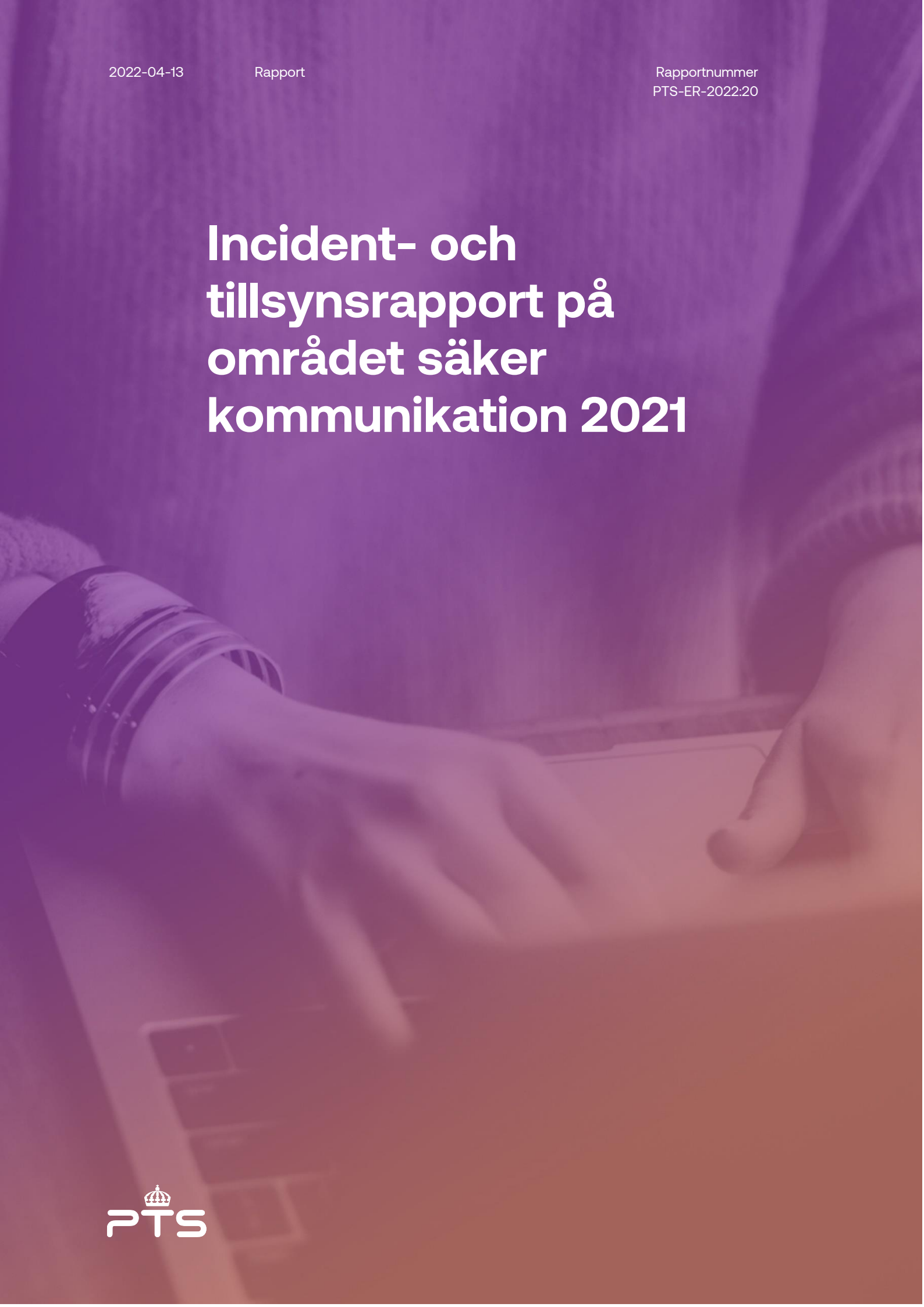
2022-04-13 Rapport

Rapportnummer
PTS-ER-2022:20

Incident- och tillsynsrapport på området säker kommunikation 2021



Rapportnummer
PTS-ER-2022:20

Diarienummer
22–4400

ISSN
1650–9862

Författare
Therese Braathen, avdelningen för säker kommunikation
Bahare Gazani, avdelningen för säker kommunikation

Post- och telestyrelsen
Box 6101
102 32 Stockholm

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

Innehåll

Sammanfattning

Incidenter

Tillhandahållare av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster, i rapporten kallade operatörer, är skyldiga att rapportera vissa incidenter till Post- och telestyrelsen (PTS) enligt lagen (2003:389) om elektronisk kommunikation (LEK). PTS är tillsynsmyndighet på området.

Totalt under 2021 har PTS registrerat 429 inrapporterade incidenter. Det rör sig om 25 driftsincidenter och 404 integritetsincidenter. Detta är det lägsta antalet driftsincidenter som har rapporterats under ett år, och det högsta antalet integritetsincidenter sedan rapporteringsskyldigheten trädde ikraft.

PTS har här sammanställt och grupperat de rapporterade driftsincidenterna och integritetsincidenterna från 2021. PTS kommenterar också vilken typ av orsak som är vanligast till driftsincidenter, och vilken typ av integritetsincident som är mest allvarlig enligt PTS mening. Här finns också övergripande jämförelser med tidigare år samt med EU-länder överlag. Integritetsskyddsmyndighetens (IMY) och europeiska unionens cybersäkerhetsbyrå ENISA:s uppställningar av orsaker har använts för att skapa jämförbarhet.

Den vanligaste grundorsaken till rapporterade driftsincidenter under 2021 var systemfel (15 av incidenterna), varav åtta incidenter berodde på strömavbrott genom att reservkraften eller övergången till reservkraft inte fungerade. De allvarligaste integritetsincidenterna 2021 var intrång i röstbrevlådor där 944 personer drabbades av intrången, och röjande av hemliga uppgifter till abonnentupplysning där sammanlagt 48 132 personer drabbades.

Integritetsincidenterna drabbade totalt 64 497 användare eller abonnenter och driftsincidenterna drabbade minst 435 000 användare eller aktiva anslutningar.

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

Under 2022 utfärdar PTS nya säkerhetsföreskrifter som bland annat innebär delvis nya regler för incidentrapporteringen.

Tillsyn

PTS ska genom tillsyn granska och säkerställa efterlevnaden av LEK vad gäller driftsäkerhet och skydd av uppgifter samt de föreskrifter som meddelats med stöd av densamma.

Under 2021 avslutade PTS årlig tillsyn av inrapporterade incidenter hos åtta operatörer. Den årliga tillsynen omfattade ett urval av operatörer och inrapporterade driftsincidenter.

PTS avslutade även en tillsyn rörande skyddet av sjökablar, vilka störningar som förekommit samt vilka riktlinjer som operatörer använder vid förläggning av sjökablar.

PTS har en pågående tillsyn gällande sårbarheter i Border Gateway Protocol (BGP) samt en pågående tillsyn kring efterlevnaden av reservkraftsregler vid strömavbrott.

Under 2022–2023 planerar PTS att bedriva ett antal tillsynsinsatser, bland annat utifrån det som incidentrapporteringen 2021 visar, och som redogörs för nedan i rapporten.

Det regelverk som gäller på området säker elektronisk kommunikation nu beskrivs närmare i bilaga 3. Under år 2022 träder nya lagen om elektronisk kommunikation i kraft, grundad på EU-direktiv, och PTS kommer att utfärda nya föreskrifter i anledning av den nya lagen. Mot bakgrund av detta är nuvarande regler beskrivna på en övergripande nivå.

Incidentrapport 2021

Driftsincidenter och integritetsincidenter 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 driftssäkerhet eller skydd av uppgifter efterföljs, och huruvida tillsyn behöver inledas. Det finns även andra syften med incidentrapporteringen, till exempel för att skapa en överblick över operatörernas säkerhetsproblem, som underlag till nya regler, för att identifiera informationsbehov eller behov av främjandeinsatser. Totalt under 2021 har PTS registrerat 429 ärenden med inrapporterade incidenter, varav 406 slutligt har bedömts som rapporteringspliktiga incidenter. Det har rört sig om 25 inrapporterade driftsincidenter och 404 rapporterade incidenter där skydd av uppgifter har brustit, så kallade integritetsincidenter.

Syftet med incidentrapporten är att kunna ge rapporterande operatörer, andra intressenter och PTS en överblick av fjolårets incidentrapportering. PTS vill också sprida kunskap om incidenterna till flera operatörer. Genom sammanställningen vill PTS förmedla sin uppfattning om var det finns mönster som kan vara intressanta utifrån reglerna om driftsäkerhet och skydd för uppgifter. Sammanställningen kan också användas för planeringen av tillsynsinsatser hos PTS och för planering av operatörernas förebyggande arbete. PTS vill utifrån de rapporterade incidenterna även förmedla en bild av var operatörerna lämpligen kan planera att utveckla säkerhetsarbetet för driftsäkerhet och skydd för uppgifter. Det är ett för litet antal rapporter för att uppnå någon statistisk signifikans och PTS avser inte att ge en statistiskt säkerställd analys eller statistiskt säkerställd bild med den här rapportens innehåll.

I rapporten kallas de tillhandahållare som rapporterar incidenterna i elektroniska kommunikationer för operatörer. För vidare information om metod till denna incidentrapport, se bilaga 1.

[1] Regler kring rapporteringsskyldigheten finns i 5 kap 6 c § och 6 kap 4 a § LEK och i PTS föreskrifter och allmänna råd (PTSFS 2012:2) om rapportering av störningar eller avbrott av betydande omfattning, samt i 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).

Integritetsincidenter 2021

Sedan 2011 är operatörer skyldiga att rapportera inträffade integritetsincidenter till PTS.[2] Skyldigheten grundas på att operatörerna ska skydda alla uppgifter som behandlas i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster.[3] Det innebär att skyldigheten att skydda uppgifter inte bara avser personuppgifter, utan skyddet ska avse *alla uppgifter* som operatörerna behandlar i samband med tillhandahållandet av elektroniska kommunikationstjänster.

