2025-03-05 Rapport RapportnummerPTS-ER-2025:5

Incident- och tillsynsrapport inom området säker kommunikation 2024

Rapportnummer
PTS-ER-2025:5

Diarienummer
25-2886

ISSN
1650-9862

Författare
Kristin Liljegren och Melinda Nilsson, avdelningen för säker kommunikation

Post- och telestyrelsen
Box 6101
102 32 Stockholm

08-678 55 00
pts@pts.se
www.pts.se

Innehåll

Sammanfattning

Tillhandahållare av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster (nät och tjänster eller elektroniska kommunikationer) är skyldiga att rapportera vissa incidenter till Post- och telestyrelsen (PTS) enligt lagen (2022:482) om elektronisk kommunikation (LEK). PTS är tillsynsmyndighet på området. I sammanställningen kallas de aktörer som rapporterar incidenter för tillhandahållare.

PTS har i denna rapport sammanställt och grupperat dessa rapporterade integritets- och säkerhetsincidenter.[1] PTS kommenterar också fördelningen mellan olika typer av incidenter, grundorsakerna till dessa och vilka eventuella mönster som går att urskilja i de inrapporterade incidenterna. Här finns också övergripande jämförelser med tidigare år. Totalt har PTS under år 2024 registrerat 435 rapporterade incidenter. Det rör sig om 401 integritetsincidenter och 34 säkerhetsincidenter. Av de 401 inkomna integritetsincidenterna bedöms 394 av dessa utgöra regelrätta integritetsincidenter. De sju incidentrapporter som räknats bort utgörs av återkallade incidentrapporter, dubbelregistrerade incidentrapporter eller incidentrapporter där PTS bedömt att ingen incident har skett.

Totalt drabbades 79 585 användare eller abonnenter enligt rapporteringen till PTS av integritetsincidenter under 2024. Motsvarande antal år 2023 var 83 269. Säkerhetsincidenter drabbade 456 053 användare eller aktiva anslutningar under 2024. År 2023 var siffran 3 442 948. En förklaring till minskningen i antal drabbade kan vara att det under 2024 inrapporterades totalt 14 säkerhetsincidenter med 0 antal påverkade, där tillhandahållaren istället valt att beskriva ett procentuellt kapacitetsbortfall eller ett bortfall över ett geografiskt område. Således behöver det inte vara så att en stor minskning skett.

Fördelningen av de inrapporterade incidenterna är likt föregående år ojämn mellan tillhandahållarna. Det ska påpekas att det inte är säkert att det finns ett samband mellan att de tillhandahållare som rapporterar in ett högt antal incidenter har sämre säkerhet i sina nät och tjänster. Vissa tillhandahållare upptäcker fler incidenter eller kan ha mer välutvecklade rutiner för rapportering av incidenter internt, vilket gör att de därför rapporterar mer till PTS. Incidentrapporteringen utgör ett viktigt underlag både för det förebyggande säkerhetsarbetet hos rapporterande tillhandahållare och för PTS tillsynsarbete då rapporterna innehåller värdefull information om säkerhetsarbete och eventuella brister, som bland annat kan ligga till grund för PTS bedömning av om det är motiverat att inleda tillsyn. Det är därför viktigt att PTS får kännedom om samtliga rapporteringspliktiga incidenter för att kunna agera vid

[1] Se avsnitt 1.1.1 och 1.1.2 för definitioner av begreppen integritetsincident och säkerhetsincident.

misstanke om brister i tillhandahållares säkerhetsarbete. En hög rapporteringsgrad är alltså inte att se som något negativt.

De två vanligaste grundorsakerna till rapporterade integritetsincidenter under 2024 var brister i organisatoriska rutiner och processer samt mänskliga misstag eller felbedömningar. För säkerhetsincidenter under 2024 var de vanligaste grundorsakerna systemfel och antagonistiska angrepp.

PTS analyserar incidenterna och kan använda analysen som underlag vid planeringen och genomförandet av tillsynsinsatser.

Syftet med sammanställningen

PTS vill genom denna rapport sprida kunskap om föregående års incidentläge till tillhandahållare och övriga intressenter i samhället. Genom sammanställningen vill PTS förmedla information om de vanligaste orsakerna till inträffade säkerhets- och integritetsincidenter inklusive övriga orsaker till inrapporterade incidenter som kan vara intressanta utifrån gällande regler om skydd för uppgifter och säkerhet i nät och tjänster. Orsakerna till de rapporterade incidenterna kan indikera områden som kräver ytterligare tekniska eller organisatoriska åtgärder hos tillhandahållarna. Sammanställningen kan också användas för planeringen av tillsynsinsatser hos PTS och för planering av tillhandahållares förebyggande arbete.

1. Incidentrapporter under 2024

Både säkerhetsincidenter med betydande påverkan på nät och tjänster eller funktioner i samhället och integritetsincidenter är rapporteringspliktiga till PTS enligt 8 kap 3 och 8 §§ LEK, Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTSFS 2022:11) och EU-kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation (hädanefter förordning 611/2013). Händelser som utgör rapporteringspliktiga säkerhetsincidenter kan ibland även behöva rapporteras som en integritetsincident, och vice versa.

Incidentrapporterna ger PTS underlag att bedöma hur bestämmelserna om säkerhet i nät och tjänster eller skydd av behandlade uppgifter efterföljs, och om tillsyn behöver inledas. Det finns även andra syften med incidentrapporteringen, t.ex. för att skapa en överblick över tillhandahållarnas säkerhetsproblem, som underlag till ny reglering, för att identifiera informationsbehov eller behov av främjandeinsatser.

