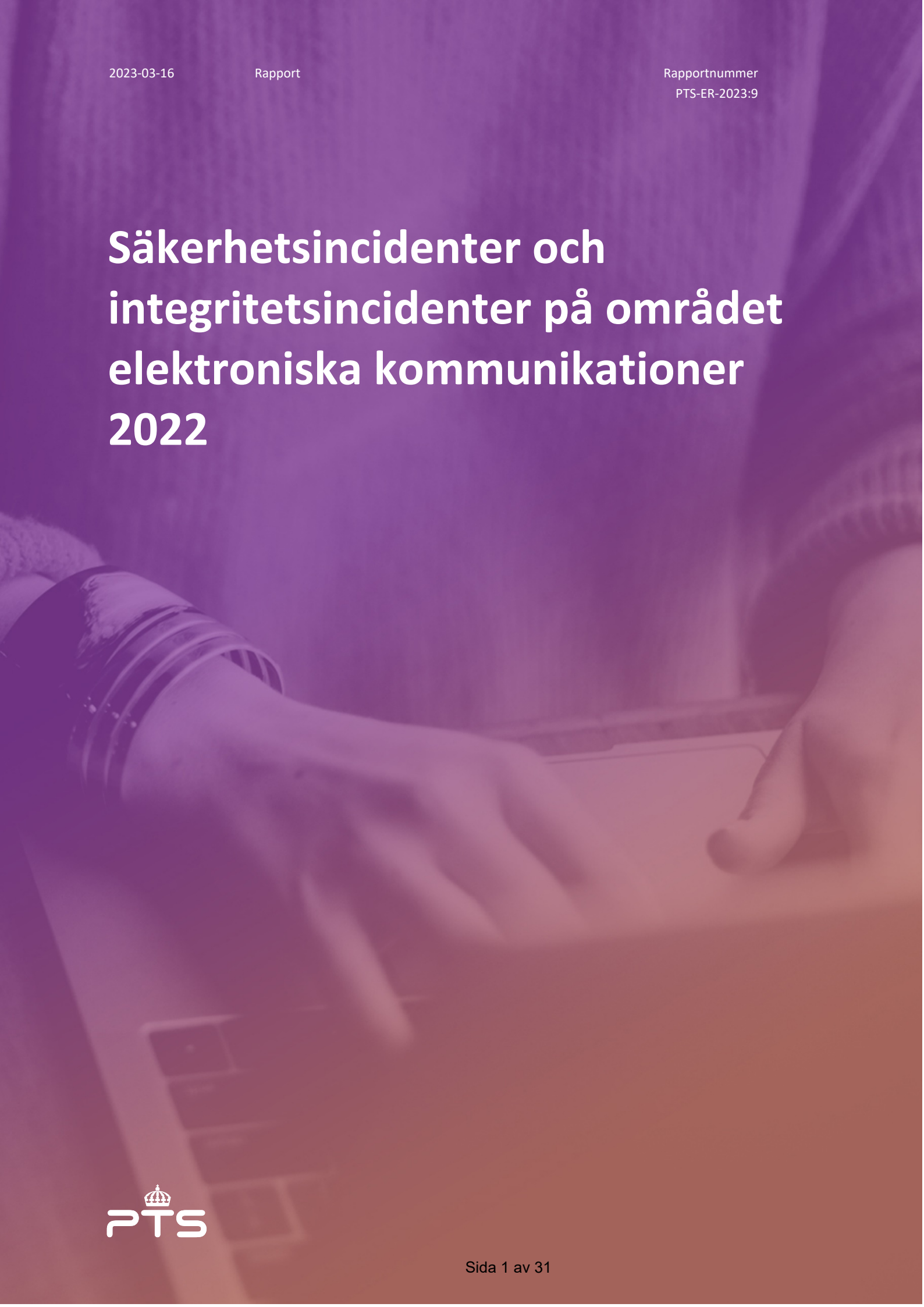
Säkerhetsincidenter och integritetsincidenter på området elektroniska kommunikationer 2022



Rapportnummer
PTS-ER-2023:9

Diarienummer
23-1574

ISSN
1650–9862

Författare
Sara Öijerholm-Ström, avdelningen för säker kommunikation

Post- och telestyrelsen
Box 6101
102 32 Stockholm

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

Innehåll

Sammanfattning

De som tillhandahåller 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.

Totalt under år 2022 har PTS registrerat 365 rapporterade incidenter. Det rör sig om 28 säkerhetsincidenter och 337 integritetsincidenter. Det är något färre incidenter än föregående år. En exakt jämförelse med tidigare år försvåras av att både lagen om elektronisk kommunikation och PTS säkerhetsföreskrifter har ändrats under året, vilket har påverkat rapporteringsplikten.

PTS har här sammanställt och grupperat dessa rapporterade incidenter. PTS kommenterar också hur fördelningen ser ut mellan integritetsincidenter och säkerhetsincidenter, hur fördelningen ser ut mellan tillhandahållarna, vilken typ av orsak eller typ som är vanligast och vilken typ av integritetsincident som är mest allvarlig. Här finns också övergripande jämförelser med tidigare år samt med EU-länder överlag.

Nytt för i år är att sammanställningen inkluderar incidenter gällande Nummeroberoende interpersonella kommunikationstjänster (NI-ICS). Sedan nya LEK trädde i kraft i juni 2022 omfattas nämligen tillhandahållare av dessa tjänster av incidentrapporteringsskyldigheten.

Fördelningen av de inrapporterade incidenterna är ojämn mellan tillhandahållarna. Det är inte säkert att de tillhandahållare som rapporterar flest incidenter till myndigheten också är de vars nät och tjänster påverkas av flest incidenter. Det kan också vara så att vissa tillhandahållare upptäcker fler incidenter och/eller har mer välkända rutiner för rapportering av incidenter internt, vilket gör att de därför rapporterar mer till PTS. Incidentrapporteringen utgör en viktig del av PTS tillsynsarbete då rapporterna innehåller värdefull information som underlättar PTS bedömning av om det är motiverat att inleda tillsyn. Det är därmed viktigt att PTS får kännedom om samtliga rapporteringspliktiga incidenter för att kunna agera vid misstanke om brister i tillhandahållares säkerhetsarbete.

