2021-01-27 Rapport

Rapportnummer
PTS-ER-2021:4

# Incident- och tillsynsrapport säker kommunikation

## En sammanfattning av incidenthantering och tillsyn 2020 samt av planerad tillsyn 2021-2022

**Rapportnummer**
PTS-ER-2021:4

**Diarienummer**
21-637

**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

Under 2020 har det kommit in 36 incidentrapporter om störningar och avbrott i elektroniska kommunikationsnät och tjänster. De vanligaste orsakerna till driftsäkerhetsincidenterna är, liksom tidigare år, konfigurations- och andra handhavandefel, hårdvarufel, kabelavgrävningar och strömavbrott. Antalet rapporterade incidenter är något lägre än föregående år, men det ser ut att vara en normal variation. Det lägre antalet kan sannolikt bero på att det inte var några större störningar eller avbrott hos kommunikationsoperatörerna, och det ledde till att färre operatörer, som är beroende av kommunikationsoperatörernas tjänster, rapporterade incidenter till PTS. Det var inte heller några större avbrott i samband med hårt väder.

Det har kommit in 305 rapporter om integritetsincidenter i samband med tillhandahållandet av elektroniska kommunikationstjänster under 2020. Det är en ökning med kring 50 procent sedan året innan, och följer trenden från de senaste åren med en kraftig ökning av antalet rapporterade integritetsincidenter. Många av integritetsincidenterna har drabbat endast en eller ett par abonnenter eller användare. Den stora ökningen beror enligt PTS uppfattning på att operatörerna blir allt duktigare på att upptäcka och rapportera incidenter. En mindre del av incidentrapporterna beror dock på att obehöriga får ut information eller ändrar i abonnemang, vilket är allvarligt och kan leda till stor integritetskränkning.

PTS har under 2020 avslutat tillsynsinsatser avseende en stor driftstörning hos Tele2 under sommaren 2019 och störningar i möjligheten att ringa 112 för IP-telefonikunder hos Telenor. Myndigheten har också bedrivit tillsyn avseende autentisering av kunder som ringer till kundtjänst hos flera operatörer, granskat sårbarheter i röstbrevlåda hos Tele2, intrång i säljstödsystem hos Telenor och Tele2 samt brister i Telias rapportering av integritetsincidenter. Vidare har PTS granskat hur flera operatörer efterlever kraven på riskanalyser, såväl vad gäller driftsäkerhet som konfidentialitet.

För åren 2021-2022 avser PTS att genomföra tillsyn bland annat vad gäller skärpta säkerhetskrav inför upphandling av utrustning eller tjänster. Vidare planeras tillsyn av operatörers förmåga att upptäcka integritetsincidenter med hjälp av tekniska lösningar och vad gäller autentisering i kundtjänst, främst vad gäller byte av SIM-kort. PTS kommer också att bedriva tillsyn utifrån den nya lagen om elektronisk kommunikation som väntas träda i kraft under perioden.

# Bakgrund

I den här rapporten beskriver Post- och telestyrelsen (PTS) arbetet med incidentrapporter och tillsyn på områdena driftssäkerhet och konfidentiell kommunikation i elektroniska kommunikationer.

Tidigare år har PTS skrivit en rapport om det utförda tillsynsarbetet och en rapport om planer för kommande arbete. Också områdena för driftsäkerhet och konfidentiell kommunikation har tidigare delats upp i skilda texter. Från och med denna rapport kommer i stället både driftområdet och området för konfidentiell kommunikation, och både rapportering av avslutade tillsynsinsatser och planerade tillsynsinsatser att publiceras i en och samma rapport. Detta ska öka överblicken över arbetet.

Rapporten är skriven i två delar.

I rapportdelen anges hur många incidentrapporter som operatörerna har lämnat till myndigheten under år 2020, och hur många av dem som avsett driftsäkerhet respektive konfidentiell kommunikation (så kallade driftsincidenter respektive integritetsincidenter). Därefter sammanfattas de tillsynsinsatser som genomförts under 2020.

I planeringsdelen beskrivs vilka tillsynsinsatser som planeras för åren 2021 och 2022. I planeringen lämnas utrymme för händelsestyrd tillsyn.

