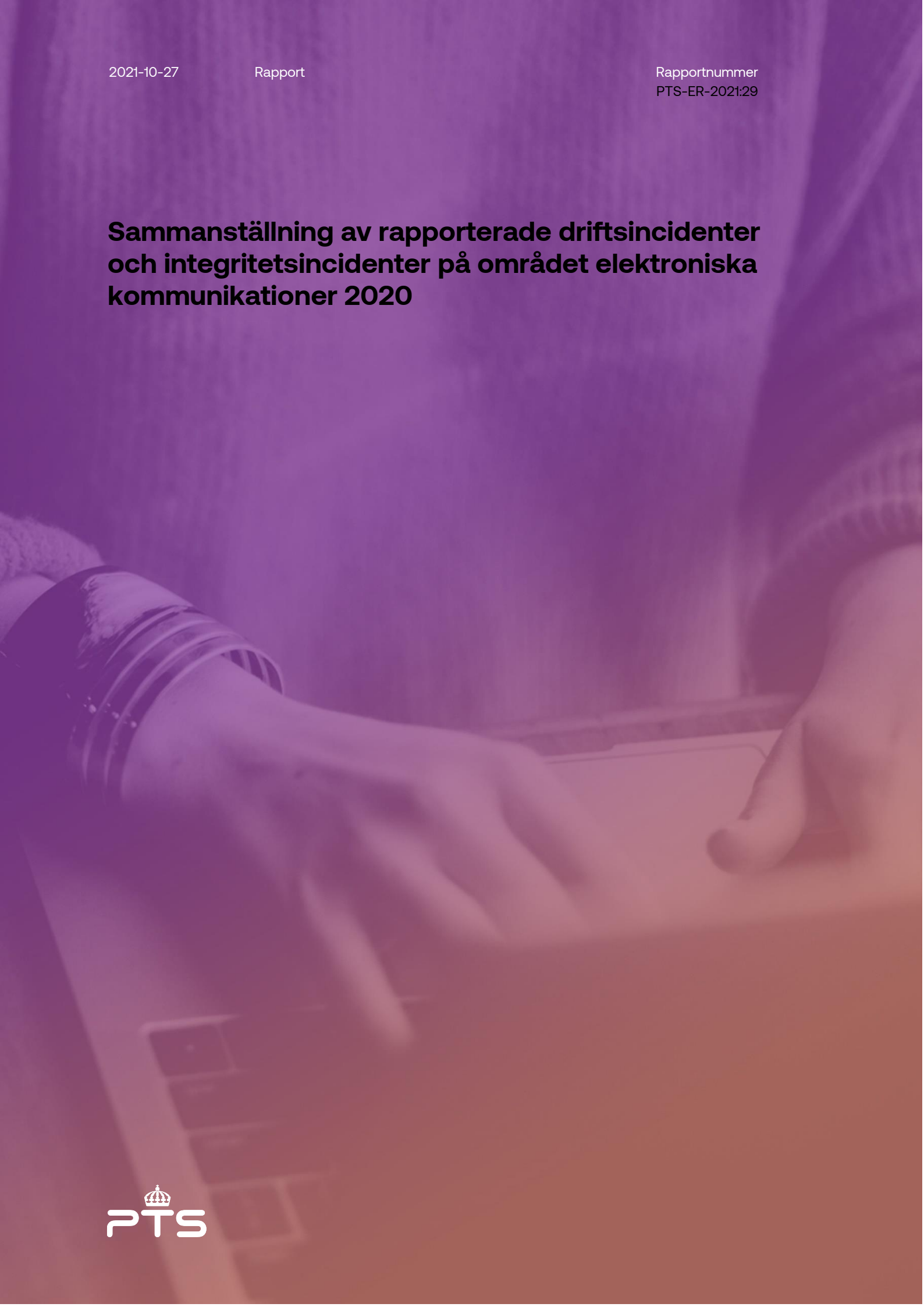
2021-10-27 Rapport

Rapportnummer
PTS-ER-2021:29

Sammanställning av rapporterade driftsincidenter och integritetsincidenter på området elektroniska kommunikationer 2020



Rapportnummer
PTS-ER-2021:29

Diarienummer
21–13846

ISSN
1650–9862

Författare
Therese Braathen, avdelningen för säker kommunikation

Post- och telestyrelsen
Box 5398
102 49 Stockholm

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

Innehåll

Sammanfattning

De som tillhandahåller elektroniska kommunikationsnät- och tjänster (operatörer) är skyldiga att rapportera vissa incidenter till Post- och telestyrelsen (PTS) enligt lagen (2003:389) om elektronisk kommunikation (LEK). Totalt under 2020 har PTS handlagt 341 ärenden med rapporterade incidenter, varav 332 slutligt har bedömts som rapproteringspliktiga incidenter. Det har rört sig om 34 driftsäkerhetsincidenter och 298 integritetsincidenter under 2020.