De två vanligaste grundorsakerna till rapporterade säkerhetsincidenter (dvs. inte integritetsincidenter) under 2022 har varit: systemfel (21 av incidenterna) och mänskliga misstag eller felbedömningar (4 av incidenterna). För integritetsincidenter var de två vanligaste grundorsakerna mänskliga misstag eller felbedömningar (115 av incidenterna) och brister i organisatoriska rutiner och processer (104 av incidenterna).

Totalt under 2022 rapporterades 5 480 329 användare eller aktiva anslutningar drabbade av säkerhetsincidenter. År 2021 var 435 000 användare eller aktiva anslutningar drabbade av

driftsincidenter men en exakt jämförelse mot 2021 är inte relevant då rapporteringsplikten ändrats under året och den tidigare formuleringen driftsincident inte inkluderade lika många typer av incidenter.

Integritetsincidenterna drabbade 96 749 användare eller abonnenter under 2022. Motsvarande siffra år 2021 var 64 497.

Som uppföljning av incidenterna bedriver och planerar PTS flera olika tillsynsinsatser.

Syftet med sammanställningen

Syftet med sammanställningen är att kunna ge tillhandahållare, andra intressenter och PTS en överblick av fjolårets incidentrapportering. PTS vill också sprida kännedom om incidenterna till flera tillhandahållare. Genom sammanställningen vill PTS förmedla sin uppfattning om var det finns mönster som kan vara intressanta utifrån reglerna om skydd för uppgifter och säkerhet i nät och tjänster. 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. I sammanställningen kallas de bolag som rapporterar incidenter för tillhandahållare.

1. Incidentrapporter under 2022

Både integritetsincidenter och incidenter gällande säkerhet i nät och tjänster är rapporteringspliktiga till PTS enligt LEK, PTS föreskrifter och enligt en förordning från EU-kommissionen.[1] 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 2022 har PTS registrerat 365 ärenden med rapporterade incidenter, varav 361 slutligt har bedömts som rapporteringspliktiga incidenter.

[1] Rapporteringsskyldigheten framgår av 8 kap 3 och 8 §§ LEK, PTSFS 2012:11 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).

2. Nya incidentrapporteringsregler 2022

Under 2022 implementerade Sverige EU:s direktiv om inrättande av en europeisk kodex för elektronisk kommunikation[2] genom införandet av en ny lag om elektronisk kommunikation (2022:482), LEK, som trädde i kraft den 3 juni 2022.

PTS nya föreskrifter om säkerhet i nät och tjänster (PTSFS 2022:11) trädde i kraft den 1 augusti 2022.[3] Reglerna för rapportering av säkerhetsincidenter finns i LEK och i PTS föreskrifter PTSFS 2022:11 (kapitel 17).

Det infördes några nyheter som rör rapporteringsplikten för säkerhetsincidenter:

- Begreppet säkerhetsincident införs och ersatte det tidigare begreppet driftsincident.[4]
- Utöver trösklarna som tidigare gällde, infördes i enlighet med Kodexen en rapporteringsplikt för säkerhetsincidenter som har betydande samhällelig eller ekonomisk påverkan.
- En säkerhetsincident ska rapporteras in inom 72 timmar från upptäckt.
- Även nummeroberoende interpersonella kommunikationstjänster ska rapportera incidenter till PTS.

Det skedde ingen förändring i PTS tröskelvärden för när en säkerhetsincident ska rapporteras i och med de nya reglerna, utöver den ovan nämnda rapporteringsplikten för betydande samhällelig eller ekonomisk påverkan.

Rapporteringsplikten för integritetsincidenter kommer att kvarstå parallellt med rapporteringsplikten för säkerhetsincidenter. Det beror på att reglerna för skydd av uppgifter kvarblir i LEK och rapportering av integritetsincidenter ska göras enligt kommissionens

[2] Europarparlamentet och rådets direktiv 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation

[3] Den nya föreskriften PTSFS 2022:11 upphävde och ersatte föreskrifterna i PTSFS 1995:1, PTSFS 2012:2, PTSFS 2012:4, PTSFS 2014:1 och PTSFS 2015:2 och ändringsföreskrifter kopplade till dessa.

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

förordning (EU) nr 611/2013. Dessa bestämmelser i LEK genomför bestämmelserna i e-dataskyddsdirektivet.[5]

2.1.1 Säkerhetsincident

I 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.[6]

Det som tidigare kallades driftsincident är en typ av säkerhetsincident - en tillgänglighetsincident.

2.1.2 Integritetsincident

I 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. [7]

Incidenter som har medfört obehörig tillgång till behandlade uppgifter, förvanskning, förlust eller radering av sådana uppgifter ska således fortsättningsvis rapporteras som integritetsincidenter.

Rapporteringsplikten för integritetsincidenter saknar tröskelvärde.

[5] e-dataskyddsdirektivet 2002/58/EG om säkerhet i samband med behandlingen av uppgifter.
[6] LEK 2022:482 1 kap 7§
[7] Ibid.

3. Integritetsincidenter under 2022

Sedan 2011 är tillhandahållare skyldiga att rapportera inträffade integritetsincidenter till PTS.[8] Skyldigheten grundas på att tillhandahållarna ska skydda alla uppgifter som behandlas i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster.[9] 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.

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.

Under 2022 diarieförde s 340 ärenden gällande integritetsincidenter hos PTS.[10] Efter genomgång och granskning har det visat sig att 335 av dessa utgör regelrätta integritetsincidenter. Det justerade antalet beror på att tillhandahållare har återkallat vissa incidentrapporter och det finns även rapporterade händelser som PTS inte klassar som integritetsincidenter eller händelser som har dubbelregistrerats hos PTS.

[8] Regler kring rapporteringsskyldigheten för integritetsincidenter finns i 8 kap 8§ LEK och i förordning (EU) nr 611/2013.

[9] Regeln om det finns i 8 kap 6 § LEK.

[10] Det kan finnas någon enstaka felräkning i den nu följande kategoriseringen av orsaker. Men det rör sig i sådant fall om endast ett litet fåtal och kan inte påverka den övergripande bilden.

Totalt har 96 749 användare eller abonnenter drabbats av integritetsincidenter 2022. Trots att antalet integritetsincidenter minskat jämfört med tidigare år har antalet drabbade ökat, även om de flesta incidenter enbart omfattar en eller ett fåtal individer.