Totalt under 2024 har PTS registrerat 435 ärenden med rapporterade incidenter, varav 428 slutligt har bedömts som rapporteringspliktiga incidenter. Av de rapporterade incidenterna finns det fall, två stycken år 2024, då incidenten är både en säkerhetsincident och integritetsincident. Incidenten har då i statistiken redovisats endast som en av incidenttyperna om inte tillhandahållaren skickat in två separata incidentrapporter.

1.1 Integritetsincident

I 1 kap. 7 § LEK definieras *integritetsincident* som:

En händelse som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster.

Incidenter som har medfört obehörig tillgång till behandlade uppgifter, förvanskning, förlust eller radering av sådana uppgifter ska således rapporteras som integritetsincidenter. Även händelser som innebär att tillhandahållare tillfälligt inte kan komma åt uppgifter (temporär förlust), t.ex. som en följd av en överbelastningsattack, utgör en integritetsincident.

1.2 Säkerhetsincident

I 1 kap. 7 § LEK definieras *säkerhetsincident* som:

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

Begreppet tar sikte på förmågan att upprätthålla avsedd funktion och skydd mot oönskad påverkan eller förändring i ett nät eller system. Det tar också sikte på skydd mot att uppgifter som har lagrats eller överförts oavsiktligt eller olagligt förstörs, förloras eller ändras.

Säkerhetsincidenter ska rapporteras utifrån vissa angivna tröskelvärden som anges i PTS föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTSFS 2022:11).

2. Integritetsincidenter under 2024

Under 2024 registrerades 401 ärenden gällande integritetsincidenter hos PTS. Efter genomgång och granskning anses 394 av dessa utgöra regelrätta integritetsincidenter. Det justerade antalet beror på att tillhandahållare återkallat vissa incidentrapporter, några rapporterade händelser som PTS inte bedömer som integritetsincidenter och händelser som dubbelregistrerats hos PTS.

Totalt har 79 585 användare eller abonnenter drabbats av integritetsincidenter 2024.

Antal incidenter har alltså ökat samtidigt som antal drabbade har minskat något sedan föregående år då motsvarande siffra 2023 var 304 incidenter och 83 269 drabbade.

2.1 Bakgrund

Sedan 2011 är tillhandahållare skyldiga att rapportera inträffade integritetsincidenter till PTS. Skyldigheten grundas på att tillhandahållarna ska skydda alla uppgifter som behandlas i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster. Det innebär att skyldigheten att skydda uppgifter inte bara avser personuppgifter, utan skyddet ska avse *alla uppgifter* som tillhandahållarna behandlar i samband med tillhandahållandet av elektroniska kommunikationstjänster.

Utöver kravet att skydda uppgifter som behandlas har tillhandahållarna också en uttrycklig tystnadsplikt för uppgifter om abonnemang, innehållet i ett elektroniskt meddelande eller annan uppgift som angår ett särskilt elektroniskt meddelande. Tillhandahållarna får som huvudregel inte föra sådana uppgifter vidare.

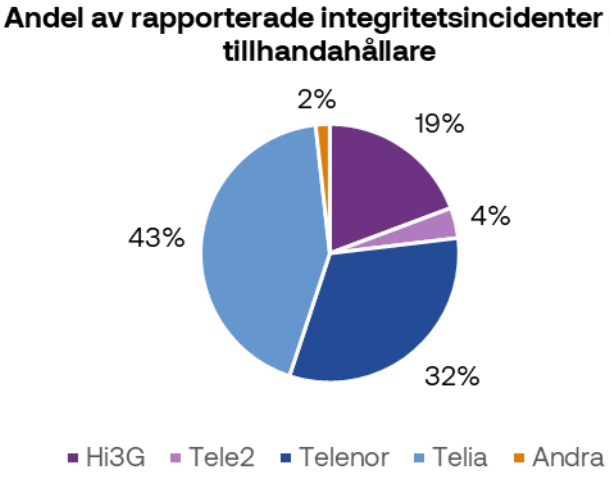
Händelser med olovliga avslöjanden, olovliga ändringar av uppgifter/tjänster och förluster av uppgifter/tjänster hos tillhandahållarna är integritetsincidenter enligt LEK. Det rör sig om sådana händelser som att uppgifter raderas eller registreras in fel hos tillhandahållaren, obehöriga ändringar eller nytecknande av abonnemang, eller läckta uppgifter till obehöriga.

Integritetsincidenter utgör potentiellt allvarliga hot mot tilltron till elektroniska kommunikationstjänster. När uppgifter som behandlas av tillhandahållaren sprids till utomstående, ändras obehörigen eller går förlorade, kan det få allvarliga konsekvenser. Om sådana händelser inte hanteras på ett lämpligt sätt kan det leda till såväl ekonomisk skada som personlig kränkning och skada för abonnenter och användare.

2.2 Alla tillhandahållare rapporterar inte lika många integritetsincidenter

PTS kan även i detta års sammanställning konstatera en ojämn fördelning av rapporterade incidenter mellan tillhandahållare.

PTS bedömning är att den ojämna fördelningen inte är relaterad till tillhandahållarnas storlek. Orsaken till den ojämna fördelningen är inte känd. Det kan vara så att vissa tillhandahållare upptäcker fler incidenter eller har mer välutvecklade rutiner för rapportering av incidenter internt, vilket gör att de rapporterar mer till PTS.



PTS uppmanar alla tillhandahållare att vid tveksamheter kring huruvida en händelse utgör en integritetsincident hellre rapportera händelsen än att inte göra det.

2.3 Orsaker till integritetsincidenter 2024

För att synliggöra grundorsaker och mer detaljerade orsaker, typer eller konsekvenser av integritetsincidenter under 2024 presenteras här nedan en tabell.