PTS har här sammanställt och grupperat dessa rapporterade driftstörningar och integritetsincidenter. PTS kommenterar också hur fördelningen ser ut mellan operatörerna, vilken typ av orsak eller typ som är vanligast och vilken typ integritetsincident som är mest allvarlig. Här finns också övergripande jämförelser med tidigare år samt med orsaker som är vanligast i europeiska länder överlag.

Fördelningen av de inrapporterade incidenterna är ojämn mellan operatörerna. Det är inte säkert att de operatörer som rapporterar flest incidenter till myndigheten är de där flest incidenter inträffar. Det kan också vara så vissa operatörer upptäcker fler incidenter och därför rapporterar mer till PTS. PTS ser obalansen i rapporteringen mellan operatörerna som problematiskt.

Den vanligaste orsaken till rapporterade driftsäkerhetsincidenter är avgrävda fiberkablar, därefter följer hårdvaru- mjukvaru-eller systemfel.

Den vanligaste typen av rapporterade integritetsincidenter är de som beror på felregistrerade kontaktuppgifter och förväxling av kontaktuppgifter, därefter följer incidenter där obehöriga personer har kunnat få ut information av operatören eller kunnat ändra i abonnemang.

Enligt PTS är den allvarligaste typen av integritetsincident den då obehöriga får ut information eller ändrar i abonnemang. Det beror både på antalet och på grund av den möjliga allvarliga kränkningen av kunders privatliv. Av årets totalt 298 integritetsincidenter var dessa 100 st.

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

Incidentrapporter 2020

Vid driftsstörnings- och integritetsincidenter vid tillhandahållande av elektroniska kommunikationer som är rapporteringspliktiga enligt LEK ska operatörerna lämna incidentrapporter till PTS.[1] Incidentrapporterna ger PTS underlag att bedöma hur bestämmelserna om driftssäkerhet eller skydd av uppgifter följs, och huruvida tillsyn behöver inledas. Det finns även andra syften med kravet på incidentrapportering, 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 2020 har PTS handlagt 341 ärenden med rapporterade incidenter, varav 332 slutligt har bedömts som rapproteringspliktiga incidenter. Det har rört sig om 34 driftstörningsincidenter och 298 integritetsincidenter.

Syfte med sammanställningen

Syftet är att kunna ge operatörer, andra intressenter och PTS en överblick av fjolårets incidentrapportering. PTS vill också sprida kunskap om incidenterna till flera än de operatörer som är föremål för tillsynen. Genom sammanställningen vill myndigheten förmedla PTS 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 kunna förmedla var operatörerna lämpligen kan planera att utveckla säkerhetsarbetet för driftsäkerhet och skydd för uppgifter. I sammanställningen kallas de bolag som rapporterar incidenterna i elektroniska kommunikationer för operatörer.

[1] Regler kring rapporteringsskyldigheten finns i 5 kap 6 c § och i 6 kap 4 a § lagen (2003:389) om elektronisk kommunikation (LEK), (PTSFS 2012:2) föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning (hädanefter PTSFS 2021:2) och i 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).

Driftsäkerhetsincidenter 2020

Sedan 2012 är operatörer skyldiga att incidentrapportera betydande störningar och avbrott till PTS.[2]

Under 2020 har PTS diarieförd 36 rapporter om driftsstörningar och avbrott i elektroniska kommunikationer. Två av händelserna visade sig inte utgöra rapporteringspliktiga driftsäkerhetsincidenter. PTS har alltså behandlat 34 driftsäkerhetsincidenter under 2020.

Orsaker till driftsäkerhetsincidenter 2020

De inrapporterade 34 incidenterna kan delas in i kategorier baserade på orsaker till störningen eller avbrottet. PTS har grupperat incidenterna i sju typer.

Här presenteras orsakerna till rapporterade driftstörningar och avbrott 2020 i en enkel tabell:

Orsaker till rapporterade driftsäkerhetsincidenter	**Antal rapporterade driftsäkerhetsincidenter**
Avgrävda fiberkablar	8 st.
Hårdvaru-, mjukvaru- och systemfel	7 st.
Övrig mänsklig felbedömning eller misstag	6 st.
Strömavbrott	6 st.
Planerade arbeten	3 st.
Fel i brandväggar	3 st.
Överbelastningsattack	1 st.