3.1 Alla tillhandahållare rapporterar inte lika många integritetsincidenter

PTS kan liksom i förra årets sammanställning konstatera en ojämn fördelningen av rapporterade incidenter mellan tillhandahållare. Den ojämna fördelningen under 2022 består i att en stor tillhandahållare har rapporterat få integritetsincidenter i jämförelse med de andra stora tillhandahållarna. PTS ser den ojämna fördelningen som problematisk.

Den ojämna fördelningen är inte relaterad till bolagens storlek. Det är inte heller säkert att de tillhandahållare som rapporterar flest incidenter är de vars nät och tjänster påverkas av flest incidenter. Det kan också vara så att vissa tillhandahållare upptäcker fler incidenter och därför rapporterar mer till PTS. Även om en tillhandahållare rapporterar få incidenter under ett år kan det fåtalet röra allvarliga incidenter.

PTS uppmanar alla tillhandahållare att vid tvekan huruvida en händelse är en integritetsincident hellre rapportera den än att inte göra det. Det går att återkalla ingivna rapporter.

PTS åtgärder hittills: PTS har tidigare år genomfört tillsyn av tillhandahållare för att säkerställa och förbättra incidenthantering och rapportering. Dessutom för PTS en löpande dialog kring incidentrapportering och mallarna kring detta.

PTS fortsatta arbete med problemet: PTS avser att undersöka vilken förmåga tillhandahållare har att förebygga, upptäcka och rapportera integritetsincidenter. En tillsyn planeras under 2023 att omfatta den tillhandahållare som nu avviker från de övriga stora tillhandahållarna i antal rapporterade incidenter.

3.2 Orsaker till integritetsincidenter 2022

För att visa grundorsaker och mer detaljerade orsaker eller konsekvenser av integritetsincidenter under 2022 presenteras här nedan en tabell.

I tabellen har PTS utgått från EU:s nätverks- och informationssäkerhetsbyrås (Enisa) uppställning av grundorsaker till incidenter i nät och tjänster samt

Integritetsskyddsmyndighetens (IMY) uppställning av grundorsaker till personuppgiftsincidenter som rapporterats till IMY.[11]

Redan förra året skedde en förändring av uppställningen i jämförelse med PTS sammanställning av 2020 års incidenter. Förändringen görs för att skapa en jämförbarhet med hur Enisa behandlar incidentuppföljning och för jämförbarhet med personuppgiftsincidenter enligt dataskyddsförordningen.[12] Denna sammanställning överensstämmer med förra årets uppställning.

PTS presenterar också detaljerade orsaker, typer och konsekvenser, utöver grundorsaker, som återfinns i incidenterna. De detaljerade orsakerna, typerna och konsekvenserna fördjupar bilden av vad incidenterna rör för händelser. 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 endast en grundorsak men kan innehålla flera detaljerade orsaker eller konsekvenser. 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. Det leder till att det totala antalet i kolumnen för detaljerade orsaker och konsekvenser blir något högre än det totala antalet incidenter av den grundorsaken. 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 tillhandahållaren att identifiera om någon riktad teknisk eller organisatorisk åtgärd kan motverka fler incidenter i framtiden.

Grundorsaker till 337 integritetsincidenter 2022	**Detaljerade orsaker, typer och konsekvenser som återfinns i incidenterna. En incident kan ha flera detaljerade orsaker.**
	43 handhavandefel 24 felaktiga kontaktuppgifter (ej e-post) 22 kunder förväxlades

[11] 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.

[12] 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 sådana uppgifter och om upphävandet av direktiv 95/46/EG (allmän dataskyddsförordning).

115 st berodde på mänskliga misstag eller felbedömningar	9 felpackningar 7 olagliga kreditupplysningar 6 extern leverantör/underleverantör 6 bristande autentisering 5 fel e-postadress 5 kundtjänst per telefon 4 fel företrädare för företagskund 4 portering 4 kundtjänst/självbetjäning på webbsida/app. 3 kundtjänst via chatt 2 fel i mjukvara 2 SIM-kort 2 butik 1 migrering 1 bedrägeri **= 150**
104 st orsakades av brister i organisatoriska rutiner och processer	36 bristande autentisering 33 olagliga kreditupplysningar 19 fel företrädare för bolagskund 15 handhavandefel 9 extern leverantör/underleverantör 5 förväxlingar av kunder 5 nyteckning 4 fel e-post 4 kundtjänst per telefon 4 butik 4 kundtjänst/självbetjäning på webbsida/app. 3 bedrägeri 2 fel i mjukvara 1 systemfel 1 chatt

	1 kommunikationsrapportör 1 förvaltare/god man 1 SIM-kort **= 148**
37 st orsakades av tekniska fel	70 fel e-postadress 10 fel i mjukvara 7 systemfel 5 fel kontaktuppgift 5 mina sidor 4 brister i autentisering av kunder 3 olovligt spridande till abonnentupplysning 3 förväxling 1 olovlig kreditupplysning 1 migrering 1 person med skyddad identitet 1 butik 1 förvaltare/god man 1 extern leverantör/underleverantör **= 113**
19 berodde på antagonistiska angrepp 4 av dessa 19 berodde på medvetna angrepp av någon inom organisationen	12 bristande autentisering 11 bedrägerier 1 cybersäkerhetsangrepp 2 olagliga kreditupplysningar 2 mina sidor 2 NI-ICS 2 handhavandefel 1 extern leverantör/underleverantör 1 nyteckning av tjänst 1 chatt

	1 kundtjänst per telefon 1 person med skyddad identitet 1 SIM **= 45**
1 incident orsakades av tredje part	Systemfel hos underleverantör

3.3 PTS kommentarer till 2022 års rapporterade orsaker

3.3.1 Incidenter kring röstbrevlådor

De incidenter som under 2022 drabbat flest användare är ett antal incidenter kring röstbrevlådor. Totalt drabbades 29 602 användare av incidenter kopplade till deras röstbrevlådor. Dels har tekniska fel och systemfel lett till att användare kopplats till någon annans röstbrevlåda, eller på annat sätt fått tillgång till annan kunds röstbrevlåda. Dels har incidenter inträffat där den sparade informationen, i form av välkomstmeddelande samt sparade meddelanden raderats från kundens röstbrevlåda. Dessa två typer av röstbrevlådeincidenter har tillsammans haft ett stort antal drabbade, trots att det gäller ett fåtal enskilda incidenter. PTS ser allvarligt på det stora antalet drabbade av denna typ av incidenter.