I tabellen har PTS utgått från EU:s cybersäkerhetsbyrå (Enisa) klassificering av grundorsaker till incidenter i nät och tjänster samt Integritetsskyddsmyndighetens (IMY) uppställning av grundorsaker till personuppgiftsincidenter som rapporterats till IMY.[2]

[2] Tilläggen som PTS har gjort till IMY:s orsaker är i kategorin för antagonistiskt angrepp där PTS lagt till cyberattack. PTS har även lagt till orsaken medvetet angrepp från någon utanför organisationen. I den avses inte antagonistiska angrepp som cyberattacker, utan sådant som bedrägerier eller förföljelse av kunder.

Utöver grundorsaker i tabellen, presenteras också detaljerade orsaker, typer och konsekvenser som återfinns i incidenterna. Dessa detaljer fördjupar bilden av vilka typer av incidenter det rör sig om. Syftet är att åskådliggöra var det kan finnas anledning att införa riktade åtgärder, eller för att kartlägga eller följa upp en viss specifik händelse av någon annan anledning.

En incident tilldelas en grundorsak (vänstra kolumnen) men kan innehålla flera detaljerade orsaker, typer och konsekvenser (högra kolumnen). T.ex. kan en incident där en olovlig kreditkontroll gjorts kategoriseras som grundorsak *brister i organisatoriska rutiner och processer* och sedan både med *olovliga kreditupplysningar* och *felaktiga e-postadresser* i kolumnen detaljerade orsaker, typer och konsekvenser. Det leder till att det totala antalet i kolumnen för detaljerade orsaker, typer och konsekvenser blir något högre än det totala antalet grundorsaker. Syftet med att ange fler detaljerade orsaker är att PTS vill tydliggöra de särskilt problematiska situationer som upprepar sig, när det är möjligt. På så vis är sammanställningen tänkt att kunna vara en utgångspunkt för tillhandahållarens arbete med att identifiera om någon riktad teknisk eller organisatorisk åtgärd kan motverka eller förebygga incidenter i framtiden i tillhandahållarens egen verksamhet.

Grundorsaker till integritetsincidenter	**Detaljerade orsaker, typer och konsekvenser till integritetsincidenterna**
276 incidenter orsakades av brister i organisatoriska rutiner och processer	Varav 135 olovliga kreditupplysningar 64 felaktiga e-postadresser 61 extern leverantör/underleverantör 55 förväxlingar av kunder 53 butik 52 handhavandefel 30 bristande autentiseringar 21 brister i kundtjänst per telefon 16 nyteckningar 15 bedrägeri 14 felaktiga kontaktuppgifter (ej e-post) 8 SIM-kort 6 brister i kundtjänst via chatt 4 förvaltare/god man

	2 systemfel 2 fel i mjukvara 1 skyddad identitet 1 dummy-uppgift 1 felpackning 1 försäkringar 1 mina sidor **= 543**
79 berodde på mänskliga misstag eller felbedömningar	Varav 52 handhavandefel 30 felaktiga e-postadresser 18 förväxlingar av kunder 11 SIM-kort 10 butik 7 olovliga kreditupplysningar 6 felpackningar 6 felaktiga kontaktuppgifter (ej e-post) 6 bristande autentiseringar 4 brist i kundtjänst per telefon 4 extern leverantör/underleverantör 3 nyteckningar 2 porteringar 1 brist i kundtjänst via chatt 1 migrering 1 förvaltare/god man 1 mina sidor 1 bedrägeri **= 164**
24 orsakades av tekniska fel	Varav 13 systemfel 8 fel i mjukvara 4 mina sidor 4 extern leverantör/underleverantör

	3 planerat arbete 2 förväxling av kunder 2 bristande autentisering 2 migreringar 1 portering 1 kommunikationsoperatör 1 felaktiga kontaktuppgifter 1 nyteckning **= 42**
6 incidenter berodde på antagonistiska angrepp 2 av dessa berodde på ett medvetet angrepp av någon inom organisationen	Varav 2 bedrägerier 2 cybersäkerhetsangrepp 2 handhavandefel 1 automatiserat angrepp 1 mina sidor 1 butik **= 9**
6 incidenter orsakades av tredje part	Varav 3 extern leverantör/underleverantör 1 cybersäkerhetsangrepp 1 handhavandefel 1 förväxling avkund 1 felaktiga kontaktuppgifter 1 felaktig e-postadress 1 systemfel **= 9**
1 incident hade oklar orsak	Varav 1 systemfel **= 1**

2.3.1 PTS kommentarer till 2024 års rapporterade orsaker

2.3.2 Olovliga kreditupplysningar

PTS har under 2024, likt föregående år, fått in ett stort antal incidenter gällande kreditupplysningar tagna olovligt i samband med tillhandahållandet av elektroniska kommunikationstjänster. I de flesta fall handlar det om en fysisk person som efterfrågat en prisuppgift, utan någon avsikt att teckna avtal, och där det av misstag inhämtats en kreditupplysning på individen.

PTS inledde en tillsyn mot Telia och Telenor för att följa upp detta, se kapitel 4.1.1. Antalet incidenter har efter avslutad tillsyn märkbart minskat. De enskilda incidenterna omfattar enbart en drabbad slutanvändare per incident. Det går inte att utesluta att det kan uppstå negativa konsekvenser för drabbade i de enskilda fallen då kreditupplysningar har tagits ut på personer utan laglig grund för det.

2.3.3 Felaktig e-postadress

Under 2024 var en av de mest rapporterade integritetsincidenterna felaktiga e-postadresser. Ofta har personal hos tillhandahållare alternativt underleverantör, eller kunden själv, av misstag blandat ihop e-postadressen eller stavat fel vilket lett till att e-post skickats till fel person med uppgifter om exempelvis abonnemang, utskick av bekräftelse och liknande.

Denna typ av incident drabbar oftast en eller ett par personer åt gången. PTS bedömer att riskerna för större personliga integritetsskador till följd av den här typen av incidenter är minde än vid andra typer, t.ex. då obehörig uppsåtligt orsakat incidenten.