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

Händelser med olovliga avslöjanden, olovliga ändringar av uppgifter/tjänster och förluster av uppgifter/tjänster hos operatörerna är integritetsincidenter enligt LEK. Det rör sig om sådana händelser som att uppgifter raderas eller registreras in fel hos operatören, obehöriga ändringar eller obehörigt nytecknande av abonnemang, eller läckta uppgifter till obehöriga. Se vidare om förhållandet till Dataskyddsförordningen (GDPR) och specifikt kring rapporteringsplikt i bilaga 2.

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

Under 2021 diarieförde**s 404** inrapporterade integritetsincidenter hos PTS. Under handläggning och granskning har det visat sig att **382** av dessa utgör regelrätta integritetsincidenter. Det justerade antalet beror på att operatörer har återkallat vissa

[2] Regler kring rapporteringsskyldigheten för integritetsincidenter finns i 6 kap 4a § LEK och i förordning 611/2013.
[3] Regeln om det finns i 6 kap 3 § LEK.

incidentrapporter. Det finns även rapporterade händelser som PTS inte klassar som integritetsincidenter eller som har dubbelregistrerats hos PTS.

Totalt har 64 497 användare eller abonnenter drabbats i integritetsincidenterna 2021. Utöver dessa har 1 024 429 användare eller abonnenter rapporterats som potentiellt drabbade, d.v.s. dessa har inte bestämt kunnat konstateras att de har drabbats.

De ärenden där flest abonnenter och användare drabbats är sådana där sekretessbelagda uppgifter olovligen har spritts till abonnentupplysning. 48 132 personer, bland dem 182 personer med skyddad identitet, drabbades i sju olika incidenter under året.

Alla operatörer rapporterar inte lika många integritetsincidenter. PTS kan liksom i förra årets sammanställning konstatera en ojämn fördelning av rapporterade incidenter mellan de största operatörerna. Den ojämna fördelningen under 2021 består i att en större operatör har rapporterat få integritetsincidenter i jämförelse med de andra större operatörerna.

Den ojämna fördelningen är inte relaterad till bolagens storlek. Det är inte heller säkert att de operatörer som rapporterar flest incidenter är de där flest incidenter inträffar. Det kan också vara så att vissa operatörer upptäcker fler incidenter och därför rapporterar mer till PTS. Även om en operatör rapporterar få incidenter, kan fåtalet röra allvarliga incidenter.

Åtminstone en operatör har förbättrat sin incidentrapportering till PTS under 2021. Enligt PTS genomgång av incidentrapporteringen syns att operatören genomfört en förbättring både av verktygen för upptäcktsförmåga och av rapporteringen i sig.

PTS uppmanar alla operatörer att vid tvekan av om 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 mot operatörer för att förbättra incidenthantering och rapportering.

PTS fortsatta arbete med problemet: PTS har en planerad tillsynsinsats om förmågan att förebygga och upptäcka integritetsincidenter och att incidentrapportera.

Orsaker till integritetsincidenter 2021

För att visa grundorsaker och mer detaljerade orsaker eller konsekvenser av integritetsincidenter under 2021 presenteras här en tabell och två figurer.

En integritetsincident tilldelas endast en grundorsak men kan ha flera detaljerade orsaker eller konsekvenser. Till exempel: En incident där en obehörig företrädare för bolagskund fått teckna nya tjänster kan ha grundorsak *mänskligt misstag* och sedan ha både *fel företrädare för bolaget* och *bristande autentisering* som detaljerad orsak eller konsekvens.

Detta leder till att summorna för detaljerade orsaker och konsekvenser blir något högre än summan incidenter som beskriver grundorsaken.

Det är också så att en specifik detaljerad orsak/konsekvens, till exempel felpackning eller fel kontaktuppgift, kan ha visat sig ha olika grundorsaker vid olika incidenter. Det är exempelvis möjligt att felpackning främst skett på grund av ett mänskligt misstag eller på grund av att det finns brister i rutinerna. Felpackningar som har berott på mänskliga misstag räknas då endast till den nämnda grundorsaken, medan felpackningar som visat sig bero på bristande rutiner räknas till den senare grundorsaken. Det här leder till att en specifik detaljerad orsak/konsekvens återfinns inom olika grundorsakskategorier.

Syftet med att ange fler detaljerade orsaker är att PTS vill tydliggöra de problematiska situationer som upprepar sig, när det är möjligt. På så vis är sammanställningen tänkt att kunna vara en utgångspunkt för operatörerna att identifiera om någon riktad teknisk eller organisatorisk åtgärd kan motverka fler incidenter i framtiden.

PTS har utgått från ENISA:s uppställning av grundorsaker till incidenter i nät och tjänster samt lagt till IMY:s uppställning av grundorsaker till personuppgiftsincidenter som rapporterats till IMY.[4]

Det har skett 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 att skapa jämförbarhet med personuppgiftsincidenter enligt Dataskyddsförordningen.[5]

PTS presenterar också detaljerade orsaker, typer och konsekvenser, 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.

[4] Tilläggen som PTS har gjort till IMY:s orsaker är i kategorin för antagonistiskt angrepp där PTS lagt till cyberattack.

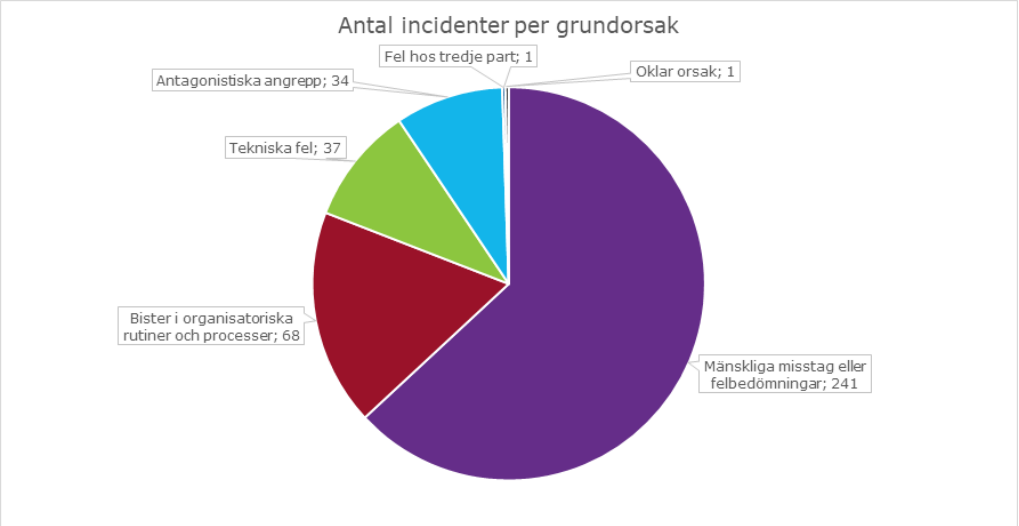
[5] Europaparlamentets och Rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävandet av direktiv 95/46/EG (allmän dataskyddsförordning).

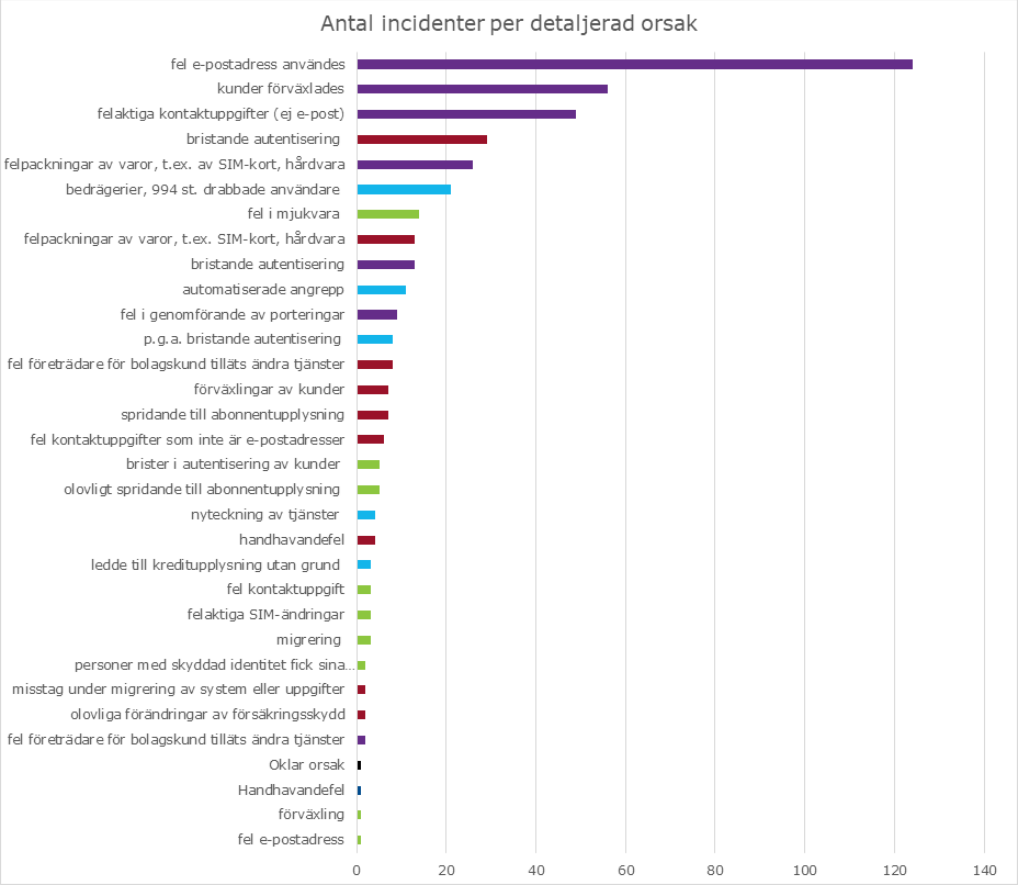
Grundorsaker till samtliga 382 integritetsincidenter 2021	**Detaljerade orsaker, typer och konsekvenser som återfinns i incidenterna 2021** [6]
241 incidenter hade mänskliga misstag eller felbedömningar som grundorsak	Av de 241 incidenterna med mänskliga misstag eller felbedömningar som grundorsak berodde: 124 på att fel e-postadress användes, 49 på att felaktiga kontaktuppgifter (ej e-post) användes, 56 på att kunder förväxlades, 26 på felpackningar av varor, t.ex. av SIM-kort, hårdvara, 13 på bristande autentisering, 9 på fel i porteringar, 2 fel företrädare för bolagskund tilläts ändra tjänster. Antal detaljerade orsaker: 279
68 incidenter hade brister i organisatoriska rutiner och processer som grundorsak	Av de 68 incidenterna med bristande rutiner och processer som grundorsak berodde: 29 på bristande autentisering, 13 på felpackningar av varor, t.ex. SIM-kort, hårdvara, 8 på fel företrädare för bolagskund tilläts ändra tjänster, 7 på spridande till abonnentupplysning, 7 på förväxlingar av kunder, 6 på fel kontaktuppgifter (e-post), 4 på handhavandefel, 2 på olovliga förändringar av försäkringsskydd, 2 på misstag under migrering av system eller uppgifter. 182 personer med skyddad identitet drabbades i de sju incidenterna med spridande till abonnentupplysning Antal detaljerade orsaker: 79
37 incidenter hade tekniska fel som grundorsak	Av de 37 incidenterna med tekniska fel som grundorsak berodde: 14 på fel i mjukvara 5 på olovligt spridande till abonnentupplysning 5 på brister i autentisering av kunder 3 på migrering 3 på felaktiga SIM-ändringar 3 på fel kontaktuppgift (ej e-post)