[2] Reglerna om incidentrapportering finns i 5 kap. 6 c § LEK och PTSFS 2012:2, ändrade genom PTSFS 2018:4

Indelningen är skapad för att förtydliga orsaker och var det kan finnas anledning att införa åtgärder. Den följer i stort EU-organet ENISAS indelning. Kategorierna av orsaker när det gäller driftsäkerhetsincidenter går dock delvis in i varandra. PTS vill med tabellen tydliggöra en särskild problematisk situation, när det är möjligt. Syftet är att orsakskategoriseringen därmed ska kunna användas för att identifiera om någon riktad teknisk eller organisatorisk åtgärd kan motverka fler incidenter i framtiden.

Det finns en utmaning i att orsaker går in i varandra. Flera av orsakskategorierna ovan har sin grund i mänsklig felbedömning eller misstag, men på mer detaljerad nivå framträder en tydligare bild av vad som går fel. Till exempel är planerade arbeten som orsakar en störning eller avbrott, eller avgrävda fiberkablar, i denna sammanställning båda detaljerade varianter av mänsklig felhantering. Mänsklig felhantering är också en egen kategori i den här sammanställningen, och i den har de incidenter som inte har en mer detaljerad orsak placerats. Incidenter har endast räknats en gång, och förekommer alltså inte i två orsakskategorier.

Under 2020 förekom inte några större avbrott i samband med hårt väder.

Endast en driftstörningsincident under året orsakades av en överbelastningsattack eller antagonistiskt angrepp.

PTS kommentarer om årets rapporterade orsaker

PTS rapporteringströsklar: PTS rapporteringströsklar påverkar vilka incidenter som blir vanligast i sammanställningen. För att en störning eller ett avbrott ska rapporteras till PTS krävs att incidenten når upp till en betydande omfattning, och mer i detalj, till vissa trösklar[3]. Därför blir bedömningen av vad som är vanligast i den här sammanställningen inte nödvändigtvis det som är vanligast utifrån operatörernas perspektiv. Det beror på att PTS saknar information om de incidenter som inte når upp till trösklarna för incidentrapportering. Andra incidenter kan därför vara vanligare utifrån operatörernas perspektiv[4].

Exempelvis når inte relativt stora och timslånga regionala avbrott i de stora operatörernas nät upp till rapporteringsplikt utifrån PTS trösklar. Det beror på att operatörerna både har stora nät och att det i landsbygdsregioner inte bor tillräckligt många abonnenter. Därför aktualiseras i vissa fall inte rapporteringsplikt med

[3] Trösklarna för rapportering av driftsäkerhetsincidenter finns i 8 § PTSFS 2012:2.

[4] Det ska tilläggas att operatörerna också har interna trösklar för vad som klassas som incidenter i operatörernas bolagsinterna incidenthantering.

nuvarande regler även om avbrott eller störningar kan ha samhällspåverkan i de drabbade regionerna.

Det är också så att vissa typer av avbrott och störningar rapporteras till PTS i mycket hög utsträckning. Det rör till exempel incidenter orsakade av avgrävda kablar, som i regel tar lång tid att laga. Trösklarna kan då vara en bidragande anledning till varför den orsaken, när vi sammanställer alla årets incidenter, blir vanligast.

Avgrävda kablar: Den vanligast förekommande orsaken till driftsäkerhetsincidenter 2020 är avgrävda kablar. 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.

Hårdvaru-, mjukvaru- och systemfel: Operatörerna 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 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.

Strömavbrott: När det gäller störningar som orsakas av strömavbrott finns en förhoppning från PTS från att incidenter med denna orsak kommer att börja minska under 2021. Anledningen är att PTS föreskrifter om reservkraft trädde i kraft den 10 juni 2020. 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.[5]

Övrig mänsklig felbedömning eller misstag:[6] I den här orsakskategorin har de incidenter som inte kan hänföras till en mer detaljerad orsak placerats, det vill säga sådan mänsklig felhantering som inte varit på grund av felutförda planerade arbeten eller avgrävda kablar. Incidenterna räknas endast i en kategori. En incident som berodde på ett planerat arbete har alltså inte räknats in i kategorin övrig mänsklig

