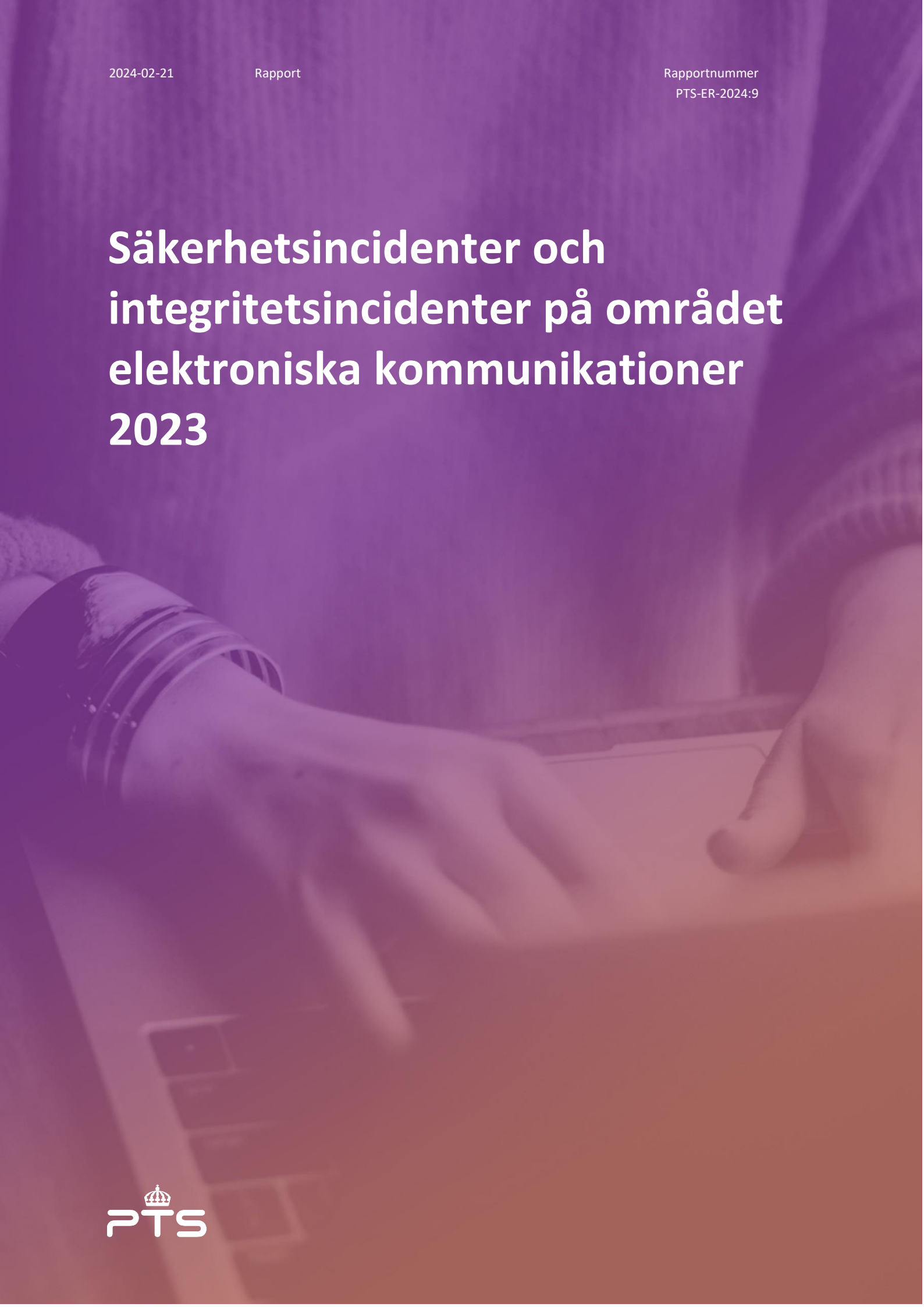
2024-02-21 Rapport Rapportnummer
PTS-ER-2024:9

Säkerhetsincidenter och integritetsincidenter på området elektroniska kommunikationer 2023



Rapportnummer
PTS-ER-2024:9

Diarienummer
24-1250

ISSN

Författare
Sara Öijerholm-Ström, Catherine Persson, 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 bolag som rapporterar incidenter för tillhandahållare.

PTS har i denna rapport sammanställt och grupperat dessa rapporterade incidenter. 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 2023 registrerat 346 rapporterade incidenter. Det rör sig om 304 integritetsincidenter och 42 säkerhetsincidenter[1]. Totalt rapporterades att 83 269 användare eller abonnenter drabbades av integritetsincidenter under 2023. Motsvarande antal år 2022 var 96 749. Säkerhetsincidenter drabbade 3 442 948 användare eller aktiva anslutningar under 2023. År 2022 var siffran 5 480 329.

