finland har det dock inte ännu meddelats några sektorsspecifika föreskrifter som reglerar identifiering av betydande incidenter inom telekom, men den finska regulatoriska myndigheten Traficom avser att göra det.*

Danmarks motsvarande föreskrifter om säkerhet och beredskap i telekomsektorn⁴ innehåller flera bestämmelser om trösklar för betydande incidenter som i sak motsvarar de kriterier och bedömningar som föreslås i PTS föreskrifter. Exempelvis omfattar den danska regleringen krav på bedömningar av antalet berörda slutanvändare, incidenter som påverkar lagrade, överförda eller behandlade uppgifter, incidenter som påverkar riktighet, autenticitet eller konfidentialitet, särskilda bedömningar av påverkan på försvars-, polis- och räddningsverksamhet, påverkan på

⁴ Bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed og beredskab i telesektoren, BEK nr 1069 af 27/08/2025, Ministeriet for Samfundssikkerhed og Beredskab. Länk 260714: [Exekutivorder om informations- og underrettelseskyldigheder rørende sikkerhed og beredskab ved nødsituationer inom telekommunikationssektorn](#)

nödkommunikation, internationell trafik samt krav på informationsinhämtning från andra telekomaktörer som använder verksamhetsutövarens nät. Den danska regleringen bygger, i likhet med de föreslagna svenska föreskrifterna, på att verksamhetsutövaren i vissa fall behöver göra kvalificerade bedömningar av incidentens konsekvenser för andra – och det finns i Danmark en uttrycklig bestämmelse om krav på att inhämta information från andra verksamhetsutövare i leverantörskedjorna. PTS bedömer därför inte att jämförelsen med Danmark ger stöd för uppfattningen att en mer minimalistisk reglering utan sådana bedömningar skulle vara tillräcklig för att uppfylla kraven enligt NIS2-direktivet och cybersäkerhetslagen.

PTS bedömer mot denna bakgrund att föreskrifterna inte behöver ändras i detta avseende.

4. Närmare synpunkter på förslaget

Flera remissinstanser har haft synpunkter på ordval och också föreslagit förtydliganden i föreskrifterna för att skapa större tydlighet. PTS har genomfört justeringar i föreskriftstexten mot bakgrund av dessa synpunkter, i syfte att avgränsa reglerna tydligare, och redovisar de mest relevanta nedan.

4.1 Tillämpningsområde

4.1.1 Förhållandet till föreskrifter om rapporteringsskyldigheter

MCF och SKR har påpekat att hänvisningen till föreskrifter om rapporteringsplikten för betydande incidenter enligt cybersäkerhetslagen, som numer FRA meddelar bör ändras.

PTS kommentar och åtgärd: *PTS ändrar bestämmelsen så att den hänvisar till bemyndigandet i cybersäkerhetsförordningen i stället för till en specifik myndighet eller ett visst föreskriftsnummer. En sådan lösning är mer långsiktigt hållbar och innebär att bestämmelsen inte behöver ändras om ansvarig myndighet meddelar nya eller ändrade föreskrifter.*

4.1.2 Planerade arbeten blir planerade förändringar

Sammanfattning av synpunkter: Stadsnätetsföreningen, OneMore Secure och andra remissinstanser är positiva till bestämmelsen men efterlyser en tydligare koppling till

verksamhetsutövarens interna risk- och förändringsanalyser inför planerade arbeten och förändringar. De ber även om exempel på vad som kan anses vara "oförutsedda" negativa konsekvenser av planerade arbeten. Telenor och Tre efterfrågar även ett förtydligande av hur uppgifter kan omfattas av bestämmelsen om planerade förändringar. Flera remissinstanser tycks missförstå syftet att skapa ett undantag från vad som ska bedömas utgöra betydande incidenter.

PTS kommentar och åtgärd: *Bestämmelsen syftar till att utgöra ett undantag från tröskelvärdena för betydande incidenter. Förväntade störningar som har identifierats och bedömts inom ramen för dokumenterade risk- och förändringsanalyser ska inte i sig leda till bedömningen att en betydande incident anses ha inträffat, även om de förväntade störningarna och effekterna når upp till något av tröskelvärdena i föreskrifterna. Bestämmelsen tar sikte på situationer där verksamhetsutövaren före den planerade förändringen har genomfört en riskanalys och har förutsett eller skäligen borde ha kunnat förutse vissa skadeeffekter, men det vid genomförandet har inträffat andra effekter och händelser, eller andra nivåer av effekter, som inte har förväntats i analyserna och som dessutom överskrider minst ett av tröskelvärdena i föreskrifterna. Liksom för all bedömning av vad som utgör en betydande incident ska effekterna bedömas mot samtliga tröskelvärden i föreskrifterna.*

Detta leder till att endast oförutsedda negativa konsekvenser som varken har förutsetts eller skäligen har bort kunnat förutses inom ramen för den genomförda riskanalysen, och som når upp till något av tröskelvärdena i 4 kap. utgör en betydande incident. Bedömningen ska göras enligt bestämmelserna i 3 kap.

Exempel på konsekvenser som ska anses vara sådana oförutsedda negativa konsekvenser kan inte generellt beskrivas i en vägledning, såsom efterfrågats i remissvar. Konsekvenserna är kopplade till vad som har förutsetts eller skäligen kunnat eller bort förutses i verksamhetsutövarens riskanalyser före det att förändringen eller arbetet utförs. Riskanalyserna ska genomföras enligt PTS säkerhetsföreskrifter. Det går inte att överdriva riskerna i en analys för att undgå eventuell identifiering av betydande incidenter.

Planerade förändringar avseende uppgifter:

PTS ser behov av att förtydliga att undantaget, liksom föreskrifterna i övrigt, ska tillämpas utifrån cybersäkerhetslagens definitioner av incident och betydande incident. Det innebär att undantaget omfattar planerade förändringar som avser både nät, tjänster och också uppgifter som lagras, överförs eller på annat sätt behandlas.

Om uppgifter undantogs från bestämmelsens tillämpningsområde finns en risk att bestämmelsen uppfattas som begränsad till sådana tröskelvärden som uttryckligen avser nät och tjänster. En sådan tolkning skulle vara alltför snäv i förhållande till

föreskrifternas syfte och de överordnade regelverken. Undantaget ska därför även omfatta planerade förändringar som avser uppgifter, exempelvis migrering av abonnentuppgifter eller andra uppgifter som omfattas av föreskrifterna.

En remissinstans har anført att förändringsarbeten inte utförs i uppgifter utan att det är en planerad hantering av uppgifterna som riskanalyseras. PTS delar uppfattningen att det är den planerade behandlingen som är föremål för riskanalys. I den analysen ingår dock även vad som kan hända med uppgifterna under den planerade hanteringen. Om en planerad förändring leder till en oförutsedd skadeeffekt som medför att uppgifter exempelvis försvansas, förstörs eller röjs, ska det bedömas om någon av föreskrifternas trösklar har eller kan överskridas. Om så är fallet kan händelsen utgöra en betydande incident.

PTS flyttar bestämmelsen till slutet av 4 kap. för att tydliggöra att den utgör ett undantag från de övriga bestämmelserna i kapitlet.

PTS ändrar även uttrycket planerade arbeten till planerade förändringar. Samtidigt utgår formuleringen nät, tjänster eller uppgifter ur bestämmelsen eftersom dessa "säkerhetsområden" redan omfattas av cybersäkerhetslagens definitioner av incident och betydande incident. Bestämmelsen omfattar därmed även förändringar som avser sådana uppgifter som omfattas av definitionen av uppgifter i 2 kap. 1 §.

Bestämmelsen kompletteras också för att tydliggöra sambandet mellan oförutsedda negativa konsekvenser och verksamhetsutövarens riskanalyser inför den planerade förändringen.

4.2 Ordförklaringar

MCF har påpekat att det är otydligt var en ordförklaring slutar och en annan börjar, och efterfrågar därför en bättre struktur på uppställningen.

PTS kommentar och åtgärd: PTS instämmer med MCF:s synpunkt. Dessutom är cybersäkerhetslagens definitioner uppställda med numrerade punkter. Ord och ordförklaringar ställs upp tydligare i föreskrifterna med numrerade punkter.

4.2.1 Avsaknad av definitioner

Några remissinstanser har framfört att det i 2 kap. saknas några definitioner. Det rör främst begreppen organisationskund och landsbygds- eller glesbygdskommun.

MCF anser också att begreppen användare och slutanvändare ska definieras i föreskrifterna.

PTS kommentarer och åtgärd: Användare och slutanvändare är definierade i lagen om elektronisk kommunikation och föreskrifterna hänvisar till dem.

PTS lägger till begreppen:

- företagskund, i stället för organisationskund och
- landsbygds kommun, i stället för glesbygds- och landsbygds kommun.

4.2.2 Frågor om definitioner

Några remissinstanser har givit förbättringsförslag till de definitioner som finns i 2 kap. PTS går igenom det mest relevanta kring frågorna om definitionerna här.

4.2.2.1 Aktiva anslutningar

Telenor har efterfrågat ett förtydligande av hur aktiva anslutningar ska beräknas när en tillgång eller förbindelse används som insatsvara för andra tillhandahållare av elektroniska kommunikationstjänster.

PTS kommentar: Begreppet aktiva anslutningar är inte nytt. Det infördes 2018 genom säkerhetsföreskrifterna i PTSFS 2018:4. PTS avser inte att ge begreppet någon annan innebörd i dessa föreskrifter än den som kommer att följa av PTS nya säkerhetsföreskrifter enligt cybersäkerhetslagen. Frågor om hur aktiva anslutningar ska beräknas eller avgränsas kan därför inte avgöras inom ramen för detta föreskriftsarbete.

I konsekvensutredningen till de sedan längre upphävda föreskrifterna i PTSFS 2018:4 förklarades begreppet för kännedom aktiv anslutning så här. Denna äldre tolkning kan dock komma att förändras:

Enligt trösklarna i 8 § i föreskrifterna är antalet drabbade abonnenter en av de konsekvenser som kan föranleda att en incident kommer upp i tillräcklig nivå för att den ska rapporteras till PTS. I PTS driftsäkerhetsföreskrifter, används begreppet aktiva anslutningar för att bedöma betydelsen av en viss tillgång i ett elektroniskt kommunikationsnät. Begreppet anses på ett mer rättvisande sätt än andra möjliga begrepp, kunna användas för att kvantifiera omfattningen av de som är drabbade av inträffade driftstörningar liksom vilka tillhandahållare som är skyldiga att rapportera inträffade incidenter. Det är vidare en fördel att använda samma begrepp som i driftsäkerhetsföreskrifterna när det gäller kvantifiering av omfattningen av en inträffad störning eftersom en förnyad riskanalys ska ske efter driftstörningar som ska rapporteras enligt 5 § i PTS driftsäkerhetsföreskrifter.

Definitionen av aktiv anslutning anger att anslutningen ska kopplas till ett allmänt tillgängligt kommunikationsnät eller allmänt tillgänglig elektronisk kommunikationstjänst. Det innebär att anslutningar inom ett nät eller en tjänst som inte är allmänna, inte omfattas av föreskrifterna. Detta gäller exempelvis antalet användare bakom en företagsväxel, så länge dessa användare endast är anslutna till det slutna företagsnätet. Om användarna bakom företagsväxeln i stället använder mobiltelefoner som ansluter till ett allmänt nät, ska dessa

räknas som enskilda aktiva anslutningar i tröskelvärde enligt 8 § i föreskrifterna. För de mobila accessnäten, beräknas antalet aktiva anslutningar som antalet samtidigt möjliga aktiva anslutningar till basstationen, dvs. det maximala antalet samtidigt användare för respektive basstation. En ändring från begreppet kunder till begreppet aktiva anslutningar innebär att det förtydligas att det inte endast är tillhandahållare med abonnenter som omfattas av tröskelvärdena, utan även att till exempel kommunikationsoperatörer omfattas, eftersom dessa i sin verksamhet känner till eller kan ta reda på hur många aktiva anslutningar som de betjänar. Kommunikationsoperatörerna har en överblick i näten som gör att de kan notera störningar och avbrott som drabbar flera tillhandahållare som var för sig kanske inte når upp till en störning som ska rapporteras men det totala antalet drabbade, som kommunikationsoperatörerna ser, leder till en rapport. Detta gör att myndigheten får en bättre överblick av hur statusen i näten är och hur kopplingarna mellan de olika tillhandahållarna ser ut.

Valet av begreppet aktiv anslutning medför även följdändringar i definitionen av kapacitetsbortfall.

PTS bedömer att införandet av begreppet aktiva anslutningar i 2, 5, 7 och 8 §§ i föreskrifterna medför begränsade konsekvenser och kostnader för tillhandahållarna. PTS bedömning är att tillhandahållarna kan komma upp i de nivåer som påkallar incidentrapportering i något större utsträckning än med den tidigare termen abonnent eftersom vissa större organisationer kan ha setts som en abonnent men kan ha flera aktiva anslutningar. Förändringen medför främst konsekvenser för de tillhandahållare som inte har abonnenter men som har aktiva anslutningar, främst kommunikationsoperatörer. Det kommer att vara tydligare när de ska rapportera störningar eller avbrott. Följdändringen i definitionen av kapacitetsbortfall om termen aktiva anslutningar väljs, bedöms inte medföra några konsekvenser för de redan rapporterade tillhandahållarna.

4.2.2.2 Betydande sårbarhet

OneMore Secure har framfört att det bör tydliggöras att en betydande sårbarhet i sig inte utgör en incident och att det finns en risk att definitionen annars kan uppfattas som att föreskrifterna inför en allmän skyldighet att identifiera eller rapportera sårbarheter.

PTS kommentar och åtgärd: *PTS delar uppfattningen att en betydande sårbarhet måste sättas i relation till den påverkan som sårbarheten har eller kan ha på säkerheten i nät, tjänster eller uppgifter. PTS instämmer i att det finns en risk att definitionen kan uppfattas som att föreskrifterna inför en skyldighet att identifiera betydande sårbarheter, utan någon riskbedömning, som betydande incidenter. Det är inte syftet. PTS bedömer inte att problemet med den alltför stora bredden genom "betydande sårbarhet" löses genom en ändring av definitionen. PTS justerar i stället bestämmelsernas struktur och skapar ett enskilt kapitel för att ge vägledning till*

bedömningar av vad som utgör betydande incidenter, inklusive sådana händelser som ännu inte har lett till skedeffekter som kan göra det. Syftet är att förtydliga att betydande sårbarheter behöver ha en sannolik påverkan på säkerheten för att vara en betydande incident. Se mer nedan under avsnittet om den enskilda bestämmelsen om bedömningar av betydande sårbarheter.

Genom dessa ändringar av bestämmelserna tydliggörs att bedömningen ska utgå från både från den betydande sårbarhetens betydelse för säkerheten i nät, tjänster eller uppgifter, exempelvis verksamhetsutövarens kännedom om hur den betydande sårbarheten utnyttjas hos andra, och från verksamhetsutövarens bedömda risk för att sårbarheten leder till sådana effekter som omfattas av föreskrifterna hos verksamhetsutövaren själv. Se mer om den tillhörande bestämmelsen i 3 kap. 1-2 §§ och tillhörande allmänt råd.

4.2.2.3 Kapacitetsbortfall

Trafikverket har påpekat att definitionen av kapacitetsbortfall kan uppfattas som otydlig när det gäller situationer där kapaciteten visserligen finns kvar men har reducerats till en nivå som avviker väsentligt från den normala eller avtalade nivån. Telia anser att bedömningen måste göras i förhållande till något - att kapacitetsbortfallet i sig behöver avgränsas. Telia frågar om bedömningen ska göras i förhållande till en specifik gata, ett område eller en nod.

