2026-04-08 Rapport Rapportnummer PTS-ER-2026:10

Incident- och tillsynsrapport inom området säker kommunikation 2025

Rapportnummer
PTS-ER-2026:10

Diarienummer
26-3752

ISSN
1650-9862

Författare
Kristin Liljegren och Monica Blomström med hjälp av Stefan Mikaelsson, avdelningen för cybersäkerhet, enheten för säkra nät och tjänster

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 2025 registrerat 334 rapporterade incidenter. Det rör sig om 303 integritetsincidenter och 31 säkerhetsincidenter. Av de 303 inkomna integritetsincidenterna bedöms 299 av dessa utgöra regelrätta integritetsincidenter. Av de 31 säkerhetsincidenterna bedöms 28 av dessa vara regelrätta säkerhetsincidenter. De fyra integritetsincidentrapporterna respektive 3 säkerhetsincidentrapporterna som räknats bort utgörs av återkallade incidentrapporter, dubbelregistrerade incidentrapporter eller incidentrapporter där PTS bedömt att ingen incident har skett.

Totalt drabbades 25 100 användare eller abonnenter enligt rapporteringen till PTS av integritetsincidenter under 2025. Motsvarande antal år 2024 var 79 585. Säkerhetsincidenter drabbade 4 400 003 användare eller aktiva anslutningar under 2025. År 2024 var siffran 456 053. En förklaring till ökningen 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 ökning faktiskt har 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

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

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 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 2025 var brister i organisatoriska rutiner och processer samt mänskliga misstag eller felbedömningar. För säkerhetsincidenter under 2025 var de vanligaste grundorsakerna systemfel och incidenter orsakade av tredje part.

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 2025

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 säkerhetsbrister som underlag till ny reglering, för att identifiera informationsbehov eller behov av främjandeinsatser.

Totalt under 2025 har PTS registrerat 334 ärenden med rapporterade incidenter, varav 327 slutligt har bedömts som rapporteringspliktiga incidenter. Av de rapporterade incidenterna finns det fall, sju år 2025, 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 numera upphävda 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 skulle rapporteras utifrån vissa angivna tröskelvärden som angavs i numera upphävda PTSFS 2022:11.

1.3 Ny cybersäkerhetslag

Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) implementerades genom den nya cybersäkerhetslagen (2025:1506) i januari 2026. I samband med detta upphävdes delar av LEK. Även PTSFS 2022:11 upphävdes i januari 2026. Begreppet säkerhetsincident försvann med den nya lagstiftningen och istället pratar man om ”betydande incidenter”. Rapporteringen av betydande incidenter sker inte heller direkt till PTS längre utan rapporteras via Myndigheten för civilt försvar (MCF). Mer detaljerade regler om rapportering av incidenter och trösklar är under framtagning av både MCF och av PTS men är ännu inte på plats. För incidenter under året 2025 gällde dock tidigare regler i LEK samt PTSFS 2022:11 för säkerhetsincidenter och denna incident- och tillsynsrapport kommer därför utgå ifrån att det är de gamla reglerna som gäller.

2. Integritetsincidenter under 2025

Under 2025 registrerades 303 ärenden gällande integritetsincidenter hos PTS. Efter genomgång och granskning anses 299 av dessa utgöra regelrätta integritetsincidenter. Det justerade antalet beror på att tillhandahållare återkallat vissa incidentrapporter och några rapporterade händelser som PTS inte bedömer som integritetsincidenter.

Totalt har 25 100 användare eller abonnenter drabbats av integritetsincidenter 2025.

Antal incidenter har alltså minskat samtidigt som antal drabbade också har minskat sedan föregående år då motsvarande siffra 2024 var 394 incidenter och 79 585 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