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 väsentligt sämre säkerhet i sina nät och tjänster. Vissa tillhandahållare upptäcker fler incidenter eller kan ha mer välkända rutiner för rapportering av incidenter internt, vilket gör att de därför rapporterar mer till PTS. Incidentrapporteringen utgör ett viktigt underlag för PTS tillsynsarbete då rapporterna innehåller värdefull information som underlättar 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 misstanke om brister i tillhandahållares säkerhetsarbete. En hög rapporteringsgrad är alltså inte är att se som något negativt.

De två vanligaste grundorsakerna till rapporterade integritetsincidenter under 2023 har varit *brister i organisatoriska rutiner och processer* (170 av incidenterna) och *mänskliga misstag eller felbedömningar* (91 av incidenterna). För säkerhetsincidenter under 2023 var de vanligaste grundorsakerna *systemfel* (22 av incidenterna), *antagonistiska angrepp* (sju av incidenterna).

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

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 rapporterade 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. PTS vill utifrån de rapporterade incidenterna även förmedla var tillhandahållarna lämpligen kan planera att utveckla sitt säkerhetsarbete.

1. Incidentrapporter under 2023

Både integritetsincidenter och incidenter gällande säkerhet i nät och tjänster 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). Incidentrapporterna ger PTS underlag att bedöma hur bestämmelserna om säkerhet i nät och tjänster eller skydd av behandlade uppgifter efterföljs, och huruvida tillsyn behöver inledas. Det finns även andra syften med incidentrapporteringen, till exempel för att skapa en överblick över tillhandahållarnas säkerhetsproblem, som underlag till nya regler, för att identifiera informationsbehov eller behov av främjandeinsatser. Totalt under 2023 har PTS registrerat 346 ärenden med rapporterade incidenter, varav 336 slutligt har bedömts som rapporteringspliktiga incidenter.

Till skillnad från 2022 har inga nya regler trätt i kraft under 2023. Dock är det viktigt att ha i åtanke att statistiken för år 2022 delvis var baserad på de tidigare rapporteringsreglerna och att en jämförelse mellan åren därför kan vara missvisande.

1.1.1 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.

1.1.2 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.[2]

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.

Begreppet säkerhetsincident infördes i samband med lagändringar 2022 och innebär ett utvidgad säkerhetsbegrepp. Innan lagändringen var endast incidenter kopplade till tillgänglighet, t.ex. störningar och avbrott, rapporteringspliktiga. Händelser som utgör säkerhetsincidenter kan ibland helt eller delvis även behöva rapporteras som en integritetsincident, och *vice versa*.

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 2023

Under 2023 diarieförde**s 304** ärenden gällande integritetsincidenter hos PTS. Efter genomgång och granskning har det visat sig att **298** av dessa utgör regelrätta integritetsincidenter. Det justerade antalet beror på att tillhandahållare har återkallat vissa incidentrapporter. Det finns även rapporterade händelser som PTS inte klassar som integritetsincidenter eller händelser som har dubbelregistrerats hos PTS.

Totalt har **83 269** användare eller abonnenter drabbats av integritetsincidenter 2023.

Antal incidenter och antal drabbade har alltså minskat något sedan föregående år då motsvarande siffra var 337 incidenter och 96 749 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 således 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. Även temporär förlust av uppgifter, t.ex. som en följd av en överbelastningsattack, utgör en integritetsincident.

Integritetsincidenter utgör potentiellt ett allvarligt hot mot tilltron till elektroniska kommunikationstjänster. När uppgifter som behandlas av tillhandahållaren sprids till utomstående, ändras obehörigen eller går förlorad, 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. Den ojämna fördelningen har under 2023 minskat något men är fortfarande tydlig.

PTS bedömning är att den ojämna fördelningen inte är relaterad till operatörernas storlek. Orsaken till den ojämna fördelningen är inte känd. Det kan vara så att vissa tillhandahållare upptäcker fler incidenter eller har mer välkända 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. Det går att återkalla ingivna rapporter.

PTS åtgärder hittills: Under 2023 inledde PTS en tillsyn mot en av tillhandahållarna för att granska dess rutiner kring incidentrapportering. PTS har även tidigare år genomfört tillsyn mot flera tillhandahållare för att säkerställa och förbättra incidenthantering och rapportering.

PTS fortsatta arbete: PTS fortsätter bevaka och granska tillhandahållarnas arbete med incidentrapportering.

2.3 Orsaker till integritetsincidenter 2023

För att synliggöra grundorsaker och mer detaljerade orsaker eller konsekvenser av integritetsincidenter under 2023 presenteras här nedan en tabell.