3.3.2 Tidigare intrång i röstbrevlådor

Under vintern 2021 rapporterades inledningsvis en incident på grund av ett cyberangrepp i form av automatiserade intrångsförsök av en tillhandahållares röstbrevlådor. Den rapporten följdes sedan av ytterligare nio incidentrapporter från ett antal andra tillhandahållare. Totalt är det konstaterat att 944 användare/abonnenter har drabbats av intrång i sina röstbrevlådor i denna attack. Men här finns ett mörkertal. Det går inte att reda ut i efterhand hur många personer som har drabbats. Det har rapporterats till PTS att så många som 1 024 429 användare/abonnenter potentiellt kan vara drabbade av intrången i detta cyberangrepp. Det finns även kännedom om att kapade röstbrevlådor som berörts av denna incident har använts för att skapa falska användarkonton på sociala medier.

3.3.3 PTS åtgärder hittills

PTS inledde tillsyn mot en tillhandahållare gällande intrång i röstbrevlådor under våren 2021. Den bedrevs under 2022 för att avslutas i januari 2023. PTS har i tillsynen angett

myndighetens uppfattning om vilka säkerhetsåtgärder som är nödvändiga för att tillhandahållaren ska upprätthålla skydd av uppgifter i röstbrevlådor. Tillhandahållaren förbättrade under tillsynen sina skyddsåtgärder och tillsynen är nu avslutad.

3.3.4 PTS fortsatta arbete med problemet

PTS fortsätter att bevaka problemet med röstbrevlådor. Även om den genomförda tillsynen ledde till förbättringar står det klart – utifrån det fortsatt höga antalet drabbade under 2022 – att det kvarstår problem i fråga om säkerheten för röstbrevlådor. PTS är inte främmande för att genomföra ytterligare tillsyner med fokus på problem relaterade till röstbrevlådor.

3.3.5 Olovlig spridning av kunders uppgifter till abonnentupplysning

En av de incidenttyper som orsakat flest drabbade användare gäller tillhandahållares olovliga spridning av abonnentuppgifter till abonnentupplysningsföretag. Detta var även den typ av incident som drabbade flest under 2021. PTS ser allvarligt på att 8 703 personer drabbades av att deras hemliga uppgifter spridits till abonnentupplysningsföretag under 2022. I vissa fall, beroende på mottagande abonnentupplysningsföretag, kan heller inte uppgifterna raderas när den obehöriga spridningen väl har ägt rum. Extra graverande har denna typ av incident blivit sedan krav på kontantkortsregistrering infördes den 1 augusti 2022. Oregistrerade kontantkort har i stor utsträckning använts av personer med skyddade personuppgifter– personer vars liv och hälsa kan hotas om deras uppgifter olovligen sprids till abonnentupplysningsföretag.

I Sverige finns abonnentförteckning som elektronisk katalog (på internet), olika typer av nummerupplysningstjänster på internet eller via 118-nummer. Tillhandahållaren är skyldiga att lämna ut uppgifter om abonnenter till företag som bedriver abonnentupplysning om sådana uppgifter begärs. Skyldigheten finns *endast* om inte uppgifterna skyddas av tystnadsplikt.

Tystnadsplikt gäller som huvudregel för alla kunduppgifter hos tillhandahållaren. För att uppgifter ska kunna lämnas ut till ett abonnentupplysningsföretag krävs att kunden har lämnat sitt samtycke. Alla kunder som är fysiska personer har rätt att få information om ändamålen med en abonnentförteckning och att informeras om de sökfunktioner som en sådan tjänst möjliggör. Kunderna har enligt LEK rätt att neka tillhandahållaren att överlåta deras uppgifter till sådana ändamål och kan, om de lämnat samtycke, när som helst återkalla det samtycket.

Flera av de berörda abonnenterna är dessutom personer med skyddad identitet. Detta är incidenter där tillhandahållare olovligen överlåtit sina abonnenters uppgifter till abonnentupplysningsföretag trots att kunden inte har samtyckt till detta. Sådana läckor av

hemliga uppgifter kan leda till allvarliga konsekvenser för de drabbade personerna. Bedömningen av allvarligheten ligger också i att en stor mängd kunder drabbats.

När abonnentupplysningsföretag även har utgivningsbevis från Myndigheten för press, radio och tv innebär det att de har en grundlagsstadgad rätt att publicera personuppgifter de en gång har fått tillgång till och behöver alltså inte iaktta dataskyddsförordningens regler. Det leder till att en incident, där tillhandahållaren inte har skyddat hemliga uppgifter, inte garanterat går att avhjälpa genom att tillhandahållaren i sina egna system rättar det inträffade. Sådana incidenter där abonnentuppgifter en gång har spridits kan därför ha kvarvarande konsekvenser utanför tillhandahållarens kontroll. Detta är särskilt allvarligt i de fall tillhandahållaren har spridit uppgifter för personer som har skyddade personuppgifter.

3.3.6 PTS åtgärder

PTS har genomfört flera tillsynsinsatser genom åren angående olovligt spridande av kunders uppgifter, bland annat rörande hemliga uppgifter som spritts till abonnentupplysning.

PTS har startat tematisk tillsyn om spridning av abonnentuppgifter till abonnentupplysning i februari 2023. Tillsynen omfattar flera tillhandahållare. Tillsynen har föranletts av upprepade och allvarliga incidenter av detta slag sedan den senaste tillsynen.

3.3.7 Förväxling av kunder

En av de mest frekvent rapporterade integritetsincidenterna innefattar någon typ av förväxling av kundbilder. Ofta har personal hos tillhandahållare eller underleverantör av misstag blandat ihop två kundbilder varvid resultatet blivit felaktigt, exempelvis 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.

Tillhandahållaren uppger regelmässigt i incidentrapporteringen att denna typ av incident inträffar på grund av mänskliga misstag. PTS misstänker att, mot bakgrund av den frekvens varmed förväxlingsincidenterna inträffar, det finns brister i organisatoriska rutiner och processer.