[6] De detaljerade orsakerna och konsekvenserna är alltså fler till antalet än totalantalet. Det beror på att en incident märkts upp med fler detaljerade orsaker/konsekvenser.

	2 innebar att personer med skyddad identitet fick sina kontaktuppgifter röjda 1 på fel e-postadress 1 på förväxling av kunder. Antal detaljerade orsaker: 37
34 incidenter hade antagonistiska angrepp som grundorsak. 16 av dessa var medvetna angrepp från någon inom organisationen inklusive underleverantörer	Av de 34 incidenterna med antagonistiskt angrepp som grundorsak berodde: 21 på bedrägerier, 11 på automatiserade angrepp, 8 skedde på grund av bristande autentisering, 3 ledde till kreditupplysning utan grund. 994 personer drabbades i de 21 bedrägerierna Antal detaljerade orsaker: 43
En incident hade fel hos tredje part (partner eller underleverantör som grundorsak)	Handhavandefel
En incident hade oklar orsak som grundorsak	Även den detaljerade orsaken är oklar.

I nedan cirkeldiagram visas de olika grundorsakerna. Varje grundorsak presenteras i en enskild färg. Färgerna i cirkeldiagrammet upprepas sedan i följande stapeldiagram som visar de detaljerade orsakerna och konsekvenserna, knutna till grundorsaker.


Antal incidenter per grundorsak
Fel hos tredje part; 1
Oklar orsak; 1
Antagonistiska angrepp; 34
Tekniska fel; 37
Bister i organisatoriska rutiner och processer; 68
Mänskliga misstag eller felbedömningar; 241


Antal incidenter per detaljerad orsak
fel e-postadress användes
kunder förväxlades
felaktiga kontaktuppgifter (ej e-post)
bristande autentisering
felpackningar av varor, t.ex. av SIM-kort, hårdvara
bedrägerier, 994 st. drabbade användare
fel i mjukvara
felpackningar av varor, t.ex. SIM-kort, hårdvara
bristande autentisering
automatiserade angrepp
fel i genomförande av porteringar
p.g.a. bristande autentisering
fel företrädare för bolagskund tilläts ändra tjänster
förväxlingar av kunder
spridande till abonnentupplysning
fel kontaktuppgifter som inte är e-postadresser
brister i autentisering av kunder
olovligt spridande till abonnentupplysning
nyteckning av tjänster
handhavandefel
ledde till kreditupplysning utan grund
fel kontaktuppgift
felaktiga SIM-ändringar
migrering
personer med skyddad identitet fick sina...
misstag under migrering av system eller uppgifter
olovliga förändringar av försäkringsskydd
fel företrädare för bolagskund tilläts ändra tjänster
Oklar orsak
Handhavandefel
förväxling
fel e-postadress
0
20
40
60
80
100
120
140

PTS kommentarer

Olovlig spridning av kunders uppgifter till abonnentförteckningar (abonnentupplysning): De ärenden där flest abonnenter och användare drabbats under 2021 är sådana där deras operatör olovligen har spritt deras uppgifter till abonnentupplysning. PTS ser allvarligt på att 48 132 personer under 2021 drabbades av att deras uppgifter spreds till abonnentupplysning trots att det förelåg tystnadsplikt för operatören. Det faktum att 182 personer med skyddade personuppgifter under året drabbades av att deras uppgifter offentliggjorts inskärper i högsta grad allvaret.

I vissa fall, beroende på om mottagande abonnentupplysningsföretag har utgivningsbevis[7], kan heller inte uppgifterna raderas när den obehöriga spridningen väl har gjorts, vilket gör incidenterna särskilt allvarliga.

I Sverige finns abonnentförteckningar som elektronisk katalog på internet, tryckt katalog och olika typer av nummerupplysningstjänster på internet eller via 118-nummer. Operatörerna 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 abonnentuppgifter hos operatörerna. För att uppgifter ska kunna lämnas ut till ett abonnentupplysningsföretag krävs att abonnenten har lämnat sitt samtycke. Alla abonnenter 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. Abonnenterna har enligt LEK rätt att neka operatörerna att överlåta deras uppgifter till sådana ändamål och kan, om de lämnat samtycke, när som helst återkalla det samtycket.

Detta är händelser där operatörer olovligen överlåtit sina abonnenters uppgifter till abonnentupplysningsföretag trots att kunden inte har samtyckt till detta. Bland de drabbade abonnenterna finns även personer med skyddad identitet. Sådana läckor av hemliga uppgifter kan leda till allvarliga konsekvenser för de drabbade personerna. Särskilt hög risk löper de med skyddade personuppgifter.

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 GDPR. Det leder till att en incident där operatören inte har skyddat hemliga uppgifter inte garanterat går att läka genom att operatören i sina egna system rättar det inträffade.

[7] För att läsa mer om utgivningsbevis: Utgivningsbevis - Myndigheten för press, radio och tv (mprt.se)

Sådana incidenter där abonnentuppgifter som en gång har spritts kan därför ha kvarvarande konsekvenser utanför operatörens kontroll. Detta är särskilt allvarligt i de fall operatören har spritt uppgifter för personer som har skyddad identitet i folkbokföringen.

PTS åtgärder hittills: PTS har under åren genomfört flera tillsynsinsatser angående olovligt spridande av kunders uppgifter, bland annat rörande uppgifter som obehörigen spritts till abonnentupplysning.

PTS fortsatta arbete med problemet: PTS planerar tillsyn om obehörig spridning av hemliga nummer och kunders personuppgifter till abonnentförteckningar och nummerupplysningsföretag. Tillsynen planeras att riktas mot flera operatörer. Planen har föranletts av upprepade och allvarliga incidenter av detta slag sedan den senaste tillsynen.

Intrång i röstbrevlådor: I början av 2021 rapporterades inledningsvis en incident på grund av ett cyberangrepp i form av automatiserade intrångsförsök mot en operatörs röstbrevlådor. Den rapporten följdes sedan av ytterligare nio incidentrapporter från andra operatörer. Totalt har det konstaterats att 944 användare/abonnenter har drabbats av intrång i sina röstbrevlådor i de nio incidenterna. Det totala antalet drabbads kan vara högre. Det finns kännedom om att kapade röstbrevlådor i dessa händelser har använts för att skapa falska användare på sociala medier.

PTS åtgärder hittills: PTS inledde tillsyn våren 2021 mot en operatör och den pågår under 2022. PTS har i tillsynen angett myndighetens uppfattning i en underrättelse om vilka säkerhetsåtgärder som är nödvändiga för att upprätthålla skydd av uppgifter i röstbrevlådor.

Antagonistiska angrepp inom och utanför organisationen: En allvarlig form av integritetsincident är när operatörens personal luras av obehöriga att lämna ut information om abonnemang, eller låter obehöriga (ej tillräckligt autentiserade) ändra i abonnemang. Dessa incidenter innebär allvarliga kränkningar av kunders privatliv. I det här årets sammanställning har PTS även urskilt hur många av incidenterna som beror på medvetna angrepp av någon inom organisationen, vilket även omfattar operatörernas underleverantörers personal.

PTS åtgärder hittills: Under de senaste åren har det bedrivits tillsyn av PTS för att minska problemet med att operatörer lämnar ut information eller låter obehöriga personer ändra i kunders abonnemang. Under 2020 förelade PTS de fyra största operatörerna att införa en tekniskt tvingande autentisering av de kunder som ringer till kundtjänst. De tekniska skyddsåtgärderna är nu på plats. PTS har inte ställt krav på att operatörerna ska använda BankID eller liknande. Valet av tekniskt säker lösning

görs av operatörerna. Även kunder som saknar tillgång till BankID ska ges tillgång till en säker teknisk autentisering för att skydda deras uppgifter.