Tillhandahållarna uppger regelmässigt i incidentrapporteringen att denna typ av incident inträffar p.g.a. mänskliga misstag. PTS uppfattar snarare att den frekvens med vilken e-postincidenterna inträffar tyder på brister i organisatoriska rutiner och processer hos tillhandahållarna eller deras återförsäljare. Det bör finnas utrymme för tillhandahållarna att utveckla metoder för att minska utrymmet för dessa mänskliga felskrivningar och därmed även minska incidenterna med felaktiga e-postadresser.

2.3.4 Rapportering från tillhandahållare av nummeroberoende interpersonella kommunikationstjänster

PTS noterar att få tillhandahållare av nummeroberoende interpersonella kommunikationstjänster har rapporterat incidenter under 2024. Endast en integritetsincident har rapporterats. Denna grupp av aktörer innefattar tillhandahållare av t.ex. e-posttjänster och olika typer av kommunikationsapplikationer (t.ex. tjänster för meddelanden, chatt, röstsamtal, videosamtal och gruppsamtal).

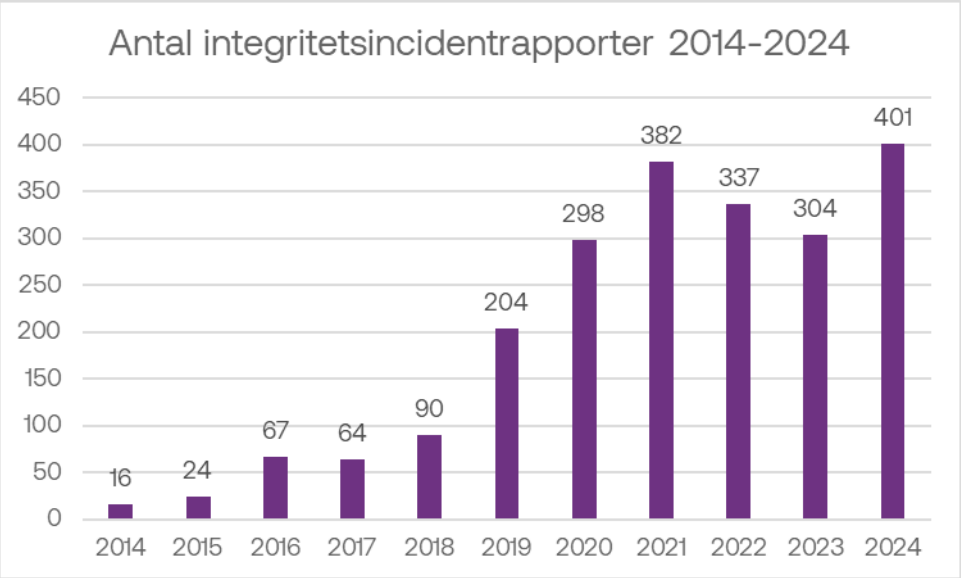
Rapporteringsplikten gäller för dessa tillhandahållare om de tillhandahåller sina tjänster i Sverige, oavsett var de är etablerade.

2.3.5 Sent inrapporterade integritetsincidenter

PTS har under året konstaterat att rapporter även under 2024 inkommer efter den fastslagna tidsfristen, enligt PTSFS 2022:11 samt LEK. I stället för att lämna in en inledande rapport när incidenten upptäcks tycks tillhandahållare invänta att incidenten är sluthanterad internt, varpå PTS erhåller en fullständig rapport. Detta ser PTS som problematiskt då tidsfristerna är tydligt fastslagna och inte ger utrymme för en sådan hantering av tillhandahållarna.

2.4 En jämförelse med tidigare års integritetsincidenter

Under 2024 vände de två senaste årens trend med färre integritetsincidenter än föregående år. Antalet inrapporterade integritetsincidenter har ökat från 2023 års antal om 304 stycken till 401 stycken år 2024, se tabell nedan.



PTS vill förmedla är att de senaste fem årens totala ökning av incidentrapporter inte nödvändigtvis beror på en motsvarande ökning av faktiska incidenter, utan kan till viss del bero på tillhandahållarnas förbättrade arbete med att upptäcka och rapportera incidenter till PTS. Myndigheten utgår ifrån att det har funnits och fortfarande finns ett mörkertal av integritetsincidenter som inte upptäcks eller rapporteras. Vidare PTS noterar att det har skett en ökning av inrapporterade integritetsincidenter det senaste året. Det är möjligt att ett ökat säkerhetsarbete och

ökat fokus på säkerhet p.g.a. omvärldsläget samt förändringar i tillhandahållarnas rapporteringsprocess påverkat förekomsten av incidenter. Ovanstående möjliga förklaringar till de högre siffrorna för 2024 är endast PTS antaganden och kan inte utläsas från statistiken.

3. Säkerhetsincidenter 2024

Enligt LEK är tillhandahållare skyldiga att rapportera säkerhetsincidenter med betydande påverkan på nät och tjänster till PTS.