PTS kommentar och åtgärd: Definitionen av kapacitetsbortfall är ärvd från PTS tidigare säkerhetsföreskrifter, men PTS kommande säkerhetsföreskrifter enligt cybersäkerhetslagen kommer inte att omfatta begreppet. Därför kan definitionen tydliggöras i dessa föreskrifter.

PTS håller med Telia om att det behöver förtydligas vad kapacitetsbortfallet ska bedömas mot. Begreppet är inte nytt och kapacitetsbortfall har alltid bedömts i förhållande till verksamhetsutövarens totala kapacitet och totala antal aktiva anslutningar eller användare av nät eller tjänster. PTS håller även med Trafikverket om att ett kapacitetsbortfall kan bestå i reduktion av kapacitetsnivåer. En bedömning av om en sådan reduktion är tillräcklig för att identifiera ett kapacitetsbortfall ska dock alltid göras av verksamhetsutövaren.

PTS delar alltså bedömningen att definitionen kan förtydligas. Definitionen ändras och förenklas därför. Det beskrivs även i definitionen att kapacitetsbortfall ska bedömas utifrån verksamhetsutövarens totala kapacitet och utifrån verksamhetsutövarens totala antal aktiva anslutningar, användare och slutanvändare.

Se mer om den tillhörande bestämmelsen i 4 kap. 1 § 1 p.

4.2.2.4 *Kritisk internationell, nationell eller regional infrastruktur blir central infrastruktur*

Sammanfattning av synpunkter: Stokab har påpekat att en renodlad svartfiberleverantör endast kan identifiera viss infrastruktur som kritisk enligt definitionen – Knutpunkter i passiva nät kan inte identifieras som kritiska i sig själva. Det behövs ytterligare kunskap om till exempel hur många kunder som har inplacerad utrustning för elektronisk kommunikation i passiva knutpunkter, för att veta om de utgör central infrastruktur. Stokab föreslår därför att definitionen av central infrastruktur kompletteras med ett tillägg med, ”eller knutpunkter i ett passivt allmänt elektroniskt kommunikationsnät där minst 50 organisationskunder har inplacerad utrustning för elektronisk kommunikation.”

PTS kommentar och åtgärd: *Både definitionerna och själva bestämmelsen om betydande incidenter i kritisk infrastruktur, numer central infrastruktur, har avgränsats och förtydligats enligt inkomna remissvar. För att förenkla läggs definitionerna för internationell kritisk infrastruktur och nationell, regional kritisk infrastruktur samman till en definition. Den döps om till central infrastruktur för att inte riskera sammanblandning med CER-direktivets definierade begrepp kritisk infrastruktur. Förändringen åtföljs av en förändring i bestämmelserna i 4 kap. 5 § 3 p och 4 p. Se mer om dessa i avsnitt 4.7.5.*

PTS vill undvika för hög detaljering i föreskrifterna för specifika former av tillhandahållanden och lägger därför inte till det Stokab föreslår som tillägg i definitionen. PTS anser dock att Stokabs förslag är en bra indikation på när passiva knutpunkter ska anses utgöra central infrastruktur, och förslaget är därför användbart för tillhandahållare och inför förtydliganden om hur knutpunkter i passiva nät kan bedömas omfattas av central infrastruktur i FAQ och en planerad kommande vägledning. Se mer om de tillhörande bestämmelserna i 4 kap. 5 § 3 p och 4 p.

4.2.2.5 *Skadlig handling*

SKR har sett att begreppet skadlig handling inte användas i någon bestämmelse och därför bör tas bort. Begreppet hänger samman med förslaget till bestämmelsen i förslagets bestämmelse om en betydande incident som har orsakats av ett angrepp på eller obehörigt intrång i verksamhetsutövarns nät, tjänster eller uppgifter.

PTS kommentar och åtgärd: *Definitionen tas bort och i stället ändras bestämmelsen i om internt eller externt angrepp som bedöms kunna skapa allvarliga driftstörningar. Se mer om den tillhörande bestämmelsen i 4 kap. 5 § 2 p.*

4.2.2.6 Naturkatastrof

Sammanfattning av synpunkter: MCF och SKR har angett att begreppet naturkatastrof beskriver omfattande naturhändelser. MCF önskar att naturolycka som är ett mindre omfattande ord ska användas.

PTS kommentarer och åtgärd: *Naturkatastrofbegreppet skapar avsiktligt ett mycket högt tröskelvärde. Det ska enligt definitionen röra sig om extrema väderförhållanden, jordbävning, översvämning, pandemi, skogs- eller gräsbrand, skred eller liknande, det vill säga extrema naturhändelser, som dels måste ha orsakat omfattande skador på människor, miljö eller egendom, dels måste ha lett till en tillgänglighetsincident hos verksamhetsutövare för att vara en betydande incident enligt den tillhörande bestämmelsen i 4 kap. 5 § 1 p.*

Definitionen ändras endast på så att det förtydligas att det ska röra sig om extrema väderförhållanden, jordbävning, översvämning, pandemi, skogs- eller gräsbrand, skred eller liknande som orsakar omfattande skador för människor, miljö eller egendom. Se mer om den tillhörande bestämmelsen i 4 kap. 5 § 1 p.

PTS kan även komma att ge exempel eller beskriva begreppet mer utförligt i FAQ eller i en vägledning.

4.2.2.7 Viktig samhällsfunktion

MCF föreslår att information om hur och var vägledning kan hittas inte utvecklas i föreskrifterna. MCF föreslår därför att formuleringen "vilka definieras närmare av Myndigheten för civilt försvar" stryks.

PTS kommentar och åtgärd: *PTS delar uppfattningen att närmare information om viktiga samhällsfunktioner lämpligen bör framgå av vägledning från MCF och att PTS i stället kan hänvisa till den i frågor och svar eller en kommande planerad vägledning. Hänvisningen till Myndigheten för civilt försvar tas därför bort från föreskriftstexten. Se mer om den tillhörande bestämmelsen i 4 kap. 4 § 1 p.*

4.2.2.8 Uppgifter

Sammanfattning av synpunkter: OneMore Secure, Svenska Stadsnätetsföreningen och Stokab anser att definitionen av uppgifter, särskilt i punkt 2 i det remitterade förslaget, är alltför bred och riskerar att leda till ett alltför omfattande tillämpningsområde. Stokab efterfrågar även vägledning med konkreta exempel på vilka uppgifter som saknar tillräckligt nära koppling till nät och tjänster för att anses ske i "samband" med tillhandahållande av nät och tjänster, och därför inte bör omfattas av bestämmelserna.

PTS kommentar och åtgärd:

Enligt cybersäkerhetslagens definition av en incident är en incident bland annat en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter. PTS uppdrag är att ge vägledning om när en sådan incident hos uppgifter blir betydande.

PTS konstaterar att all behandling av uppgifter, kan medföra negativ påverkan på såväl nät som tjänster, som uppgifter, eller på andra, eller innebära sådana betydande incidenter som ännu inte nått fram till skadeeffekter men som sannolikt kan göra det.

PTS ser i remissvaren att det finns behov av att skapa klarhet i:

1. vad som omfattas av ordet uppgifter
2. vad som omfattas av hanteringsflödena lagring, överföring eller behandling av uppgifter, och
3. vad som utgör samband med tillhandahållandet av nät och tjänster

vilket sammantaget skulle besvara frågan om hos vilka uppgifter som betydande incidenter kan inträffa.

1. Ordet uppgifter

Inledningsvis kan PTS peka på att "uppgifter", engelskans "data"⁵, är alla uppgifter, inklusive tekniska data, som finns i eller passerar i nätverks- och informationssystem.

Det kan vara exempelvis uppgifter som:

- kunduppgifter,
- abonnentuppgifter,
- trafikuppgifter,
- signaleringsinformation,
- routningstabeller,
- konfigurationsdata,
- autentiseringsuppgifter,
- loggar,
- policyfiler,
- databasinnehåll,
- meddelanden som passerar nätet,
- uppgifter i applikationers arbetsminne,

⁵ Som referens uttrycker den engelska versionen av NIS2-direktivet incidentdefinitionen så här: "Incident means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data [...]"

- uppgifter som bearbetas i realtid i ett system.

Därefter kan det konstateras att det för att en sådan uppgift ska omfattas av föreskrifterna om betydande incidenter inom telekomområdet krävs dels att den lagras, överförs eller på annat sätt behandlas av verksamhetsutövaren, dels att hanteringen har samband med tillhandahållandet av nät eller tjänster. Bedömningen utgår således inte enbart från uppgiften som sådan, utan från dess samband med nät eller tjänster och hur den hanteras.

2. Lagring, överföring eller annan behandling av uppgifter

Samlingsuttrycket "lagras, överförs eller behandlas" är ett vedertaget sätt inom cybersäkerhetsområdet att beskriva uppgiftens tillstånd, dvs hur den hanteras. Uttrycket har förekommit i såväl kodexen som i LEK. Det förekommer i NIS2-direktivet och cybersäkerhetslagen och även i Dataskyddsförordningen. Den svenska översättningen av "data at rest, in transit or in use" till "data som lagras, överförs eller behandlas" kan innebära att det uppstår tolkningssvårigheter då ordet "behandlas" är snarlikt ordet "behandling" på svenska. Att en uppgift behandlas innebär att en människa eller ett system aktivt arbetar med uppgiften, den analyseras, beräknas eller på annat sätt bearbetas.

Vid tolkningen av föreskrifterna om betydande incidenter inom telekom bör därför dock begreppet behandling av uppgifter förstås som ett överordnat begrepp som omfattar olika former av hantering av uppgifter, däribland lagring och överföring.

Detta ligger i linje med cybersäkerhetslagens definition av nätverks- och informationssystem i 1 kap. 2 § 16 c, där definitionen omfattar uppgifter som lagras, behandlas, hämtas eller överförs. De olika uttrycken för hanteringen i definitionen överlappar varandra och beskriver olika former av behandling av uppgifter. Att lagstiftaren uttryckligen nämner flera olika sådana former kan enligt PTS uppfattning dels syfta till att undanröja oklarheter kring vilka slags hanteringar som omfattas av lagen, till exempel även åtkomst till uppgifterna, dels till att synliggöra olika säkerhetsrelaterade riskmoment.

PTS bedömer därför att cybersäkerhetslagens definitioner av incident respektive nätverks- och informationssystem innebär att all hantering av uppgifter omfattas, inklusive läsning eller hämtning av uppgifter.

Dataskyddsförordningen innehåller en definition av begreppet behandling. Definitionen avser personuppgifter, men de exempel på olika former av behandling som anges där kan ge viss vägledning. Till skillnad från dataskyddsförordningen är tillämpningen av föreskrifterna om betydande incidenter i nät eller tjänster inte begränsad till personuppgifter.

3. Sambandet med tillhandahållande av nät eller tjänster

PTS har hittills gjort en vid tolkning av begreppet "samband med tillhandahållandet". Exempelvis har behandling av faktureringsuppgifter och uppgifter som används för kreditupplysning i tillsynsärenden och integritetsincidentrapportering bedömts ha samband med tillhandahållandet av nät och tjänster. Även loggdata och återställningsdata kan omfattas.

Genom PTS erfarenheter av incidentrapportering inom telekomområdet, tillsammans med de synpunkter som lämnats under remissen, är myndigheten medveten om att det finns behov av exemplifiering av vad som utgör "samband med tillhandahållandet"

PTS har dock efter remissen valt att hålla begreppet uppgifter mer övergripande än i det remitterade förslaget. Det kan framöver uppstå behov av ytterligare avgränsningar eller förtydliganden av begreppet i föreskrifterna om betydande incidenter, men PTS bedömer att underlag för sådana ställningstaganden ännu saknas.

PTS åtgärd: "Behandling av uppgifter" tas bort ur definitionerna i föreskrifterna. Definitionen av uppgifter görs samtidigt mer övergripande.

Det finns fortsatt behov av vägledning, särskilt avseende vilka former av behandling eller vilket samband med nät eller tjänster som inte omfattas av föreskrifterna. PTS avser därför att vid behov ta fram ytterligare vägledning, exempelvis genom FAQ, handbok eller genom tillsynsverksamhet.

4.2.2.9 Organisationskund blir företagskund

Telenor har efterlyst ett förtydligande av begreppet organisationskund.

PTS kommentar och åtgärd: PTS instämmer i att begreppet organisationskund behöver definieras närmare. Begreppet ersätts med företagskund och en definition införs i föreskrifterna. Med företagskund avses i dessa föreskrifter företag, myndigheter och andra organisationer som har flera slutanvändare knutna till den köpta tjänsten. Begreppet omfattar därmed kunder i företags- och organisationsled där den köpta tjänsten används av flera slutanvändare inom den egna organisationen. I den tillhörande bestämmelsen i 3 kap. 2 § 3 p, där begreppet används är det inte lämpligt att använda begreppet användare enligt 1 kap. 7 § LEK, eftersom användarbegreppet omfattar aktörer som efterfrågar en allmänt tillgänglig elektronisk kommunikationstjänst utan att ännu vara kund samt också aktörer som köper en tjänst för tillhandahållande i en leveranskedja.

PTS ersätter därför begreppet organisationskund med företagskund och inför en definition av begreppet. Syftet med ändringen är att tydliggöra bestämmelsens tillämpningsområde. Se mer om den tillhörande bestämmelsen i 4 kap.1 § 5 p.

4.2.2.10 Glesbygds- och landsbygdskommun blir landsbygdskommun

Sammanfattning av synpunkter: Ett flertal remissinstanser har påpekat att det behövs en definition av vad som utgör en landsbygds- eller glesbygdskommun.

PTS kommentar och åtgärd: *PTS instämmer att begreppet landsbygds - eller glesbygdskommun behöver definieras genom tydligt mätbara variabler, som resulterar i en lista på specifika kommuner som omfattas av bestämmelsen. I syfte att tydliggöra vilka kommuner som faktiskt omfattas kommer PTS att använda samma mått som myndigheten Tillväxtanalys definierat i sin rapport 2014:04, "Bättre statistik för bättre regional- och landsbygdsolitik". I den har kommunkategorier tagits fram i samråd med andra myndigheter. De kategorier som Tillväxtanalys kallar glesa landsbygdskommuner och mycket glesa landsbygdskommuner är de kategorier som enligt dessa föreskrifter kommer att utgöra en landsbygdskommun.*

PTS lägger till begreppet landsbygdskommun i föreskrifternas ordförklaringar. Den lista med kommuner som omfattas enligt definitionen, som uppdateras av myndigheten Tillväxtanalys, kommer att hänvisas till i FAQ och framtida vägledning. Verksamhetsutövarna kan utgå ifrån den kommunlistan, med medvetenhet om att den uppdateras av Tillväxtanalys allteftersom befolkningsmönster ändras. Se mer om den tillhörande bestämmelsen i 4 kap. 1 § 3 p.

4.3 Betydande incidenter

4.3.1 En incident ska prövas mot samtliga tröskelvärden

Sammanfattning av synpunkter: OneMore Secure och Stadsnätetsföreningen tillstyrker bestämmelsen och delar PTS uppfattning att en incident ska bedömas mot samtliga relevanta bedömningsgrunder i föreskrifterna. MCF ifrågasätter om bestämmelsen behövs. Tre och Stadsnätetsföreningen efterfrågar förtydliganden om hur de olika tröskelvärdena förhåller sig till varandra och hur överlappande bedömningsgrunder ska hanteras. Det har även framförts farhågor om att en händelse blir flera betydande incidenter om flera tröskelvärden uppfylls. OneMore Secure anser att ett dokumentationskrav bör införas. Flera remissinstanser har vidare efterfrågat förtydliganden om vilket underlag som är tillräckligt för bedömningen och hur långt verksamhetsutövarns utredningsskyldighet sträcker sig.

PTS kommentarer och åtgärder: PTS hänvisar inledningsvis till avsnitten 3.1.2 och 3.1.3 om bedömning av vad som utgör betydande incidenter. Mot bakgrund av remissvaren har PTS samlat bestämmelser om bedömning och informationsunderlag i 3 kap. för att skapa en tydligare och mer enhetlig struktur.