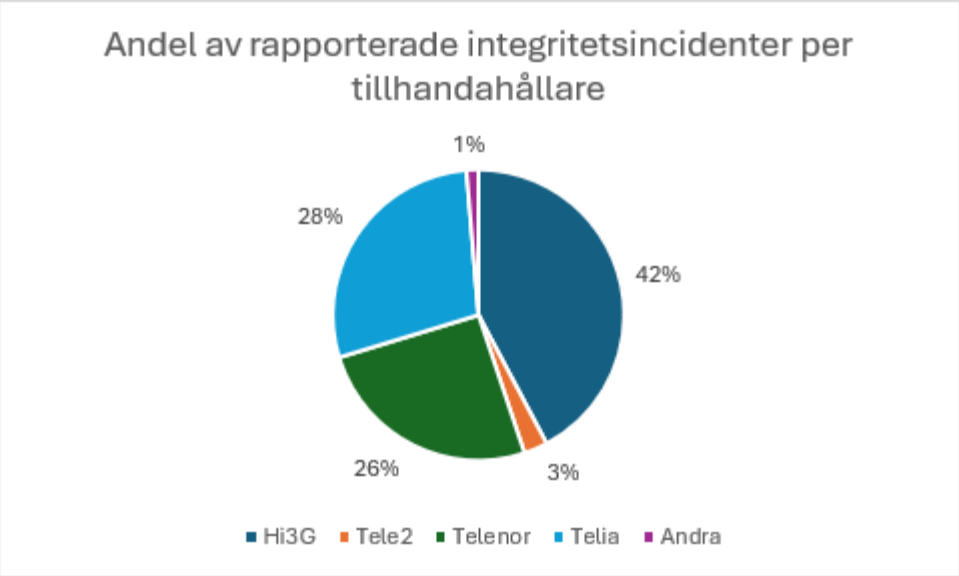
PTS kan även i detta års sammanställning konstatera en ojämn fördelning av rapporterade incidenter mellan tillhandahållare.

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.

Under 2025 var Hi3G den tillhandahållare som rapporterade in flest integritetsincidenter. Detta är en skillnad från 2024 då Telia var den operatör som rapporterade in flest integritetsincidenter.

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

Figur 1: cirkeldiagram över andel av rapporterade integritetsincidenter per tillhandahållare.



2.3 Orsaker till integritetsincidenter 2025

För att synliggöra grundorsaker och mer detaljerade orsaker, typer eller konsekvenser av integritetsincidenter under 2025 presenteras här nedan en tabell.

I tabellen har PTS utgått från EU:s cybersäkerhetsbyrås (Enisa) klassificering av grundorsaker till incidenter i nät och tjänster samt Integritetsskyddsmyndighetens

(IMY) uppställning av grundorsaker till personuppgiftsincidenter som rapporterats till IMY.[2]

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**
233 incidenter orsakades av brister i organisatoriska rutiner och processer	Varav 83 förväxlingar av kunder 55 felaktiga e-postadresser 47 olovliga kreditupplysningar 34 butik 34 felaktiga kontaktuppgifter (ej e-post) 33 handhavandefel 17 extern leverantör/underleverantör 13 brister i kundtjänst per telefon 12 brister i kundtjänst via chatt 8 bristande autentiseringar 6 olovlig ändring 5 förvaltare/god man 5 SIM-kort

[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 och inom organisationen. I den avses inte antagonistiska angrepp som cyberattacker, utan sådant som bedrägerier eller förföljelse av kunder.

	4 bedrägeri 4 nyteckningar 4 systemfel 4 felpackning 2 dummy-uppgift 2 mina sidor 2 portering 1 fel företrädare för bolagskund 1 fel i mjukvara 1 migrering 1 planerat arbete = **378**
31 incidenter berodde på mänskliga misstag eller felbedömningar	Varav 17 handhavandefel 8 förväxlingar av kunder 5 butik 4 olovliga ändringar 3 brister i kundtjänst per telefon 2 extern leverantör/underleverantör 2 felaktiga e-postadresser 2 fel företrädare för bolagskund 2 felpackningar 2 förvaltare/god man 1 brist i kundtjänst via chatt 1 dummyuppgift 1 felaktig kontaktuppgift (ej e-post) 1 kommunikationsoperatör 1 mina sidor 1 nyteckning 1 planerat arbete 1 skyddad identitet 1 systemfel **= 56**
13 incidenter orsakades av tredje part	Varav 5 felpackning 5 förväxlingar av kunder 5 SIM-kort 3 extern leverantör/underleverantör 3 fel i mjukvara 2 planerat arbete