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

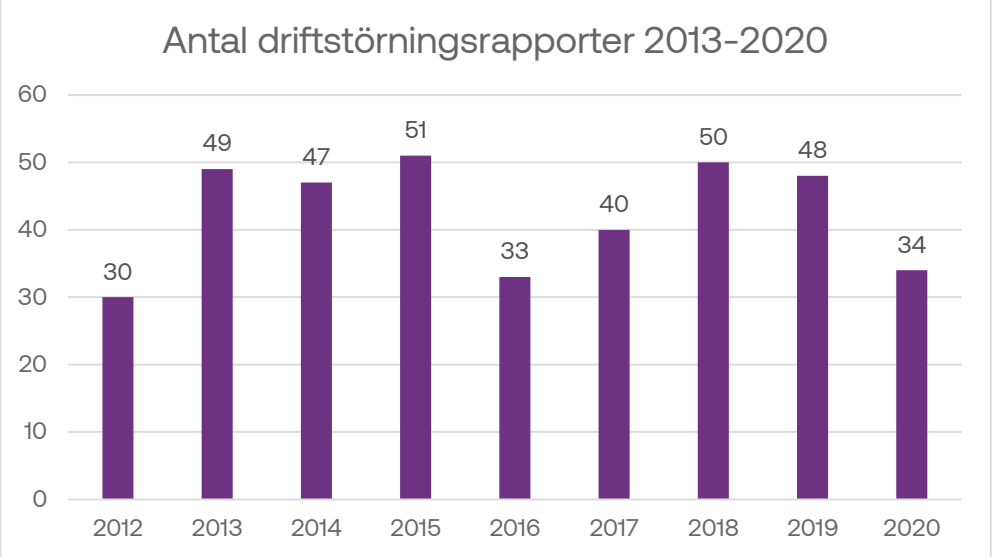
[6] Uttrycket är en översättning av ENISAS uppföljningsbegrepp ”human error”

felbedömning eller misstag. Ett exempel på sådana misstag är när en tekniker ger felaktigt kommando i löpande verksamhet som leder till driftsproblem.

Överbelastningsattacker och antagonistiska angrepp: Det finns få rapporter som handlar om antagonistiska angrepp men även antagonistiska angrepp är en incident i lagens mening och omfattas av rapporteringsskyldigheten

En jämförelse med tidigare år

Antalet rapporterade driftsäkerhetsincidenter var något lägre 2020 än närmast föregående år, men året betraktas ändå som ett normalår.



Årligen brukar cirka 30 till 50 händelser med betydande störningar och avbrott i elektronisk kommunikation rapporteras till PTS.

De år med högre antal rapporter har ofta störningar eller avbrott drabbat en kommunikationsoperatör[7]. Sådana störningar och avbrott genererar flera rapporter,

[7] 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

eftersom många operatörer är beroende av kommunikationsoperatörens tjänster. Samtliga drabbade av en händelse ska rapportera incidenten självständigt till PTS. En och samma händelse som drabbar flera operatörer ska leda till att samtliga drabbade rapporterar till PTS, om trösklarna för rapporteringsplikten är uppnådda även i deras fall.

Under 2020 har visserligen ett driftsavbrott rapporterats av en kommunikations-operatör. Det rörde ett strömavbrott i en datahall, där reservkraften inte fungerade. PTS mottog endast en driftstörningsrapport från kommunikationsoperatören kring detta. Fler operatörer, som varit beroende av kommunikationsoperatörens tjänster som drabbades av avbrottet, torde då också ha drabbats av driftavbrott. Några rapporter om från dessa operatörer kom dock inte in till PTS. Det kan bero på att de operatörer som drabbades som en följd av kommunikationsoperatörens avbrott inte nådde upp till trösklarna för rapportering.

Typiskt sett rapporteras incidenter av lokala eller regionala aktörer och incidenterna har oftast lokal, eller regional påverkan. Det är bara en liten del av driftsäkerhets-incidenterna som får nationell påverkan. Detta typiska scenario stämmer med hur det sett ut 2020. Fyra incidenter av 34 hade nationell eller regional påverkan.

Från 2012 till och med 2020 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.[8]

I jämförelse med vad orsakerna varit 2020 kan det konstateras att det rör sig om samma orsaker, och att den främsta orsaken 2020 också varit mänsklig felhantering. De främsta skälen till störningar och avbrott är att någon grävt av kablar, felkonfigurerat eller på annat sätt av ovarsamhet orsakat störningar. Det har dock under 2020 inte funnits några sådana störningar som orsakats av bristande kapacitet p.g.a. att nätutbyggnaden inte har hängt med.

tjänster till operatörerna. Om kommunikationsoperatören administrerar nätet dirigeras ofta datatrafiken via en plattform där slutanvändaren väljer vilken operatör denne vill köpa bredbandstjänster av.

[8] 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.