PTS vidhåller att en incident ska prövas mot samtliga relevanta bedömningsgrunder i föreskrifterna. Syftet är att incidentens samlade orsaker, skadeeffekter och potentiella konsekvenser ska kunna identifieras och bedömas av såväl verksamhetsutövaren som tillsynsmyndigheten.

PTS erfarenhet från tidigare incidentrapportering är att verksamhetsutövare i vissa fall har stannat vid det första identifierade tröskelvärde utan att bedöma incidentens samlade effekter. Detta har försvårat bedömningen av incidentens fulla påverkan och därmed också möjligheterna att skapa en bild av incidenter inom telekomområdet och bedöma behov och säkerhetsarbete utifrån inrapporterade incidenter.

PTS förtydligar att en incident endast utgör **en** betydande incident även om flera tröskelvärden är uppfyllda. Det är dock tillräckligt att ett tröskelvärde överskrids för att incidenten ska vara betydande. Verksamhetsutövaren ska dock, i takt med att kunskap om incidenten ökar, identifiera samtliga relevanta tröskelvärden som faktiskt har uppfyllts.

PTS delar inte uppfattningen att skyldigheten att pröva en incident mot samtliga relevanta bedömningsgrunder innebär en oproportionerlig administrativ belastning. Endast de tröskelvärden som framstår som relevanta i det enskilda fallet behöver analyseras närmare. Om flera tröskelvärden är uppfyllda ska dessa dokumenteras eftersom de belyser olika aspekter av incidentens påverkan. Det handlar inte om flera incidenter eller parallella utredningar utan om en samlad bedömning av samma incident.

PTS bedömer att den valda lösningen är proportionerlig och ändamålsenlig samt bidrar till en mer heltäckande och enhetlig identifiering av betydande incidenter i enlighet med cybersäkerhetslagens och NIS2-direktivets syften.

4.4 Allvarlig driftstörning

Telenor har frågat om behovet av att inkludera otillgänglighet till uppgifter i bestämmelserna om allvarlig driftstörning. Flera remissinstanser har uppfattningen att undergrävd riktighet, autenticitet eller konfidentialitet i nät, tjänster eller uppgifter inte kan utgöra grunder för allvarliga driftstörningar.

PTS kommentar: Att det endast är tillgänglighetsproblem som kan utgöra en allvarlig driftstörning är ett kvarlevande missförstånd som ändrades redan 2022 när kodexen

genomfördes i LEK. Se hur regeringen beskriver vidgandet av begreppet "drift" i propositionen till LEK.⁶

PTS konstaterar också att uppgifter uttryckligen omfattas av cybersäkerhetslagens definition av en incident, liksom även tidigare av definitionen av incident i LEK. Detta innebär att incidenter kan uppstå i tillgången (liksom i riktigheten, autenticiteten eller konfidentialiteten) i uppgifter som sådana. Det var så redan enligt LEK och det är så enligt cybersäkerhetslagen. Tabellen reglerar när sådana incidenter hos uppgifter når upp till den tillgänglighetsskada att de är att bedöma som betydande incidenter.

PTS bedömer därför och särskilt i förhållande till cybersäkerhetslagens definitioner av incident och betydande incident, att det är nödvändigt att föreskrifterna om betydande incidenter inom telekomområdet uttryckligen omfattar uppgifter. PTS avser att i FAQ och i en planerad vägledning ge ytterligare exempel på hur incidenter, hot och sårbarheter kan uppstå i uppgifter som omfattas av föreskrifterna enligt definitionen av uppgifter i 2 kap. 1 §.

4.4.1 Tillgänglighetsproblem enligt tabellbestämmelsen

PTS delar upp sammanfattningar, kommentarer och åtgärder under olika rubriker beträffande tabellen i 4 kap. 1 § 1 p. för att strukturera sammanställningen.

Bedömning av den betydande incidentens omfattning

Sammanfattning av synpunkterna: Digimitt, MittNät, Stadsnätetsföreningen, Netsam, SKR och delvis Telia framhåller att nätägare, stadsnät och grossistaktörer ofta saknar insyn i hur förbindelser används av kunder och vilka slutanvändare som påverkas. Tre saknar en beskrivning av skillnaden mot hur det varit tidigare när säkerhetsincidenters påverkan på slutanvändare inte behövde bedömas.

Flera remissinstanserna anser att det måste klargöras att verksamhetsutövaren inte förväntas uppskatta sådana effekter eller risker för som den saknar tillgång till, exempelvis antalet slutanvändare bakom en grossistkund, mobilmast eller svartfiberförbindelse. Flera remissinstanser framhåller att bedömningen i stället bör baseras på den information som verksamhetsutövaren faktiskt förfogar över vid rapporteringstillfället.

MCF efterfrågar ett förtydligande av hur uttrycket "slutanvändare, användare eller aktiva anslutningar" ska förstås och om kriterierna är alternativa eller kumulativa.

Netsam påpekar också att bestämmelsen innehåller flera olika bedömningsgrunder som förutsätter medverkan från flera roller och kompetenser vid bedömningen.

⁶ Prop. 2021/22:136 s. 319–320.

PTS kommentar och åtgärd: Angående Netsams påpekande om att bedömningar om betydande incidenter förutsätter medverkan från flera olika roller och kompetenser hos verksamhetsutövaren, hänvisar PTS till avsnittet avsnitt 3.1.3, angående roller och kompetenser vid bedömningen av betydande incidenter.

Verksamhetsutövaren ska - om denne inte har full kunskap om effekterna av tillgänglighetsincidenten - enligt bestämmelsen i 4 kap. 1 § 1 p. tillsammans med de generella bestämmelserna i 3 kap. göra uppskattningar av samtliga trösklar i tabellen utifrån sin kunskapssituation. Det vill säga: om inte en säker bedömning kan göras ska en uppskattning göras. Uppskattningen ska enligt 3 kap. 1 § tredje stycket göras utifrån informationen verksamhetsutövaren har eller rimligen kan skaffa sig enligt 3 kap. 1 § första stycket.

Enligt de generella bestämmelserna i 3 kap. ska alla relevanta tröskelvärden bedömas. Detta skapar en betydligt mer heltäckande bild av en inträffad betydande incident än incidentrapportering enligt PTS tidigare regler skapade. Tidigare kunde en verksamhetsutövare välja att endast rapportera en överskriden tidsomfattning och till exempel hur stort geografiskt område som hade drabbats av en incident, utan att tala om vilket kapacitetsbortfall, hur många användare eller uppskattade slutanvändare som hade drabbats. Det gav inte tillräckligt underlag för att förstå incidenters påverkan eller omfattning. En sådan fragmentarisk beskrivning av incidenter som rapporteras till myndighet leder till att incidentrapporteringsplikt inte uppnår det eftersträvade syftet enligt NIS2-direktivet eller cybersäkerhetslagen. Incidentrapportering blir med den äldre metoden endast ett administrativt krav som uppfylls. Cybersäkerhetslagens krav utgår ifrån ett allriskperspektiv. Syftet är att stärka kunskapen om bland annat incidenters påverkan och omfattning. Det finns därför inte längre utrymme för att endast bedöma ett tröskelvärde om flera tröskelvärden har passerats.

Utredningen internt av om en incident är betydande ska utgå från den information som verksamhetsutövaren har tillgång till, har fått kännedom om eller rimligen kan inhämta enligt bestämmelsen i 3 kap 1 §. Bedömningen ska göras utifrån det kunskapsläge som föreligger, och det kunskapsläge som rimligen kan skapas, vid tidpunkten för bedömningen och inte med facit i hand.

Om det är rimligt ska information inhämtas från den verksamhetsutövare i leverantörskedjan, den egna kunden eller den egna leverantören, som kan veta hur många slutanvändare som har påverkats av en incident. Detta ska göras om det kan anses vara en rimlig kontakt att ta. Andra europeiska länder, till exempel Danmark, har i stället ett uttryckligt krav att en verksamhetsutövare ska ta kontakt med övriga verksamhetsutövare i leverantörskedjan om det behövs för att bedöma en betydande incident som berör flera i leverantörskedjan. PTS har dock valt att inte kräva detta

uttryckligen utan lämnar till verksamhetsutövaren att välja metod och göra en rimlighetsbedömning.

Om en verksamhetsutövare inte har exakt vetskap exempelvis om hur många slutanvändare som använder en grossisttjänst, ska en uppskattning göras med utifrån den information som verksamhetsutövaren har eller rimligen kan inhämta enligt 3 kap. 1 § första stycket.

PTS förtydligar mot bakgrund av remissvaren bestämmelsens utformning för att undvika oklarheter.

Tillägget i tabellen av begreppet slutanvändare

Sammanfattning av synpunkterna: Flera remissinstanser lyfter att antalet slutanvändare ofta är svårt att fastställa för verksamhetsutövare som verkar på grossistnivå. Tre efterfrågar ett förtydligande kring vilken betydelse det får att begreppet slutanvändare nu uttryckligen anges i tabellen.

PTS kommentar och åtgärd: PTS har förståelse för att det finns svårigheter för alla slags tillhandahållanden i den svenska leverantörskedjan att veta hur många slutanvändare som faktiskt använder ett nät eller en tjänst.

Begreppet slutanvändare har lagts till för att tydliggöra att även påverkan på de som slutligen använder nätet eller tjänsten, vilket även inkluderar IoT-maskiner eller tekniska funktioner som är slutanvändare, ska beaktas vid bedömningen av incidentens omfattning. Påverkan på slutanvändare är en helt central faktor vid bedömningen av en incidents omfattning och konsekvenser och för cybersäkerhet i samhället. PTS har tagit hänsyn till Art. 3 3 i genomförandeförordningen om att antalet fysiska och juridiska personer som använder tjänster ska beräknas vid bedömningen av om en betydande incident har inträffat. Utöver det är det redan sedan tidigare EU-standard hos ENISA att räkna en incidents påverkan i antal slutanvändartimmar. Det är mot bakgrund av harmoniseringskravet och både tidigare gällande mått inom EU, och även nationellt hos flera andra EU-länder, samt genom harmonisering med genomförandeförordningen inte lämpligt att utesluta ett krav på att beräkna eller uppskatta hur många slutanvändare som har drabbats av en betydande incident som skapat tillgänglighetsproblem. PTS vill även peka på en överlappning i begreppen aktiv anslutning och slutanvändare. Denna överlappning bedöms vara nödvändig och acceptabel, eftersom PTS erfarenhetsmässigt ser att antal drabbade aktiva anslutningar, när dessa är slutanvändare, inte har identifierats, trots att antal drabbade aktiva anslutningar kan vara synonymt med både antalet drabbade användare i vissa

fall, och även med antalet drabbade slutanvändare i många fall. Se ovanstående avsnitt 4.2.2.1 om aktiva anslutningar.

Det finns en inskriven flexibilitet i bestämmelsen som gör att verksamhetsutövare som inte vet, ska uppskatta hur många slutanvändare som har påverkats av tillgänglighetsproblemen. Uppskattningen ska göras utifrån den information som verksamhetsutövaren har eller rimligen kan inhämta enligt 3 kap. 1 § första stycket.

Synpunkterna föranleder därför ingen ändring.

PTS avser att skapa mer vägledning i FAQ eller i en kommande vägledning.

Tillägget i tabellen av undergrävd tillgänglighet till uppgifter

Sammanfattning av synpunkterna: SKR, Stadsnätsföreningen och Telia anser att det behöver förtydligas vad som avses med att incidenter som rör uppgifter inte ska bedömas i förhållande till kapacitetsbortfall eller sammanhängande berört område. Några remissinstanser efterfrågar även ett klargörande av vilka typer av uppgifter som omfattas av bestämmelsen.

PTS kommentar och åtgärd: Inledningsvis hänvisas till avsnitten ovan om begreppet uppgifter i avsnittet 4.2.2.8 och om begreppet allvarig driftstörning i avsnittet 4.4.

Vilka uppgifter som omfattas av bestämmelsen generellt ska förstås genom definitionen av uppgifter i 2 kap. 1 §. PTS inför dock en avgränsning mot bakgrund av remissinstansernas synpunkter genom att lägga till att om incidenten avser undergrävd tillgänglighet till uppgifter som under normala förhållanden gör tillgängliga för slutanvändare eller användare ska bedömningen av incidentens omfattning endast göras utifrån de tröskelvärden som avser tid samt antal slutanvändare eller användare. Detta beror på att PTS har bedömt att incidenter som avser uppgifters tillgänglighet inte lämpar sig för bedömning utifrån parametrarna aktiva anslutningar, kapacitetsbortfall eller sammanhängande berört område.

PTS förtydligar därför bestämmelsen och avgränsar dess tillämpningsområde i denna del.

Begreppet kapacitetsbortfall

Sammanfattning av synpunkterna: Se även synpunkter på begreppet kapacitetsbortfall i avsnitt 4.2.2.3.

Netsam och Telia anser att kapacitetsbortfall kan slå olika mellan stora och små nät och efterfrågar ytterligare förtydliganden om hur kriteriet ska tillämpas i tabellen.

PTS kommentar och åtgärd: Se PTS kommentar och åtgärd kring begreppet kapacitetsbortfall i avsnitt 4.2.2.3.

PTS konstaterar att tröskelvärde kapacitetsbortfall använts i tidigare föreskrifter och nu görs endast ett tillägg med antal slutanvändare i förhållande till verksamhetsutövarens totala antal slutanvändare. Enligt tidigare föreskrifter har bedömningen enligt definitionen av kapacitetsbortfall och tröskelvärden i tabellen omfattat såväl kapacitetsbortfall utifrån verksamhetsutövarens totala kapacitet, och kapacitetsbortfall utifrån verksamhetsutövarens totala antal aktiva anslutningar eller användare. PTS pekar här på att begreppen aktiva anslutningar och slutanvändare kan överlappa, se tidigare resonemang om detta.

PTS förstår invändningen att kriteriet för kapacitetsbortfall kan träffa små nät oftare. Det är dock en avsiktlig och proportionerlig effekt. Proportionalitet betyder i detta avseende att reglerna ska vara rimliga i relation till risk, inte att alla aktörer ska rapportera lika ofta. Små nät kan ha mindre redundans, större känslighet för kapacitetsbortfall och högre risk för totalavbrott vid tekniska fel. Händelser i små nät kan därför leda till stora kapacitetsbortfall. Kriteriet är därför utformat för att fånga allvarliga tekniska incidenter oavsett nätets storlek, medan de övriga kriterierna i tabellen fångar kundpåverkan respektive geografisk spridning. Tillsammans ger de en balanserad och riskbaserad modell för att identifiera vad som utgör betydande incidenter.

PTS har genom synpunkterna insett att begreppet kan förtydligas och har därför gjort förenklingar och förtydliganden av definitionen av kapacitetsbortfall i 2 kap. 1 §.

Begreppet aktiva anslutningar

Sammanfattning av synpunkterna: Krafteringen, MittNät, Stadsnätetsföreningen och Netsam framhåller att antalet aktiva anslutningar ofta är den information som nätägare och grossistaktörer faktiskt har tillgång till. Flera remissinstanser anser att aktiva anslutningar är ett mer objektiva och verifierbart mått än antalet slutanvändare. Krafteringen efterfrågar samtidigt vägledning kring hur exempelvis mobilmaster, svartfiberförbindelser och flerfamiljsfastigheter ska räknas.

PTS kommentar och åtgärd: PTS delar uppfattningen att antalet aktiva anslutningar i många fall är en relevant uppgift vid bedömningen av incidenters omfattning. PTS har också kännedom om att det finns svårigheter med tolkningen.

PTS bedömer dock att det inte är lämpligt att i de här föreskrifterna detaljreglera hur varje typ av anslutning ska räknas. Begreppet aktiva anslutningar är ett begrepp som är centralt i PTS säkerhetsföreskrifter. Det används även i dessa föreskrifter, men begreppets närmare innebörd följer av övriga föreskrifter och etablerad tillämpning.