	1 butik 1 handhavandefel **= 25**
12 orsakades av tekniska fel	Varav 8 systemfel 7 fel i mjukvara 5 planerat arbete 3 skyddad identitet 3 spridning till abonnentupplysning 1 felaktig postadress 1 brist i kundtjänst per telefon 1 mina sidor 1 migrering **= 30**
9 incidenter berodde på antagonistiska angrepp 4 av dessa berodde på ett medvetet angrepp av någon inom organisationen	Varav 4 cybersäkerhetsangrepp 3 bedrägerier 2 extern leverantör/underleverantör 1 brist i kundtjänst per telefon 1 butik 1 handhavandefel 1 olovlig ändring **= 13**
2 incidenter hade oklar orsak	Varav 1 felaktig e-postadress 1 brist i kundtjänst per telefon **= 2**

2.3.1 PTS kommentarer till 2025 års rapporterade orsaker

2.3.2 Förväxling av kunder

Det största antalet integritetsincidenter 2025 rör förväxlingar, situationer så som när handläggare blandar ihop kunder eller kundbilder. 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 förväxlingarna 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 misstag och därmed även minska incidenter på grund av förväxlingar.

2.3.3 Felaktig e-postadress

Under 2025 var den näst 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.

Liksom vid förväxling av kunder drabbar detta oftast en eller ett par personer åt gången. Påverkansgraden kan anses låg då det ofta bara rör sig om delning med en annan person, det som sticker ut är istället mängden av incidenter.

2.3.4 Antagonistiska angrepp

En kategori som ökat något är integritetsincident på grund av antagonistiska angrepp. Under 2025 inkom det nio sådana incidenter medan det under 2024 bara rapporterades sex incidenter. Av dessa nio incidenter berodde fyra på medvetet angrepp av någon inom organisationen. Fyra av incidenterna var cybersäkerhetsangrepp medan tre av incidenterna utgjordes av bedrägerier.

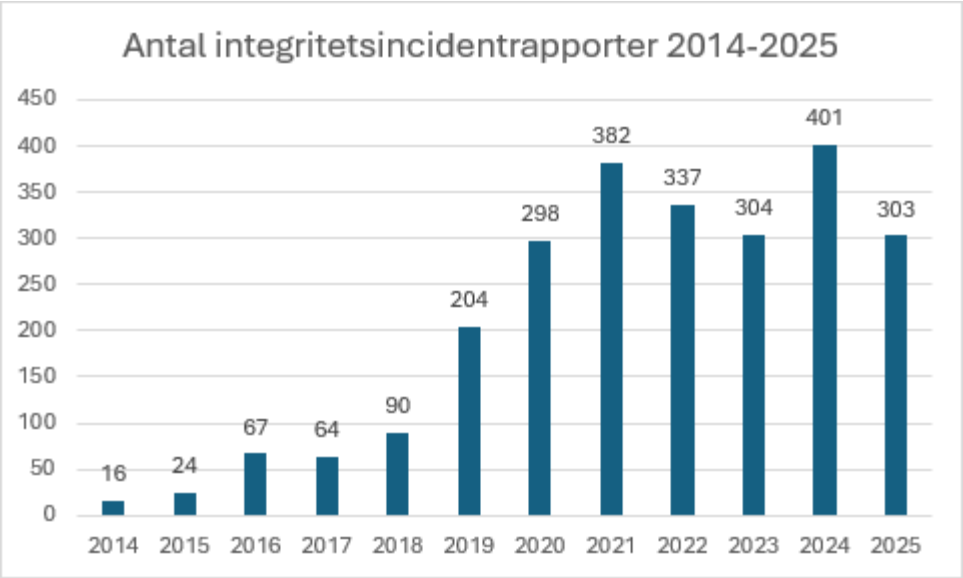
2.3.5 Olovlig kreditupplysning

PTS har under 2025 till skillnad från tidigare två år inte fått in ett lika stort antal incidenter gällande olovliga kreditupplysningar. 2024 inkom 142 rapporter om olovlig kreditupplysning medan det under 2025 endast inkom 47 rapporter. Ett skäl till denna minskning är sannolikt den tillsyn som PTS genomförde mot två av de större tillhandahållarna gällande just olovliga kreditupplysning under slutet av 2024.