## PTS arbete med säkra kommunikationer

Bestämmelserna i lagen (2003:389) om elektronisk kommunikation (LEK) syftar bl.a. till att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer.

Målet med PTS arbete med driftsäkerhetsfrågor är att nät och tjänster ska ha en nivå av driftsäkerhet som motsvarar användarnas behov. Målet med PTS arbete inom området konfidentiell kommunikation är att alla i Sverige ska kunna kommunicera förtroligt och att tillhandahållare skyddar den information om användarna och deras kommunikation som de hanterar i samband med tillhandahållandet av tjänsterna.

De aktörer som PTS granskar är tillhandahållare av allmänna kommunikationsnät och av allmänt tillgängliga elektroniska kommunikationstjänster (operatörer). Syftet med granskningarna är att se till att operatörerna följer reglerna om både driftsäkerhet och skydd för behandlade uppgifter (konfidentiell kommunikation).

PTS tar löpande emot incidentrapporter från operatörerna, granskar incidenterna och följer upp dem. Om incidentrapporterna visar behov av det, planeras och inleds tillsyn.

Det ingår också i PTS arbete att granska att operatörerna anpassar sin verksamhet för att kunna tillhandahålla uppgifter till de brottsbekämpande myndigheterna i enlighet med lagkrav. Tillsyn kan också bedrivas i denna del av arbetet.

**Hur tillsyn inleds och avslutas**

Frågan om tillsyn ska inledas kan aktualiseras på olika sätt. Ett viktigt underlag när PTS identifierar behovet av tillsyn är de incidentrapporter som operatörerna lämnar till myndigheten. Operatörernas rapporter ger PTS underlag att bedöma om bestämmelserna om driftssäkerhet eller skydd av uppgifter inte följs, och om det i så fall ska inledas tillsyn. Tillsynsinsatserna är framåtsyftande, vilket betyder att PTS följer upp operatörernas åtgärder och säkerställer att de drar lärdomar för att en liknande incident inte ska inträffa igen. Mer om reglerna kring tillsyn hittar du i bilaga 1 till denna rapport.

Utöver incidentgranskningar kan även tidigare tillsynsinsatser, information från EU-samarbeten, samverkan med andra myndigheter, rapportering i media, information från allmänheten eller annan omvärldsbevakning, föranleda tillsyn.

Behovet av tillsyn analyseras alltid innan PTS bestämmer att tillsyn ska genomföras.

En tillsyn avslutas när PTS kan se att ändamålet med tillsynen är uppfyllt. Det sker när operatören bedöms följa regelverken, har vidtagit tillräckliga åtgärder, alternativt rättat sig, eller förelagts om att vidta en åtgärd. Tillsynsprocessen kan också avslutas med att domstol, efter överklagande, upphäver PTS föreläggande.

**Tillämpliga regler vid incidentrapportering och tillsynsverksamhet**

I arbetet med incidenter och tillsyn tillämpas regler kring störningar och avbrott i nät och tjänster (driftsäkerhet), regler som rör operatörernas skydd av uppgifter som behandlas vid tillhandahållandet av elektroniska kommunikationstjänster (konfidentiell kommunikation), regler med krav på att operatörerna ska rapportera incidenter till PTS, samt regler kring anpassning av operatörernas verksamhet för uppgiftslämnande till brottsbekämpande myndigheter.

Tillämpliga regler hittar du i bilaga 1 till denna rapport.

## Ny lag om elektronisk kommunikation

EU:s nya telekomregler kommer att införas i svensk lagstiftning under 2021. Det innebär en rad förändringar i lagen (2003:389) om elektronisk kommunikation (LEK).

Operatörer som omfattas av PTS nuvarande regler samt nya aktörer kommer att påverkas.