Synpunkterna föranleder ingen ändring.

Begreppet sammanhängande berört område

Sammanfattning av synpunkterna: Krafteringen och Netsam efterfrågar förtydliganden om hur ett sammanhängande berört område ska beräknas. Det efterfrågas bland annat vägledning om bedömningen ska utgå från radie, polygon eller annan geografisk metod.

PTS kommentar och åtgärd: *Vad gäller begreppen i tabellen, förutom slutanvändare, är begreppet sammanhängande berört område ett begrepp som inte är nytt utan har använts i tidigare föreskrifter. Någon ändring är inte avsedd av användningen av begreppet i dessa föreskrifter. Bedömningen ska utgå från incidentens faktiska geografiska påverkan och göras utifrån de uppgifter som finns tillgängliga eller rimligen kan inhämtas.*

Synpunkten föranleder ingen ändring.

PTS avser att skapa mer vägledning i FAQ eller en kommande vägledning.

Nummeroberoende kommunikationstjänster

Google anser att flera av tröskelvärdena är för lågt satta för verksamheter med mycket stora användarbaser och föreslår högre nivåer.

PTS kommentar och åtgärd: *PTS bedömer att de föreslagna tröskelvärdena ger en lämplig avvägning mellan rapporteringsbörda och behovet av att identifiera incidenter med betydande påverkan. Se även ovanstående avsnitt 3.1.8.*

Synpunkten föranleder ingen ändring.

Nödkommunikation

SOS Alarm framhåller att mycket allvarliga incidenter inom nödkommunikation kan vara kortvariga och begränsade till omfattningen och därför inte nå upp till värden enligt tabellen - men ändå få stora konsekvenser och vara betydande incidenter.

PTS kommentar och åtgärd: *PTS delar uppfattningen att incidenter som påverkar nödkommunikation kan vara allvarliga även om de inte uppnår de tröskelvärden för tillgänglighetsstörningar som anges i tabellen. Sådana betydande incidenter regleras i 4 kap 4 § 3 p och 4 p i föreskrifterna och det kan genom de bestämmelserna vara nödvändigt att identifiera händelser som betydande incidenter även om tröskelvärdena i tabellen inte uppnås.*

Synpunkten föranleder ingen ändring.

4.4.2 Betydande incident i passiva fibernät

Sammanfattning av synpunkter: Digimitt och Stadsnätsföreningen anser att det behöver framgå tydligare att bedömningen av incidentens omfattning ska utgå från

den information som nätägaren faktiskt har tillgång till. Särskilt framhålls att leverantörer av passiva fiberförbindelser ofta saknar insyn i hur förbindelserna används längre ut i kundledet.

OneMore Secure, Tele2 och Telia anser att bestämmelsen bör innehålla ett tidsrekvisit. De framhåller att en incident som påverkar ett stort antal passiva fiberförbindelser under mycket kort tid inte nödvändigtvis innebär en betydande påverkan och därför inte bör vara rapporteringspliktig, varför en tidsgräns behövs. Tele2 ifrågasätter behovet av en särskild incidentkategori för passiva fiberförbindelser och menar också att det finns en oklarhet i att bestämmelsen inte uttrycker om det är den som hyr eller den som äger förbindelserna som ska identifiera betydande incidenter enligt bestämmelsen. Stokab menar å sin sida att ett tidsrekvisit inte är nödvändigt eftersom det rör ett så högt antal uthyrda passiva fiberförbindelser som 400. Om så många passiva fiberförbindelser går av eller skadas kommer det att ta minst åtta timmar, sannolikt längre tid, att laga skadorna. Den relevanta tröskeln är just 400 uthyrda passiva fiberförbindelser som skadats. Det kommer med det antalet inte att uppstå några kortvariga tillgänglighetsstörningar, utan långvariga, om denna situation infinner sig, som gör att en betydande incident ska identifieras utifrån denna bestämmelse.

PTS kommentarer och åtgärd: PTS delar uppfattningen att bedömningen ska utgå från den information som verksamhetsutövaren faktiskt har tillgång till, har fått kännedom om eller rimligen kan inhämta. Detta framgår av 3 kap. 1 §.

PTS delar inte uppfattningen att mycket kortvariga störningar riskerar att omfattas av bestämmelsen utan att incidenten är av sådan omfattning att rapportering bör krävas. PTS håller därmed med Stokab om att tidsrekvisit inte bör införas, och att det är tillräckligt att mängden 400 uthyrda passiva fiberförbindelser utgör tröskeln. Att laga en sådan mängd fiberkablar kommer att ta tid, vilket utesluter identifiering enligt bestämmelsen av kortvariga tillgänglighetsstörningar.

PTS bedömer dock fortsatt att incidenter som påverkar ett stort antal passiva fiberförbindelser behöver omfattas av en särskild rapporteringsskyldighet. Eftersom tillhandahållare av passiva fiberförbindelser ofta saknar information enligt tröskelvärdena i tabellen om undergrävd tillgänglighet till nät, tjänster eller uppgifter behövs en separat regel. Antalet berörda förbindelser är ett lämpligt och objektiva mått på incidentens omfattning.

PTS kompletterar bestämmelsen endast på det sättet att det är den verksamhetsutövare som äger den passiva fiberförbindelsen som ska bedöma om incidenten är betydande enligt denna bestämmelse.

4.4.3 Betydande skada på riktighet, autenticitet eller konfidentialitet

Sammanfattning av synpunkter: Google anser att tröskelvärdena för incidenter enligt bestämmelsen bör höjas för nummeroberoende interpersonella kommunikationstjänster, eftersom de föreslagna nivåerna riskerar att fånga mindre incidenter hos tjänster med mycket stora användarbaser. MCF, Telenor och Stadsnätetsföreningen efterfrågar en definition av begreppet organisationskund. Stadsnätetsföreningen anser också att det behöver framgå vilka uppgifter som omfattas av bestämmelsen. OneMore Secure, Telia och Stadsnätetsföreningen efterfrågar vägledning om hur begreppen riktighet, autenticitet och konfidentialitet ska förstås i en praktisk tillämpning av bestämmelsen. OneMore Secure och Stadsnätetsföreningen efterfrågar även vägledning om när en organisationskund, användare eller slutanvändare ska anses vara drabbad av en incident och hur antalet drabbade ska bedömas. Stadsnätetsföreningen och Stokab framhåller att verksamhetsutövare inte alltid har full kännedom om en incidents påverkan på användare eller slutanvändare vid rapporteringstillfället. Tele2 och Tre invänder mot bestämmelsens utformning och ifrågasätter PTS bedömning att den motsvarar tidigare reglering. Tele2 anser att bestämmelsen innebär en ny incidentkategori som går utöver rapporteringsskyldigheter enligt cybersäkerhetslagen och NIS2-direktivet. Tele2 invänder även mot linjeringen med genomförandeförordningen. Tele2 och Tre pekar på att bestämmelsen skapar dubbelrapporteringskrav i förhållande till integritetsincidenter. Tre anser att allvarig driftsstörning enbart kan bestå av tillgänglighetsproblem. Tre delar inte heller PTS uppfattning att bestämmelsen motsvarar regleringen i Myndigheten för civilt försvars föreskrifter och anser att bestämmelsen i stället bör utformas i linje med den reglering som används där.

PTS kommentarer och åtgärder: Google har föreslagit högre tröskelvärden för nummeroberoende interpersonella kommunikationstjänster. PTS anser inte att det är motiverat med högre tröskelvärden än för traditionella nummerbaserade elektroniska kommunikationstjänster. Detta eftersom bestämmelsen syftar till att fånga upp incidenter med ett visst antal drabbade företagskunder eller slutanvändare, och inte tar hänsyn till en verksamhetsutövers totala antal företagskunder eller slutanvändare. Enligt PTS uppfattning blir det dessutom allt vanligare att kommunikation endast sker genom nummeroberoende interpersonella kommunikationstjänster, framför allt bland yngre slutanvändare som ofta använder dessa tjänster som sina primära eller till och med enda kommunikationskanaler.

PTS delar Stokabs uppfattning att vissa verksamhetsutövare kan ha begränsad insyn i hur en incident påverkar användare eller slutanvändare. Bedömningen ska verksamhetsutövaren göra utifrån det kunskapsunderlag som anges i 3 kap. 1 och 2 §§. Det innebär att verksamhetsutövaren ska utgå från den information som verksamhetsutövaren har tillgång till, har fått kännedom om eller rimligen kan inhämta.

Bestämmelsen förutsätter således inte att verksamhetsutövaren har fullständig kännedom om alla konsekvenser vid bedömningstillfället. Verksamhetsutövaren ska, om det inte går att ange exakt, uppskatta antal med mera. PTS har förståelse för att det inte alltid kan göras en uppskattning. Därför är bestämmelsen om uppskattningar formulerad med viss flexibilitet. Verksamhetsutövaren ska göra en uppskattning utifrån det underlag denne har eller rimligen kan inhämta enligt 3 kap 1 § första stycket. Finns inte någon kunskap, inga rimliga kontakter att ta eller kontroller att göra, till exempel av information på hemsidor hos partners i leverantörskedjan, kan det betyda att verksamhetsutövaren inte kan, och därför inte ska, göra en uppskattning. Men utgångspunkten är att verksamhetsutövaren ska försöka göra en uppskattning.

PTS delar inte Tele2:s uppfattning att den föreslagna bestämmelsen saknar motsvarighet i PTS tidigare föreskrifter. Den tidigare bestämmelsen i 17 kap. 6 § i PTS nu upphävda rapporteringsföreskrifter omfattade betydande påverkan på nätets eller tjänstens funktion. Sådan påverkan kunde även bestå i brister avseende riktighet, autenticitet eller konfidentialitet och var inte begränsad till enbart tillgänglighetsrelaterade störningar eller betydande påverkan på funktioner i samhället.

PTS bedömer dock att det finns ett tydligt behov av att uttryckligare än tidigare reglera denna typ av incidenter. Bestämmelsen har också utformats med beaktande av motsvarande typer av incidenter som omfattas av genomförandeförordningen för andra verksamheter inom sektorn för digital infrastruktur. Syftet är att uppnå en harmoniserad reglering av incidenter som påverkar grundläggande säkerhetsegenskaper såsom riktighet, autenticitet och konfidentialitet. Att genomförandeförordningen gäller andra verksamheter inom samma sektor förändrar inte PTS bedömning att motsvarande säkerhetsintressen bör beaktas även inom området för elektronisk kommunikation.

När det gäller synpunkterna om risker med dubbelrapportering konstaterar PTS att en och samma händelse under vissa omständigheter kan omfattas av flera regelverk. Den omständigheten att en incident även kan omfattas exempelvis av regleringen om integritetsincidenter innebär dock inte att det inte samtidigt kan ha uppstått en betydande incident enligt cybersäkerhetslagen.

Tre anför att allvarlig driftsstörning endast rör tillgänglighetsproblem. Tele2 för ett liknande resonemang. Detta är inte en korrekt uppfattning. Sedan 2022, då kodexen genomfördes i svensk rätt och bland annat nya rapporteringskrav infördes i PTS säkerhetsföreskrifter, omfattar driften av nät och tjänster inte endast tillgänglighet utan även säkerhetsaspekterna riktighet, autenticitet och konfidentialitet.⁷ Följden är

⁷ Se propositionen till LEK från 2022, Prop. 2021/22:136 s. 319–320.

att begreppet allvarlig driftsstörning inte enbart omfattar tillgänglighetsproblem. Den tidigare bestämmelsen i 17 kap. 6 § i de upphävda föreskrifterna omfattade också betydande störningar i riktighet, autenticitet och konfidentialitet i nät och tjänster.

Frågan om vad som är en allvarlig driftsstörning behandlas mer utförligt ovan i avsnitt 3.1.6 om allvarlig driftsstörning. Synpunkterna föranleder därför ingen ytterligare åtgärd i denna del.

Tre har vidare anført att bestämmelsen bör utformas i linje med Myndigheten för civilt försvars motsvarande föreskrifter. PTS konstaterar att föreskrifterna har olika tillämpningsområden och delvis olika systematik. MCF:s bestämmelse tar sikte på incidenter som medför att information i behov av utökat skydd har blivit tillgänglig för obehöriga, förvanskats eller förstörts. PTS bestämmelse är däremot utformad för att fånga incidenter som undergräver riktigheten, autenticiteten eller konfidentialiteten i nät, tjänster eller uppgifter inom sektorn för elektronisk kommunikation. Den omständigheten att MCF valt en annan reglering innebär därför inte att motsvarande utformning är lämplig eller nödvändig inom detta regelverk.

Flera remissinstanser har efterfrågat förtydliganden kring hur bestämmelsen ska tillämpas i praktiken. Synpunkterna avser bland annat innebörden av begreppen riktighet, autenticitet och konfidentialitet, innebörden av att en företagskund eller slutanvändare har drabbats, vilka uppgifter som omfattas av bestämmelsen, hur antalet drabbade ska beräknas.

PTS instämmer i att det finns behov av ytterligare vägledning till denna bestämmelse. Myndigheten avser därför att ta fram frågor och svar (FAQ) och en planerad vägledning. Det kan även finnas behov av tillsyn.

Se avsnitt 4.2.2.9 om begreppet företagskund, i förslaget organisationskund.

Mot bakgrund av inkomna synpunkter ändrar PTS bestämmelsen dels genom att ersätta begreppet organisationskund med företagskund och införa en definition av begreppet företagskund i föreskrifterna,

4.4.4 Gränsöverskridande betydande incident

Sammanfattning av synpunkter: Tre verksamhetsutövare har lämnat remissvar kring denna föreslagna bestämmelse. Stadsnätetsföreningen och Telia framhåller att verksamhetsutövare inte alltid har insyn i hur många slutanvändare som påverkas av en incident, särskilt när tjänster tillhandahålls i en leverantörskedja eller till kunder med verksamhet i flera länder. De efterfrågar därför vägledning om hur antalet berörda slutanvändare ska bedömas i sådana situationer. Stadsnätetsföreningen efterfrågar även vägledning om ansvarsfördelningen mellan berörda aktörer.

Telenor avstyrker förslaget och anser att PTS inte har visat behovet av en särskild bedömningsgrund för gränsöverskridande incidenter och pekar på svårigheter att bedöma effekter i andra länder.

PTS kommentarer och åtgärder: *PTS har förståelse för synpunkterna från Stadsnätetsföreningen och Telia, och för Telenors påpekande om svårigheten att alltid kunna bedöma effekter i andra länder.*

Bedömningen av samtliga betydande incidenter ska göras enligt bestämmelserna i 3 kap. Det innebär bland annat att verksamhetsutövaren ska utgå från den information som verksamhetsutövaren har tillgång till, fått kännedom om, eller rimligen kan inhämta. Bestämmelsen förutsätter således inte att verksamhetsutövaren har fullständig kännedom om samtliga berörda slutanvändare eller incidentens fullständiga gränsöverskridande påverkan vid bedömningstillfället.

Verksamhetsutövaren ska i stället bedöma incidentens gränsöverskridande påverkan utifrån det kunskapsunderlag som finns enligt bestämmelserna i 3 kap, och ska göra en uppskattning om omfattningen av en incident eller dess konsekvenser inte säkert kan bedömas. Uppskattningen ska göras utifrån information som verksamhetsutövaren har eller rimligen kan inhämta enligt 3 kap. 1 § första stycket.

PTS delar inte Telenors bedömning att det saknas behov av en särskild bedömningsgrund för gränsöverskridande incidenter. NIS2-direktivet fäster särskild vikt vid gränsöverskridande verksamheter och incidenters gränsöverskridande konsekvenser, se bland annat artikel 23.4 a och skäl 102. Verksamhetsutövare ska vid incidentrapportering lämna information som gör det möjligt att bedöma om en incident kan få gränsöverskridande påverkan och direktivet innehåller särskilda bestämmelser om informationsutbyte och samordning mellan medlemsstater vid betydande incidenter som berör flera medlemsstater.