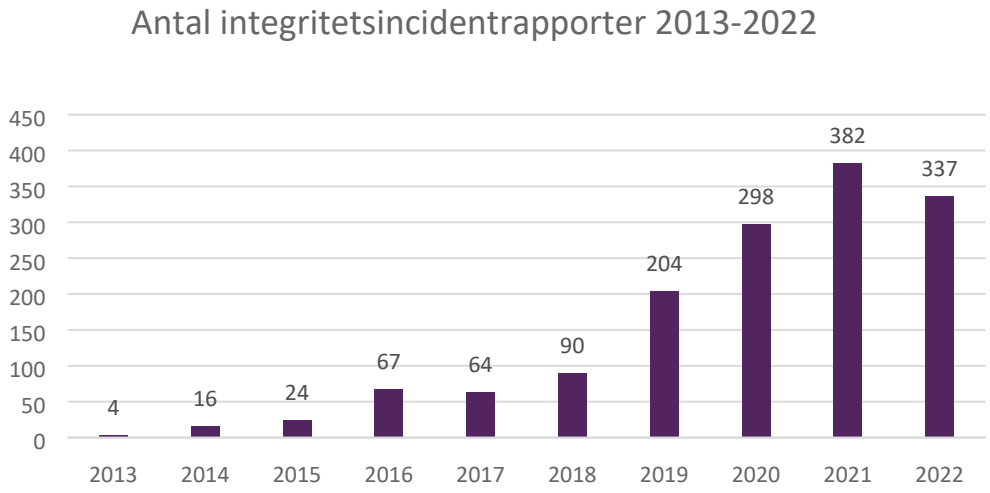
3.3.8 Rapportering från NI-ICS

Under den senare halvan av 2022 har PTS börjat få in incidentrapporter från tillhandahållare av NI-ICS. I LEK definieras dessa tjänster som ”en interpersonell kommunikationstjänst som varken etablerar en förbindelse till nummer i nationella eller internationella nummerplaner

eller möjliggör kommunikation med sådana”. Incidenter hos dessa tillhandahållare uppmärksammas inte sällan i media och hos allmänheten. PTS har fört dialog med ett flertal NI-ICS-tillhandahållare om rapporteringsplikten. I takt med att kunskapen och förståelsen om incidentrapportering ökar bedömer PTS att antalet rapporterade händelser också kommer att öka.

3.4 En jämförelse med tidigare år

Under 2022 skedde något av ett trendbrott gällande antalet incidentrapporter. Tidigare år har det skett först en successiv och på senare år kraftig ökning av antalet integritetsincidenter från år till år. Under 2021 diarieförde PTS 404 rapporter om integritetsincidenter. År 2022 visar däremot en viss minskning jämfört med åren innan då 337 integritetsincidenter rapporterades in.



Samhällets ökade användning av elektroniska kommunikationer, ökning både av förekomsten och uppmärksamheten kring identitetskapningar och cybersäkerhetsangrepp kan vara bidragande faktorer till den generella ökningen av rapporterade integritetsincidenter. PTS uppfattning är dock att den kraftiga ökningen 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

dataskyddsförordningen[13] och det arbete som tillhandahållarna genomförde och fortfarande genomför till följd av detta. LEK är speciallag, i förhållande till dataskyddsförordningen, inom sektorn för elektronisk kommunikation. Minskningen det senaste året kan även den bero på ett flertal olika faktorer. Det är möjligt att ett ökat säkerhetsarbete, och ett ökat fokus på säkerhet på grund av omvärldsläget lett till en faktisk minskning av antalet incidenter. Troligare är att minskningen av rapporterade incidenter beror på förändringar i rapporteringsskyldigheten och tillhandahållarnas arbete med detta.

LEK är den reglering som har företräde och ska tillämpas i första hand när en tillhandahållare av elektroniska kommunikationer behandlar personuppgifter i samband med tillhandahållandet av tjänsterna. Skyddet enligt LEK är mer vidsträckt än bara för personuppgifter. Tillhandahållaren ska skydda samtliga uppgifter, inklusive personuppgifter, som behandlas.[14]

IMY publicerar årligen en rapport över inrapporterade personuppgiftsincidenter.

3.5 Incidenter som rapporteras vidare till Enisa

Större incidenter ska PTS rapportera vidare till Enisa enligt gällande EU-rättsakter.[15] Vidarerapporteringen från medlemsstaterna till Enisa görs i början av varje år. Av de 28 säkerhetsincidenter som rapporterats in till PTS under 2022, 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.

3.6 Om jämförelse med EU-länder

I den här sammanställningen har jämförelse med andra europeiska länder inte kunnat genomföras för integritetsincidenter. Det beror på att det inte finns något sådant underlag att jämföra med. Enisa kommenterar att fokuset historiskt har legat på störningar och avbrott i nät och tjänster, det som tidigare kallats driftsincidenter. Implementeringen av EUs-direktiv (2018/1972) för elektroniska kommunikationer (Kodexen) är genomförd i vissa medlemsstater, men arbetet med incidentrapportering har inte kommit lika långt i medlemsstaterna, varför en jämförelse inte är möjlig.

[13] Den utfärdades av Europaparlamentet och Europeiska unionens råd den 27 april 2016 och trädde i kraft den 24 maj 2016, men blev tillämplig först den 25 maj 2018.

[14] Se prop. 2010/11:115 s. 131

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

Kodexens implementering[16] är ämnad att ge ett bredare fokus. Även incidenter som orsakats av autenticitets-, riktighets- och konfidentialitetsbrister omfattas av vidarerapporteringsplikten till Enisa. År 2020 var första året då Enisa tog emot rapportering av incidenter orsakade av konfidentialitetsbrister. Enisa tog då emot tre rapporter om konfidentialitetsbrister från andra europeiska länder. När Kodexen har implementerats i nationell lag i samtliga medlemsstater kommer sannolikt jämförelseunderlaget successivt att förändras och förbättras. Dock är Enisas trösklar för rapportering högre än de nationella trösklarna i Sverige. Trösklarna skiljer sig även något mellan medlemsstaterna, varför en exakt jämförelse inte kommer vara möjlig.

[16] Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation.