Åtgärden innebär att kundtjänstpersonal inte längre själva får avgöra om kunden är legitimerad eller autentiserad, utan den bedömningen görs genom en teknisk lösning. Först när autentiseringen är avklarad kan kundtjänstpersonal kommunicera om abonnemangsuppgifter med kunden. På det viset ska bedragare inte längre kunna lura kundtjänstpersonal att lämna ut hemlig information eller ändra i abonnemang. Under 2021 drabbades trots detta 994 abonnenter eller användare av integritetsincidenter i form av bedrägerier.

PTS fortsatta arbete med problemet: PTS planerar att följa upp tillsynen om autentisering i kundtjänst för att granska andra aspekter av autentisering.

Felregistrerade e-postadresser: Den vanligaste typen av integritetsincident under 2021 och tidigare år beror på att fel e-postadresser används vid utskick till kunder eller på att kunder förväxlas i kundtjänst. Under 2021 finns 125 incidenter som berott på att fel e-postadress har använts av operatören.

PTS bedömer att riskerna för större personliga integritetsskador till följd av den här typen av integritetsincidenter är minde än för andra typer där obehöriga personer uppsåtligen har orsakat incidenten. Det allvarliga med den här typen av incidenter är istället den stora mängden incidenter. Operatörerna uppger i incidentrapporteringen att den åtgärd som vidtas för att minska antalet incidenter med fel e-postadresser är att påminna personalen om rutiner för att skriva in e-postadresser. Likväl har rapporteringen av den här typen av incidenter ökat från år till år. Problemet finns i olika grad hos alla operatörer.

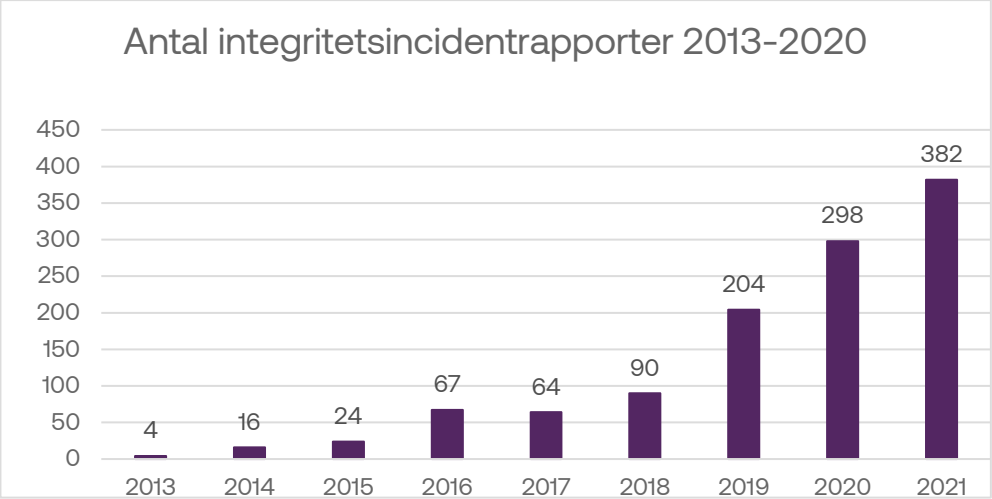
PTS ser i sin genomgång av årets incidentrapporter att en operatör under 2021 har en ny åtgärdsplan för att minska problemen med att fel e-postadress används. Åtgärderna innebär en översyn av systemstöd för verifiering av e-postadresser, en ny process för att identifiera och analysera e-postadresser som kan vara felaktiga, att kunder behöver verifiera e-postadresser och även av utökade rutiner för registrering av e-postadresser i operatörens system. PTS uppmuntrar till att införa säkerhetslösningar för att undvika denna typ av incidenter.

En jämförelse med tidigare år

Det har skett en successiv och på senare år kraftig ökning av antalet integritets-incidenter från år till år. Under 2021 har PTS diarieört 404 rapporter om integritetsincidenter, av vilka 382 har konstaterats är rapporteringspliktiga incidenter. Året visar återigen en kraftig ökning jämfört med åren innan.

I den här sammanställningen har jämförelse av orsaker eller konsekvenser av integritetsincidenter bakåt i tiden inte gjorts. Det beror på att det inte finns tillräckligt

underlag från tidigare år att jämföra med. Dessutom är orsaksindelningarna i årets sammanställning reviderad i syfte att framåt i tiden skapa både jämförbarhet bakåt i tiden av inrapporterade integritetsincidenter och jämförbarhet med IMY:s incidentsammanställningar och även ENISAs.



Samhällets ökade användning av elektroniska kommunikationer, och en ökning av telefon- och internetbedrägerier, identitetskapningar och cybersäkerhetsangrepp kan vara bidragande faktorer till fler integritetsincidenter. PTS uppfattning är dock att den kraftiga ökningen av inrapporterade incidenter inte nödvändigtvis beror på en motsvarande ökning av faktiska incidenter, utan till stor del kan bero på operatörernas 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[8] och arbetet som operatörerna genomförde och fortfarande genomför då LEK är speciallag i förhållande till GDPR i sektorn för elektronisk kommunikation.

LEK är den reglering som har företräde och ska tillämpas i första hand när en operatör av elektroniska kommunikationer behandlar personuppgifter i samband med tillhandahållandet av tjänsterna. Skyddet enligt LEK är mer vidsträckt än bara för

[8] 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.

personuppgifter. Operatören ska skydda samtliga uppgifter som behandlas, inklusive personuppgifter.

Se bilaga 2 för att läsa om förhållandet mellan LEK och GDPR. Se även IMY:s årligen publicerade rapport över inrapporterade personuppgiftsincidenter.[9]

En jämförelse med EU-länder

I den här sammanställningen har jämförelse med EU-länder inte kunnat göras för integritetsincidenter. Det beror på att det inte finns sådant material att jämföra med. ENISA kommenterar att det historiska fokuset har legat på störningar och avbrott i nät och tjänster, det vill säga på driftsincidenter.[10]

Kodexen[11] kommer 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 på grund av konfidentialitetsbrister. ENISA tog då emot tre sådana rapporter från andra europeiska länder. När Kodexen har implementerats i nationell lag i medlemsstaterna kommer sannolikt jämförelseunderlaget successivt att förändras och förbättras.

PTS uppföljning av 2021 års integritetsincidenter

I PTS tillsynsrapport 2021 återfinns mer information om de tillsynsinsatser som PTS planerar att genomföra. PTS planerade tillsynsinsatser påverkas löpande av den kunskap som kommer från incidentrapporteringen. Tillsynsplanering ska ses som preliminär och kan komma att ändras.

[9] Anmälda personuppgiftsincidenter 2020 | IMY
[10] Telecom Security Incidents 2020 - Annual Report — ENISA (europa.eu)
[11] EU-direktiv (2018/1972) för elektroniska kommunikationer som förväntas införlivas i svensk lagstiftning under 2022.

Driftsincidenter 2021

Sedan 2012 är operatörer skyldiga att incidentrapportera betydande störningar och avbrott till PTS.[12]

Under 2021 har PTS diarieförd 25 ärenden med rapporter om driftsstörningar och avbrott i elektroniska kommunikationer. En av rapporterna visade sig inte vara en rapporteringspliktig incident. Antalet konstaterat rapporteringspliktiga driftincidenter år 2021 är således 24.

Minst 434 956 användare eller aktiva anslutningar har drabbats i driftsincidenterna. I nio ärenden saknas dock uppgift om hur många användare eller aktiva anslutningar som har drabbats. Därför utgår PTS från att antal drabbade är högre den angivna siffran. I de ärenden där operatören inte har meddelat PTS hur många som har drabbats har operatören istället angett ett 100 procentigt kapacitetsbortfall.

Orsaker till driftsincidenter 2021

De 24 rapporteringspliktiga driftsincidenterna har delats in i kategorier baserade på grundorsaker och därtill de underliggande mer detaljerade orsakerna. Indelningen är skapad för att förtydliga orsaker och var det kan finnas anledning att införa åtgärder. Den följer i stort ENISA:s indelning i grundorsaker (root causes[13]) och detaljerade orsaker (detailed or technical causes[14]). PTS har översatt ENISA:s engelska begrepp, och då strävat efter att bibehålla betydelsen.

15 av de 24 incidenterna har sin grundorsak i systemfel och sju har sin grundorsak i mänsklig felbedömning eller misstag.

[12] Reglerna om incidentrapportering finns i 5 kap. 6 c § LEK och PTSFS 2012:2.

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

[14] Enisas detailed causes: Arson, cable cut, cable theft, cooling outage, DDos attack, earthquake, eavesdropping, electromagnetic interference, external environmental causes, Faulty hardware change/update, Faulty software change/update, fire, flood, Fuel exhaustion, hardware failure, hardware theft, malware and viruses, network traffic hijack, other, overload, phishing, policy flaw, power cut, Power surges, security shutdown, software bug, vulnerability exploit, wildfire.

Systemfel avser enligt ENISA incidenter som orsakats av felfungerande system, till exempel genom detaljerade orsaker som hårdvarufel, mjukvarufel, otillräckliga rutiner, processer eller riktlinjer.[15]

Mänsklig felbedömning eller misstag avser enligt ENISA incidenter som orsakats av mänskliga missbedömningar i en arbetsprocess eller i användandet av utrustning, verktyg eller liknande. [16]

I tabellen räknas en och samma incidentrapport endast en gång inom grundorsakskategorin. Inte heller de mer detaljerade orsakerna har räknats mer än en gång.

Här presenteras grundorsakerna och de detaljerade orsakerna till rapporterade driftstörningar och avbrott 2021 i en enkel tabell. Grundorsakerna anges och kopplas till den mer detaljerade orsaken till incidenterna i tabellen. Syftet är att skapa bättre jämförbarhet med ENISA:s statistik och med övriga EU-länder. PTS vill med hjälp av tabellen tydliggöra problematiska situationer, där det är möjligt. Syftet med kategoriseringen är därmed också att den ska kunna användas för att identifiera om någon riktad teknisk och/eller organisatorisk åtgärd kan motverka fler incidenter i framtiden.