Även i propositionen till cybersäkerhetslagen framhålls samordning mellan medlemsstater och vikten av kunskap om gränsöverskridande effekter, samt att det är lämpligare att sådan bedömning regleras på lägre föreskriftsnivå än i lag.⁸

Bestämmelsen ligger även i linje med den harmoniserade syn på betydande incidenter som också kommer till uttryck i kommissionens genomförandeförordning för andra verksamhetsutövare inom sektorn för digital infrastruktur. PTS utgår ifrån att verksamhetsutövare inom telekomområdet i Sverige inte sällan även omfattas av genomförandeförordningens regler i andra roller i sina verksamheter. PTS gör antagandet att bestämmelsen kommer att få genomslag för de verksamhetsutövare som tillhandahåller nummeroberoende interpersonella kommunikationstjänster.

⁸ Prop. 2025/26:28 bland annat s. 111,

PTS bedömer mot bakgrund av de överordnade regelverken och regeringens skrivningar i propositionen att incidenter med en tydlig gränsöverskridande dimension bör utgöra en självständig bestämmelse. Ingen ändring görs i den föreslagna bestämmelsen.

PTS instämmer i att det finns behov av ytterligare vägledning om bestämmelsens tillämpning. Myndigheten avser därför att behandla dessa frågor i kommande frågor och svar (FAQ) eller vägledning.

4.4.5 Betydande incident på landsbygden

Sammanfattning av synpunkter: De flesta remissinstanser anser att det behövs en definition för landsbygds- eller glesbygdskommun. MittNät, OneMore Secure, Stadsnätetsföreningen, Telenor och Telia framhåller att verksamhetsutövare inte alltid har insyn i vilka alternativa nät eller tjänster som finns tillgängliga för användare under en pågående incident. De anser därför att bedömningen bör utgå från sådana förhållanden som verksamhetsutövaren känner till eller rimligen kan fastställa vid bedömningstillfället. Läke-medelsverket anser att kriteriet om 100 procents kapacitetsbortfall inte ensamt utgör ett tillräckligt mått på påverkan och föreslår en lydelse som tar sikte på när nät eller tjänster i praktiken är obrukbara för användarna. Tele2 och Tre avstyrker bestämmelsen och anser bland annat att rapporteringströskeln är för låg, att bestämmelsen saknar motsvarighet i genomförandeförordningen och att den riskerar att medföra en oproportionerlig rapporteringsbörda. Tele2 anför också att det redan i föreskriften kan hänvisas till en vid var tid gällande myndighets lista över landsbygdskommuner.

PTS kommentarer och åtgärder: PTS instämmer i att begreppet landsbygds- eller glesbygdskommun behöver definieras. PTS har beslutat sig för begreppet landsbygdskommun, och definierar begreppet i 2 kap. 1 § 7 p. Se mer om detta i avsnitt 4.2.2.10.

PTS kommer att ange en lista med vilka kommuner som omfattas av definitionen i kommande frågor och svar (FAQ) eller i planerad vägledning.

När det gäller Tele2:s och Tres invändningar om för låg tröskel och att bestämmelsen inte är proportionerlig bedömer PTS att bestämmelsen fyller ett viktigt cybersäkerhetssyfte. Störningar i elektronisk kommunikation i områden där alternativa kommunikationstjänster helt eller delvis saknas får betydande konsekvenser även om antalet berörda användare är relativt begränsat. Sådana situationer riskerar annars att inte fångas upp av de generella tröskelvärdena trots att den faktiska påverkan på de berörda slutanvändarna är betydande. PTS bedömer därför att det finns skäl att behålla en särskild bestämmelse för denna typ av incidenter.

PTS har vidare förståelse för synpunkterna från MittNät, OneMore Secure, Stadsnätetsföreningen, Telenor och Telia om svårigheten att bedöma vilka alternativa nät eller tjänster som finns tillgängliga under en pågående incident.

PTS delar alltså remissinstansernas uppfattning att verksamhetsutövare ofta saknar tillräcklig insyn i andra verksamhetsutövares faktiska nät, tjänster och täckning för att på ett rättssäkert sätt kunna bedöma om motsvarande nät eller tjänster finns tillgängliga under incidenten. Mot denna bakgrund har kravet på att verksamhetsutövaren ska bedöma om andra verksamhetsutövare kan erbjuda motsvarande nät eller tjänst tagits bort ur bestämmelsen. Detta antas förenkla bedömningen och minska administrativa kostnader.

Bedömningen ska dock alltid göras utifrån bestämmelserna om bedömningar av vad som utgör betydande incidenter 3 kap. Det innebär bland annat att verksamhetsutövaren ska utgå från den information som verksamhetsutövaren har tillgång till, fått kännedom om, eller rimligen kan inhämta. Bestämmelsen förutsätter således inte att verksamhetsutövaren har fullständig kännedom om samtliga alternativa nät eller tjänster som kan finnas tillgängliga för användarna vid bedömningstillfället. Om ett exakt antal drabbade inte kan fastställas ska i stället en uppskattning göras. Uppskattningen ska göras utifrån den information som verksamhetsutövaren har eller rimligen kan inhämta enligt 3 kap. 1 § första stycket.

PTS delar Läke-medelsverkets uppfattning att 100 % kapacitetsbortfall inte ensamt fångar incidentens faktiska påverkan på slutanvändarna. Även mot denna bakgrund har bestämmelsen justerats. Sammantaget har begreppet landsbygdskommun definierats, det tydliggörs att nätet eller tjänsten ska vara så begränsad att den i praktiken är obrukbar för de berörda slutanvändarna, användarna eller de aktiva anslutningarna, och kravet på bedömning av andra verksamhetsutövares nät och tjänster har tagits bort.

PTS instämmer också i att det finns behov av ytterligare vägledning om bestämmelsens tillämpning och avser att publicera frågor och svar (FAQ) och en planerad vägledning.

4.5 Ekonomisk skada för verksamhetsutövaren

Sammanfattning av synpunkter: Flera remissinstanser anser att ett fast tröskelvärde om fem miljoner kronor riskerar att ge oproportionerliga effekter för större verksamhetsutövare och föreslår därför att bestämmelsen kompletteras med ett relativt tröskelvärde kopplat till omsättning, liksom det finns i genomförandeförordningen, eller som MCF har med enbart ett tröskelvärde i förhållande till årsomsättning. Remissinstanserna lyfter även att den ekonomiska skadan ofta är svår att veta under ett pågående incidentförlopp och efterfrågar

förtydliganden om när bedömningen ska göras och vilka indirekta kostnader som ska ingå i beräkningen. AC-net påpekar också att ekonomisk skada utgör företagshemligheter som omfattas av sekretess.

PTS kommentarer och åtgärder: PTS delar uppfattningen att ett absolut tröskelvärde om fem miljoner koronor får olika betydelse för verksamhetsutövare av olika storlek. Tröskelvärdet upplevs sannolikt som lägre för mycket stora operatörer och högre för mindre aktörer. Detta är en eftersträvd effekt. På det viset skyddas mindre aktörer från en hög administrativ belastning efter incidenter. Detta bör också leda till att små aktörers incidenter som inte blir mycket kostsamma inte behöver identifieras som betydande och därmed som följd inte behöver rapporteras. Dessa mindre incidenter hos mindre aktörer som underskrider en ekonomisk skada om fem miljoner hos dem ser inte PTS heller ett generellt behov av att analysera. PTS påminner om att det ändå kan vara nödvändigt att identifiera en incident som betydande, även om den inte uppnår tröskeln för ekonomisk skada, om den når upp till något eller några andra tröskelvärden i någon annan bestämmelse.

PTS bedömer att kriteriet om ekonomisk skada fyller en självständig funktion, liksom det även bedömts göra det i genomförandeförordningen och i MCF:s föreskrifter.

PTS är medveten om att bedömningar av ekonomisk skada kan göras först senare i ett incidentförlopp. Samtliga kostnader kan sällan fastställas under en pågående incidenthantering. Bedömningen ska göras utifrån bestämmelserna i 3 kap. Bestämmelsen innebär därmed att verksamhetsutövaren ska utgå från den information som verksamhetsutövaren har tillgång till, har fått kännedom om eller rimligen kan inhämta – dock inte att verksamhetsutövaren måste genomföra detaljerade beräkningar innan sådana beräkningar kan göras.

Vad gäller kostnadsslagen i 4 kap. 3 § avser uppräkningsen såväl externa som interna kostnader när dessa utgör en faktisk ekonomisk skada för verksamhetsutövaren. Exempelvis kan kostnader för utbyte eller återställning av system omfatta både externa inköp av tjänster och produkter samt interna resurser som krävs för återställningsarbetet.

Som bemötande av AC-Nets invändning om företagshemligheter påminner PTS om att det råder hög sekretess för sådan information som kommer in till PTS i incidentrapportering enligt cybersäkerhetslagen. Det har skett en lagändring i 18 kap. 8 b § offentlighets- och sekretesslagen (2009:400) som dessutom lett till ett ännu högre skydd kring uppgifter i incidentrapporteringen jämfört med tidigare.

PTS ändrar inte bestämmelsen och lägger inte till ett relativt värde kopplat till verksamhetsutövarens årsomsättning. En sådan ändring skulle innebära att fler mindre incidenter hos mindre verksamhetsutövare som inte finns anledning att

analysera skulle behöva identifieras som betydande incidenter. De större verksamhetsutövarnas incidenter som skapat interna kostnader om minst fem miljoner kronor är dock relevanta för tillsynsmyndigheten att känna till.

Ytterligare vägledning om tillämpningen kan lämnas inom ramen för PTS frågor och svar (FAQ) eller vägledning.

4.6 Betydande skada för annan än verksamhetsutövaren

4.6.1 Betydande skada för en viktig samhällsfunktion

Sammanfattning av synpunkter: MittNät, Digimitt, Stadsnätsföreningen, Stokab, Telenor, Telia, Netsam, SKR, SOS Alarm, OneMore Secure och Tre framhåller att verksamhetsutövare ofta saknar tillräcklig insyn i leverantörskedjan, det vill säga i detta avseende, insyn i sina kunders verksamhet och vad kunderna använder verksamhetsutövarens nät och tjänster till, deras interna beroenden, redundanslösningar eller konsekvenser för användare av nät eller tjänster. En återkommande synpunkt är att rapporteringsskyldighet bör bygga på information som verksamhetsutövaren faktiskt har tillgång till.

Flera remissinstanser, däribland Tele2, Telenor, Tre, MCF, SKR, Läkemedelsverket och Stokab, anser också att tröskelvärdena avseende tätorter, risk för liv, särskilt viktiga dagar och extraordinära händelser är otydliga, är svåra att tillämpa eller saknar tydlig koppling till påverkan på en enskild samhällsviktig funktion. Tele2 påpekar att det är skillnad mellan vad som påverkar en organisation som tillhandahåller en viktig samhällsfunktion och vad som påverkar samhället. Såsom bestämmelsen är skriven omfattas båda sakerna.

Tre välkomnar att PTS använder samma definition av viktig samhällsfunktion som MCF:s föreskrifter, medan Telia och Netsam efterfrågar ytterligare tydlighet kring vilka verksamheter som omfattas.

PTS kommentarer och åtgärder: *PTS bedömer sammantaget att betydande påverkan på viktiga samhällsfunktioner genom incidenter hos verksamhetsutövare inom telekom ska utgöra en självständig bestämmelse om denna specifika typ av betydande incident. Elektroniska kommunikationsnät och kommunikationstjänster utgör grundläggande beroenden för de flesta viktiga samhällsfunktioner. Incidenter som pågått minst sex timmar och som leder till **betydande störningar** i en viktig samhällsfunktion ska identifieras även när incidenten inte omfattas av andra tröskelvärden i föreskrifterna. PTS påpekar även att den här typen av störningar sedan 2022 har varit rapporteringspliktig enligt PTS tidigare rapporteringsföreskrifter. Den tidigare regeln har dock inte tillämpats enhetligt och det har över tid tagit*

resurser både hos verksamhetsutövare och hos PTS för att diskutera och bedriva tillsyn för att kräva in sådan rapportering.

Det är tydligt att beroendet av elektroniska kommunikationsnät och tjänster för viktiga samhällsfunktioner både var en del av de grundläggande utgångspunkterna för incidentrapportering enligt kodexen och även är en del av NIS2-regelverket och cybersäkerhetslagen

PTS kräver inte att verksamhetsutövaren ska kartlägga eller utreda samtliga kunders verksamheter. Det är dock nödvändigt att verksamhetsutövaren faktiskt vet om nätet eller tjänsten som tillhandahålls används i en viktig samhällsfunktion. Det innebär att om verksamhetsutövaren, genom avtal, kundkännedom, information från kunden eller annan tillgänglig information, har kännedom om att den berörda kunden eller organisationen tillhandahåller en viktig samhällsfunktion behöver incidenter hos verksamhetsutövaren bedömas med hänsyn till denna information. Information om vilka verksamheter som omfattas finns till exempel i den förteckning över verksamheter med viktiga samhällsfunktioner som MCF tillhandahåller.

PTS delar dock remissinstansernas uppfattning om att verksamhetsutövare ofta saknar fullständig kännedom om hur en incident påverkar kunders verksamhet, särskilt när det gäller verksamheter längre bort i leveranskedjan eller när konsekvenserna beror på vad kunden har köpt för tjänstenivå, kundens redundanslösningar eller dennes interna organisation.

Bedömningen enligt den enskilda bestämmelsen om vad som utgör en betydande incident som har orsakat betydande skada på en samhällsviktig verksamhet ska göras utifrån det kunskapsunderlag och den bedömning som följer av föreskrifternas allmänna bestämmelser i 3 kap. Extern information angående en incident från exempelvis en kund, leverantör, slutanvändare, myndighet eller annan källa ska kunna ingå i verksamhetsutövarens kunskapsunderlag om incidenter.

Med förändringarna av vad en säkerhetsincident var enligt LEK från 2022 och vad en betydande incident är enligt cybersäkerhetslagen från 2025, är det inte längre tillräckligt med en teknisk upptäckt för att kunna identifiera vilka händelser som utgör en betydande incident enligt cybersäkerhetslagen. Se mer om detta i avsnitt 3.1.2 och 3.1.3.

Syftet med bestämmelsen är att fånga sådana incidenter i nät, tjänster eller uppgifter som har lett till betydande störningar för en viktig samhällsfunktion. Fokus i verksamhetsutövarens bedömning av incidenten enligt denna bestämmelse ska därför ligga på följdverkningarna hos organisationen som tillhandahåller en samhällsviktig verksamhet eller på den viktiga samhällsfunktionen i sig. Incidenten hos verksamhetsutövaren måste ha varat i sex timmar för att bestämmelsen ska

aktualiseras. Verksamhetsutövaren kan enligt bestämmelsen antingen göra ett antagande om att en egen incident i egna nät och tjänster har lett till betydande störningar i en viktig samhällsfunktion, eller ha kännedom om eller rimligen kan hämta in information om att incidenten har bidragit till att organisationen som tillhandahåller den viktiga samhällsfunktionen har gått in i stabsläge eller på annat sätt har eskalerat eller ändrat sin organisation på grund av incidenten.

Tre har föreslagit att det i stället ska bedömas om påverkan på en viktig samhällsfunktion har pågått i sex timmar, men PTS anser att en överflyttning av tidströskeln riskerar att öka en administrativ börda för verksamhetsutövare. Det är enklare att mäta tiden för incidenten i näten, tjänsterna eller uppgifterna.