2.4 En jämförelse med tidigare års integritetsincidenter

Under 2025 minskade antalet inrapporterade integritetsincidenter från 2024 års antal om 401 till 303 år 2025, se tabell nedan.

Figur 2: diagram över antal integritetsincidentrapporter 2014-2025.



3. Säkerhetsincidenter 2025

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

Under 2025 har PTS registrerat 28 ärenden avseende säkerhetsincidenter.

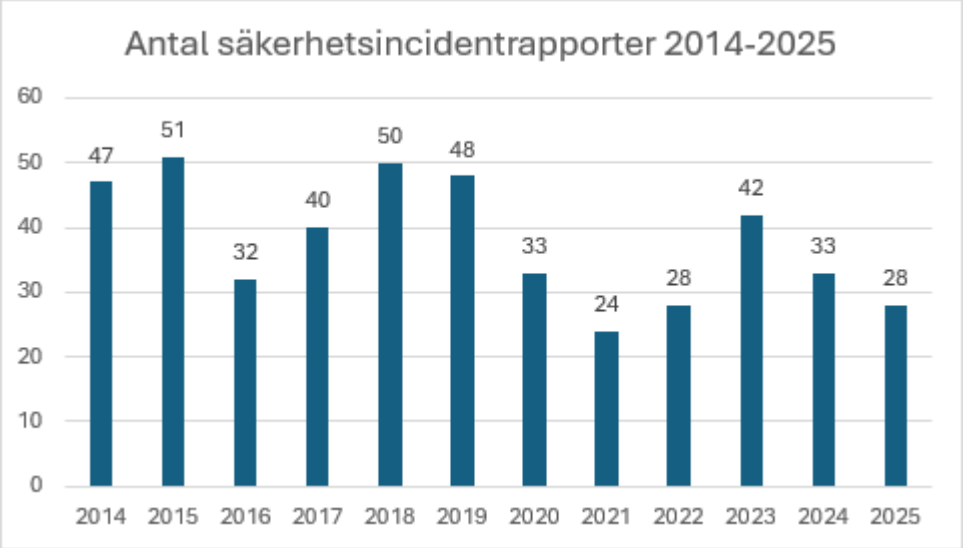
4 400 003 användare eller aktiva anslutningar[3] har enligt rapporterna drabbats av säkerhetsincidenter. I flera ärenden är det emellertid oklart, eller inte angett i rapporteringen, exakt hur många användare eller aktiva anslutningar som har drabbats. Siffran ska därför ses som ett estimat. Exempelvis 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 2025 inrapporterades totalt 7 säkerhetsincidenter utan redovisad siffra. Under 2024 rapporterades 14 säkerhetsincidenter utan redovisad siffra. Detta kan förklara skillnaden mellan 2024 års antal drabbade användare eller aktiva anslutningar jämfört med den stora ökningen år 2025.

3.1 En jämförelse med tidigare år

Antalet rapporterade säkerhetsincidenter 2025 är lägre än föregående år, och ligger lite under 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 antalet drabbade användare eller aktiva anslutningar ökat jämfört med år 2024, 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”.

Figur 3: diagram över antal säkerhetsincidentrapporter från 2014-2025.



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 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 2025 mottagit ett antal incidentrapporter med betydande påverkan på *funktioner i samhället*.[6] Totalt fem av 28 rapporterade säkerhetsincidenter under 2025 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.