I tabellen har PTS utgått från EU:s nätverks- och informationssäkerhetsbyrås (Enisa) klassificering av grundorsaker till incidenter i nät och tjänster samt Integritetsskyddsmyndighetens (IMY) uppställning av grundorsaker till personuppgiftsincidenter som rapporterats till IMY.[3]

En förändring i Enisas klassificering skedde år 2021. Förändringen gjordes för att möjliggöra en jämförelse mellan Enisas incidentuppföljning och personuppgiftsincidenter enligt Europaparlamentets och Rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av

[3] 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.

sådana uppgifter och om upphävandet av direktiv 95/46/EG (allmän dataskyddsförordning) – hädanefter GDPR.

I tabellen presenterar PTS också detaljerade orsaker, typer och konsekvenser, utöver grundorsaker, som återfinns i incidenterna. De detaljerade orsakerna, typerna och konsekvenserna fördjupar bilden av vilken typ 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 eller konsekvenser. (högra kolumnen). Till exempel kan en incident där en obehörig företrädare för en bolagskund tillåtits att ändra bolagets tjänster kategoriseras som grundorsak *mänskligt misstag* och sedan både med *fel företrädare för bolaget och bristande autentisering* i kolumnen detaljerade orsaker, typer och konsekvenser. Det leder till att det totala antalet i kolumnen för detaljerade orsaker 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 298 integritetsincidenter 2023	**Detaljerade orsaker, typer och konsekvenser som återfinns i incidenterna. En incident kan ha flera detaljerade orsaker.**
170 incidenter orsakades av brister i organisatoriska rutiner och processer	Varav 65 olovliga kreditupplysningar 54 felaktiga e-postadresser 29 förväxlingar av kunder 21 butik 16 handhavandefel 13 extern leverantör/underleverantör 12 bristande autentiseringar 11 felaktiga kontaktuppgifter (ej e-post) 8 brister i kundtjänst per telefon 4 brister i kundtjänst via chatt 4 nyteckningar

	3 SIM-kort 2 systemfel 2 felaktiga företrädare för bolag 2 spridande till abonnentupplysning 2 förvaltare/god man 1 skyddad identitet 1 portering 1 bedrägeri 1 polisanmäld **= 252**
91 berodde på mänskliga misstag eller felbedömningar	Varav 42 handhavandefel 36 förväxlingar av kunder 14 felpackningar 14 felaktiga e-postadresser 13 olovliga kreditupplysningar 13 extern leverantör/underleverantör 9 felaktiga kontaktuppgifter (ej e-post) 8 SIM-kort 6 butik 5 porteringar 3 nyteckningar 2 bristande autentiseringar 2 felaktiga företrädare för bolagskund 2 försäkringar 2 skyddad identitet 1 brist i kundtjänst per telefon 1 brist i kundtjänst via chatt 1 systemfel 1 migrering

	= 175
24 orsakades av tekniska fel	Varav 15 systemfel 9 fel i mjukvara 6 förväxling av kunder 5 felaktiga kontaktuppgifter 4 mina sidor 3 extern leverantör/underleverantör 2 felaktiga e-postadresser 2 handhavandefel 1 olovlig kreditupplysning 1 bristande autentisering 1 nyteckning 1 olovligt spridande till abonnentupplysning 1 migrering 1 NI-ICS (nummeroberoende interpersonella kommunikationstjänster) 1 planerat arbete **= 53**
6 incidenter berodde på antagonistiska angrepp En av dessa 6 berodde på ett medvetet angrepp av någon inom organisationen	Varav 4 bedrägerier 4 polisanmälda 2 handhavandefel 1 mina sidor 1 extern leverantör/underleverantör 1 bristande autentisering 1 butik **= 14**

6 incidenter hade ingen klar orsak	Varav 4 systemfel 2 fel i mjukvara 1 handhavandefel 1 planerat arbete 1 chatt **= 9**
En incident orsakades av tredje part	Varav 1 extern leverantör/underleverantör 1 felpackning **=2**

2.3.1 PTS kommentarer till 2023 års rapporterade orsaker

2.3.2 Olovliga kreditupplysningar

PTS har under året fått in ett stort antal incidenter gällande kreditupplysningar tagna utan laglig grund i samband med tillhandahållandet av elektroniska kommunikationstjänster. I de flesta fallen är det en kund som efterfrågat en prisuppgift, utan att teckna avtal, och där det av misstag tagits en kreditupplysning på kunden.

PTS fortsätter att bevaka problemet med olovliga kreditupplysningar. De enskilda incidenterna omfattar enbart en drabbad per incident och med förmodan små konsekvenser för de drabbade, även om det inte går att utesluta att det kan uppstå negativa konsekvenser för drabbade i enskilda fall.