Driftsäkerhetsincidenter som har rapporterats vidare till ENISA

Vissa större driftstörningsincidenter ska PTS rapportera till EU-kommissionen och ENISA[9] enligt gällande EU-rättsakter. Under 2020 har fyra driftsäkerhetsincidenter rapporterats vidare av PTS. Kortfattat beskrivs här vad de fyra större incidenterna under året rörde sig om:

1. Incidenten berörde drygt 156 000 användare av mobiltelefoni och mobilt och fast internet under fyra timmar. Orsaken var att det uppstod ett systemfel när näten skulle startas efter ett strömavbrott.

2. Incidenten berörde drygt 22 000 användare av fast internet under drygt åtta timmar. Orsaken var att kommunikationsoperatören i fråga flyttade sitt datacenter och när detta genomfördes uppstod ett nätverksfel som stoppade trafiken.

3. Incidenten var nationell och berörde drygt 2,2 miljoner användare av mobilt internet och drygt 633 000 användare av fast internet i tre timmar. Orsaken var att någon hade grävt av en fiberkabel. Omdirigeringen av trafiken som gjordes efter avgrävningen skapade därefter en trafikstockning som ledde till överbelastning på alla lastbalanserare i den operatörens nät i Sverige, varvid ett avbrott uppstod, först genom avgrävningen och sedan genom överbelastningen som uppstod.

4. Incidenten berörde 43 000 användare av fast telefoni i 9,5 timmar. Orsaken var att en underleverantör genomförde ett konfigurationsarbete, utan att meddela att detta skulle göras i förhand, på operatörens gränsfunktionalitet mot andra operatörers nät, s.k. session border controllers (SBCs). SBC:erna slutade svara på anrop och kommunikationsoperatören, som var beroende av SBC:erna, kunde då inte förmedla tjänster till sina kunder.

En jämförelse med Europa

Genom att alla medlemsstaterna i EU rapporterar de driftsäkerhetsincidenter med störst konsekvenser till ENISA kan ENISA se mönster i orsakerna på en paneuropeisk nivå. ENISA tar årligen emot ungefär 160 rapporter från medlemsstaterna. Med underlag i de senaste åtta årens rapporter från medlemsstaterna har ENISA konstaterat att:

[9] ENISA är en förkortning av European Union Agency for Network and Information Security. Det är ett center med expertkunskaper inom cybersäkerhet i Europa.

- cirka 65 procent av incidenterna är orsakade av systemfel – både hårdvaru- och mjukvarufel inräknade
- 20 procent beror på mänsklig felbedömning eller misstag (eng. human error)
- 10 procent beror på naturens krafter och
- 5 procent på antagonistiska angrepp såsom hackning och överbelastningsattacker
- de incidenter som fått störst tidsmässig påverkan är de som orsakas av systemfel och av naturen.

Systemfel, både hårdvaru- och mjukvarufel, är alltså den vanligaste orsaken till avbrott och störningar i Europa under åren 2012–2019. De senare fyra åren har systemfelen minskat i antal, medan störningar och avbrott orsakade av mänskligt felande ökar för varje år. Även fel orsakade av tredjeparter ökar stadigt.

Oavsett rapporterad grundorsak ser ENISA att strömavbrott är inblandade i incidenterna i över en femtedel av fallen. När det gäller uppföljningen av hur allvarliga konsekvenserna blir är systemfelen åter de allvarligaste. Under åren 2012–2019 stod systemfelen för totalt 479 miljoner förlorade användartimmar. Efter systemfel kommer naturkrafter som också de orsakar större och allvarligare konsekvenser. Fram till 2017 ökade antalet förlorade användartimmar efter incidenterna, men från 2018 och framåt minskar de förlorade timmarna på grund av incidenterna. [10]

Uppföljning på PTS av 2020 års driftssäkerhetsincidenter

Årlig tillsyn

Fjorton av årets rapporter om driftsäkerhetsincidenter följs upp i år. De har rapporterats av åtta olika operatörer. I tillsynen har PTS ställt frågor kring angivna planerade säkerhetsåtgärder, kring incidenter orsakade av brist på reservkraft eller brist på redundans och kring en överbelastningsattack.

[10] ENISA Telecom services security incidents 2019, annual analysis report, July 2020

Integritetsincidenter 2020

Sedan 2011 är operatörer skyldiga att rapportera inträffade integritetsincidenter till PTS.[11] Skyldigheten grundas på att operatörerna ska skydda alla uppgifter som behandlas i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster.[12] Det betyder att skyldigheten att skydda uppgifter inte bara avser personuppgifter, utan skyddet ska avse *alla uppgifter* som operatörerna behandlar för att tillhandahålla elektroniska kommunikationstjänster.