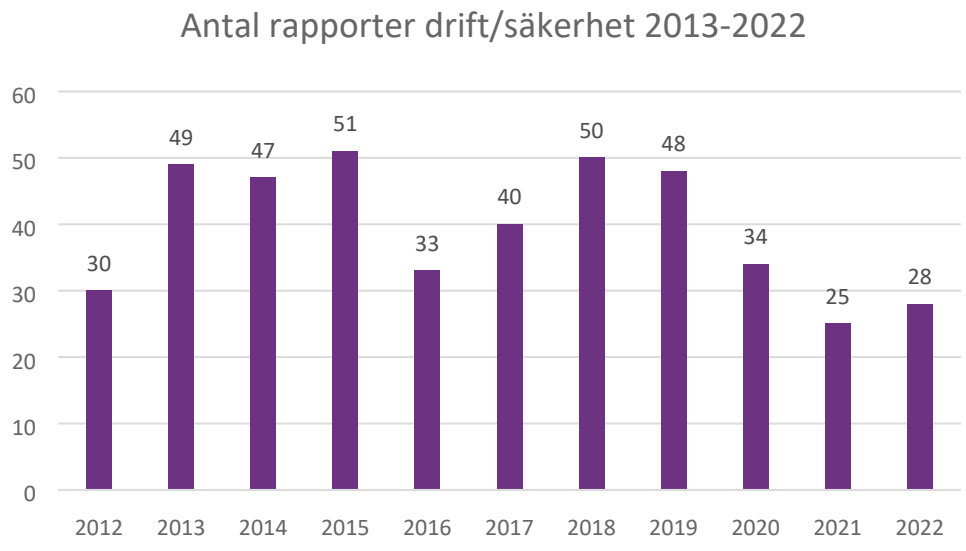
4. Säkerhetsincidenter 2022

Enligt LEK är tillhandahållare skyldiga att rapportera säkerhetsincidenter med betydande påverkan på nät och tjänster till PTS.[17]

Under 2022 har PTS diarieført 28 ärenden med rapporter om säkerhetsincidenter. 5 480 329 användare eller aktiva anslutningar har drabbats i dessa. 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 som faktiskt drabbats av störningen och i stället har antalet användare angetts. I de ärenden där tillhandahållaren inte har meddelat PTS hur många som har drabbats har tillhandahållaren istället angett ett 100 procentigt kapacitetsbortfall.

4.1 En jämförelse med tidigare år

Antalet rapporterade säkerhetsincidenter 2022 är högre än föregående år, men lägre än något år utöver detta. Årligen brukar cirka 30 till 50 händelser om säkerhetsincidenter med betydande påverkan på nät och tjänster rapporteras till PTS.



[17] Reglerna om incidentrapportering finns i 8 kap. 3 § LEK och PTSFS 2022:22.

År med fler incidentrapporter kan ofta förklaras med att en eller flera säkerhetsincidenter har drabbat någon kommunikationsoperatör (KO).[18] 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 och samtliga drabbade av en händelse ska rapportera incidenten självständigt till PTS, om trösklarna för rapporteringsplikten är uppnådda.

I och med ikraftträdandet av nya LEK har en ny typ av aktör börjat rapportera, nämligen tillhandahållare av NI-ICS. En stor del av de drabbade av årets säkerhetsincidenter är just användare av NI-ICS som rapporterat en störning i deras tjänst. Det återstår att se hur rapporteringen från denna typ av aktör kommer att påverka statistik och mönster avseende incidentrapporteringen framöver.

4.1.1 PTS om varför rapporteringen minskat de senaste två åren

Sedan PTS införde trösklarna för incidentrapportering har det skett en omfattande utbyggnad av fibernäten. Storleken på näten och mängden data som överförs över näten har ökat, både i det fasta nätet och i de mobila näten. I takt med det har den infrastruktur som påverkats av det behövt öka i kapacitet. Vad gäller mobilnäten blir näten finmaskigare och har allt högre kapacitet.

PTS föreskrifter om rapporteringskrav för inträffade säkerhetsincidenter utgår ifrån tre värden för trösklar: antal drabbade abonnenter i bestämda tal, hur stor geografisk yta som har drabbats eller bortfall av tjänstekapacitet i procent av tillhandahållarens hela nät och samtliga tjänster. Ju större nät och ju fler abonnenter en tillhandahållare har, desto ovanligare blir det att incidenter som inträffar i det nätet når upp till PTS tröskel om kapacitetsbortfall. Oavsett om de uppnår tröskelvärdena ska incidenter som på annat sätt har haft en betydande påverkan på kommunikationsnätet eller kommunikationstjänsten eller betydande påverkan på funktioner i samhället rapporteras till PTS.

Robustheten i näten har förbättrats och PTS ser klart färre fall av incidenter orsakade av avgrävda kablar eller naturhändelser.

[18] En nätägare kan lägga ut driften av den aktiva utrustningen i sitt nät till en KO. Detta gör i många fall de kommunala stadsnätsbolagen för driften av lokala fibernät. KO:n får då lokalt 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 den vill köpa bredbandstjänster av.

4.1.2 Inverkan av PTS rapporteringströsklar

Enligt LEK är det säkerhetsincidenter av betydande påverkan på nät och tjänster som ska rapporteras till PTS. PTS rapporteringströsklar styr alltså vad betydande påverkan på nät och tjänster innebär.[19] Detta leder till att en mängd säkerhetsincidenter inte anses ha en så betydande påverkan på tillgänglighet i nät och tjänster störningar och avbrott att de rapporteras till PTS, och att PTS därför inte har hela bilden av inträffade incidenter i elektroniska kommunikationer.

PTS trösklar har således betydelse för både antalet rapporterade incidenter och vilken orsak som ter vanligast i den här sammanställningen. Det betyder inte nödvändigtvis att orsaken är vanligast utifrån tillhandahållarnas perspektiv. Vissa typer av säkerhetsincidenter rapporteras till PTS i mycket hög utsträckning. Fel som tar lång tid att åtgärda är exempelvis ovanliga men rapporteras i betydligt högre utsträckning en korta men lättåtgärdade fel. Trösklarna kan då vara en bidragande anledning till varför vissa orsaker, när vi sammanställer alla årets incidenter, blir vanligare än andra.