2.3.3 Förväxling av kunder

Även under 2023 var en av de mest frekvent rapporterade integritetsincidenterna någon typ av förväxling av kundbilder. Ofta har personal hos tillhandahållare eller underleverantör av misstag blandat ihop två kundbilder varvid resultatet blivit felaktigt, exempelvis av abonnemangsförlängning, utskick av bekräftelse eller ändring av kontaktuppgift.

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 uppsåtligen har orsakat incidenten. Det särskilt allvarliga när det gäller förväxlingsincidenterna är istället den stora mängden incidenter.

Tillhandahållarna uppger regelmässigt i incidentrapporteringen att denna typ av incident inträffar på grund av mänskliga misstag. PTS har uppfattningen att den frekvens varmed förväxlingsincidenterna inträffar snarare tyder på brister i organisatoriska rutiner och processer hos tillhandahållarna eller deras återförsäljare.

2.3.4 Rapportering från tillhandahållare av nummeroberoende interpersonella kommunikationstjänster

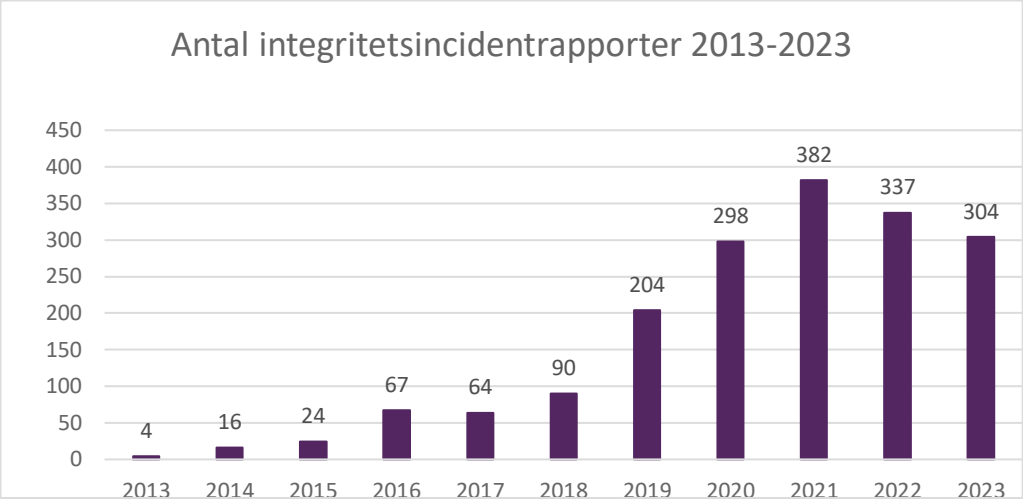
PTS har noterat att fler tillhandahållare av nummeroberoende interpersonella kommunikationstjänster har rapporterat incidenter under 2023. Denna grupp av aktörer innefattar tillhandahållare av till exempel e-posttjänster och olika typer av kommunikationsappar. Rapporteringsplikten gäller för dessa tillhandahållare om de tillhandahåller sina tjänster i Sverige, oavsett var de är etablerade. Det är vanligt att denna rapportering sker genom ombud.

2.3.5 Sent inrapporterade integritetsincidenter

PTS har under året sett en ökning av antalet rapporter som inkommer efter den fastslagna tidsfristen. I stället för att skicka 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.

2.4 En jämförelse med tidigare år

Under 2023 fortsatte trendbrottet från 2022 med färre integritetsincidenter än föregående år. Antalet inrapporterade integritetsincidenter har sjunkit från 2021 års rekordantal om 382 incidenter till 304 år 2023.



PTS uppfattning är att de senaste fem årens totala ökning av incidentrapporter inte nödvändigtvis beror på en motsvarande ökning av faktiska incidenter, utan till stor del kan 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. Ökningen kan också ha påverkats av införandet av GDPR och det arbete som tillhandahållarna genomförde och fortfarande genomför till följd av detta. LEK är en särskild sektorsreglering, så kallad *lex specialis*, i förhållande till GDPR, inom sektorn för elektronisk kommunikation. PTS kan notera att det har skett en minskning av inrapporterade integritetsincidenter de senaste två åren. Det är möjligt att ett ökat säkerhetsarbete och ett ökat fokus på säkerhet på grund av omvärldsläget samt förändringar i operatörernas rapporteringsprocess påverkat förekomsten av incidenter. Ovanstående möjliga anledningar till skiftningar i antalet rapporterade incidenter under de senaste åren är endast antaganden och kan inte utläsas från statistiken.