Grundorsaker till 24 driftsincidenter 2021	**Detaljerade orsaker till 24 driftincidenter 2021**
15 incidenter hade systemfel som grundorsak	Av dessa 15 berodde: 8 på strömavbrott och elfel, 3 på hårdvarufel, 2 på konfigurationsfel, 1 på mjukvarufel, 1 på planerat arbete.
7 incidenter hade mänskliga misstag eller felbedömningar som grundorsak	Av dessa 7 berodde: 4 på avgrävda fiberkablar, 1 på hårdvarufel, 2 på mjukvarubuggar eller konfigurationsfel.

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

1 incident hade fel hos tredje part (partner/underleverantör)	Grundorsaken och detaljerad orsak hos tredje part är oklara
En incident hade naturens kraft som grundorsak	Den incidenten berodde på vatteninträngning orsakade fiberskada
Inte någon incident hade antagonistiskt angrepp som grundorsak	Det saknades under 2021 driftsincidenter som orsakats av antagonistiska angrepp

Under 2021 rapporterades inte några större avbrott i elektroniska kommunikationer i samband med hårt väder.

Ingen inrapporterad driftstörningsincident under året orsakades av ett antagonistiskt angrepp som till exempel en överbelastningsattack.

PTS kommentarer

Grundorsaker

Systemfel var den absolut vanligaste grundorsaken under 2021 (15 av 24 incidenter) och därefter följde grundorsaken mänskligt misstag eller felbedömning (7 av 24 incidenter).

Att systemfel är den vanligast rapporterade orsaken till driftsincidenter 2021 överensstämmer med den trend som ENISA ser.[17] ENISA har tyvärr inte ännu när denna rapport skrivs publicerat sin sammanställning av incidenter för 2021.

Detaljerade orsaker

Strömavbrott: Strömavbrott som i grunden orsakats av systemfel var den vanligaste detaljerade orsaken till rapporterade driftsincidenter under 2021 (8 av 24 stycken).

[17] Telecom & Trust Services Incidents in 2020: System Failures on the Rise — ENISA (europa.eu)

I de åtta incidenterna har antingen reservkraft inte funnits eller inte fungerat, eller så har kommunikationsutrustningen slutat fungera vid övergång mellan kraftkällor. Två av incidenterna utlöstes inte av externt strömavbrott utan berodde på elfel i operatörens egen utrustning.

De nu gällande 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.[18]

Hårdvarufel: Hårdvarufelen 2021 orsakades i grunden av systemfel (3 av 24), ett hårdvarufel berodde på mänsklig felbedömning eller misstag (1 av 24).

Operatörerna drabbas 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 som kallas *supply-chain-security.* Den typen av riskanalyser som aktualiseras här innebär att även delar som produceras av annan och inhandlas av operatörerna, 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 driftssäkerhet och säkerhet för behandlade uppgifter.

Avgrävda kablar: Endast tre driftsincidenter under året berodde på avgrävda kablar. Det är färre än under tidigare år. Under de föregående åren har de avgrävda kablarna varit den klart vanligaste orsaken till driftsincidenter.

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 driftsäkerheten 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.

Antagonistiska angrepp: Det finns inte någon driftsincident inrapporterad under 2021 med denna orsak[19], och det finns få rapporter över åren – men även antagonistiska angrepp som orsak till en incident omfattas av rapporteringsskyldigheten.

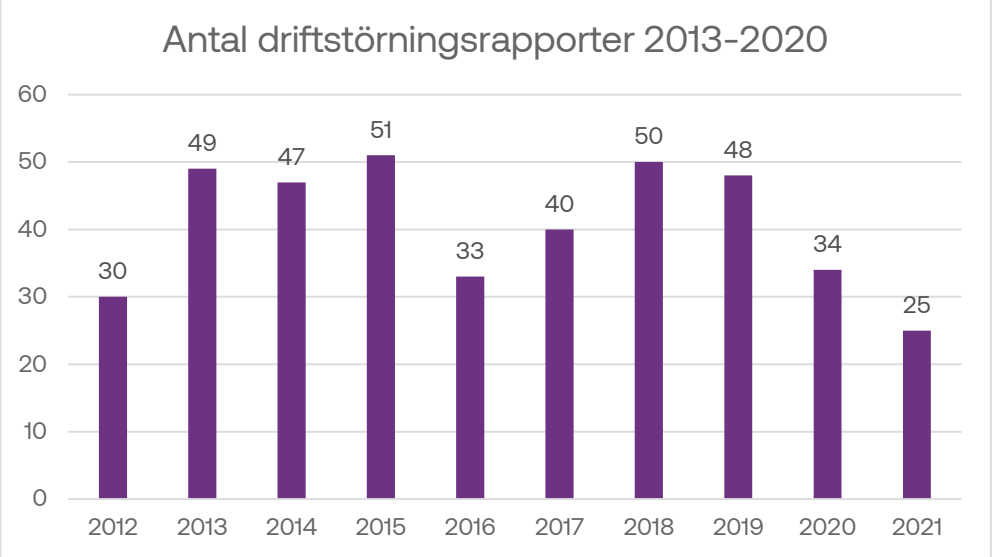
[18] PTSFS 2015:2 ändrad genom PTSFS 2020:1, se särskilt 15 § och 21–22 §§.

[19] Se s. 9 om antagonistiska angrepp som orsakat integritetsincidenter under 2021 varav 11 stycken orsakades av automatiserade angrepp.

PTS om de färre rapporterade driftsincidenterna i år: Det är för tidigt att dra någon slutsats av denna utveckling och någon närmare analys av minskningen har inte gjorts.

En jämförelse med tidigare år

Antalet rapporterade driftsäkerhetsincidenter 2021 är lägre än något tidigare år sedan rapporteringen startade år 2012. Årligen brukar cirka 30 till 50 händelser med betydande störningar och avbrott i elektronisk kommunikation rapporteras till PTS.



De åren med fler rapporter har ofta avbrott eller störningar drabbat en kommunikationsoperatör (KO).[20] Störningar och avbrott hos en KO ska generera flera rapporter till PTS, eftersom många operatörer är beroende av KO:ns tjänster och samtliga drabbade av en händelse ska rapportera incidenten självständigt till PTS. En och samma händelse som drabbar flera operatörer ska rapporteras till PTS av var och en av dem, om trösklarna för rapporteringsplikten är uppnådda.

[20] En nätägare kan lägga ut driften av den aktiva utrustningen i sitt nät till en så kallad kommunikationsoperatör. Detta gör i många fall de kommunala stadsnätsbolagen för driften av lokala fibernät. Kommunikationsoperatören får då lokalt tillträde till fibernätet och kan producera förädlade tjänster till operatörerna. Om kommunikationsoperatören administrerar nätet dirigeras ofta datatrafiken via en plattform där slutanvändaren väljer vilken operatör denne vill köpa bredbandstjänster av.

Under 2021 har ett driftsavbrott rapporterats av en KO. Samma händelse rapporterades av en operatör som var beroende av denna KO.

Sommaren 2021 med stora översvämningar och regnoväder ledde inte till att någon incident rapporterades till PTS.

Typiskt sett rapporteras incidenter med lokal eller regional påverkan. Det är bara en liten del av driftsincidenterna som får nationell påverkan. Detta typiska scenario stämmer med hur det sett ut 2021. Fem incidenter av 24 hade nationell påverkan och fyra stycken hade regional påverkan.

Från 2012 till och med 2021 har sammanlagt 72 nationella störningar och avbrott rapporterats till PTS. När det gäller dessa 72 nationella avbrott och störningar är konfigurationsfel och andra mänskliga handhavandefel den vanligaste orsaken (50 av 72 st., då ofta i kombination med andra fel eller brister). Den näst största felkategorin (13 st.) har varit fel i hård- och mjukvara. Resterande nationella störningar och avbrott (7 st.) har orsakats av överbelastningsattacker eller bristande kapacitet där nätutbyggnaden inte har hängt med.[21]

En annan jämförelse över tid är vilka nät och tjänster som har drabbats av rapporterade incidenter. Här presenteras en enkel tabell som visat antal:

Vilka nät och tjänster har drabbats?	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
Enbart mobila nät och tjänster	15	20	19	21	6	10	10	5	4	8
Enbart fasta tjänster	10	18	17	23	24	26	35	36	23	15
Både mobila och fasta nät och tjänster	4	11	5	7	3	4	5	5	2	1
Övriga nät och tjänster	1	0	6	0	0	0	0	2	5	1
Totalt	30	49	47	51	33	40	50	48	34	25

Inverkan av PTS rapporteringströsklar

Enligt LEK är det driftsincidenter av betydande omfattning som ska rapporteras till PTS. PTS rapporteringströsklar styr vad betydande omfattning innebär.[22] Detta leder

[21] Risk- och sårbarhetsanalys för PTS och dess ansvarsområden 2020 - PTS-ER-2020:32 | PTS, elektroniska kommunikationer i kapitel 5 s. 42–67., kapitel 5 s. 42–67.
[22] Trösklarna för rapportering av driftsäkerhetsincidenter finns i 8 § PTSFS 2012:2.

till att en mängd störningar och avbrott inte ska rapporteras till PTS, och att PTS därför inte har hela bilden av driftstörningarna i elektroniska kommunikationer.

PTS trösklar har således betydelse för både antal rapporterade incidenter och vilken orsak som ser vanligast ut i den här sammanställningen. Det betyder inte nödvändigtvis att orsaken är vanligast utifrån operatörernas perspektiv. Vissa typer av driftsincidenter rapporteras till PTS i mycket hög utsträckning. Det rör till exempel incidenter orsakade av avgrävda kablar, eftersom sådant i regel tar lång tid att laga. Trösklarna kan då vara en bidragande anledning till varför vissa orsaker blir vanligare än andra, när vi sammanställer alla årets incidenter.