En ny bestämmelse i PTS föreskrifter[20] gör dock att säkerhetsincidenter med betydande ekonomisk eller samhällspåverkan ska rapporteras till PTS. Detta innebär alltså att incidenter som inte är tillräckligt omfattande för att komma över PTS rapporteringströsklar ändå kan vara rapporteringspliktiga, om de har en betydande påverkan på funktioner i samhället.

PTS har inte mottagit incidentrapporter med betydelser på funktioner i samhället i någon större utsträckning. Funktioner i samhället kan vara exempelvis påverkan på möjligheten att nå 112 eller nationell nödkommunikation, mediapublicering eller en hög risk för allmänhetens säkerhet.[21] PTS har fört en dialog med vissa tillhandahållare om rapportering med basis i denna rapporteringsskyldighet och följer noggrant utvecklingen med rapporteringen.

4.2 Orsaker till säkerhetsincidenter 2022

De inrapporterade, rapporteringspliktiga säkerhetsincidenterna, 28 stycken, har delats in i kategorier baserade på grundorsaker och därtill mer detaljerade orsaker.

21 av de 28 incidenterna har sin grundorsak i systemfel och sju har sin grundorsak i mänsklig felbedömning eller misstag. Incidenter har endast räknats en gång i tabellen och förekommer

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

[20] 17:6 PTSFS 2022:11.

[21] Technical Guideline on Incident Reporting under the EECC — ENISA (europa.eu)

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 störningar och avbrott under 2022 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 incidenter. Den följer i stort Enisas indelning i grundorsaker (root causes[22]) och detaljerade orsaker (detailed or technical causes).

Grundorsaker till de 28 säkerhetsincidenterna	**Detaljerade orsaker till de 28 incidenterna**
21 st. orsakades av systemfel	Varav 8 hårdvarufel 8 mjukvarubugg 5 felaktig uppdatering av mjukvara 3 strömavbrott 1 felaktig uppdatering av hårdvara 1 ”övrigt”
4 st. berodde på mänskliga misstag eller felbedömningar	Varav 3 felaktig uppdatering av mjukvara 1 avgrävd fiberkabel
2 orsakades av fel hos tredje part (partner/underleverantör)	1 hårdvarufel 1 ”övrigt”
En incident orsakades av brister i organisatoriska rutiner och processer	Felaktigt utfört redundanstest

Under 2022 rapporterades inte några större avbrott i elektroniska kommunikationer i samband med hårt väder, inte heller 2021 rapporterades någon sådan händelse.

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

4.3 PTS kommentarer om årets rapporterade grundorsaker och detaljerade orsaker

4.3.1 Hårdvarufel

Tillhandahållarna drabbas också av fel och sårbarheter i nät och tjänster orsakade av delar som de har köpt av annan och därefter byggt sitt nät eller tjänst med. Det finns ett europeiskt och internationellt ökat fokus på området säkerhet i leveranskedjor (supply-chain-security). Den typen av riskanalyser som aktualiseras här innebär att även delar som produceras av annan och inhandlas av tillhandahållarna, eller transporter av delar, behöver bedömas ur säkerhetssynpunkt. PTS utgår ifrån att analyser kring denna typ av säkerhet i näten i framtiden kommer att bli mer centralt för säkerhet i nät och tjänster samt säkerhet för behandlade uppgifter.

4.3.2 Mjukvarubugg

En av de vanligaste orsakerna till säkerhetsincidenter 2022 var buggar. Ofta uppmärksammas dessa buggar i samband med en uppdatering av mjukvara men i vissa fall har buggen upptäckts spontant.

4.3.3 Mänsklig felbedömning eller misstag[23]

Antalet anmälda incidenter beroende på mänskliga fel och misstag har minskat något sedan föregående år.

4.3.4 Strömavbrott

I fjol hade PTS förhoppningen om att incidenter med denna orsak skulle minska under 2022. Anledningen var att PTS föreskrifter om reservkraft trädde i kraft den 10 juni 2020 och behållits i princip oförändrade i och med PTSFS 2022:11. Föreskrifterna om reservkraft innebär att nätens tillgångar ska förses med reservkraft för att klara av driften under strömavbrott under en viss stadgad tid, som beror på hur många användare som är beroende av tillgången och om den ligger i tätort eller på landsbygd.[24] I år kan vi se en minskning av incidenter kopplade till strömavbrott, samt att det i de kvarvarande fallen ofta är att strömavbrottet orsakade ett annat problem snarare än att det varit problemet i sig. År 2022 var strömavbrott den bakomliggande orsaken till tre incidenter. År 2021 var motsvarande

[23] Uttrycket är en översättning av Enisas uppföljningsbegrepp för ”root cause human error”
[24] PTSFS 2022:11, 11 kap

siffra åtta incidenter. PTS förhoppning verkar ha infriats men det är för tidigt att säga om denna minskning kvarstår över tid.

4.3.5 Avgrävda kablar

Tidigare år har en av de vanligast förekommande orsakerna till säkerhetsincidenter varit avgrävda kablar. En god nyhet är att under 2022 inträffade enbart en sådan incident. Det går inte att helt eliminera risken för att någon gräver av en kabel som ligger i marken. Problemet med avgrävningar av kablar är välkänt både på EU-nivå och nationellt. PTS driver sedan 2010 den kostnadsfria webbtjänsten ledningskollen.se. Ledningskollen är avsedd att minska antalet grävskador, öka säkerheten och sänka ledningsägarnas kostnader till följd av grävskadorna. Nätägare uppmuntras därför att registrera sig som ledningsägare i Ledningskollen, och också att sprida kunskapen om att Ledningskollen finns till sina affärspartners och abonnenter.

4.3.6 Överbelastningsattacker och antagonistiska angrepp

Det finns inte någon incident under 2022 med denna orsak, och få rapporter över åren – men även antagonistiska angrepp är en incident i lagens mening och omfattas av rapporteringsskyldigheten.

4.4 En jämförelse med EU-länder

Genom att alla medlemsstaterna i EU vidarerapporterar de incidenter med störst konsekvenser till Enisa, kan Enisa se mönster i orsakerna på en paneuropeisk nivå. Enisa tar årligen emot ett par hundra rapporter från medlemsstaterna och analyserar i en årlig rapport både orsaker till incidenterna, och hur många förlorade användartimmar varje orsak leder till.