3. Säkerhetsincidenter 2023

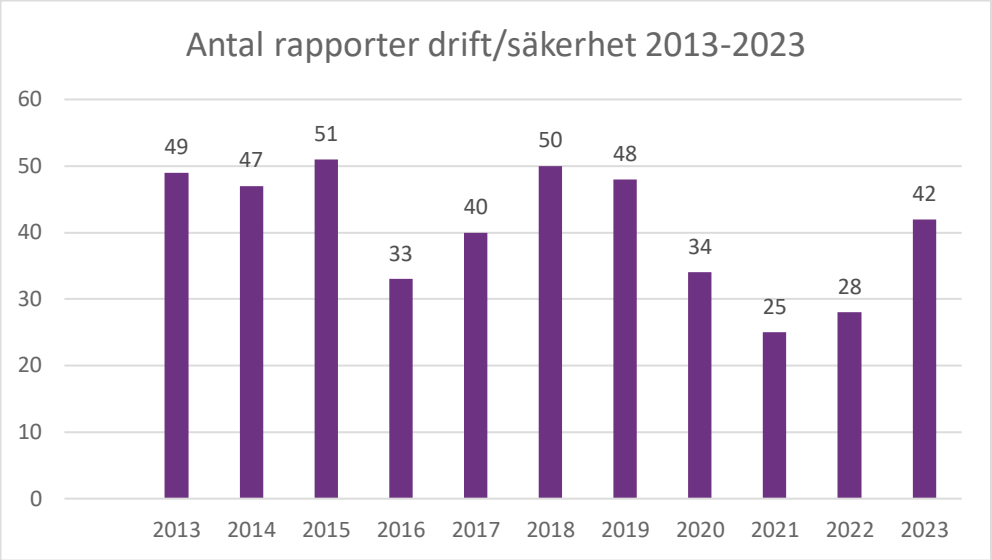
Enligt LEK är tillhandahållare skyldiga att rapportera säkerhetsincidenter med betydande påverkan på nät och tjänster till PTS.

Under 2023 har PTS diarieförtt **42** ärenden med rapporter om säkerhetsincidenter. Efter vidare granskning har det visat sig att **35** av dessa utgör säkerhetsincidenter. 4 av 42 incidenter har återkallats av operatören. Det finns även incidenter som har dubbelregistrerats hos PTS.

3 442 948 användare eller aktiva anslutningar har enligt rapporterna drabbats av säkerhetsincidenter. I flertalet ärenden är det oklart 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.

3.1 En jämförelse med tidigare år

Antalet rapporterade säkerhetsincidenter 2023 är högre än föregående år, men inom normalintervallen för rapportering. PTS brukar få in mellan ungefär 30 och 50 rapporter om säkerhetsincidenter som påverkat nät och tjänster per år. Samtidigt som antalet rapporter har ökat så har antalet drabbade användare eller aktiva anslutningar minskat något jämfört med år 2022.



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.

I och med ikraftträdandet av nya LEK i juni 2022 omfattas även tillhandahållare av nummeroberoende interpersonella kommunikationstjänster av reglerna om incidentrapportering. En stor del av de som drabbats av årets säkerhetsincidenter är just användare av sådana tjänster. Det återstår att se hur rapporteringen från denna typ av aktör kommer att påverka statistik och mönster avseende incidentrapporteringen framöver i och med dessa aktörer varit skyldiga att rapportera incidenter endast sedan juni 2022.

[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.

3.1.1 PTS om ökningen sedan föregående år

PTS har i år mottagit fler rapporter för säkerhetsincidenter jämfört med de senaste tre åren. Det är inte möjligt att fastställa vad ökningen som skett 2023 beror på. Flera av de inrapporterade incidenterna har uppstått i samband med förändringsarbete, varför en potentiell eller bidragande faktor möjligen skulle kunna vara ett ökat säkerhetsarbete hos tillhandahållarna.

3.1.2 Alla säkerhetsincidenter ska inte rapporteras till PTS

Enligt reglerna i LEK är det säkerhetsincidenter med betydande påverkan på nät och tjänster som ska rapporteras till PTS. PTS har i sina föreskrifter om säkerhet i nät och tjänster (PTSFS 2022:11) tydliggjort 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 rapportering av säkerhetsincidenter som når upp till dessa tröskelvärden ska säkerhetsincidenter, oavsett om de avser störningar och avbrott eller berör någon av 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 till exempel:

- 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.

Ovanstående faktorer utgör endast exempel på omständigheter som kan vara aktuella att beakta vid bedömningen av betydande påverkan. PTS har under 2023 mottagit ett fåtal incidentrapporter med betydande påverkan på *funktioner i samhället*. Funktioner i samhället kan vara exempelvis påverkan på möjligheten att nå 112 eller nationell nödkommunikation eller andra samhällsnummer såsom 114 14 eller 1177. PTS följer noggrant utvecklingen av rapporteringen vad gäller händelser som påverkar funktioner i samhället.