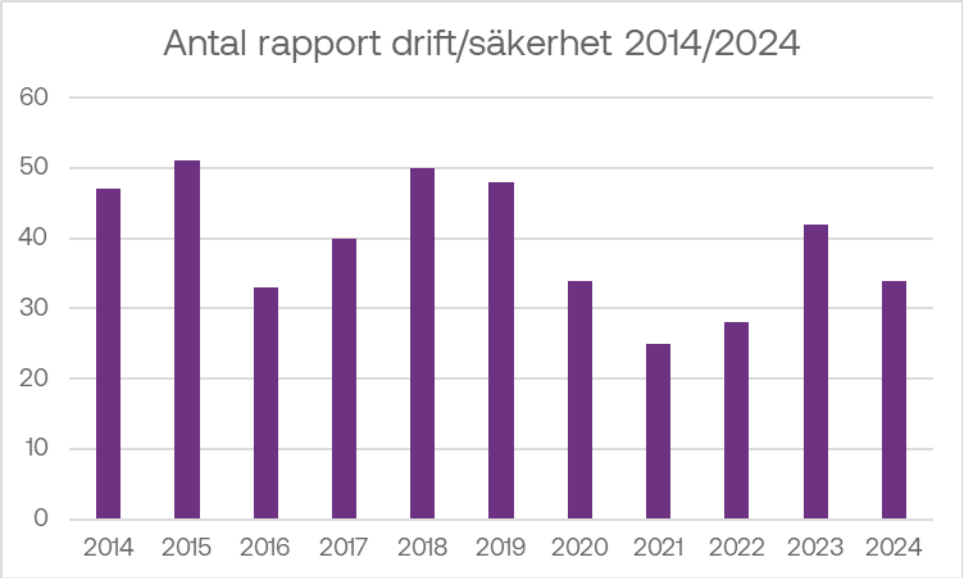
Under 2024 har PTS registrerat 34 ärenden avseende säkerhetsincidenter.

456 053 användare eller aktiva anslutningar[3] har enligt rapporterna drabbats av säkerhetsincidenter. I flera ärenden är det emellertid oklart, eller inte angett i rapporteringen, exakt hur många användare eller aktiva anslutningar som har drabbats. Siffran ska därför ses som ett estimat. Exempelvis har det i vissa ärenden gällande störning i tjänster inte gått att avgöra hur många användare eller aktiva anslutningar som faktiskt drabbats av störningen och i stället har det totala antalet användare som använder tjänsten angetts. I andra ärenden där tillhandahållaren inte har meddelat PTS hur många som har drabbats har tillhandahållaren istället angett ett 100 procentigt kapacitetsbortfall men antalet drabbade visas som 0. Under 2024 inrapporterades totalt 14 säkerhetsincidenter med angiven siffra 0. Detta kan förklara skillnaden mellan 2023 års antal drabbade användare eller aktiva anslutningar jämfört med den stora minskningen år 2024.

3.1 En jämförelse med tidigare år

Antalet rapporterade säkerhetsincidenter 2024 är lägre än föregående år, men inom normalintervallen för rapportering. PTS brukar få in mellan 30 och 50 rapporter om säkerhetsincidenter som påverkat nät och tjänster per år. Samtidigt som antalet rapporter har minskat så har också antalet drabbade användare eller aktiva anslutningar minskat jämfört med år 2023, dock med reservation för ospecificerade bortfall som beskrivits i stycket ovan.

[3] Begreppet ”aktiv anslutning” används i föreskriften PTSFS 2022:11 för att beteckna en anslutning till ett kommunikationsnät eller en kommunikationstjänst som möjliggör omedelbar användning av kommunikationstjänster. Uttrycket har införts då det finns aktörer (tillhandahållare) i värdekedjan av allmänna elektroniska kommunikationsnät och -tjänster som inte innehar slutkunder, men väl tjänsteleverantörer som i sin tur har slutkunder, ”användare”.



År med fler incidentrapporter kan ofta förklaras med att en eller flera säkerhetsincidenter har drabbat någon av kommunikationsoperatörerna (s.k. KO).[4] Störningar och avbrott hos en KO kan med stor sannolikhet generera flera enskilda incidentrapporter till PTS, eftersom många tillhandahållare är beroende av KO:ns tjänster. Samtliga tillhandahållare som berörs av en händelse ska rapportera incidenten självständigt till PTS om trösklarna för rapporteringsplikten är uppnådda.

3.1.1 Alla säkerhetsincidenter ska inte rapporteras till PTS

Enligt reglerna i LEK och PTS föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTSFS 2022:11) är det säkerhetsincidenter med betydande påverkan på nät och tjänster eller betydande påverkan på funktioner i samhället som ska rapporteras till PTS. PTS har i sin rapporteringsblankett givit vägledning gällande vad som utgör betydande påverkan på nät och tjänster. För säkerhetsincidenter som innebär störningar och avbrott (tillgänglighet) finns särskilda tröskelvärden för rapporteringsplikt angivna.[5]

Utöver störningar och avbrott som når upp till dessa tröskelvärden ska säkerhetsincidenter, oavsett om de avser störningar och avbrott eller berör någon av

[4] En nätägare kan lägga ut driften av den aktiva utrustningen i sitt nät till en KO. Så gör i många fall de kommunala stadsnätsbolagen vad gäller driften av lokala fibernät. KO:n får då tillträde till fibernätet och kan producera förädlade tjänster till tillhandahållarna. Om KO:n administrerar nätet dirigeras ofta datatrafiken via en plattform där slutanvändaren väljer vilken tillhandahållare denne vill köpa bredbandstjänster av.

[5] Trösklarna för rapportering av säkerhetsincidenter med betydande påverkan på tillgänglighet i nät och tjänster finns i 17 kap.5 § PTSFS 2022:11.

de andra säkerhetsaspekterna (autenticitet, riktighet eller konfidentialitet), rapporteras till PTS om incidenten på annat sätt har haft en betydande påverkan på kommunikationsnätet eller kommunikationstjänsten eller betydande påverkan på funktioner i samhället. Omständigheter som särskilt har betydelse för bedömningen av om en säkerhetsincident har haft en betydande påverkan är t.ex.:

- antal användare som påverkas av incidenten
- hur länge säkerhetsincidenten varar
- storleken på det drabbade geografiska området
- i vilken utsträckning nätet eller tjänsten påverkas
- i vilken utsträckning ekonomisk och samhällelig verksamhet påverkas.