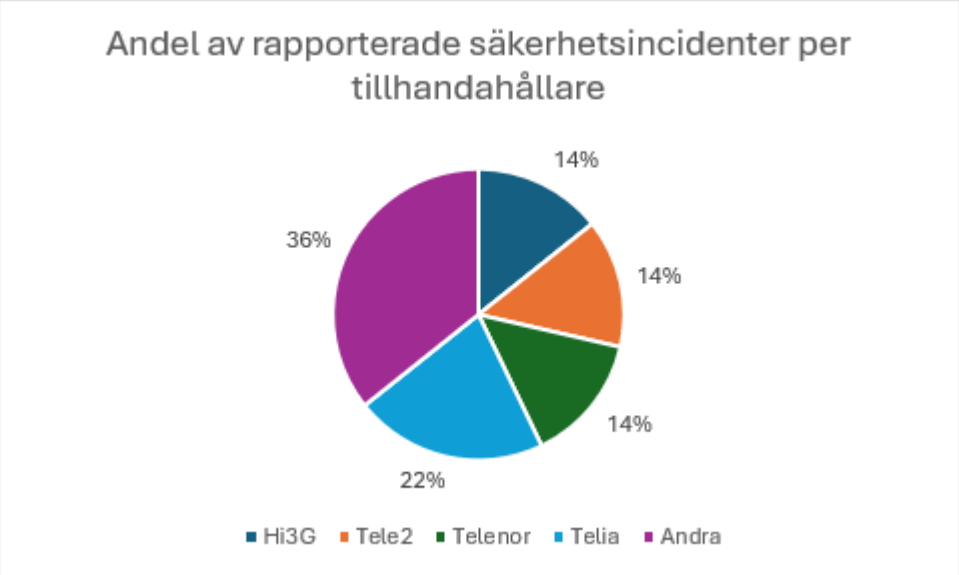
Det är enbart säkerhetsincidenter som har *en betydande* påverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten i nät och tjänster som är rapporteringspliktiga till PTS. PTS har därför inte en heltäckande bild av samtliga säkerhetsincidenter som inträffar inom området elektroniska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

3.2 Jämn fördelning av inrapporterade säkerhetsincidenter

PTS kan se att fördelningen av inrapporterade säkerhetsincidenter är jämn mellan de fyra största tillhandahållarna. PTS noterar också att andra tillhandahållare än de största har rapporterat in incidenter i större utsträckning än vid integritetsincidenter, jämför med kapitel 2.2.

[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

Figur 4: Cirkeldiagram över andel av rapporterade säkerhetsincidenter per tillhandahållare.



3.3 Orsaker till säkerhetsincidenter 2025

De inrapporterade, rapporteringspliktiga säkerhetsincidenterna, 28 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).

14 av de 28 incidenterna har sin grundorsak i *systemfel*[8] och åtta har sin grundorsak i *tredje part*. Incidenter har endast räknats en gång i tabellen och 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 2025 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.

[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

Grundorsaker till säkerhetsincidenterna	**Detaljerade orsaker, typer och konsekvenser till integritetsincidenterna**
14 incidenter orsakades av systemfel	Varav 8 felaktiga uppdateringar av mjukvara 4 mjukvarubuggar 2 hårdvarufel 1 överbelastning 1 strömavbrott 1 avgrävd kabel **= 17**
8 incidenter orsakades av tredje part	Varav 3 avgrävda kablar 3 felaktiga uppdateringar av mjukvara 1 mjukvarubugg 1 strömavbrott **= 8**
3 incidenter berodde på antagonistiska angrepp	Varav 1 avgrävd kabel 1 exploatering av sårbarhet 1 cybersäkerhetsangrepp **= 3**
1 incident orsakades av brister i organisatoriska processer och rutiner	Varav 1 avgrävd kabel **= 1**
1 incident berodde på mänskliga misstag eller felbedömningar	Varav 1 avgrävd kabel **= 1**
1 incident berodde på naturfenomen	Varav 1 ”övrigt” **= 1**

3.4 PTS kommentar om årets rapporterade grundorsaker och detaljerade orsaker

3.4.1 Systemfel

Den vanligaste grundorsaken bakom de säkerhetsincidenter som rapporterades in till PTS under 2025 var systemfel. 14 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.

3.4.2 Felaktiga uppdateringar av mjukvara

Den vanligaste detaljerade orsaker, typer och konsekvenser under 2025 var felaktiga uppdateringar av mjukvara. 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.

3.4.3 Strömavbrott

PTS ser en fortsatt låg rapportering av säkerhetsincidenter orsakade av strömavbrott. Endast två incidenter har rapporterats in under 2025. Under 2024 rapporterades fyra sådana incidenter. År 2023 var motsvarande siffra två och år 2022 var siffran tre. PTS förhoppning är att incidenter med denna orsak ska fortsätta ligga kvar på en låg nivå.

3.4.4 Avgrävda kablar

Avgrävda kablar orsakade sju rapporterade säkerhetsincidenter under 2025 till skillnad från 2024 då fem säkerhetsincidenter orsakades av avgrävda kablar. 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.