Följaktligen innebär detta att de säkerhetsincidenter som inte har en betydande påverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten i nät och tjänster inte är

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

rapporteringspliktiga till PTS. PTS har därför inte en heltäckande bild av samtliga säkerhetsincidenter som inträffar i elektroniska kommunikationer utan endast över de incidenter som rapporterats till PTS.

3.2 Orsaker till säkerhetsincidenter 2023

De inrapporterade, rapporteringspliktiga säkerhetsincidenterna, 35 stycken, har delats in i kategorier baserade på *grundorsaker* och därtill mer *detaljerade orsaker*.

22 av de 35 incidenterna har sin grundorsak i *systemfel* och sju har sin grundorsak i *antagonistiska angrepp*. Incidenter har endast räknats en gång i tabellen och förekommer alltså inte i två grundorsakskategorier, däremot kan en incident ha flera detaljerade orsaker varvid summan av dessa orsaker överstiger totalen.

Här presenteras grundorsaker och detaljerade orsaker till rapporterade säkerhetsincidenter under 2023 i en enkel 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. Den följer i stort Enisas indelning i grundorsaker (root causes[6]) och detaljerade orsaker (detailed or technical causes).

Grundorsaker till de 35 säkerhetsincidenterna	**Detaljerade orsaker till de 35 incidenterna**
22 incidenter orsakades av systemfel	Varav 6 felaktig uppdatering av mjukvara 6 hårdvarufel 5 mjukvarubugg 2 överbelastning 2 strömavbrott 1 felaktig uppdatering av hårdvara 1 avgrävd kabel **= 23**
7 berodde på antagonistiska angrepp	Varav 3 DDoS attack 2 skadlig programvara 2 exploateringar av sårbarhet 1 ”övrigt”

[6] Enisas fem root causes: System failure, Human error, Third party failure, Natural phenomena, Malicious action

	= 8
5 orsakades av fel hos tredje part (partner/underleverantör)	Varav 3 avgrävd kabel 2 felaktig uppdatering av mjukvara **=5**
En incident orsakades av hårt väder	Kraftig snö och is **=1**

3.3 PTS kommentar om årets rapporterade grundorsaker och detaljerade orsaker

3.3.1 Mjukvarubugg

En av de vanligaste orsakerna bakom de säkerhetsincidenter som rapporterades in till PTS under 2023 var fel eller sårbarheter i programkod (buggar). Denna orsak var vanligast även föregående år. Ofta uppmärksammades dessa buggar i samband med en uppdatering av mjukvara eller vid andra förändringsarbeten men i vissa fall har buggen upptäckts av en ren händelse.

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 har varit har varierat men god förberedelse och väl utarbetade rutiner motverkar och förkortar incidenter generellt.

3.3.3 Strömavbrott

PTS ser en fortsatt låg rapportering av säkerhetsincidenter orsakade av strömavbrott. Under 2023 rapporterades endast två sådana incidenter. År 2022 var motsvarande siffra 3 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 PTSFS 2022:11 som trädde i kraft under 2020 och uppdaterades 2022.

3.3.4 Avgrävda kablar

Avgrävda kablar orsakat fyra rapporterade säkerhetsincidenter under 2023. Avbrott i tjänsterna uppstod då en redundant kabel antingen inte fungerade, eller var placerad så nära den ordinarie kabeln att båda skadades. PTS vill påtala vikten av att tillhandahållare bör använda Ledningskollen[7] samt att se över redundanta kablar.

3.3.5 Överbelastningsattacker och antagonistiska angrepp

PTS har under 2023 sett en ökning av inrapporterade säkerhetsincidenter som gäller cybersäkerhetsangrepp. Totalt mottogs sju rapporter gällande dessa angrepp under 2023. Under 2022 rapporterades ingen incident med en sådan orsak. DDoS-attacker (överbelastningsattacker) är vanligast.

3.3.6 Väder

Under 2023 rapporterades en incident som orsakades av hårt väder. Under 2022 rapporterades inte några större avbrott i elektroniska kommunikationer i samband med hårt väder, inte heller 2021 rapporterades någon sådan händelse.

3.4 Incidenter som rapporteras vidare till Enisa

Större incidenter ska PTS rapportera vidare till Enisa enligt gällande EU-rättsakter.[8] Vidarerapporteringen från medlemsstaterna till Enisa sker i början av varje år. Av de 42 säkerhetsincidenter som rapporterats in till PTS under 2023, har PTS bedömt att två incidenter ska vidarerapporteras till Enisa. Båda incidenterna berodde på systemfel. Anledningen till att så få av de incidenter som rapporteras till PTS vidarerapporteras till Enisa är att Enisa har andra rapporteringströsklar än PTS.