PTS har under 2024 mottagit ett antal incidentrapporter med betydande påverkan på *funktioner i samhället*.[6] Totalt tolv av 34 rapporterade säkerhetsincidenterna under 2024 har påverkat funktioner i samhället. Funktioner i samhället kan vara exempelvis påverkan på möjligheten att nå nödkommunikation eller andra samhällsviktiga nummer såsom 114 14 eller 1177. PTS följer noggrant utvecklingen av rapporteringen vad gäller händelser som påverkar funktioner i samhället.

Det är enbart säkerhetsincidenter som har *en betydande* påverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten i nät och tjänster som är rapporteringspliktiga till PTS. PTS har därför inte en heltäckande bild av samtliga säkerhetsincidenter som inträffar inom området elektroniska kommunikationer utan endast beträffande de säkerhetsincidenter som rapporterats till PTS.

3.2 Orsaker till säkerhetsincidenter 2024

De inrapporterade, rapporteringspliktiga säkerhetsincidenterna, 34 stycken, har delats in i kategorier baserade på *grundorsaker* och *detaljerade orsaker, typer och konsekvenser*. Indelningen följer i stort Enisas indelning i grundorsaker (root causes[7]) och detaljerade orsaker (detailed or technical causes).

15 av de 34 incidenterna har sin grundorsak i *systemfel*[8] och sex har sin grundorsak i *antagonistiska angrepp*. Incidenter har endast räknats en gång i tabellen och

[6] ENISA har lämnat exempel på påverkan på ekonomisk och samhällelig verksamhet (eller på funktioner i samhället enligt uttrycket i prop. 2021/22:136). Se ENISA Technical Guideline on Incident Reporting under the EECC.pdf

[7] Enisas fem root causes: System failure, Human error, Third party failure, Natural phenomena, Malicious action. SE ENISA Technical Guideline on Incident Reporting under the EECC.pdf

[8] Enligt Enisa så bör kategorin "systemfel" användas för incidenter som orsakats av fel i ett system, till exempel hårdvarufel, mjukvarufel eller brister i manualer, rutiner eller policyer. Se ENISA Technical Guideline on Incident Reporting under the EECC.pdf s.26

förekommer alltså inte i två grundorsakskategorier. Däremot kan en incident ha flera detaljerade orsaker, typer och konsekvenser varvid summan av dessa orsaker överstiger totalen.

Här presenteras grundorsaker och detaljerade orsaker, typer och konsekvenser till rapporterade säkerhetsincidenter under 2024 i en tabell. Indelningen är skapad för att förtydliga orsaker och för att belysa de områden där det kan finnas anledning att vidta åtgärder för att förhindra ytterligare säkerhetsincidenter.

Grundorsaker till säkerhetsincidenterna	**Detaljerade orsaker, typer och konsekvenser till säkerhetsincidenterna**
15 incidenter orsakades av systemfel	Varav 6 felaktiga uppdateringar av mjukvara 5 mjukvarubuggar 2 strömavbrott 2 hårdvarufel 1 kylaravbrott 1 avgrävd kabel 1 ”övrigt” **= 18**
6 incidenter berodde på antagonistiska angrepp	Varav 1 anlagd brand 1 DDoS attack 1 eldsvåda 1 skadlig programvara 1 exploatering av sårbarhet 1 identitetsstöld **= 6**
5 incidenter orsakades av brister i organisatoriska rutiner och processer	Varav 3 felaktiga uppdateringar av mjukvara 2 avgrävda kablar **= 5**
5 incidenter orsakades av tredje part	Varav 2 avgrävda kablar 1 strömavbrott 1 eldsvåda **= 5**

2 incidenter berodde på mänskliga misstag eller felbedömningar	Varav 1 felaktig uppdatering av mjukvara 1 felaktig uppdatering av hårdvara 1 strömavbrott **= 3**
1 incident hade oklar grundorsak	Varav 1 ”övrigt” **= 1**

3.3 PTS kommentar om årets rapporterade grundorsaker och detaljerade orsaker

3.3.1 Systemfel

Den vanligaste grundorsaken bakom de säkerhetsincidenter som rapporterades in till PTS under 2024 var systemfel. 15 incidenter inrapporterades med denna grundorsak. Ofta har felet inträffat i samband med en uppdatering av mjukvara eller vid andra förändringsarbeten, men i vissa fall har det varit tekniska brister i programvara (buggar) som upptäckts av en ren händelse eller genom att påverkade kunder kontaktat kundtjänst.

3.3.2 Planerat arbete

Det är vanligt att inrapporterade säkerhetsincidenter har inträffat i samband med förändringsarbete. I vissa fall orsakades incidenten av mänskliga misstag och felbedömningar, i andra fall var det ett tekniskt problem som upptäcktes till följd av arbetet. Hur allvarlig incidenten varit har varierat men goda förberedelser och väl utarbetade rutiner motverkar och förkortar incidenters varaktighet generellt.

3.3.3 Strömavbrott

PTS ser en fortsatt låg rapportering av säkerhetsincidenter orsakade av strömavbrott. Endast fyra sådana incidenter har rapporterats under 2024. Under 2023 rapporterades två sådana incidenter. År 2022 var motsvarande siffra tre och år 2021 var siffran åtta. PTS förhoppning är att incidenter med denna orsak ska fortsätta ligga kvar på en låg nivå efter de bestämmelser om reservkraft i PTS föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTSFS 2022:11).

3.3.4 Avgrävda kablar

Avgrävda kablar orsakade fem rapporterade säkerhetsincidenter under 2024. Avbrott i tjänsterna uppstod då en redundant kabel antingen inte fungerade,

saknades eller var placerad så nära den ordinarie kabeln att båda skadades. PTS vill påtala vikten av att tillhandahållare bör använda tjänsten Ledningskollen[9] samt att se över redundanta kablar.