PTS behöver dock avgränsa bestämmelsen bättre och instämmer i Tele2s påpekande om att de tidigare tröskelvärdena pekade åt två olika håll. Tröskelvärdena i förslaget om påverkan på tätorter, risk för liv eller allvarlig skada för allmänheten, eller på särskilt viktiga dagar för politisk verksamhet, försvarsverksamhet eller extraordinära händelser tog i första hand sikte på faktiska samhällskonsekvenser - och inte på påverkan på en viktig samhällsfunktion. Dessa tröskelvärden, även om de omfattas av ENISA:s vägledning för incidentrapportering, har därför tagits bort ur bestämmelsen. PTS bedömer att sådan påverkan kommer att identifieras genom andra bestämmelser i föreskrifterna.

Mot denna bakgrund behålls bestämmelsen och samtidigt förenklas den väsentligt. Bedömningen fokuserar nu enbart på betydande skada på en viktig samhällsfunktion, och inte på skador i samhället i stort.

PTS avser att skapa en FAQ och en planerad vägledning.

4.6.2 Betydande skada för nödkommunikation eller på VMA

Sammanfattning av synpunkter: OneMore Secure och SOS Alarm tillstyrker bestämmelserna och anser att nödkommunikation och viktiga meddelanden till allmänheten (VMA) har sådan samhällskritisk betydelse att när den lagstadgade medverkan till förmedling av nödkommunikation eller VMA inte har fungerat ska det anses ha uppstått en betydande incident. SOS Alarm framhåller att verksamhetsutövare inom telekom, som har skyldighet att medverka till avbrottsfri nödkommunikation enligt lag, ofta saknar tillräcklig insyn i hur deras egna incidenter påverkar nödkommunikationen i praktiken och efterfrågar ökad informationsdelning mellan berörda aktörer. Tele2 och Tre avstyrker bestämmelserna och anser att de saknar proportionerliga tröskelvärden samt riskerar att leda till rapportering av incidenter med mycket begränsad faktisk påverkan. Både Tre och Tele2 anser att PTS i stället ska använda information som PTS har i sin samverkande roll, bland annat

från NTSG och ett system som heter Navet dit alla verksamhetsutövare inom telekom rapporterar alla täckningsbortfall.

Flera remissinstanser efterfrågar tydligare avgränsningar för när påverkan på nödkommunikation eller VMA ska anses ha inträffat. Tre framhåller att när nödkommunikation har kunnat genomföras via nödroaming, kan inte en betydande incident anses ha uppkommit och Tre önskar en bättre förklaring till överlappningen mellan olika bestämmelser i föreskrifterna som även de kan ha påverkat möjligheterna till förmedling av nödkommunikation. Inte heller kännedom om ett täckningsbortfall bör vara tillräckligt för att identifiera en betydande incident enligt denna bestämmelse enligt Tele2.

Tre uppger att operatörernas kännedom om att nödkommunikation eller VMA inte förmedlas i hög grad varierar och i många fall är begränsad eller t.o.m. saknas och ställer även frågan om andra EU-länder har motsvarande tolkning av rapporteringsplikt vid misslyckad förmedling av nödkommunikation eller VMA. Tre undrar även hur rapportering av en betydande incident förhåller sig till säkerhetsskyddslagen och eventuell rapportering enligt den lagen.

Tele2 har anfört att det inte kan anses vara en allvarlig driftstörning att nödkommunikation eller VMA inte har kunnat förmedlas via verksamhetsutövaren - om inte några andra tröskelvärden för tillgänglighetsbortfall är uppfyllda. Tele2 anser också att tidigare rapporteringsföreskrifter inte omfattade en självständig rapporteringsplikt för störningar i medverkan till förmedling av brottsfri nödkommunikation eller VMA och att det också i nuläget saknas sådan rapporteringsplikt i genomförandeförordningen eller uttryckligen i cybersäkerhetslagen.

Tele2 anför att bestämmelsen dessutom skulle innebära att varje täckningsbortfall alltid ska innebära en betydande incident enligt bestämmelserna om nödkommunikation och VMA. Dessutom meddelar Tele2 att det inte finns tillräcklig information om nödroaming fungerar eller inte när en slutanvändare haft behov av att kontakta 112, och inte heller finns systemstöd internt för att se om ett VMA har förmedlats när uppdraget är att förmedla VMA. Verksamhetsutövare vet helt enkelt inte om deras medverkan enligt reglerna i LEK har eller kan genomföras i de enskilda fallen. Det verksamhetsutövare vet är att det finns en systematik för förmedling av nödkommunikation och för VMA, men inte om den fungerar när det behövs. Vad gäller VMA finns komponenter på verksamhetsutövarens sida, så kallad CBC, som lagrar data och som till viss del monitorerar vad som har fungerat och inte. Telia efterfrågar förtydliganden om tillämpningen, särskilt när det gäller medverkan till VMA och verksamhetsutövarens ansvar när funktionen tillhandahålls genom underleverantörer, medan Telenor påpekar skiftet från att motsvarande incidenter

sedan tidigare har rapporterats som en obligatorisk uppgift i varje ingiven incidentrapport om säkerhetsincidenter, till att nu bli en betydande incident i sig. SKR och Telia anser att bestämmelserna bör avgränsas till tillgänglighetsaspekter och ifrågasätter hur konfidentialitet kan undergrävas i samband med VMA. Tre efterfrågar även förtydliganden om bestämmelsernas förhållande till säkerhetsskyddslagstiftningen.

PTS kommentarer och åtgärder kring betydande incidenter i medverkan till avbrottsfri förmedling av **nödkommunikation**: *PTS instämmer i behovet av avgränsning och tydlighet och ändrar bestämmelsen om nödkommunikation för att tydliggöra att det inte är tillräckligt med endast täckningsbortfall för att konstatera att det har inträffat en betydande incident.*

För att förtydliga – PTS anser inte att det uppstår en betydande incident enligt den föreslagna bestämmelsen om nödkommunikation har genomförts via nödroaming. Det krävs, utöver ett täckningsbortfall, vetskap eller särskild anledning att anta att verksamhetsutövarens medverkan till avbrottsfri nödkommunikation har misslyckats. Det är dock inte tillräckligt att utan att kontrollera de verkliga möjligheterna för nödroaming, utgå ifrån att det funnits möjligheter till nödroaming på platsen för tillgänglighetsbortfall eller vid de verkliga omständigheterna. PTS utgår ifrån att det både finns vissa områden och också vissa verkliga inträffade omständigheter där det finns särskild anledning att anta att nödroaming inte kan genomföras. I de fallen har verksamhetsutövaren antingen vetskap om eller särskild anledning att anta att avbrottsfri nödkommunikation inte har kunnat förmedlas.

Till de avsedda incidenterna hör alltså fall där det kunnat konstateras, eller det annars finns en särskild anledning att anta, att en hjälpsökandes nödkommunikation inte kunnat förmedlas men också fall där det utifrån en sammantagen bedömning av ett större antal berörda slutanvändare, en större geografisk yta eller att incidenten pågått en viss tid och andra omständigheter finns en särskild anledning att anta att medverkan eller förmedling av nödkommunikation i praktiken inte har kunnat ske. Det är tillräckligt med vetskap eller särskild anledning att anta att en (1) hjälpsökande inte har kunnat nödkommunicera.

Avsikten är alltså inte att verksamhetsutövaren, vid varje täckningsbortfall som inte i sig är långvarigt eller täcker stor eller välbefolkad yta, alltid ska efterforska aktivt om någon försökt nå 112 under bortfallen. Det krävs enligt bestämmelsen vetskap eller någon särskild anledning att anta att förmedlingen inte har fungerat. Det krävs således kvalificerade omständigheter som talar för att förmedlingen av nödkommunikationen inte har fungerat. Bedömningen ska också göras utifrån bestämmelserna och de allmänna råden i 3 kap. där det generellt stadgas att bedömningen av om en betydande incident har inträffat ska utgå från den information

som verksamhetsutövaren faktiskt har tillgång till, har fått kännedom om eller rimligen kan inhämta. Information kan komma från verksamhetsutövarens egen verksamhet men även från exempelvis en kund, leverantör, slutanvändare, myndighet eller annan källa. Vid information från externa källor om att förmedling inte har fungerat uppstår enligt PTS mening oftast vetskap hos verksamhetsutövaren, och inte särskild anledning att anta att förmedlingen inte har fungerat.

Särskild anledning att anta att nödkommunikation inte har kunnat förmedlas exempelvis kan grundas i kännedom om tekniska omständigheter eller omständigheter som att det är en stor yta som omfattas av tillgänglighetsstörningar i ett område där verksamhetsutövaren har många slutanvändare och varaktigheten av störningarna har pågått under en viss tid. Ju större yta, ju fler slutanvändare och ju längre tid tillgänglighetsstörningar pågår, desto större skäl att anta att någon har försök nå nödkommunikation och inte lyckats.

Som svar på Tre:s fråga om hur det ser ut i Europa har PTS kännedom om andra europeiska länders rapporteringsplikt vid misslyckad förmedling av nödkommunikation eller VMA. I flera länder är nationella regler inte klara för vad som är betydande incidenter inom telekomområdet. Se även bilagan till konsekvensutredningen med mer underlag för utredningen om hur andra europeiska länder har gjort. I Danmark är påverkan genom incidenter i nät och tjänster för nödsituationer (112) betydande utan tröskelvärden. I Spanien är telekomstörningar på nödkommunikation eller VMA rapporteringspliktiga oberoende av hur många uppkopplingar som störs. I Luxemburg är händelser hos en telekomverksamhetsutövare som skapat en risk för allmän säkerhet eller har lett till dödsfall, händelser som påverkat larmsystem eller händelser som har påverkat räddningstjänstens funktion alla rapporteringspliktiga. I Finland är störningar i möjligheten att ringa 112, störningar i överföring av nödsamtal, störningar i prioriterad trafik och störningar i funktioner som krävs för att nödsamtal ska fungera alla rapporteringspliktiga. I Kroatien är incidenter rapporteringspliktiga där tillgång till 112-centralens tjänster eller andra räddningstjänster inte varit möjlig, oavsett avbrottets längd och antalet berörda mottagare.

Som svar på Tre:s fråga om förhållandet till säkerhetsskyddslagen och eventuell rapportering enligt den lagen påpekar PTS att det kan finnas överlappning av skyldigheter enligt olika regelverk. Enligt 1 kap. 13 § cybersäkerhetslagen gäller att säkerhetsskyddsklassade uppgifter inte ska in i en incidentrapport, trots att en incident kan omfatta den typen av uppgifter. Det här undantaget om vilka uppgifter som skrivs in i en incidentrapport rör reglerna om incidentrapportering som meddelas av FRA, och inte om själva identifieringen av betydande incidenter. Regeringen berör också den här frågan om eventuella konflikter mellan lagarna i propositionen till cybersäkerhetslagen, efter att flera remissinstanser ställt frågor kring detta på

lagstiftningsnivå. Regeringen påpekar att det inte finns utrymme, givet direktivets innehåll och regelverkens olika syften och tillämpningsområden, att till exempel låta ett av regelverken vara subsidiärt i förhållande till det andra. Regeringen har vidare i propositionen till cybersäkerhetslagen bedömt att den administrativa börda som dubbla anmälningar kan innebära är godtagbar.⁹

PTS bemöter Tele2s invändningar enligt följande: De föreslagna reglerna avser inte kategorin allvarliga driftsstörningar. Bestämmelserna avser sådana incidenter som blir betydande för att en incident hos verksamhetsutövaren har påverkat andra genom att vålla dem betydande skada. Dessutom är det ett missförstånd att en liknande identifieringsskyldighet som nu föreslås, inte fanns i nu upphävda föreskriften i 17 kap. 6 § PTSFS 2022:11. Det stämmer dock att det funnits ett krav att alltid inkludera information i en incidentrapport enligt de tidigare reglerna om ifall incidenten också medfört störningar på nödkommunikation. Men utöver detta fanns kravet på rapporteringsskyldighet enligt den nu upphävda enligt 17 kap. 6 § PTSFS 2022:11. Det har till den regeln funnits vägledning i PTS dåvarande rapporteringsblankett om rapporteringsplikten vid brister i nödkommunikation eller VMA skulle rapporteras enligt ENISA:s technical guidelines for incident reporting.¹⁰ PTS har i konsekvensutredningen till de nu upphävda rapporteringsföreskrifterna hänvisat tydligt till att rapportera ”security incidents which affect the access to 112 or national emergency numbers, have impact on public warning systems.”

Det stämmer att genomförandeförordningen inte omfattar en beskrivning av en betydande incident när förmedling av 112 eller VMA har misslyckats. Enligt PTS mening beror detta på att genomförandeförordningen inte omfattar telekomområdet, och det är telekomområdet som har plikterna att medverka till förmedling av nödkommunikation och VMA, inte några andra delar av sektorn för digital infrastruktur.

Tele2 och Tre har föreslagit att PTS i stället för bestämmelserna om betydande incidenter vid brister i förmedling av nödkommunikation eller VMA ska använda information från PTS samverkande roller. PTS tillsynande och sanktionsbestämmande roll har dock inte tillgång till den informationen, och det är viktigt att skilja mellan PTS samverkande och PTS tillsynande delar. Dessutom är medverkan till förmedling av nödkommunikation och VMA inte några samverkanskrav utan krav enligt lag. Det innebär att verksamhetsutövare ska uppfylla sin medverkan enligt lag och behöver ha kännedom om de har kunnat efterleva lagkraven.

SKR och Telia har påpekat att skyldigheterna för telekomverksamhetsutövarna endast rör tillgänglighet av nödkommunikation och VMA. Störningar av

⁹ Prop. 2025/26:28 s. 76–77 och s. 114–115.

¹⁰ [ENISA Technical Guideline on Incident Reporting under the EECR.pdf](#) s 21

konfidentialitet, autenticitet och riktighet i nödkommunikation eller VMA kan därför inte omfattas av vad som är en betydande incident inom telekomområdet.

PTS instämmer i påpekanden om att det utifrån hur lagkraven är formulerade är otydligt om störningar av konfidentialitet, autenticitet och riktighet i nödkommunikation, på grund av incidenter hos verksamhetsutövarna, kan vara betydande incidenter. Det är medverkan till avbrottsfri förmedling av nödkommunikation och VMA som avses i lagen.

PTS avgränsar därför båda reglerna till att endast omfatta de fall då verksamhetsutövaren vet eller har särskild anledning att anta att deras medverkan till förmedlingen av nödkommunikation eller VMA har misslyckats.

SOS Alarm och Tre beskriver att telekomverksamhetsutövare ofta inte känner till händelsekedjan vid nödkommunikation och inte har kännedom om vilka konsekvenser i nödkommunikation som kan uppstå vid verksamhetsutövarens egna driftsstörningar, trots att dessa incidenter kan ha allvarliga konsekvenser för nödkommunikation samt liv och hälsa.

Kunskapsbristen om ifall förmedling av nödkommunikation och VMA inte har fungerat medför att incidenter med potentiellt allvarlig påverkan riskerar att inte identifieras som betydande. SOS Alarm pekar på behovet av mer informationsdelning mellan aktörer inom nödkommunikationskedjan. SOS Alarm vill att verksamhetsutövarens dialog med beroende aktörer (till exempel SOS Alarm) ska vara mer omfattande, särskilt vid misstanke om påverkan på nödkommunikation.

PTS kan återkomma i frågor om kunskap, dialog och prioritering i tillsyn i syfte att skapa vägledning kring reglerna.

PTS avser att återkomma med exempel och ytterligare förtydligande i FAQ och en planerad vägledning.

PTS kommentarer och åtgärder kring betydande incidenter i förmedling av **VMA**:
Telia anför att bolaget inte har kännedom om huruvida VMA har kunnat förmedlas, eftersom den operativa funktionen är överlämnad till en underleverantör, och att bolaget därför inte har möjlighet att efterleva rapporteringsplikten. Telia anför också att det alltid föreligger viss felmarginal vid förmedling av VMA och att rapporteringsplikt borde utlösas först när en viss procentuell andel av VMA inte når fram.