PTS föreskrifter om rapporteringskrav för driftsincidenter utgår i nuläget ifrån tre värden (trösklar): antal drabbade abonnenter i bestämda tal, hur stor geografisk yta som har drabbats eller bortfall av tjänstekapacitet i procent av operatörens hela nät och alla tjänster. Det har sedan PTS införde trösklarna för driftsincidentrapportering skett en omfattande utbyggnad av näten. Större nät och fler abonnenter hos en operatör påverkar rapporteringsskyldigheten när det användbara värdet (tröskeln) är bortfall i kapacitet, och inte antal drabbade eller storleken på den geografiska ytan. Det kan leda till att mindre nätägare med färre användare rapporterar störningar och avbrott i högre utsträckning till PTS, än vad större nätägare med fler användare gör.

PTS uppföljning av 2021 års driftsincidenter

En uppföljning av 2021 års driftsincidenter sker genom denna sammanställning. Uppföljning kan i övrigt ske genom planerade tillsynsinsatser.

Incidenter som rapporteras vidare till ENISA

Större incidenter rapporterar PTS årligen vidare till den europeiska unionens cybersäkerhetsbyrå ENISA enligt gällande EU-rättsakter.[23] Vidarerapporteringen görs varje år i februari månad. Följande fem driftsincidenter har vidarerapporterats:

1. Ett avbrott som varade i åtta timmar, som drabbade 289 000 kunder i hela landet i operatörens stamnät för maskin till maskin-kommunikation. Grundorsaken var ett systemfel. På detaljerad nivå rörde det sig om en mjukvarubugg som gjorde att en router slutade fungera.

2. En incident som gav intermittenta avbrott och störningar i hela landet under två timmar och 30 minuter. Incidenten drabbade ca 15 000 kunder i operatörens mobila nät. Grundorsaken var ett mänskligt misstag i ett planerat konfigurationsarbete.

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

3. En incident som orsakade störningar och avbrott under tre timmars tid i hela landet i operatörens mobila nät. Incidenten drabbade dock inte alla operatörens 2,7 miljoner mobilkunder. Grundorsaken var ett systemfel och på detaljerad nivå rörde det sig om ett mjukvarufel.

4. En incident hos en kommunikationsoperatör gav korta avbrott och störningar i hela landet under 40 minuter. Kommunikationsoperatören har uppskattat att ca 9 000 kunder drabbades. Grundorsaken var ett systemfel. På detaljerad nivå rörde det sig om en brist i hårdvara som skapade överbelastning i BGP-routrar.

5. Ett avbrott om nära tre timmar drabbade 38 912 användare av fast IP-telefoni i hela landet. Felet berodde på ett mänskligt misstag under en mjukvaruuppdatering, som ledde till mjukvarufel.

En jämförelse med EU-länder

Genom att alla medlemsstaterna i EU vidarerapporterar de driftsincidenter med störst konsekvenser till ENISA, kan ENISA se mönster i orsakerna på en paneuropeisk nivå. ENISA tar årligen emot ungefär 160 rapporter från de 26 medlemsstaterna och analyserar i en årlig rapport både grundorsaker och detaljerade orsaker till driftsincidenterna, och hur många förlorade användartimmar det leder till.

ENISA skriver i analysen över 2020 års incidenter i EU-länder att användarmönster och trafikmängder förändrades drastiskt under Covid-pandemin och operatörernas nät och tjänster visade sig kunna hantera dessa förändringar bra. Rapporten från ENISA för 2021 har inte publicerats när denna rapport skrivs. Se dock nedan några publicerade diagram från ENISA.

Utifrån de senaste nio årens rapporter från medlemsstater har ENISA konstaterat att:

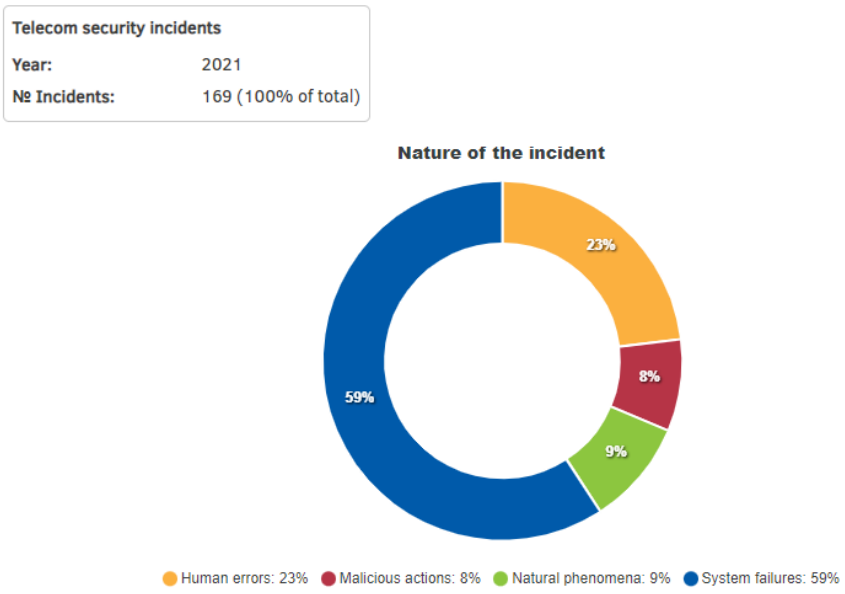
- Antalet rapporterade incidenter ligger relativt konstant från år till år.
- Systemfel är den vanligaste grundorsaken. De förlorade användartimmarna efter systemfel har ökat något. Den vanligaste detaljerade orsaken inom systemfelen är hårdvarufel (36 %) och mjukvarubuggar (28 %).
- Samtliga förlorade användartimmar ligger stabilt under de senare åren. Det rör sig om runt 900 miljoner förlorande timmar/år i hela EU.
- Grundorsaken mänskliga misstag (eng. *human error*) har ökat årligen sedan 2016. De förlorade användartimmarna efter mänskliga misstag ökar årligen.
- De förlorade användartimmarna efter påverkan av naturkrafter har minskat kraftigt sedan 2018.
- Antagonistiska angrepp såsom hackning och överbelastningsattacker orsakar endast omkring 5 % av alla driftsincidenter.

Systemfel är den orsak som leder till mest negativa konsekvenser sett till antal förlorade användartimmar. De senare åren har antalet inrapporterade incidenter orsakade av systemfel minskat i antal inom EU, medan störningar och avbrott orsakade av mänskliga misstag ökar för varje år. Även fel orsakade av tredje part ökar stadigt. Oavsett rapporterad grundorsak ser ENISA att strömavbrott är inblandade i incidenterna i över en femtedel av fallen.

Fram till 2017 ökade antalet förlorade användartimmar efter incidenterna, men från 2018 och framåt minskar de förlorade timmarna på grund av incidenterna. När det gäller fel orsakade av tredje part (29 %) konstaterar ENISA att orsaken har ökat.[24]

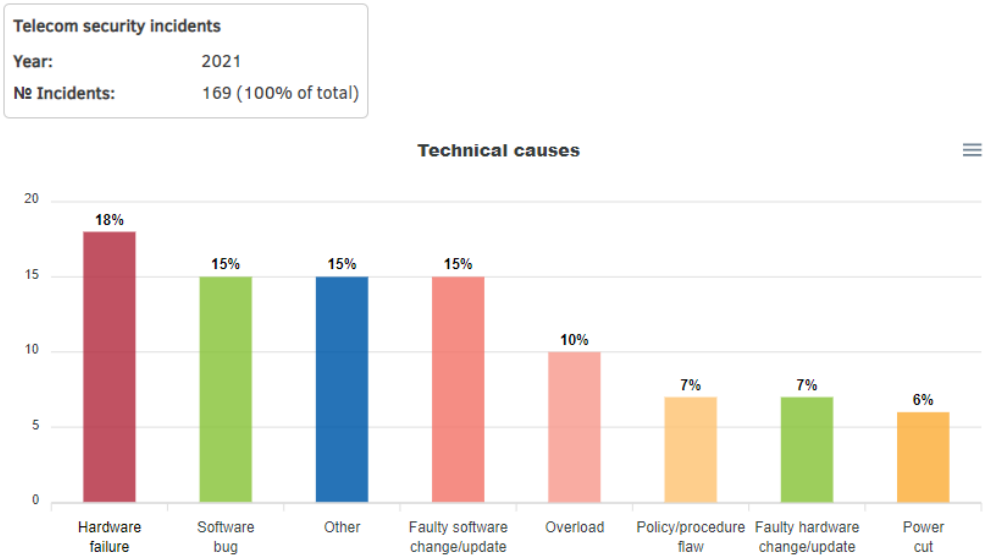
ENISA har inte ännu publicerat sin årliga rapport som kategoriserar de 169 incidentrapporter från 2021 som medlemsstaterna har vidareförmedlat till ENISA. Det finns dock ett par publicerade diagram från ENISA. Dessa presenteras här för att ge en preliminär bild av incidentläget i Europa 2021. Notera att det endast är incidenter med mycket allvarliga konsekvenser, t.ex. nationella avbrott, eller störningar som pågått under mycket lång tid som vidarerapporteras av medlemsstaterna till ENISA. De tre diagrammen nedan är tagna från ENISA och presenteras oredigerat och på engelska.