3.5 Om jämförelse med EU-länder

Enisa kommenterar att fokuset på uppmärksammade och inrapporterade incidenter historiskt har legat på störningar och avbrott i nät och tjänster. 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 (kodex-direktivet) är nu genomfört i de flesta medlemsstater. Arbetet med incidentrapportering har dock kommit olika långt i medlemsstaterna, varför en jämförelse inte är möjlig. Dessutom är Enisas trösklar för rapportering högre än de nationella trösklarna i

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

[8] Se mer om Enisas arbete och rapporter här: ENISA (europa.eu)

Sverige. Trösklarna skiljer sig även något mellan medlemsstaterna, varför en exakt jämförelse inte kommer vara möjlig.

4. Tillsynsrapport

Här beskriver PTS tillsynsinsatser under 2023 inom områdena **säkerhet i nät och tjänster** och **skydd av de uppgifter som behandlats för att tillhandahålla elektroniska kommunikationer.** Syftet med tillsynsrapporten är att kunna ge rapporterande tillhandahållare, andra intressenter och PTS en överblick över genomförda och pågående tillsynsinsatser.

Bestämmelserna på området finns i 8 och 9 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 kommunikationer och att de uppgifter som tillhandahållarna behandlar för att tillhandahålla tjänsterna skyddas.

De aktörer som PTS granskar på området är tillhandahållare av allmänna 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 2023

Under 2023 har tre tillsynsinsatser avslutats.

4.1.1 Tillsyn av WhatsApp på grund av misstanke om bristande incidentrapportering

PTS inledde under 2023 en tillsyn mot tillhandahållaren av kommunikationstjänsten WhatsApp eftersom misstankar fanns att bolaget inte levt upp till reglerna om incidentrapportering. WhatsApp hade ett globalt avbrott i sin kommunikationstjänst, vilket enligt regelverket utgjorde en rapporteringspliktig säkerhetsincident.

Tillsynen syftade främst till att granska om WhatsApp efterlevt skyldigheten att rapportera säkerhetsincidenten och WhatsApp underrättades om att PTS misstänkte att bolaget inte levt upp till reglerna. Granskningen avslutades efter att WhatsApp lämnat de uppgifter som efterfrågats av PTS i enlighet med gällande rapporteringsregler i Sverige. Enligt reglerna i LEK ska PTS i vissa fall ta ut en sanktionsavgift från tillhandahållare, bland annat vid överträdelse av rapporteringsreglerna. I denna tillsyn gjorde myndigheten bedömningen att det fanns särskilda skäl att inte ta ut en sanktionsavgift från WhatsApp.

Tillsynen har bidragit till att uppmärksamma de nya regler som trädde ikraft under 2023, där en ny grupp av aktörer, bland annat WhatsApp, träffas av reglerna. Det är viktigt att de bolag som verkar på den svenska marknaden och tillhandahåller tjänster i Sverige känner till och följer de regler som gäller här.

4.1.2 Tillsyn över hur Telia, Tele2 och Telenor skyddar kunders uppgifter vid utlämnande till abonnentupplysning

PTS inledde i början av året en tillsyn över hur de granskade operatörerna skyddar kundernas uppgifter i samband med att de lämnar ut abonnentuppgifter till abonnentupplysning och hur operatörerna hanterar kundernas medgivande för detta.

Bakgrunden till tillsynen var att PTS under flera år mottagit incidentrapporter från operatörerna där de har lämnat ut abonnentuppgifter till abonnentupplysning utan kundernas medgivande eller där kunden har skyddade personuppgifter eller hemligt nummer. Incidentrapporterna visar att ett stort antal kunder har drabbats av felaktig hantering hos operatörerna. Operatörerna är skyldiga att lämna ut abonnentuppgifter till abonnentupplysning men det får bara ske för de kunder som har gett sitt medgivande. Även uppgifter om kunder som anmält hemligt nummer eller har skyddade personuppgifter har lämnats ut, med potentiellt mycket allvarliga konsekvenser till följd för de drabbade individerna.

PTS avslutade tillsynen då granskningen visade att operatörerna vidtagit tillräckliga tekniska och organisatoriska säkerhetsåtgärder för att skydda abonnentuppgifter som lämnas ut till abonnentupplysning. Granskningen visar bland annat att operatörernas riskanalyser i relevanta delar uppdaterats och åtgärder har vidtagits för riskhantering för att minska risken för att integritetsincidenter inträffar.

Tillsynen har lett till att operatörernas säkerhetsarbete har förbättrats vad gäller att minska risken för integritetsincidenter vid utlämnade av uppgifter till abonnentupplysning.

4.1.3 Tillsyn avseende Tele2:s rutiner för att identifiera och rapportera integritetsincidenter

PTS startade i augusti 2023 en tillsyn som syftade till att säkerställa att Tele2 har rutiner för att identifiera och rapportera integritetsincidenter. Bakgrunden är att PTS under flera år noterat att Tele2 avviker i rapporteringsmönstret jämfört med de övriga stora operatörerna på marknaden då Tele2 rapporterar in betydligt färre integritetsincidenter än övriga. Tillsynen syftade till att säkerställa att det låga antalet inrapporterade incidenter inte är orsakat av brister i Tele2:s rutiner.