Här vidhåller PTS det som framgår i konsekvensutredningen. Skyldigheten till medverkan till VMA åvilar den utpekade verksamhetsutövaren i 7 kap. 36 § LEK. Om en verksamhetsutövare har valt att anlita en underleverantör är verksamhetsutövaren fortfarande ansvarig enligt 7 kap. 36 § LEK och därmed ansvarig för identifiering av

betydande incidenter. Verksamhetsutövaren är också skyldig att säkerställa att tillräcklig information finns rörande underleverantörens drift för att kunna efterleva bestämmelser om vad som utgör betydande incidenter inom telekomområdet.

PTS vill förtydliga att det är verksamhetsutövarens medverkan till utsändningen av ett viktig meddelande till allmänheten både genom Cell Broadcast och genom SMS som är i fokus vid identifiering av en betydande incident av detta slag. Om ett meddelande skickats från nätet till avsedd terminalutrustning men inte kunnat tas emot av terminalutrustningen förutsätts det för att identifiera en betydande incident hos verksamhetsutövaren, att felet varit i verksamhetsutövarens nät, tjänst eller komponent för vidarebefordran av VMA.

Cell Broadcast är en envägstjänst utan återrapportering från terminalerna men komponenten för Cell Broadcast - CBC - hos verksamhetsutövaren kan normalt övervaka och logga hur en SE-Alert-begäran har behandlats och distribuerats i mobilnätet, exempelvis genom mottagande från komponenten CBE, distribution till berörda basstationer, kvittenser, felutfall och tidsförlopp, även kvittenser att VMA har levererats till basstation finns rimligen. CBC kan däremot normalt inte verifiera hur många mobiltelefoner som faktiskt mottagit eller visat ett VMA. Bedömning av utsändningens träffsäkerhet får därför i huvudsak baseras på nätets distributionsresultat och radiotäckning, snarare än på faktisk mottagning hos slutanvändarna.

Liksom vid betydande incidenter i medverkan till förmedling av nödkommunikation krävs det vetskap eller särskild anledning för verksamhetsutövaren att anta att dennes medverkan till förmedling av VMA har misslyckats. Sådan vetskap eller särskild anledning att anta ett misslyckat försök, kan verksamhetsutövaren få exempelvis genom den egna komponenten för VMA via Cell broadcast (CBC), genom information från SOS Alarm eller från annan involverad part i exempelvis ett kris- eller räddningsarbete, eller från berörda kunder eller slutanvändare som självant lämnar sådan information till verksamhetsutövaren. Det kan som Telia påpekar vara så att det finns en felmarginal eller andel av VMA som inte når fram. Det kan bero på flera olika anledningar. Men om det uppstår en särskild anledning för verksamhetsutövaren att anta att VMA inte har förmedlats av verksamhetsutövaren då ska en betydande incident identifieras.

Vad avser hur långt en telekomverksamhetsutövarens undersökningsinsatser sträcker sig för att identifiera den här typen av betydande incidenter gäller även här de generella bestämmelserna om bedömningen och informationsunderlag i 3 kap. i föreskrifterna. PTS kan komma att bedriva tillsyn i syfte att utreda frågorna som kan uppstå kring tillämpning av bestämmelserna.

PTS ändrar båda bestämmelserna för att skapa avgränsningen att det krävs särskild anledning att anta att förmedlingen inte har genomförts av verksamhetsutövaren, och för att tydliggöra att endast ett täckningsbortfall inte är tillräckligt för att identifiera betydande incidenter enligt dessa två bestämmelser.

4.6.3 Fysisk persons dödsfall, eller betydande skada på en fysisk persons hälsa

Både SOS Alarm och Myndigheten för delaktighet (MFD) ser positivt på regeln. Telenor har anfört att otillgänglighet till en tjänst i sig inte orsakar dödsfall eller personskador och att ett samband mellan en incident och sådana konsekvenser ofta kan vara svårt att fastställa.

PTS kommentar: PTS noterar Telenors synpunkt att otillgänglighet till en tjänst inte i sig orsakar dödsfall eller personskador och att sambandet mellan en incident och sådana konsekvenser ofta kan vara svårt att fastställa. PTS bedömer att det kan finnas situationer där en incident i ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har orsakat eller bidragit till en fysisk persons dödsfall eller betydande skada på hälsan. Detta kan exempelvis vara fallet om en fysisk person till följd av incidenten inte har kunnat kommunicera när sådan kommunikation varit nödvändig, exempelvis för att tillkalla hjälp eller ta emot viktig information. För att tydliggöra bestämmelsens tillämpningsområde ändras bestämmelsen så att den omfattar incidenter som har orsakat eller bidragit till en fysisk persons dödsfall eller betydande skada på hälsan. Det ska finnas ett faktiskt samband mellan incidenten och konsekvensen. Något krav på att incidenten ska vara den enda orsaken uppställs däremot inte.

PTS ändrar efter synpunkterna bestämmelsen genom kravet ”har orsakat eller bidragit till”.

4.7 Incidenter som alltid är betydande

PTS ändrar strukturen på föreskrifterna på så vis att det remitterade förslagets 3 kap. 7 § 1 p flyttas till 3 kap 2 §. Denna förändring genomförs efter flera frågor och farhågor från remissinstanserna om bedömningarna av de betydande incidenter som kan leda till skadeeffekter, men som inte ännu har gjort det. 3 kap. 2 § tydliggör nu att en betydande incident är:

1. En händelse som har medfört sådan påverkan eller sådana konsekvenser som anges i någon bestämmelse i denna författning.
2. Ett betydande cyberhot eller en betydande sårbarhet som innebär en risk som sannolikt kan orsaka, bidra till eller möjliggöra sådan påverkan eller sådana konsekvenser som anges i någon bestämmelse i denna författning.

3. En annan upptäckt risk eller händelse som sannolikt kan orsaka, bidra till eller möjliggöra sådan påverkan eller sådana konsekvenser som anges i någon bestämmelse i denna författning.

De resterande punkterna i det remitterade förslaget om sådana betydande incidenter som innebär risk för allvarlig driftstörning, ekonomisk skada för verksamhetsutövarens eller betydande skada för annan ligger kvar under förslagets bestämmelse. Den paragrafen i 4 kap. 5 § beskriver nu incidenter som alltid ska utgöra betydande incidenter, enligt följande:

1. En incident till följd av en naturkatastrof, oavsett incidentens omfattning enligt tabellen ovan, om den har undergrävt tillgängligheten i verksamhetsutövarens nät, tjänster eller uppgifter.
2. Ett internt eller externt angrepp på eller intrång i verksamhetsutövarens nät, tjänster eller uppgifter som innebär en identifierad risk för att orsaka allvarliga driftsstörningar.
3. En incident i central infrastruktur hos verksamhetsutövaren som under minst sex timmar har medfört betydande påverkan på den centrala infrastrukturens eller nätets stabilitet, motståndskraft eller på förmågan att skydda nät, tjänsters eller uppgifters tillgänglighet, riktighet, autenticitet eller konfidentialitet.
4. Nedsatt redundans i sådan central infrastruktur hos verksamhetsutövaren som har betydelse för nät eller tjänster mellan Sverige och ett annat land.

Förändringarna går igenom mer i detalj här nedanför.

4.7.1 Det remitterade förslaget ”identifierad risk för skadeeffekter” flyttas

Sammanfattning av synpunkter: AC-Net, Digimitt, Telia och Telenor anser att bestämmelsen riskerar att leda till bedömningar som bygger på antaganden eller spekulationer snarare än på objektiva konstaterbara omständigheter. Digimitt, Stadsnätetsföreningen och Telenor framhåller att bedömningen bör utgå från den information som verksamhetsutövaren faktiskt har tillgång till eller rimligen kan inhämta. Läkemedelsverket och Tre anser att bestämmelsen är språkligt och systematiskt svår att förstå. MCF, OneMore Secure och SKR efterfrågar ett tydligare samband mellan incidenter, betydande cyberhot och betydande sårbarheter. Sinch, Stokab, SKR och Telenor anser att sannolikhets- eller risktröskeln bör förtydligas eller höjas för att undvika att teoretiska risker eller identifierade sårbarheter utan tillräckligt konkret risk leder till rapporteringsplikt. OneMore Secure anser särskilt att betydande cyberhot och betydande sårbarheter inte bör behandlas som betydande incidenter utan en tydligare koppling till faktisk eller sannolik påverkan.

PTS kommentarer och åtgärder: Se ovan avsnitt 3.1.2 och 4.3.1.

PTS delar uppfattningen att bestämmelsen kan förenklas och att det behöver tydliggöras mer samlat att både incidenter som har lett till skadeeffekter och sådana incidenter som kan leda till skadeeffekter omfattas av vad som utgör betydande incidenter. Syftet med bestämmelsen är att säkerställa att inte enbart redan inträffade incidenter omfattas av identifieringsskyldigheten utan även situationer där det finns en identifierad risk för skadeeffekter ska inträffa, samt situationer där ett betydande cyberhot eller en betydande sårbarhet innebär en sådan risk. Mot denna bakgrund har bestämmelsen i förslaget 3 kap 7 § 1 p i stället i sin helhet arbetats in i 3 kap 2 §.

*PTS delar inte uppfattningen att endast redan realiserade skadeeffekter ska omfattas av vad som utgör en betydande incident. Cybersäkerhetslagen omfattar uttryckligen även incidenter och händelser som **kan** orsaka allvarlig driftsstörning, ekonomisk skada eller betydande skada för andra. Bedömningen måste därför också göras framåtblickande.*

Bestämmelsen tar inte sikte på rent teoretiska möjligheter eller allmänna säkerhetsbrister utan på situationer där det finns en kvalificerad och konkret risk för att en betydande incident ska inträffa.

PTS instämmer också i att bedömningen behöver göras utifrån en gemensamt känd bas för alla bedömningar och att det är lämpligt att dessa regleras i föreskrifterna. Detta genomför PTS genom att det nu uttryckligen framgår av 3 kap 1 § att bedömningar av betydande incidenter ska baseras på den information som verksamhetsutövaren faktiskt har tillgång till, har fått kännedom om eller rimligen kan inhämta, samt genom att 3 kap 2 § och de allmänna råden till båda bestämmelserna uttrycker att både händelser som har och som kan leda till skadeeffekter inom avgränsningarna som anges, är betydande incidenter.

PTS bedömer att den nya strukturen med att flytta bestämmelserna om bedömningar och informationsunderlag för varje typ av betydande incident till ett inledande kapitel i föreskrifterna gör regleringen tydligare, mer systematisk och enklare att tillämpa samtidigt som den tydliggör att betydande incidenter ska identifieras i vissa fall redan innan de negativa konsekvenserna fullt ut har realiserats.

4.7.2 Incidenter som alltid är betydande

4 kap. 5 § 1 – 4 p beskriver incidenter som alltid ska bedömas utgöra betydande incidenter. De händelser som anges i paragrafen är sådana att de, på grund av sin karaktär och den riskbild som normalt är förknippad med dem, typiskt sett innebär en påtaglig risk för elektroniska kommunikationens funktion, säkerhet eller motståndskraft. Sådana händelser är normalt förenade med en förhöjd sannolikhet

att orsaka, bidra till eller möjliggöra sådan påverkan eller sådana konsekvenser som anges i denna författning. Bestämmelsen innebär därför att de händelser som omfattas av paragrafen presumeras uppfylla förutsättningarna för att utgöra en betydande incident.

Bestämmelsen syftar till att underlätta verksamhetsutövarens bedömning genom att peka ut vissa incidenter och händelser som typiskt sett ska bedömas som betydande incidenter på grund av de risker som är förknippade med dem, eller de orsaker de har.

4.7.3 Tillgänglighetsstörningar till följd av naturkatastrof

Första punkten i 4 kap. 5 § avser incidenter till följd av naturkatastrofer och som har undergrävt tillgängligheten i nät, tjänster eller uppgifter. Naturkatastrofer kännetecknas av svårförutsägbara och ofta eskalerande följdverkningar som kan påverka återställningsförmåga, redundans och fortsatt drift. Även incidenter med begränsad initial omfattning kan därför medföra betydande konsekvenser eller skapa förutsättningar för ytterligare störningar.

Sammanfattning av synpunkter: Google, Tele2, Telenor och Tre ifrågasätter behovet av en särskild bestämmelse för betydande incidenter som har orsakats av naturkatastrofer. Tele2, Telenor och Tre framhåller även att den föreslagna bestämmelsen saknar tydliga tröskelvärden. Telia undrar om strömavbrott på grund av naturkatastrofer, där strömavbrottet i sin tur orsakar tillgänglighetsproblemen i nät och tjänster är samma sak som att tillgänglighetsproblemen har orsakats av en naturkatastrof. Telia undrar också om det har uppstått en betydande incident i de fall där verksamhetsutövaren har uppfyllt reservkraftskraven i PTS säkerhetsföreskrifter men incidenter pågår även efter att tiden för reservkraftskraven har löpt ut. Några remissinstanser ifrågasätter även kriteriet att den berörda naturkatastrofen ska omfatta minst en kommun och anser att det i sig saknar självständig betydelse. Telenor och Telia anser att det är svårt för en verksamhetsutövare att veta om andra verksamhetsutövare har nät eller tjänster i ett område och också om de därefter har påverkats av samma naturkatastrof.

PTS kommentarer och åtgärder: *PTS hänvisar inledningsvis till definitionen av naturkatastrof i 2 kap 1 § 8 p och till avsnittet om begreppet naturkatastrof i 4.2.2.6 ovan. Definitionen av naturkatastrof omfattar extrema naturhändelser som orsakar omfattande skador på människor, miljö eller egendom. Detta innebär en hög tröskel för vilka händelser som kan utlösa tillämpning av bestämmelsen. Eftersom naturkatastrofer är sällsynta händelser kommer ett lågt antal betydande incidenter behöva identifieras enligt denna bestämmelse.*

Det behöver samtidigt förtydligas, utifrån frågor i remissvaren, att förekomsten av en naturkatastrof i sig inte innebär att en betydande incident har inträffat. Det krävs att naturkatastrofen har lett till en incident som undergräver tillgängligheten till nät eller tjänster hos verksamhetsutövaren. Som svar på Telias fråga om strömavbrott till följd av en naturkatastrof omfattas av vad som är orsakat av en naturkatastrof anför PTS att alla sådana direkta och indirekta orsaker som har sin grund i naturkatastrofen omfattas av bestämmelsen. Om strömavbrottet har orsakats av en naturkatastrof och tillgänglighetsproblem i nät, tjänster och uppgifter uppstår till följd av strömavbrottet, har tillgänglighetsproblemen i grunden skett till följd av naturkatastrofen. Som svar på Telias fråga om en betydande incident anses uppkomma efter att verksamhetsutövaren har uppfyllt sina reservkraftskrav anför PTS att om tillgänglighetsproblem finns efter att tidskraven i PTS säkerhetsföreskrifter för reservkraft har löpt ut, uppstår en betydande incident.

Naturkatastrofer skiljer sig från andra incidentorsaker genom att de kännetecknas av ett omfattande samhällspåverkande förlopp och ett stort behov av fungerande elektronisk kommunikation. Liksom bestämmelsen om angrepp eller intrång i nät, tjänster eller uppgifter tar bestämmelsen sikte på en särskild incidentorsak där verksamhetsutövarens möjligheter att förebygga eller kontrollera händelseutvecklingen ofta är begränsade. Även en begränsad påverkan på tillgängligheten kan under sådana extrema förhållanden få betydande konsekvenser för slutanvändare och samhällsviktig verksamhet.

Erfarenhetsmässigt har incidenter som orsakats av naturkatastrofer endast rapporterats av vissa av de verksamhetsutövare som drabbats av säkerhetsincidenter, även i situationer där tidigare gällande tröskelvärden enligt PTS nu upphävda rapporteringsföreskrifter har uppnåtts. Detta har inneburit bristande enhetlighet i rapporteringen och en ofullständig bild av hur tillgängligheten till nät och tjänster påverkas under sådana förhållanden.