Integritetsincidenterna inträffar när operatörerna inte har skyddat uppgifter tillräckligt väl eller olovligen sprider uppgifter som operatörerna behandlar. Det kan röra sådana händelser som att uppgifter raderas eller registreras in fel hos operatören, eller obehöriga ändringar av ett abonnemang eller läckta uppgifter till personer eller andra bolag som inte har rätt att se uppgifterna. 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, och får som huvudregel inte heller föra sådana uppgifter vidare.

Integritetsincidenter, det vill säga händelser då operatörerna inte har skyddat uppgifter eller har brutit mot tystnadsplikten, utgör potentiellt ett allvarligt hot mot tilltron till elektroniska kommunikationstjänster. När uppgifter som behandlas av operatören 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 2020 diarieförde PTS 305 ärenden med integritetsincidenter hos PTS. Sju av de ärendena visade sig efter utredning inte vara rapporteringspliktiga integritetsincidenter. PTS har alltså behandlat 298 integritetsincidenter under år 2020.[13]

[11] Regler kring rapporteringsskyldigheten för integritetsincidenter finns i 6 kap 4a LEK och i förordning 611/2013.

[12] Regeln om det finns i 6 kap 3 § LEK.

[13] 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 – som är syftet med genomgången.

Alla operatörer rapporterar inte lika många incidenter

PTS kan konstatera att fördelningen av rapporterade incidenter är ojämn mellan operatörerna, och ser det som problematiskt. PTS ser att detta inte enbart är relaterat till bolagens storlek. Det är dock inte säkert att de operatörer som rapporterar flest incidenter är de där flest incidenter inträffar. Det kan också vara så vissa operatörer upptäcker fler incidenter och därför rapporterar mer till PTS. Även om en operatör rapporterar få incidenter, kan fåtalet röra allvarliga incidenter. PTS uppmanar 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 genomfört tillsyn mot några operatörer för att förbättra incidenthanteringen och det kan ha fått den eftersträvade effekten - att fler incidenter hos operatörerna upptäcks och rapporteras.

PTS fortsatta arbete med problemet: PTS avser att undersöka vilken förmåga operatörerna har att förebygga och upptäcka integritetsincidenter. Tillsynen planeras att omfatta ett urval av större operatörer.

Typer av integritetsincidenter 2020

Här presenteras typerna av rapporterade integritetsincidenter 2020 i en enkel tabell:

Typer av integritetsincidenter 2020	**Antal integritets-incidentrapporter**
Felregistrerade kontaktuppgifter och förväxling av uppgifter och adresser i kundtjänst. Inklusive felpackningar på packbordet	177
Systemfel som lett till förväxling av kunder	3
Bedrägerier och försök till bedrägerier, samt obehöriga personer som vilseleder operatören om sin behörighet och får ut information eller ändrar i abonnemang	93
Obehöriga SIM-ändringar (SIM-swapping m.m.)	7
Olovligt spridande av kunders uppgifter till abonnentupplysningsföretag eller andra bolag	7
Ändring av kundens försäkringsskydd av misstag	11

Indelningen i typer är skapad för att förtydliga när integritetsincidenterna inträffar och var det kan finnas anledning att införa riktade åtgärder, eller för kartlägga eller följa upp en viss specifik händelse av någon annan anledning. Kategorierna av typer går dock delvis in i varandra. Det beror på viljan att tydliggöra t.ex. en särskild problematisk situation, när det är möjligt, för att sammanställningen ska kunna vara en utgångspunkt för operatörerna att identifiera om någon riktad teknisk eller organisatorisk åtgärd kan motverka fler incidenter i framtiden.

Ett exempel på överlappande kategorier är SIM-swapping[14] och kategorin att obehöriga personer har fått ut information. Trots att SIM-swapping är ett exempel på när obehöriga personer fått ut information, eller på bedrägeri, har SIM-ändringarna fått en egen kategori. Det beror delvis på att det finns ett särskilt fokus just nu bl.a. från ENISA:s håll om just SIM-swapping, där man vill kartlägga omfattningen och avgöra om det är ett ökande problem. Samma sak gäller typen obehörigt spridande av abonnenternas uppgifter till abonnentupplysningsföretag och kategorin obehöriga personer har fått ut information. Där beror den specifika kategorin på att så många abonnenter skadas i en och samma incident, och att de incidenterna även kan omfatta personer som har fått sina personuppgifter skyddade på grund av skyddsbehov.

I kategoriseringen har incidentrapporterna endast räknats in i den mer specifika gruppen, dvs. i exempelfallen har de incidenterna alltså endast räknats in i typen SIM-swapping eller typen obehörigt spridande av abonnenternas uppgifter till abonnentupplysningsföretag.