Vidare har PTS noterat att det under året har skett flera sjökabelbrott från Sverige till andra länder som fått mycket uppmärksamhet i media. Dessa händelser har dock inte lett till någon formell incidentrapportering till PTS.

3.3.5 Antagonistiska angrepp

PTS har under 2024 sett en fortsatt jämn nivå av inrapporterade säkerhetsincidenter som gäller cybersäkerhetsangrepp. Totalt mottogs sex rapporter beträffande sådana angrepp under 2024. Under 2023 rapporterades sju incidenter med en sådan orsak.

3.4 Incidenter som rapporteras vidare till Enisa

Större säkerhetsincidenter ska PTS rapportera vidare till Enisa enligt gällande EU-rättsakter.[10] Vidarerapporteringen från medlemsstaterna till Enisa sker kvartalsvis samt i början av varje år. Av de säkerhetsincidenter som rapporterats in till PTS under 2024, har PTS bedömt att inga incidenter ska vidarerapporteras till Enisa. Anledningen är att Enisa har andra rapporteringströsklar än PTS.

3.5 Jämförelse med andra EU-länder

Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation EUs-direktiv (2018/1972) för elektroniska kommunikationer (Kodexen) ska sedan ett par år tillbaka vara implementerat i medlemsstaterna. Länderna har dock implementerat direktivet med olika trösklar för incidentrapporteringsskyldighet, varför en exakt jämförelse med andra medlemsstaters incidenter inte är möjlig.

Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) skulle varit implementerat i medlemsstaterna den 18 oktober 2024. Trots att denna tidpunkt passerat har endast ett fåtal medlemsstater implementerat direktivet vid tidpunkten för denna rapport. Det är därför i nuläget svårt att göra en jämförelse enligt de nya reglerna. Det är även svårt att bedöma hur väl framtida jämförelser kommer kunna göras.

[9] Undvik avgrävningar och förenkla planering av markarbeten (ledningskollen.se)

[10] Se artikel 40 i Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation. Se mer om Enisas arbete och rapporter här: ENISA (europa.eu)

Enligt SOU 2024:18 finns ett förslag på bland annat en ny cybersäkerhetslag och cybersäkerhetsförordning samt förslag om ändringar i lag (2022:482) om elektronisk kommunikation (LEK) och förordning (2022:511) om elektronisk kommunikation (FEK).[11] Det är troligt att det kommer att behöva tas fram föreskrifter med mer detaljerade regler för incidentrapportering enligt den nya lagen.

[11] Nya regler om cybersäkerhet, SOU 2024:18

4. Tillsynsrapport för 2024

Här beskriver PTS tillsynsinsatser under 2024 inom områdena **säkerhet i nät och tjänster** och **skydd av de uppgifter som behandlats för att tillhandahålla elektroniska kommunikationstjänster.** Syftet med tillsynsrapporten är att kunna ge tillhandahållare, andra intressenter och PTS en överblick över genomförda och pågående tillsynsinsatser.

Bestämmelserna på området finns i 8 kap. LEK och i PTS föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTSFS 2022:11). Reglerna syftar bland annat till att användare ska få tillgång till säkra och effektiva elektroniska kommunikationstjänster och att de uppgifter som tillhandahållarna behandlar i samband med tillhandahållandet av tjänsterna skyddas.

De aktörer som PTS granskar på området är tillhandahållare av allmänna elektroniska kommunikationsnät och av allmänt tillgängliga elektroniska kommunikationstjänster (tillhandahållare). Tillsynsinsatserna är avsedda att granska och se till att tillhandahållarna följer reglerna om både säkerhet i nät och tjänster och skydd av behandlade uppgifter.

4.1 Avslutade tillsynsärenden 2024

Under 2024 har tre tillsynsinsatser avslutats.

4.1.1 Tillsyn av Telenor och Telia på grund av olovliga kreditprövningar

Den 20 augusti 2024 inledde PTS tillsyn av Telenor och Telia med anledning av att bolagen de senaste åren rapporterat in ett stort antal integritetsincidenter där kreditupplysningar tagits på fysiska personer utan att de berörda ingått eller avsett att ingå avtal med respektive tillhandahållare eller genom deras återförsäljare.

Bakgrunden till tillsynen var att undersöka om Telenor och Telia brister i sina rutiner och processer samt om tillhandahållaren vidtagit lämpliga åtgärder för att förhindra och minimera antalet olovliga kreditupplysningar som inhämtas.

Utöver att ställa skriftliga frågor till operatörerna gjorde PTS även tillsynsbesök i operatörernas och deras återförsäljares butiker. Vid besöken demonstrerades bland annat de digitala systemstöd som används vid försäljning av abonnemang.

Efter granskning av inkomna uppgifter och bedömning av det som framkommit vid tillsynsbesök, ansåg PTS att båda tillhandahållarna har vidtagit lämpliga tekniska och organisatoriska åtgärder för att förhindra och minimera antalet olovliga kreditupplysningar som inhämtas. Tillsynerna avslutades därför utan vidare åtgärd.

4.1.2 Tillsyn avseende säkerhetsåtgärder med anledning av säkerhetsincident vid planerat förändringsarbete

Med anledning av en säkerhetsincident som inträffade i januari 2023 hos Telia inledde PTS i juni 2023 en tillsyn. Säkerhetsincidenten påverkade många kunder i samband med ett planerat förändringsarbete. Syftet med tillsynen var att granska om säkerhetsincidenten hade inträffat till följd av brister i Telias säkerhetsarbete vid förändringshantering samt att granska hur Telia hanterade den aktuella incidenten och framåt säkerställer att liknande incidenter inte inträffar igen.

PTS avslutade tillsynen då granskningen visade att Telia har en process för förändringshantering och att Telia skyndsamt hade vidtagit åtgärder för att hantera den uppkomna incidenten. PTS konstaterade även att Telia dragit lärdomar av incidenten samt att erfarenheterna beaktats i riskanalyser, inom ramen för processen för förändringshantering, för att undvika liknande incidenter i framtiden.