PTS har förståelse för synpunkterna om svårigheten att bedöma om andra verksamhetsutövare har drabbats av samma naturkatastrof samt den administrativa börda som följer av att behöva bedöma geografisk utbredning på kommunnivå. PTS delar däremot inte uppfattningen att bestämmelsen bör utgå. Med hänsyn till remissvaren har bestämmelsen dock förenklats och flyttats bestämmelsen från avsnittet om allvarliga driftstörningar, till avsnittet om incidenter som alltid ska bedömas som betydande.

Kraven tas bort om att verksamhetsutövaren ska fastställa att även andra verksamhetsutövare har drabbats av samma naturkatastrof eller att minst en kommun har drabbats har tagits bort för att minska den administrativa bördan och förenkla bedömningen. Förenklningarna och förflyttningen av bestämmelsen syftar till

att minska komplexiteten i att göra bedömningar enligt bestämmelsen för verksamhetsutövare.

Bestämmelsen ska tillämpas tillsammans med de generella bestämmelserna om bedömningen av betydande incidenter i 3 kap 1–2 §§. Det är också sannolikt att sådana extrema naturhändelser diskuteras inom Nationella telesamverkansgruppen (NTSG). PTS vill i sammanhanget framhålla att information som delas inom NTSG:s samverkansarbete inte generellt förs över till PTS tillsynsverksamhet. Information som delas i NTSG ska inte omedelbart riskera att en verksamhetsutövare påförs till exempel sanktionsavgifter.

Den förändrade bestämmelsen innebär att en incident som undergräver tillgängligheten till nät eller tjänster till följd av en naturkatastrof ska identifieras som en betydande incident. PTS bedömer att detta är proportionerligt eftersom naturkatastrofbegreppet har getts en snäv innebörd och endast omfattar extrema naturhändelser som orsakar omfattande skador på människor, miljö eller egendom.

PTS flyttar bestämmelsen från vad som anses utgöra allvarliga driftstörningar till avsnittet i föreskrifterna om incidenter som alltid ska bedömas som betydande incidenter. PTS anser att bestämmelsen är viktig för att skapa en bredare kunskap om cybersäkerheten under svåra naturförhållanden för de delar av PTS som arbetar med tillsyn av säkerhetsarbetet hos verksamhetsutövare inom telekomområdet.

PTS avser att komplettera bestämmelsen med frågor och svar (FAQ) eller vägledning som innehåller exempel på extrema naturhändelser som kan omfattas av bestämmelsen.

4.7.4 Intrång och angrepp

Andra punkten i 4 kap. 5 § avser interna eller externa angrepp och intrång i verksamhetsutövarens nät, tjänster eller uppgifter. Sådana händelser är typiskt sett förenade med risk för fortsatta angrepp, förlust av uppgifter, avbrott eller tillgänglighetsproblem i nät eller tjänster. Om angreppet eller intrånget av verksamhetsutövaren bedöms sannolikt kunna orsaka, bidra till eller möjliggöra allvarliga driftsstörningar ska incidenten alltid bedömas vara betydande.

Sammanfattning av synpunkter: OneMore Secure föreslår att bedömningen ska grundas på objektiva omständigheter som ger grundad anledning att anta att ett angrepp eller intrång har inträffat. Sinch, Stokab, Telenor och Tre anser att bestämmelsen bör knytas tydligare till en sannolik risk för allvarlig driftsstörning. Stokab föreslår att uttrycket "kan orsaka" ersätts med "sannolikt kan" eller "med hög grad av sannolikhet", medan Telenor och Tre efterfrågar ett tydligare krav på att risken för en allvarlig driftsstörning ska vara "påtaglig" och möjlig att konstatera på

objektiva grunder. Trafikverket ifrågasätter behovet av att bedöma om handlingen varit avsiktlig och föreslår att rekvisitet "avsiktlig" utgår. Telia är positiv till bestämmelsen på så vis att den är att föredra framför den uppsamlingsbestämmelse som föreslås om händelser som kan orsaka skadeeffekter enligt föreskrifterna och därför ska identifieras som betydande incidenter, eftersom den tar sikte på en konkret handling och inträffad incident.

PTS kommentar och åtgärd: *PTS noterar att flera remissinstanser har efterfrågat tydligare och mer objektiva kriterier för när ett angrepp eller intrång ska anses utgöra en betydande incident. OneMore Secure har anført att bestämmelsen bör kopplas till objektiva omständigheter som ger grundad anledning att anta att ett angrepp eller intrång har inträffat. Sinch, Stokab, Telenor och Tre har på olika sätt framhållit att uttrycket "kan orsaka" en allvarlig driftsstörning innebär en alltför låg eller oklar tröskel och riskerar att omfatta händelser där risken för allvarliga konsekvenser är endast teoretisk.*

PTS delar uppfattningen att bestämmelsen behöver vara tydligare. Syftet med bestämmelsen är att fånga upp situationer där verksamhetsutövarns nät, tjänster eller uppgifter har utsatts för ett angrepp eller intrång som innebär en sannolik risk för allvarlig driftsstörning, även om någon sådan driftsstörning ännu inte har inträffat.

PTS instämmer däremot inte i synpunkten att bestämmelsen bör begränsas till situationer där en allvarlig driftsstörning varit omedelbart förestående eller nära att realiseras. Ett framgångsrikt angrepp eller intrång mot nät, tjänster eller uppgifter kan innebära betydande risker för verksamhetsutövaren även om angreppet eller intrånget upptäcks och hanteras innan någon faktisk driftspåverkan uppstår. Det finns ett behov av en särskild bestämmelse som fångar denna typ av händelser.

Även genomförandeförordningen har bestämmelser som liknar denna bestämmelse och skäl 102 i NIS2-direktivet anger särskilt att en tidig varning bör ange om en betydande incident misstänks vara orsakad av olagliga eller avsiktligt skadliga handlingar. Också regeringen lyfter i propositionen fram vikten av att arbeta riskbaserat för att höja cybersäkerhetsnivån i Sverige och uttalar att krav på både säkerhetsåtgärder och incidentrapportering kan hjälpa till att förebygga avsiktliga angrepp. Regeringen lägger till att de riskbaserade bedömningarna kan leda till att brott som riktas mot tjänster inom kritiska sektorer förebyggs, upptäcks, förhindras och beivras.

Mot denna sammantagna bakgrund bedömer PTS att bestämmelsen ska finnas kvar men den har omformulerats för att förenkla.

PTS bedömer att den ändrade bestämmelsen ger en tydligare avgränsning av vilka händelser som ska identifieras som betydande incidenter samtidigt som den

säkerställer att angrepp och intrång uppmärksammas och identifieras som betydande och också rapporteras i ett tidigt skede.

4.7.5 Betydande incident i central infrastruktur

Tredje punkten avser incidenter i central infrastruktur som under minst sex timmar har medfört betydande påverkan på den centrala infrastrukturens eller nätets stabilitet, motståndskraft eller förmåga att skydda nät, tjänsters eller uppgifters tillgänglighet, riktighet, autenticitet eller konfidentialitet. Central infrastruktur har en särskild betydelse för elektroniska kommunikationers funktion. En betydande påverkan på sådan infrastruktur innebär normalt en förhöjd risk för störningar eller säkerhetsrelaterade konsekvenser även i andra delar av nätet.

Fjärde punkten har brutits ut och avser nedsättning av redundans i central infrastruktur mellan Sverige och ett annat land. Även om någon allvarig driftsstörning ännu inte har inträffat innebär en sådan händelse att nätets motståndskraft har försämrats. Detta medför normalt en förhöjd sannolikhet för framtida betydande konsekvenser och motiverar att incidenten alltid ska bedömas vara betydande.

Sammanfattning av synpunkter: OneMore Secure tillstyrker bestämmelsen men efterfrågar exempel på vilka typer av infrastruktur och händelser som omfattas. Tele2 och Telenor anser att bestämmelsen är för bred och riskerar att omfatta incidenter i infrastruktur där redundans redan har byggts in för att motverka negativa konsekvenser, och att det därför inte kommer att inträffa negativa konsekvenser. Telenor anser att bestämmelsen bör begränsas till kritisk gränsöverskridande infrastruktur, medan Telia liksom Tele2 och Telenor efterfrågar en tydligare avgränsning mot redundanta lösningar och anser att incidenter inte bör betraktas som betydande om tillräckliga alternativa förbindelser fortfarande finns tillgängliga.

Stokab anser att det finns skäl att även renodlade svartfiberleverantörer ska omfattas av kravet att identifiera betydande incidenter i central infrastruktur på det vis som PTS avser med definitionen och den särskilda bestämmelsen. Men Stokab informerar om att det är svårt att identifiera vilka passiva knutpunkter som är så betydelsefulla för kommunikationen eller näten regionalt, nationellt eller internationellt att dessa knutpunkter omfattas av definitionen. Detta beror bland annat på hur många kunder som har utrustning inplacerad i de passiva knutpunkterna. Stokab föreslår därför att det görs ett uttryckligt tillägg i definitionen av central infrastruktur med: ”knutpunkter i ett passivt allmänt elektroniskt kommunikationsnät där minst 50 organisationskunder har inplacerad utrustning för elektronisk kommunikation.” Stokab föreslår också ett tillägg i bestämmelsen med av betydande påverkan på ”den centrala infrastrukturens” eller nätets ...

PTS kommentar och åtgärd: Se även avsnitt 4.2.2.4 om definitionen av central infrastruktur.

Enligt artikel 23 i NIS2-direktivet ska behöriga myndigheter kunna bedöma om en betydande incident har eventuella gränsöverskridande verkningar. Också skäl 102 i NIS2-direktivet anger särskilt att en tidig varning bör ange om det är troligt att den betydande incidenten kommer få gränsöverskridande verkningar.

Utöver det skriver regeringen utförligt i propositionen om sådana incidenter som skapar skada på redundans:

”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. 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.”¹¹

PTS delar därför inte remissinstansers uppfattning om att förekomsten av redundans i nät med regional, nationell eller internationell betydelse innebär att incidenter i central telekominfrastruktur saknar betydelse. Syftet med redundans är att upprätthålla driften vid tillgänglighetsstörningar, men en incident som innebär att nätets stabilitet, motståndskraft och förmåga att hantera ytterligare störningar försämrats avsevärt är enligt PTS en betydande incident. Även om omedelbara konsekvenser för slutanvändare uteblir kan sådana incidenter därför vara av stor betydelse ur ett regionalt, nationellt och internationellt robusthets- och säkerhetsperspektiv.

PTS instämmer däremot i att den tidigare lydelsen var alltför öppen och att det fanns behov av en tydligare avgränsning. Bestämmelsen har därför omarbetats. Kravet på

¹¹ Prop. 2025/26:28 s. 105.

enbart en försämring av nätets stabilitet eller motståndskraft har ersatts med ett krav på att händelsen ska ha medfört en **betydande påverkan** på nätets stabilitet, motståndskraft eller förmåga att skydda nät, tjänster eller uppgifter. Därutöver införs ett krav på att sådan påverkan ska ha varat under **minst sex timmar**.

PTS lägger också till "betydande påverkan på "den centrala infrastrukturen" i bestämmelsen enligt Stokabs förslag. Stokabs andra förslag om ett tillägg i definitionen för att omfatta passiva knutpunkter kommer PTS att ta med sig till FAQ eller kommande vägledning om hur även ägare av passiva nät eller svartfibernät kan göra en bedömning. Exempelvis kan en sådan bedömning göras utifrån att ägaren till det passiva nätet vet att minst x antal kunder har utrustning placerad i den passiva knutpunkten. Stokab föreslår att ett bra gränsvärde för en sådan bedömning är att minst 50 organisationskunder har inplacerad utrustning för elektronisk kommunikation. PTS ser inte något hinder att med de föreskrifter som nu presenteras göra den typen av bedömningar för att avgöra om passiva knutpunkter utgör central infrastruktur.

PTS har ersatt uttrycket "kritisk internationell, nationell eller regional infrastruktur" med "central infrastruktur" och brutit ut den enskilda bestämmelsen på nedsatt redundans i central infrastruktur mellan Sverige och ett annat land till en enskild punkt. Ändringen till central infrastruktur görs för att tydligare beskriva vilken typ av infrastruktur som avses och för att undvika sammanblandning med begreppet kritisk infrastruktur enligt CER-direktivet och den reglering som genomför detta direktiv i svensk rätt.

PTS bedömer att det finns behov av att särskilt uppmärksamma situationer där redundans i central infrastruktur försämras mellan Sverige och andra länder. Därför skapas en enskild punkt i bestämmelsen om nedsatt redundans i central infrastruktur som har betydelse för nät eller tjänster mellan Sverige och ett annat land. Sådana situationer kan innebära att den internationella konnektiviteten blir särskilt sårbar även om någon tillgänglighetsstörning ännu inte har uppstått, men sannolikt kommer att uppstå. Erfarenhetsmässigt har PTS inte tidigare fått in någon incidentrapport om sådana kabelbrott, sabotage eller olycksfall med undervattenskablar mellan Sverige och andra länder som nu kommer att träffas av bestämmelsen.

PTS bedömer att de ändrade bestämmelserna ger en tydligare och mer proportionerlig avgränsning av vilka incidenter som ska identifieras som betydande samtidigt som incidenter som påverkar central infrastruktur och internationell konnektivitet fångas upp. PTS avser även att i vägledning eller FAQ lämna exempel på den typ av infrastruktur och incidenter som normalt omfattas av bestämmelsen.

4.8 Återkommande incidenter

Sammanfattning av synpunkter: Digimitt, Stadsnätsföreningen och Telenor efterfrågar förtydliganden om hur bestämmelsen ska tillämpas i praktiken, särskilt när det gäller bedömningen av om flera incidenter har samma bakomliggande orsak. Digimitt framhåller att återkommande incidenter inte bör bedömas som en sammanhållen betydande incident enbart på grund av likartade symptom, utan att det behöver finnas ett dokumenterat eller rimligt klarlagt samband mellan incidenterna. OneMore Secure och SOS Alarm anser att bestämmelsen inte bör begränsas till ekonomisk skada utan även omfatta återkommande incidenter som sammantaget orsakar betydande påverkan på exempelvis nödkommunikation eller samhällsviktiga funktioner.

PTS kommentar: PTS delar uppfattningen att det måste finnas ett tydligt samband mellan de återkommande incidenterna för att bestämmelsen ska vara tillämplig. Kravet på att incidenterna ska bedömas ha samma orsak, sårbarhet, bristande säkerhetsåtgärd, rutin eller redundanta lösning innebär att det inte är tillräckligt att incidenterna uppvisar likartade symptom eller effekter. Bestämmelsen tar sikte på situationer där återkommande incidenter kan härledas till samma underliggande problem.

PTS delar däremot inte synpunkten att bestämmelsen bör utvidgas till att omfatta andra typer av skadeeffekter än ekonomisk skada. Bestämmelsen motsvarar i huvudsak regleringen i kommissionens genomförandeförordning (EU) 2024/2690 för återkommande incidenter. Syftet är att fånga situationer där flera mindre incidenter, som var för sig inte uppnår tröskelvärdena för en betydande incident, sammantaget orsakar en ekonomisk skada av sådan omfattning att incidenterna bör betraktas som betydande.

PTS bedömer därför att bestämmelsen är ändamålsenligt utformad och behåller den utan ändringar. Frågor om tillämpningen, bland annat bedömningen av gemensam orsak och dokumentation av sambandet mellan återkommande incidenter, kommer att besvaras i frågor och svar (FAQ) och i en planerad vägledning.

I konsekvensutredningen till dessa föreskrifter slogs följande fast: 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.

1. Avslutning

PTS vill tacka samtliga remissinstanser för alla inkomna synpunkter.