Grundorsaker till driftsincidenter 2021 i EU-länder

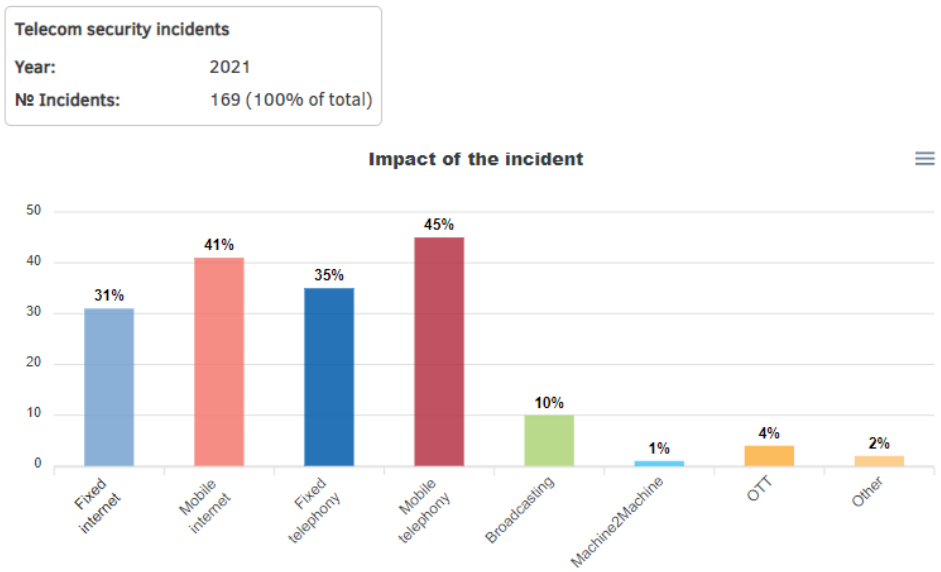


[24] Telecom Security Incidents 2020 - Annual Report — ENISA (europa.eu). Publicerad i juli 2021

Tekniska detaljerade orsaker till driftsincidenter 2021 i EU-länder



Nät och tjänster som drabbats av driftsincidenterna 2021 i EU-länderna



Nya incidentrapporteringsregler 2022

Under 2022 kommer Sverige att implementera EU:s direktiv om inrättande av en europeisk kodex för elektronisk kommunikation (Kodexen).[25] En ny lag om elektronisk kommunikation (nya LEK) införs.

PTS nya föreskrift om säkerhet i nät och tjänster avses att träda i kraft under 2022.[26] Reglerna för rapportering av säkerhetsincidenter kommer att finnas i nya LEK och i PTS kommande nya föreskrift. En driftsincident är en typ av säkerhetsincident.

Det kommer några nyheter som rör rapporteringsplikten för säkerhetsincidenter:

- I enlighet med Kodexen införs rapporteringsplikt för säkerhetsincidenter som har betydande påverkan på nät och tjänster.
- Även nummeroberoende interpersonella kommunikationstjänster (NI-ICS) ska rapportera incidenter till PTS.

PTS nuvarande tröskelvärden för när en driftsincident ska rapporteras kommer inte att förändras i PTS nya regler om säkerhetsincidenter.

Rapporteringsplikten för integritetsincidenter kommer att kvarstå parallellt med rapporteringsplikten för säkerhetsincidenter. Det beror på att reglerna för skydd av uppgifter kvarblir i nya LEK och rapportering av integritetsincidenter ska göras enligt kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets

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

[26] Den nya föreskriften kommer att upphäva och ersätta föreskrifterna i PTSFS 1995:1, PTSFS 2012:2, PTSFS 2012:4, PTSFS 2014:1 och PTSFS 2015:2 och ändringsföreskrifter kopplade till dessa.

direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation (förordning 611/2013).

Säkerhetsincidenter

En säkerhetsincident kommer i nya LEK att definieras 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.[27]

Integritetsincidenter

I nya 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. [28]

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

Rapporteringsplikten för integritetsincidenter saknar tröskelvärde.

[27] Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation (regeringen.se). Prop. 2021/22:136 s. 15–16

[28] Prop. 2021/22:136 s. 14

Tillsynsrapport

Här beskriver PTS tillsynsinsatser under 2021 och framåt på områdena driftssäkerhet i nät och tjänster och skydd av de uppgifter som behandlats för att tillhandahålla elektroniska kommunikationer. Syftet med tillsynsrapporten är att kunna ge rapporterande operatörer, andra intressenter och PTS en överblick över genomförda och planerade tillsynsinsatser.

Bestämmelserna på området finns i 5 och 6 kap. LEK och i PTS föreskrifter om krav på driftsäkerhet (PTSFS 2015:2, ändrade genom PTSFS 2020:1) samt i PTS föreskrifter om allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1). Reglerna syftar bl.a. till att användare ska få tillgång till säkra och effektiva elektroniska kommunikationer och att de uppgifter som operatörerna behandlar för att tillhandahålla tjänsterna skyddas. Se mer om reglerna i bilaga 3.

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

Avslutade tillsynsärenden 2021

Under 2021 har två tillsynsinsatser avslutats.

Årlig tillsyn av fjolårets inrapporterade incidenter

I den årligt återkommande tillsynen av inrapporterade incidenter granskades rapporteringen från åtta operatörer: Telenor Sverige AB, AddSecure AB, GlobalConnect AB, iTUX Communication AB, Njudung Energi Vetlanda AB, Open Infra Operator AB, Tele2 AB och Telia Company AB.

Tillsynen omfattade sexton inrapporterade driftsincidenter. Dessa valdes ut eftersom operatörerna i incidentrapporterna meddelat att specifika säkerhetsåtgärder skulle vidtas. Därutöver inkluderades även incidenter som berott på problem med reservkraft eller redundans samt den incident som orsakats av ett angrepp i form av en överbelastningsattack. Den årliga tillsynen avslutades efter att det konstaterats att operatörerna vidtagit lämpliga tekniska och organisatoriska åtgärder för att undvika att liknande incidenter inträffar igen. Tillsynen pågick mellan augusti och november 2021.

Tillsyn av sjökablar

Granskningen omfattade Telia Company AB, GlobalConnect AB och Telenor Sverige AB och inleddes i syfte att undersöka hur sjökablar är skyddade, vilka störningar som förekommit samt vilka riktlinjer som används vid förläggning. Resultatet visade att operatörerna har dokumenterade riskanalyser för sjökablar som uppdateras regelbundet och vid behov samt att de följer gällande riktlinjer som finns i Robust fiber vid förläggning av sjökablar. [29] De avbrott och störningar som operatörerna har haft på sina sjökablar under de senaste fem åren gav även en indikation på att skyddet av sjökablar i dagsläget kan anses tillräckligt. PTS avslutade därför tillsynen. Tillsynen pågick mellan juni 2020 och april/maj 2021.

Pågående tillsynsärenden 2021

Nedan följer en kort genomgång av i dagsläget pågående tillsynsinsatser.

Röstbrevlådetillsyn

PTS granskar säkerhetsåtgärder i röstbrevlådor hos Telenor Sverige AB med anledning av att obehöriga gjort intrång i abonnenters och användares röstbrevlådor. I tillsynen granskas rutiner, förmåga att upptäcka intrång samt åtgärder för skydd av uppgifter som behandlas i röstbrevlådor enligt LEK och PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1). Tillsynen inleddes i april 2012 och kommer att avslutas under 2022.

Reservkrafttillsyn

PTS granskar hur fem operatörer [30] efterlever myndighetens regler om reservkraft som återfinns i PTS föreskrifter om krav på driftsäkerhet (PTSFS 2015:2, ändrade genom PTSFS 2020:1). Tillsynen inleddes i november 2020 och kommer att avslutas under 2022.

Tillsyn över säkerhetsåtgärder och kända sårbarheter i trafikutbyte på internet

PTS granskar säkerhetsarbetet för att motverka kända risker och sårbarheter med Border Gateway Protocol (BGP) hos fem olika operatörer [31], i enlighet med LEK och PTSFS 2015:2, ändrade genom PTSFS 2020:1, samt PTS föreskrifter om allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1). Tillsynen inleddes i oktober 2020 och kommer att avslutas under 2022.

[29] Anvisningar för anläggning av robusta fiberoptiska bredbandsnät, Huvuddokument Version 1.3.1.
[30] Telia Company AB, Hi3G Access AB, Tele2 AB, A3, Bahnhof AB och Telenor Sverige AB.
[31] Netnod Internet Exchange AB, Telia Company AB, Tele2 AB, Telenor Sverige AB och Hi3G Access AB.

Tillsynsplan 2022–2023

Planerade tillsynsinsatser

PTS har identifierat ett antal områden som skulle kunna utgöra grund för möjliga tillsynsinsatser framöver.

Årlig tillsyn av fjolårets inrapporterade incidenter

PTS har under år 2021 skapat en ny process för den årliga tillsynen av fjolårets inrapporterade incidenter. Den nya processen innebär att ett urval av de inrapporterade incidenterna granskas. Urvalet baseras på en analys av inrapporterade incidenter och myndighetens planerade tillsynsinsatser. Syftet med den nya processen är att den årliga tillsynsinsatsen ska utföras baserat på det som behöver granskas utifrån operatörernas egna rapporter.

År 2022 kommer PTS inte att genomföra årlig tillsynsinsats, bland annat med hänsyn till det kommande regelskiftet. En noggrann genomgång har dock gjorts av 2021 års incidenter och den presenteras tidigare i denna rapport.

PTS kommer att följa upp vissa misstänkta brister i enskilda planerade tillsynsinsatser.

Tillsyn av obehörig spridning av abonnentuppgifter till abonnentupplysning

Tillsynen skulle omfatta ett par operatörer som enligt rapporterade incidenter obehörigen spritt behandlade uppgifter till abonnentupplysning. Incidenterna kan få allvarliga konsekvenser för drabbade, särskilt de med skyddad identitet. Tillsynen skulle syfta till att säkerställa att operatörer har lämpliga tekniska och organisatoriska åtgärder för att skydda abonnenters uppgifter. Förberedelser inför tillsynen är gjorda och den eventuella tillsynen kan möjligen inledas under 2022.

Tillsyn av mobilnät och säkerhet i leverantörskedjan

PTS har i en rapport till regeringen konstaterat att det föreligger säkerhetsbrister i vissa operatörers leverantörskedja för komponenter i mobilnät. Vissa komponenter har till exempel skickats i vanliga paket, vilket innebär en säkerhetsrisk. Syftet med

tillsynen skulle vara att säkerställa att tillhandahållarna vidtar lämpliga säkerhetsåtgärder i detta avseende.