4.1.3 Informationsinhämtande tillsyn om 5G-nät och tjänster

PTS inledde i november 2023 en informationsinhämtande tillsyn av ett urval av verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät med 5G-teknik och deras säkerhetsarbete i allmänna 5G-nät och allmänna 5G-tjänster.

Syftet med tillsynen var att inhämta uppgifter om hur långt de utvalda tillhandahållarna har kommit i utbyggnaden av allmänna 5G-nät och -tjänster och om eventuella gjorda anpassningar i deras processer och rutiner för säkerhetsarbete relaterat till detta. Efter att begärd information redovisats för PTS avslutades tillsynen utan vidare åtgärd.

4.2 Pågående tillsynsinsatser

4.2.1 Säkerhet i kundportaler

2024 inledde PTS en tillsyn mot bakgrund av att myndigheten under flera år mottagit integritetsincidenter avseende kundportaler för privatpersoner. Dessa kallas ofta Mina Sidor eller liknande. Incidenterna har varierat vad gäller antalet drabbade samt orsak, från enskilda berörda till tusentals, med ursprung i buggar, brister i rutiner och obehöriga intrångsförsök.

Bristande säkerhet vid inloggningsförfarandet till kundportaler kan ha stor påverkan på de som använder elektroniska kommunikationstjänster. Är säkerheten låg kan

kunder förlora tillgängligheten till deras egna uppgifter, bli betalningsansvariga för oriktiga köp samt bli utsatta för otillåten åtkomst och ändring av sina uppgifter.

Frågor som behandlas i den pågående tillsynen är bland annat krav för lösenord, möjlighet till tvåfaktorsautentisering och lösenordsåterställning.

Tillsynen pågår fortfarande vid denna rapports upprättande.

4.2.2 Avbrott i Telias nät och tjänster i Ammarnäs, Sorsele

PTS inledde i oktober 2024 tillsyn av Telia med anledning av ett kabelavbrott som inträffade i Ammarnäs, Sorsele kommun, under sommaren 2024. Bakgrunden till tillsynen var att nätkabeln, som normalt är upphängd, under en tid blivit liggandes på marken sedan den rivits ned från stolparna. Den lagades provisoriskt under 2023, men därefter, under sommaren 2024, gick den sönder igen.

PTS har ställt frågor till Telia angående kabelavbrottet och kring bolagets arbete med riskanalys och underhåll mm.

Tillsynen pågår fortfarande vid denna rapports upprättande.

4.3 Tillsynsarbete framåt

PTS har identifierat ett antal områden som skulle kunna utgöra grund för möjliga tillsynsinsatser framöver. Ny teknik, händelser i omvärlden, nya regler samt underlag från inrapporterade incidenter. kan utgöra grund för olika teman för PTS framtida tillsynsinsatser.

Utöver detta kan PTS inleda tillsyn i samband med principiellt viktiga eller särskilt allvarliga händelser som exempelvis drabbar ett stort antal användare. Genom den här typen av tillsynsinsatser granskar PTS att tillhandahållarna drar lärdomar av inträffade händelser och vidtar åtgärder i enlighet med regelverket.

Myndighetens tillsyn inriktas på områden som är av särskild betydelse för en välfungerande och säker marknad för säkra allmänna elektroniska kommunikationsnät och säkra allmänna elektroniska kommunikationstjänster.

PTS bedömer och prioriterar behovet av tillsynsinsatser utifrån ett löpande arbete med prioritering och urval.

Under 2025 väntas nya regler på området, då NIS2-direktivet föreslås genomföras i Sverige genom en ny cybersäkerhetslag. När de nya reglerna träder i kraft kommer PTS ambition vara att kontrollera regelefterlevnaden enligt den nya lagen,

5. BILAGA 1

5.1 Metod och arbetsprocess för incidentsammanställning

Arbetet med sammanställningen av incidenter har genomförts på följande sätt.

Inledningsvis gjordes flera genomgångar av alla incidentrapporter från 2024. I det arbetet identifierades orsaker, och mönster framträdde vid kategorisering utifrån orsakerna. Det är innehållet i tillhandahållarnas rapporter som legat till grund för orsakskategoriseringen.

En utgångspunkt i skapandet av orsakskategorierna har dels varit Enisas orsakskategori *grundorsaker* i den årliga uppföljning som görs på europeisk nivå, dels IMY:s orsaksindelning i sin rapport om anmälda personuppgiftsincidenter. Dessa har använts för att skapa grund för jämförbarhet.

I framtida års sammanställningar från PTS kan orsakskategoriseringen se annorlunda ut beroende på innehållet i det årets incidenter, eller p.g.a. andra behov av att följa upp detaljerade orsaker.

PTS strävar efter att över tid kunna följa samma orsakskategorier, om det är möjligt eller lämpligt. Eftersom regler om vad som ska rapporteras och tillämpning av dessa regler påverkar vilka incidenter som rapporteras till PTS, styr även detta underlaget för sammanställningen.

PTS har även tidigare genom exempelvis myndighetens risk- och sårbarhetsanalys för sektorn elektronisk kommunikation,[12] till viss del men mer summariskt och endast för regionala och nationella avbrott, beskrivit orsaker till säkerhetsincidenter. I den här sammanställningen ingår alla incidentrapporter under år 2024.

Det är fjärde året PTS gör denna orsaksindelning, lämnar kommenterar till mönster som framträder och publicerar sammanställningen.

[12] Risk- och sårbarhetsanalys för PTS och dess ansvarsområden 2022 - PTS-ER-2022:31 | PTS, läs om elektroniska kommunikationer i kapitel 5 s. 46–70.