Enisas rapport Telecom Security Incidents[25] publiceras årligen i juli och därmed är det siffrorna från 2021 som analyseras nedan.

Med underlag i de senaste nio årens rapporter från medlemsstaterna har Enisa konstaterat att:

- Antalet rapporterade incidenter ligger relativt konstant från år till år.
- Systemfel är den vanligaste grundorsaken. De förlorade användartimmarna efter systemfel minskade något. Den vanligaste detaljerade orsaken inom systemfelen är hårdvarufel (34 %) och mjukvarubuggar (27 %).

[25] Telecom Security Incidents 2021 - Annual Report — ENISA (europa.eu). Publicerad i juli 2022

- Samtliga förlorade användartimmar ökade drastiskt jämfört med tidigare år. 5,106 miljoner timmar jämfört med 841 år 2020. Ökningen beror i stor del på att olika medlemsstater rapporterat samma gränsöverskridande incident separat.
- För första gången har incidenter gällande autenticitet och konfidentialitet rapporterats. Antalet rapporter av denna typ antas öka.
- Grundorsaken mänskliga misstag (*human error*) ligger stabilt jämfört med 2020, efter en tidigare årlig ökning sedan 2016.
- De förlorade användartimmarna efter mänskliga misstag står dock för 91% av förlorade användartimmar.
- Antagonistiska angrepp såsom hackning och överbelastningsattacker orsakar endast kring 8 % av alla säkerhetsincidenter.

Mänskliga misstag är den orsak som leder till mest negativa konsekvenser sett till antal förlorade användartimmar. Tidigare var det systemfel men de senare åren har systemfelen minskat i antal, medan störningar och avbrott orsakade av mänskliga misstag ökar för varje år.

När det gäller hur allvarliga incidenterna anses vara har det skett en tydlig nedgång i antalet incidenter som klassas som väldigt stora. Skalan är fyrgradig med alternativen ingen, liten, stor eller väldigt stor påverkan. Tidigare år har väldigt stor påverkan varit den vanligaste av de rapporterade incidenterna men 2021 hade minskningen av den klassningen samtidigt som ökningen av kategorin stor gjort att de nu bytt plats. Trots fler förlorade användartimmar minskar alltså konsekvenserna av incidenterna.

Vanligast grundorsaker till driftsincidenter 2021 i EU-länder:

- Systemfel 59 %
- Mänskliga misstag 23 %
- Naturkrafter 10%
- Antagonistiska angrepp 8%

5. Tillsynsrapport

Här beskriver PTS tillsynsinsatser under 2022 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 om krav på 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.

5.1 Avslutade tillsynsärenden 2022

Under 2022 har tre tillsynsinsatser avslutats.

5.1.1 Tillsyn över säkerhetsåtgärder och kända sårbarheter i trafikutbyte på internet

PTS har granskat säkerhetsarbetet för att motverka kända risker och sårbarheter med Border Gateway Protocol (BGP) hos fem olika tillhandahållare[26], i enlighet med LEK och PTS föreskrifter om säkerhet i nät och tjänster[27]. Tillsynen inleddes i oktober 2020 och har avslutats för samtliga granskade tillhandahållare under 2022. PTS anser att tillhandahållarna har vidtagit lämpliga åtgärder för att höja säkerheten vid externt trafikutbyte på internet.

Reservkrafttillsyn

PTS har granskat hur fem tillhandahållare efterlever myndighetens regler om reservkraft som återfinns i PTS föreskrifter om säkerhet i nät och tjänster[28]. Tillsynen inleddes i november 2020 och avslutades under 2022. Tillsynen avslutades utan vidare åtgärd då PTS identifierat ett behov av att utreda reservkraftskraven närmare i en intern utredning.

[26] Netnod Internet Exchange AB, Telia Company AB, Tele2 AB, Telenor Sverige AB och Hi3G Access AB.
[27] Numera PTSFS 2022:11, tidigare PTSFS 2015:2 och 2014:1
[28] Numera PTSFS 2022:11, tidigare 2015:2

Röstbrevlådetillsyn

PTS har granskat säkerhetsåtgärder i röstbrevlådor hos Telenor Sverige AB med anledning av att obehöriga gjort intrång i abonnenters och användares röstbrevlådor. I tillsynen har PTS granskat rutiner, förmåga att upptäcka intrång samt åtgärder för skydd av uppgifter som behandlas i röstbrevlådor enligt LEK och PTS föreskrifter om säkerhet i nät och tjänster[29]. Tillsynen inleddes i april 2021 och avslutades den 13 januari 2023. PTS anser att Telenor Sverige AB har vidtagit lämpliga åtgärder för att höja säkerheten i röstbrevlådor.

5.2 Pågående tillsynsinsatser

5.2.1 Tillsyn avseende otillåtet utlämnande av abonnentuppgifter till abonnentupplysning

Tillsynen omfattar tre tillhandahållare[30] som enligt rapporterade incidenter har lämnat ut behandlade uppgifter, i det här fallet abonnentuppgifter, till abonnentupplysning utan kundernas medgivande, för kunder med skyddade personuppgifter eller med hemligt nummer. Incidenterna kan ha inneburit allvarliga konsekvenser för de drabbade, särskilt för personer med skyddade personuppgifter. Tillsynen syftar till att säkerställa att de granskade tillhandahållarna har vidtagit lämpliga tekniska och organisatoriska åtgärder för att skydda abonnenters uppgifter. Tillsynen startades i februari 2023.

5.3 Tillsynsarbete framåt

PTS har identifierat ett antal områden som skulle kunna utgöra grund för möjliga tillsynsinsatser framöver. Nya regler, nya aktörer som omfattas av reglerna, erfarenheter från inrapporterade incidenter, samt ny teknik är exempel på teman av intresse för PTS tillsyn.

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 säkerställer 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.

[29] Numera PTSFS 2022:11, tidigare 2014:1

[30] Telia Company AB, Telenor Sverige AB och Tele2 AB

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

6. BILAGA 1

6.1.1 Metod och arbetsprocess för incidentsammanställning

Arbetet med sammanställningen av incidenter har genomförts på följande sätt.

Inledningsvis gjordes flera genomgångar av alla incidentrapporter från 2022. 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,[31] 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,[32] 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 2022.

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

[31] Telecom Security Incidents 2021 - Annual Report — ENISA (europa.eu)

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