PTS kommentarer om årets rapporterade orsaker

Felskick och förväxlingar samt felregistrerade kontaktuppgifter i operatörernas system: Den vanligaste typen av integritetsincident under 2020 beror på fel kontaktuppgifter och adresser till kunder eller förväxlingar av kunder i kundtjänst och utskick av en kunds information till en annan, obehörig kund.

Konsekvenserna för kunden när kundens adress har blivit felaktigt registrerad hos operatörerna, eller där kund A förväxlas med kund B av kundtjänstmedarbetare -

[14] SIM-swapping är ett bedrägeriförfarande där en obehörig person lurar teleoperatören att abonnentens nummer ska flyttas över till en annan telefon, som den obehörige kontrollerar. Abonnenten förlorar då kontrollen över sitt nummer. Detta görs ofta genom att operatören porterar numret till den obehöriges telefon. Det kan också genomföras med ett utskickat nytt SIM-kort, men det är inte nödvändigt med ett nytt SIM-kort. Bedrägerimetoden används både för att den obehöriga ska kunna utge sig för att vara abonnenten i olika sammanhang och för att kunna utnyttja sårbarheter i tvåfaktors-autentisering, som till en del kräver ett SMS.

drabbar oftast en eller ett par personer åt gången. Den obehöriga mottagaren har inte själv drivit fram incidenten. PTS bedömer därför 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.

Den här typen av incidenter utgör den största andelen av rapporterade integritetsincidenter, och har gjort så under de senaste åren. Operatörerna uppger sedan flera år, genomgående i rapporterna, att den åtgärd som vidtas för att inte liknande incidenter ska upprepa sig är påminnelser till personal om organisatoriska rutiner. Likväl har rapporteringen av den här typen av incidenter ökat. Problemet finns i olika grad hos alla operatörer.

Obehöriga personer får ut information eller ändrar i abonnemang, bedrägerier och försök till bedrägerier: Den allvarligaste typen av integritetsincident är att obehöriga får information om, eller ändrar i, abonnemang. Både på grund av antalet, och på grund av den möjliga allvarliga kränkningen av kunders privatliv, ser PTS dessa 100 incidenter som de allvarligaste integritetsincidenterna. [15]

SIM-swapping har i sammanställningen brutits ut för att förtydliga bilden, eftersom det finns både nationellt och europeiskt fokus kring bedrägliga SIM-byten.

PTS åtgärder hittills: Under de senaste åren har det bedrivits tillsyn 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. Den tekniska skyddsåtgärden ska nu vara på plats. Åtgärden innebär att kundtjänstpersonal inte längre 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. PTS har i föreläggandet inte specifikt utalat vilken teknisk lösnings som ska väljas, till exempel måste det inte göras med till exempel BankID. Valet av tekniskt säker lösning görs av operatörerna.

PTS fortsatta arbete med problemet: Eftersom den förelagda skyddsåtgärden för att skydda uppgifter i kundernas abonnemang trätt i kraft under 2021, kan effekterna av skyddsåtgärden inte följas upp ännu. Uppfattningen är dock att den här typen av allvarliga integritetsincidenter bör sjunka med denna skyddsåtgärd.

PTS planerar att följa upp tillsynen om autentisering i kundtjänst och granska om operatörerna har infört de tekniska lösningar som säkerställer att fel person inte ges tillgång till uppgifter eller har möjligheter att ändra abonnemang, samt även att

[15] 100 st. är en hopslagen summa av 93 incidenter där obehöriga som fått ut information eller ändrat abonnemang och sju incidenter med SIM-swapping.

utvidga tillsynen till att omfatta andra kontaktvägar till operatören än kundtjänst per telefon och SIM-swapping.

Olovlig spridning av kunders uppgifter till abonnentförteckningar (abonnentupplysning): 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.

PTS ser allvarligt på de sju incidenter under året där operatörer 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 drabbas i en och samma incident.