Mobilnättillsyn, konfiguration och incidenthantering

Tillsynen skulle granska det systematiska säkerhetsarbetet i samband med införandet av virtuella nätverkstillgångar. Särskild fokus skulle ligga på så kallad *Change Management* då PTS kunnat konstatera att många driftsincidenter beror på konfigurering av mobilnäten. Det huvudsakliga syftet med den möjliga tillsynen skulle vara att säkerställa att operatörerna har rutiner för ett systematiskt, långsiktigt och kontinuerligt säkerhetsarbete avseende de virtuella nätverkstillgångarna.

Tillsyn av operatörers förmåga att upptäcka och förebygga integritetsincidenter

Tillsynsinsatsen skulle avse granskning av operatörers förmåga att upptäcka, förebygga, hantera och rapportera integritetsincidenter. Tillsynen skulle granska ett antal större operatörer och ett urval metoder såsom till exempel behörighetsspärrar och automatiserad logganalys. Syftet skulle vara att stärka operatörernas förmåga att upptäcka, rapportera och minska antalet integritetsincidenter enligt LEK.

Tillsyn av operatörers förmåga att legitimera (autentisera) personer

Tillsynen skulle delvis vara en uppföljning av PTS tidigare tillsyn avseende autentisering av redan befintliga kunder i kundtjänst per telefon. Tillsynen kan innefatta sådant som att kontrollera att säker och effektiv autentisering finns i alla kontaktkanaler, kontroll av hur autentisering utförs vid nyteckning av tjänster eller andra specifika frågor som till exempel säkerhet vid SIM-byten eller så kallad *SIM-swapping* [32]. Syftet med tillsynen skulle vara att minska antalet integritetsincidenter där orsaken är bristande legitimering (autentisering) av den som kontaktar operatören.

Händelsestyrd tillsyn

PTS kan 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 operatörerna drar lärdomar av inträffade händelser och vidtar åtgärder i enlighet med regelverket.

[32] Obehörig förflyttning av telefonnummer, utan ett fysiskt SIM-kort, till annans utrustning i syfte att skapa tillgång till nummerinnehavarens konton.

BILAGA 1

Metod och arbetsprocess för incidentsammanställningen

Arbetet med sammanställningen av incidenter har genomförts på följande sätt.

Inledningsvis gjordes flera genomgångar av alla incidentrapporter från 2021. I det arbetet identifierades och markerades orsaker, och mönster framträdde vid gruppering utifrån orsakerna. Det är innehållet i operatörernas rapporter som legat till grund för orsakskategoriseringen.

En utgångspunkt i skapandet av orsakskategorierna har dels varit ENISA:s orsakskategori grundorsaker och detaljerade orsaker i den årliga uppföljning som görs på europeisk nivå,[33] dels IMY:s orsaksindelning i sin rapport om anmälda personuppgiftsincidenter. [34] Dessa har använts för att skapa grund för jämförbarhet.

I kommande 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 och 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,[35] till viss del men mer summariskt och endast för regionala och nationella avbrott, beskrivit vilka orsaker till driftsäkerhetsincidenter som funnits. I den här sammanställningen ingår alla incidentrapporter under år 2021.

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

[33] Telecom Security Incidents 2020 - Annual Report — ENISA (europa.eu)
[34] Anmälda personuppgiftsincidenter 2020 | IMY
[35] Risk- och sårbarhetsanalys för PTS och dess ansvarsområden 2020 - PTS-ER-2020:32 | PTS, läs om elektroniska kommunikationer i kapitel 5 s. 42–67.

BILAGA 2

Förhållandet mellan integritetsbestämmelserna i lagen om elektronisk kommunikation (LEK) och dataskyddsförordningen (GDPR)

EU:s dataskyddsförordning (GDPR) är direkt tillämplig i svensk rätt, och skyddar, utöver reglerna om integritet i lagen (2003:389) om elektronisk kommunikation (LEK), också enskildas personuppgifter. Både LEK och GDPR innehåller krav på att integritetsincidenter ska rapporteras. Om det är LEK som tillämpas ska incidenten rapporteras till PTS. Om det är GDPR som tillämpas ska incidenten rapporteras till Integritetsskyddsmyndigheten (IMY).

Hur operatörerna kan avgöra vilken lag och vilken rapporteringsskyldighet som gäller

LEK är speciallag i förhållande till GDPR i sektorn för elektronisk kommunikation. Det betyder att LEK är den reglering som har företräde och ska tillämpas i första hand när ett företag behandlar uppgifter – såväl personuppgifter som andra uppgifter – i samband med tillhandahållandet av en elektronisk kommunikationstjänst. Skyddet avser både fysiska och juridiska personer.

Skyddet enligt LEK är också mer vidsträckt än bara för personuppgifter, och omfattar samtliga uppgifter som överförs, lagras eller på annat sätt behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster (se prop. 2010/11:115 s. 131).

GDPR är en allmän reglering som gäller behandling av personuppgifter. Den är tillämplig i förhållande till alla företag och organisationer.

För operatörernas del kan man beskriva det som att GDPR fångar upp personuppgiftsincidenter som faller utanför LEK:s tillämpningsområde. Först när en fråga inte specifikt regleras i LEK ska alltså GDPR tillämpas. Utöver detta innehåller LEK i vissa fall en hänvisning till GDPR. Regelverken kompletterar och påverkar på så sätt varandra.

Vad gäller operatörernas rapportering av integritetsincidenter är det alltså bara om en incident inte ska rapporteras till PTS enligt LEK som den ska rapporteras till IMY enligt GDPR; dubbel rapportering av samma incident är inte nödvändig.

BILAGA 3

Sammanställning av nuvarande regler om driftsäkerhet, regler vid incidentrapportering och tillsynsverksamhet. Observera att det kommer nya regler under 2022 – en ny lag om elektronisk kommunikation samt PTS nya säkerhetsföreskrifter.

Utgångspunkten för PTS arbete med incidentrapporter och med tillsyn av driftsäkerhet och konfidentiell kommunikation är de skyldigheter som gäller för tillhandahållare som framgår av lagen (2003:389) om elektronisk kommunikation (LEK) och EU-förordningen nr 611/2013[36].

Regler om tillsyn

Att PTS är tillsynsmyndighet enligt LEK framgår av 2 § förordningen (2003:396) om elektronisk kommunikation. Att PTS får begära in upplysningar och handlingar i tillsynen samt kan få tillträde till bl.a. lokaler för tillsynen framgår av 7 kap. 2–3 §§ LEK. Vilka medel som PTS har för att skapa regelefterlevnad framgår av bl.a. 7 kap. 3–5 §§ LEK[37].

Regler om driftsäkerhet och om skydd av behandlade uppgifter

Reglerna om driftsäkerhet och konfidentiell kommunikation finns i femte och sjätte kapitlen i LEK.

Enligt 5 kap. 6 b § LEK ska tillhandahållare allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet.

Skyldigheterna preciseras sedan i PTS föreskrifter om krav på driftsäkerhet (PTSFS 2015:2, ändrade genom 2020:1).

I 6 kap 3 § LEK finns regler om skydd av behandlade uppgifter, som gäller för tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster. Bl.a. finns regler med krav på att vidta lämpliga tekniska och organisatoriska åtgärder för att

[36] 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.

[37] 3 a § behandlar dock roaming och öppen internetanslutning och avgifter, vilket inte har med detta sammanhang att göra.

säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas.

Dessa regler kompletteras sedan av PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1).

Incidentrapportering driftsäkerhet

Enligt 5 kap. 6 c § LEK ska tillhandahållare rapportera störningar och avbrott av betydande omfattning till PTS.

När rapportering ska ske och vilka uppgifter som rapporterna ska innehålla preciseras i PTS föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning (PTSFS 2012:2 ändrade genom 2018:4).

Definitionen av betydande omfattning finns i 8 § PTSFS 2012:2. Bedömningen ska göras efter den tid en störning eller avbrott har pågått parallellt med störningens eller avbrottets uppskattade omfattning. Regeln kommer att föras över till PTS nya säkerhetsföreskrifter.

Tröskelvärden för rapportering

8 § Tillhandahållare ska rapportera nedanstående störningar eller avbrott i kommunikationstjänster till Post- och telestyrelsen.

Tid som störningen eller avbrottet pågått	*Störningens eller avbrottets uppskattade omfattning*
≥ 1 timme	**≥ 150 000 abonnenter eller** **≥ 15 000 km² sammanhängande berört område eller** **≥ 50 % kapacitetsbortfall**
≥ 2 timmar	**≥ 30 000 abonnenter eller** **≥ 5 000 km² sammanhängande berört område eller** **≥ 30 % kapacitetsbortfall**
≥ 6 timmar	**≥ 5 000 abonnenter eller** **≥ 2 500 km² sammanhängande berört område eller** **≥ 20 % kapacitetsbortfall**
≥ 24 timmar	**≥ 2000 abonnenter eller** **≥ 1 000 km² sammanhängande berört område eller** **≥ 10 % kapacitetsbortfall**

Incidentrapportering integritet

Enligt 6 kap 4a § LEK är tjänstetillhandahållare skyldiga att rapportera inträffade integritetsincidenter till PTS. Tillhandahållarna ska också, enligt samma bestämmelse i LEK, om incidenten kan antas inverka negativt på de abonnenter eller användare som de behandlade uppgifterna berör, eller om tillsynsmyndigheten begär det, även underrätta dessa om incidenten. Enligt 6 kap. 4 b § LEK ska tillhandahållare även föra en förteckning över inträffade incidenter. Bestämmelserna är tillämpliga tillsammans med kommissionens förordning (EU) nr 611/2013.

Definitionen av vad som är en integritetsincident finns i 6 kap 1 § LEK. Det är 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.