Den nu gällande lagen om elektronisk kommunikation kommer att ersättas med en ny lag. Detta sker eftersom EU i december 2018 antog ett nytt EU-direktiv om att inrätta en kodex för elektronisk kommunikation[1]. Målet med kodexen är att inrätta ett harmoniserat regelverk för elektroniska kommunikationsnät och tjänster. Kodexen innehåller bl.a. bestämmelser om vilka uppgifter nationella regleringsmyndigheter ska ha liksom en rad regler för att säkerställa en harmoniserad tillämpning av regelverket inom hela unionen. Den nya lagen kommer att ha ett bredare och tydligare säkerhetsbegrepp jämfört med nuvarande lag. Av de kommande reglerna framgår att nät och tjänster ska ha en förmåga, att vid en viss tillförlitlighetsnivå, motstå åtgärder som undergräver säkerheten i dessa fyra aspekter: tillgänglighet, riktighet, integritet och konfidentialitet.

Med en ny lag kommer även föreskrifterna till lagen skrivas om. PTS har påbörjat arbete med att se över befintliga föreskrifter och allmänna råd på områdena som berörs samt att utreda vilka ytterligare regler som behövs för att genomföra EU:s telekomregler [2]. De nya reglerna ska vara tydliga, ändamålsenliga och proportionerliga. Förslag på föreskrifter kommer att skickas på remiss efter att regeringen har överlämnat sin proposition till riksdagen.

Myndigheten arbetar just nu efter en tidplan som innebär att remiss av nya föreskrifter skickas ut under 2021. Förslag på föreskrifter skickas tillsammans med en redogörelse för vilka konsekvenser som kan bli följden av förslagen.

Operatörer och andra aktörer som vill svara på remiss kommer att behöva ta ställning till många förslag under relativt kort tid. Målgruppen för föreskrifterna är framför allt tillhandahållare av allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster.

## Förhållandet mellan lagen om elektronisk kommunikation och EU:s dataskyddsförordning

Det kan ibland vara svårt att avgöra om uppgifter skyddas av LEK, eller av dataskyddsförordningen (GDPR[3]). För att förtydliga vilka regler som skyddar vilka

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

[2] Enligt förordningen (2003: 396) om elektronisk kommunikation är det PTS som ansvarar för sådana föreskrifter som behövs för att förtydliga skyldigheter och uppgifter för driftsäkerhet och konfidentiell kommunikation.

[3] General Data Protection Regulation

uppgifter beskrivs här kort skillnaderna och det finns en fördjupning i bilaga 2 till denna rapport.

Reglerna i LEK ger skydd åt *alla uppgifter* som behandlas *i samband* med tillhandahållandet av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster. De uppgifter som omfattas av reglerna i LEK kan exempelvis vara adressuppgifter, telefonnummer, vem du ringer till och när, dina surfvanor, innehållet i kommunikationen och var din mobiltelefon befunnit sig vid olika tidpunkter. Sådana uppgifter hanterar operatörerna för att kunna tillhandahålla telefoni och internetabonnemang.

Annan hantering, specifikt av personuppgifter, d.v.s. när personuppgifterna *inte* behandlas *i samband* med tillhandahållande av elektronisk kommunikation regleras istället av GDPR och Integritetsskyddsmyndigheten är tillsynsmyndighet och rapportmottagare för sådan hantering.

Den här rapporten redogör för tillsyn som PTS genomför för att säkerställa att operatörerna skyddar uppgifter som de får tillgång till i samband med tillhandahållande av telefoni och internetabonnemang.

# Incidentrapportering under 2020

I det här avsnittet beskrivs incidenthantering och specifikt den incidentrapportering som PTS mottagit under 2020.

När det inträffar driftsstörnings- och integritetsincidenter som är rapporteringspliktiga ska operatörerna lämna incidentrapporter till PTS. Regler kring detta hittar du i bilaga 1 till denna rapport.

Incidentrapporterna ger PTS underlag att bedöma om bestämmelserna om driftssäkerhet eller skydd av uppgifter inte följs, och om det i så fall ska inledas tillsyn. 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.