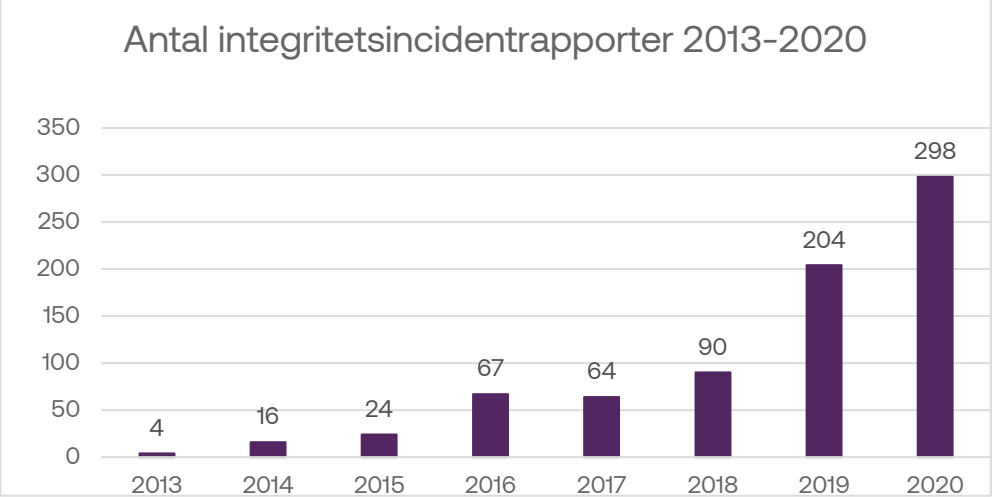
När abonnentupplysningsföretag även har utgivningsbevis från Myndigheten för press, radio och TV innebär det att de har en grundlagsstadgad rätt att publicera personuppgifter de en gång har fått tillgång till och behöver alltså inte iaktta GDPR. Det leder till att en incident där operatören inte har skyddat hemliga uppgifter inte garanterat går att läka genom att operatören i sina egna system rättar det inträffade. 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 genomfört flera tillsynsinsatser genom åren angående olovligt spridande av kunders uppgifter, bland annat hemliga nummer.

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

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 2020 har PTS diarieför 305 rapporter om integritetsincidenter, av vilka sju stycken vid behandlingen visade sig inte vara integritetsincidenter. PTS har alltså hanterat 298 integritetsincidenter. Året visar i vart fall en ökning med nära 50 procent jämfört med 2019.



Samhällets ökade användning av elektroniska kommunikationer, och en ökning av telefon- och internetbedrägerier och identitetskapningar kan vara bidragande till fler 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 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 EU:s allmänna dataskyddsförordning (GDPR) och arbetet som operatörerna genomförde och fortfarande genomför för att skydda personuppgifter med bl.a. ökad bemanning. Detta arbete har höjt medvetenheten kring integritetsfrågor och kan även vara anledningen till att PTS får fler integritetsincidentrapporter.

En jämförelse med Europa

I sammanställningen av incidentrapporter 2020 har denna jämförelse inte genomförts vad gäller integritetsincidenter. Det beror det på att det inte funnits samma slags material att jämföra med som för driftsäkerhetsincidenter. När Kodexen[16] har implementerats i nationell lag kommer jämförelseunderlaget att förändras. Även vid en sådan utveckling kan det sannolikt finnas större utmaningar i att göra jämförelser på integritetsområdet än vad gäller driftsäkerhetsområdet.

Uppföljning på PTS av 2020 års integritetsincidenter

De planerade tillsynerna vad avser integritetsincidenter och skydd av uppgifter finns att läsa mer om i PTS publicerade Incident- och tillsynsrapport 2020–2022.[17]

PTS tillsynsplan påverkas till stor del av den kunskap som kommer från incidentrapporterna. Den kan därför förändras genom inträffade incidenter efter det att planeringen gjordes.

[16] EU-direktiv (2018/1972) för elektroniska kommunikationer som förväntas införlivas i svensk lagstiftning under 2022.

[17] Tillsynsplan och-rapport säker kommunikation 2020–2022 (pts.se)

Bilaga 1

Metod och arbetsprocess

Arbetet med sammanställningen har genomförts på följande sätt.

Inledningsvis gjordes flera genomgångar av alla incidentrapporter från 2020. 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 *root causes* i den årliga uppföljning som görs på europeisk nivå[18], dels de behov som funnits att följa upp vissa mönster i det här årets incidenter på mer detaljerad nivå (exempelvis SIM-swapping, avgrävda kablar eller planerade arbeten som gått fel).

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[19], 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 2020.

Det är första gången PTS gör denna orsaksindelning, lämnar kommenterar till mönster som framträder och publicerar sammanställningen. Det finns utvecklingsmöjligheter i orsakskategorisering och i vilka jämförelser som kan göras. Bland annat behovet av sådana jämförelser både hos PTS och hos operatörerna, och tillgängliga resurser, får styra en sådan utveckling.

[18] Telecom Security Incidents 2020 - Annual Report — ENISA (europa.eu)

[19] Risk- och sårbarhetsanalys för PTS och dess ansvarsområden 2020 - PTS-ER-2020:32 | PTS, läs om elektroniska kommunikationer i kapitel 5 s. 42–67.