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

3.4.5 Antagonistiska angrepp

PTS har under 2025 sett en sänkt nivå av inrapporterade säkerhetsincidenter som gäller cybersäkerhetsangrepp. Totalt mottogs tre rapporter beträffande sådana angrepp under 2025. Under 2024 rapporterades sex incidenter med en sådan orsak[10].

3.5 Incidenter som rapporteras vidare till Enisa

Större säkerhetsincidenter ska PTS rapportera vidare till Enisa enligt gällande EU-rättsakter.[11] Vidarerapporteringen från medlemsstaterna till Enisa sker kvartalsvis samt i början av varje år. Av de säkerhetsincidenter som rapporterats in till PTS under 2025, har PTS bedömt att en incident ska vidarerapporteras till Enisa. Anledningen till det låga antalet är att Enisa har högre rapporteringströsklar än PTS.

[10] Det är svårt att dra några statistiska slutsatser när det varierar mellan så få incidenter som 3-6.

[11] 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)

4. Tillsynsrapport för 2025

Här beskriver PTS tillsynsinsatser under 2025 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 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 2025

Under 2025 har tre tillsynsinsatser avslutats.

4.1.1 Tillsyn av säkerhet i kundportaler

I slutet av 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 och möjlighet till tvåfaktorsautentisering.

PTS avslutade tillsynen sommaren 2025 då granskningen visade att samtliga operatörer antingen hade infört eller skulle, innan året är slut, införa tvåfaktorsautentisering för sina kunder på sina inloggningssidor.

4.1.2 Tillsyn efter avbrott i Telias nät och tjänster i Ammarnäs, Sorsele

Under slutet av 2024 inledde PTS tillsyn mot Telia Sverige AB med anledning av en säkerhetsincident inträffade i Ammarnäs i Sorsele kommun. Incidenten, som orsakades av att en fiberkabel skadades under en dikesklippning, medförde att Telia förlorade mobiltäckning i området. Den aktuella fiberkabeln skulle egentligen ha varit stolphängd i luften men revs ned och blev sedan liggande på marken. PTS ville få klarhet i hur, när och varför kabeln hamnade på marken och hur Telias säkerhetsarbete hade sett ut sedan dess. Telia informerade PTS om den riskanalys som bolaget hade gjort och vilka åtgärder som vidtagits för att minska riskerna. Dessutom informerade Telia om planerad teknisk lösning som ska förhindra liknande händelser i framtiden. PTS bedömde sammantaget att Telia vidtagit ändamålsenliga och proportionerliga åtgärder för att hantera de risker som hotar säkerheten i denna typ av fiberkablar. Tillsynen avslutades därför i mars 2025 utan åtgärd.

4.1.3 Tillsyn efter inträffad incident hos Tele2

I början av 2025 tog PTS emot rapporter från Tele2 om inträffade integritetsincidenter. Av incidentrapporterna framgick att Tele2 hade lämnat ut för- och efternamn, telefonnummer och adresser för abonnenter med skyddad folkbokföring till företag som bedriver abonnentupplysning.

Efter genomförd tillsyn kan PTS konstatera att Tele2 har brustit i efterlevnaden av myndighetens säkerhetsföreskrifter. Bland annat bedömer PTS att Tele2 inte har upprättat tillräckliga riskanalyser, samt att bolaget inte vidtagit tillräckliga tekniska och organisatoriska åtgärder för att skydda abonnentuppgifterna.

PTS beslutade i december 2025 att Tele2 ska betala 8,1 miljoner kronor i sanktionsavgift för det inträffade.

4.2 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 2026 väntas nya regler på området, då NIS2-direktivet genomförs i Sverige genom en ny cybersäkerhetslag och PTS håller på att ta fram nya föreskrifter. Dessa nya föreskrifter kommer ligga till grund för framtida tillsynsarbete.

5. BILAGA

Metod och arbetsprocess för incidentsammanställning

Arbetet med sammanställningen av incidenter har genomförts på följande sätt.

Inledningsvis gjordes flera genomgångar av alla incidentrapporter från 2025. 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 underlag för sammanställningen.

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