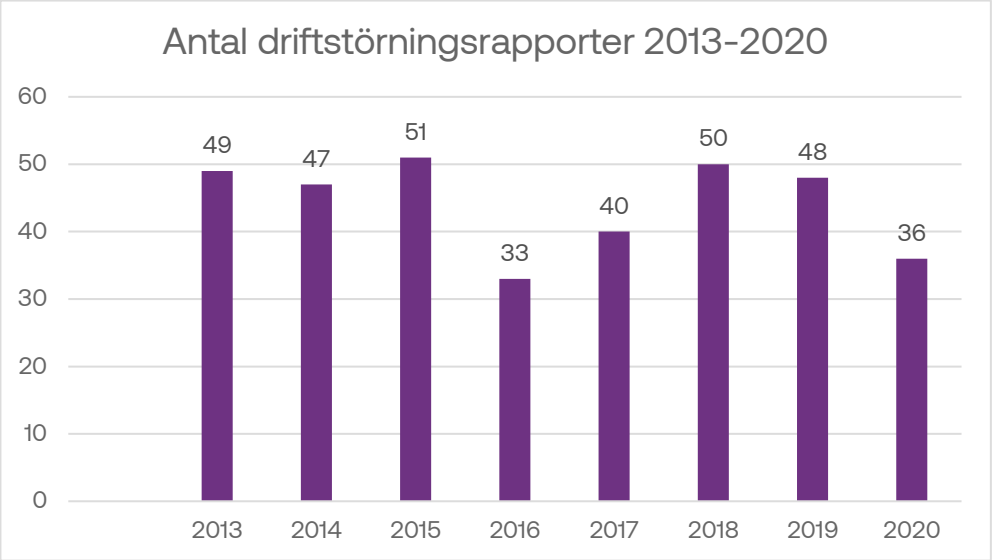
## Driftsäkerhetsincidenter

Operatörer är skyldiga att rapportera inträffade störningar och avbrott till PTS om de överskrider vissa kvantitativa och kvalitativa tröskelvärden[4]. Sådana inträffade händelser kallas driftsäkerhetsincidenter.

Ett krav på incidentrapporten är att den ska vara så tydlig och detaljerad att PTS kan bilda sig en uppfattning om orsaker och åtgärder, och kan bedöma om det finns behov av att inleda tillsyn eller vidta andra åtgärder.

Under 2020 har PTS mottagit 36 stycken rapporter om driftsstörningar och avbrott av betydande omfattning.

[4] Tröskelvärdena hittar du i bilaga 1 till denna rapport.




Diagrammet visar antal inrapporterade driftstörningar per år, mellan åren 2013 och 2020.

Antalet driftsstörningsincidenter under 2020 är något lägre än närmast föregående år, men året kan betraktas som ett normalår.

Det har över åren visat sig att det är vanligast att fasta tjänster[5] drabbas av driftssäkerhetsincidenter. Mobila nät och tjänster drabbas inte lika ofta. Typiskt rapporteras incidenter av lokala eller regionala aktörer och har regional eller lokal påverkan.

De år när antalet rapporter har varit högre är det ofta en följd av en störning eller avbrott hos en kommunikationsoperatör[6]. Då många operatörer är beroende av kommunikationsoperatörens tjänster blir följden många incidentrapporter med anledning av samma händelse.

Den vanligaste orsaken till driftssäkerhetsincidenter som får nationell påverkan är, och har under flera år varit, konfigurations- och andra handhavandefel. Den näst

[5] Till exempel fast telefoni och fast bredband.

[6] 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.

största felkategorin för nationella störningar och avbrott är fel i hård- och mjukvara. En annan vanlig orsak är kabelavgrävningar eller strömavbrott till följd av stormar.

Huvuddelen av alla störningar och avbrott pågår en kortare tid, från någon timma upp till åtta timmar.

Vissa större driftstörningsincidenter ska PTS enligt regelverket rapportera till EU-kommissionen[7] och Enisa[8]. Dessa rapporter skickas från PTS i början av varje år. I nuläget (januari 2021) arbetas tröskelvärdena om för vilka incidenter som ska rapporteras till EU-organen, varför de som rapporteras för 2020 inte redovisas i den här rapporten. År 2019 skickade PTS in tre sådana rapporter.