PTS har sedan tillsynen inleddes sett en ökning av antalet inrapporterade integritetsincidenter från Tele2.

Tillsynen avslutades utan vidare åtgärd då PTS efter genomförd granskning inte kunnat konstatera några brister i Tele2:s rutiner för incidenthantering.

4.2 Pågående tillsynsinsatser

4.2.1 Händelsestyrd tillsyn av Telia avseende säkerhetsincident vid planerat förändringsarbete

PTS inledde i juni 2023 tillsyn mot Telia Sverige AB (Telia) med anledning av en inrapporterad säkerhetsincident med betydande påverkan på nät och tjänster och funktioner i samhället hos Telia som inträffade i januari 2023. Incidenten skedde i samband med en konfigurationsändring i ett av Telias interna system i Telias datacenter som orsakade en loop. Incidenten var rikstäckande, påverkade ca 150 000 – 225 000 användare och pågick i ca 4,5 timmar. Därutöver fick incidenten betydande påverkan på nät och tjänster samt på funktioner i samhället då användare till följd av Incidenten inte kunde nå 114 14 och 1177.

PTS granskning syftar till att utreda om Telias rutiner och processer för riskanalys och riskhantering för förändringsarbete uppfyller kraven i PTS föreskrifter om säkerhet i nät och tjänster.

Tillsynen beräknas avslutas under första kvartalet 2024.

4.2.2 Informationsinhämtande tillsyn om uppbyggnad av 5G-nät och säkerhet i 5G-nät och 5G-tjänster

PTS inledde i november 2023 en grundläggande, informationsinhämtande tillsyn av ett urval av företag som tillhandahåller allmänna elektroniska kommunikationsnät med 5G-teknik och deras säkerhetsarbete i allmänna 5G-nät och allmänna 5G-tjänster. Tillsynen genomförs inte i syfte att granska och bedöma regelefterlevnad.

Syftet med tillsynen är att inhämta uppgifter om hur långt de utvalda tillhandahållarna har kommit i utbyggnaden av allmänna 5G-nät och 5G-tjänster, om utpekade ansvariga roller för säkerhetsarbetet i 5G, genomförd kompetensutveckling med anledning av 5G-uppbyggnaden, upprättandet av processer och rutiner för säkerhetsarbetet samt operatörernas val av 5G-infrastruktur och -arkitektur. PTS vill utifrån svaren kunna planera framtida tillsynsinsatser, och få en bild av operatörernas nya och förändrade tillgångar i samband med införandet av 5G-nät i Sverige.

Tillsynen beräknas avslutas under första kvartalet 2024.

4.3 Tillsynsarbete framåt

PTS har identifierat ett antal områden som skulle kunna utgöra grund för möjliga tillsynsinsatser framöver. Ny teknik, händelser i omvärlden 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 bör inriktas på områden som är av särskild betydelse för en välfungerande och säker marknad för säkra allmänna elektroniska kommunikationsnät och säkra allmänna kommunikationstjänster.

PTS bedömer och prioriterar behovet av tillsynsinsatser utifrån ett löpande arbete med prioritering och urval. För att kunna prioritera och välja ut relevanta tillsynsinsatser mer löpande under året har PTS inte längre en fastslagen tillsynsplan på samma sätt som i tidigare års tillsynsrapporter.

5. BILAGA 1

5.1.1 Metod och arbetsprocess för incidentsammanställning

Arbetet med sammanställningen av incidenter har genomförts på följande sätt.

Inledningsvis gjordes flera genomgångar av alla incidentrapporter från 2023. I det arbetet identifierades och markerades orsaker, och mönster framträdde vid gruppering 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,[9] 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 på grund av andra behov av att följa upp detaljerade orsaker.

Med detta sagt är det eftersträvansvärt att över tid kunna följa samma orsakskategorier, om möjligt eller lämpligt. Det ska också tilläggas att styrande regler om vad som ska rapporteras och tillämpning av reglerna om incidentrapportering också de påverkar vilka incidenter som rapporteras till PTS, och därmed också styr underlaget för sammanställningen.

PTS har även tidigare genom exempelvis myndighetens Risk- och sårbarhetsanalys för sektorn elektronisk kommunikation,[10] till viss del men mer summariskt och endast för regionala och nationella avbrott, beskrivit vilka orsaker till säkerhetsincidenter som funnits. I den här sammanställningen ingår alla incidentrapporter under år 2023.

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

[9] Telecom Security Incidents 2021 — ENISA (europa.eu)

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