## Integritetsincidenter

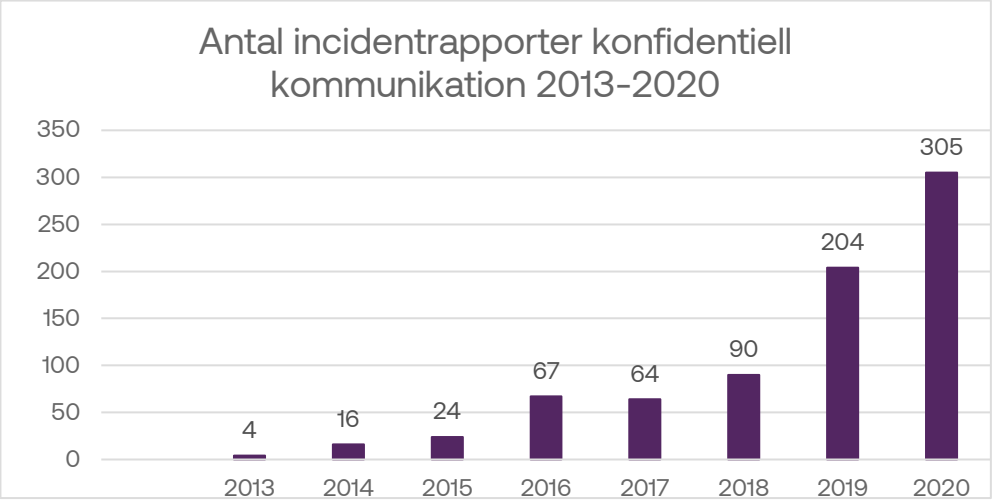
Operatörerna hanterar stora mängder uppgifter om enskilda och deras kommunikation för att kunna tillhandahålla nät och tjänster till kunderna. Det finns en skyldighet att skydda uppgifterna så att de inte förstörs, ändras eller att obehöriga kommer åt dem. Skulle det ändå hända kallas det integritetsincident. Mer om reglerna hittar du i bilaga 1 till denna rapport.

Integritetsincidenter utgör potentiellt ett allvarligt hot mot tilltron till elektroniska kommunikationstjänster. Om uppgifter som behandlas inom ramen för en elektronisk kommunikationstjänst, till exempel sprids till utomstående eller går förlorad, kan det få allvarliga konsekvenser. Om sådana händelser inte hanteras på ett lämpligt sätt kan det leda till att individer råkar ut för såväl ekonomisk skada som personlig kränkning.

Det har skett en successiv och på senare år kraftig ökning av antalet integritetsincidenter från år till år. Under 2020 har PTS mottagit 305 stycken rapporter om integritetsincidenter, vilket är en ökning med nära 50 procent jämfört med året innan, 2019.

[7] Vid större störningar och avbrott är PTS skylig att rapportera vidare till EU-kommissionen enligt Europaparlamentets och rådets direktiv 2009/140/EG av den 25 november 2009 om ändring av direktiv 2002/21/EG om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/19/EG om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande faciliteter och direktiv 2002/20/EG om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster.

[8] Enisa = European Union Agency for Network and Information Security, ett center med expertkunskaper inom cybersäkerhet i Europa.




Diagrammet visar antalet inrapporterade integritetsincidenter per år, mellan åren 2013 och 2020.

Samhällets ökade användning av elektroniska kommunikationer, och en ökning av telefon- och internetbedrägerier och identitetskapningar [9] kan vara bidragande till fler integritetsincidenter. PTS uppfattning är dock att den kraftiga ökningen inte beror på en motsvarande ökning av faktiska incidenter, utan till stor del beror på operatörernas förbättrade arbete med att upptäcka och rapportera incidenter till PTS. Operatörerna har också meddelat PTS att de har ökad kunskap och fokus på frågorna genom det arbete som gjordes kring införandet av dataskyddsförordningen. Myndigheten utgår ifrån att det har funnits och fortfarande finns ett mörkertal av integritetsincidenter som inte upptäcks eller rapporteras, men det är möjligt att mörkertalet har minskat med en förbättrad förmåga till upptäckt och rapportering. PTS har bedrivit, och planerar även att bedriva ytterligare tillsyn för att granska operatörernas förmåga att upptäcka och rapportera integritetsincidenter[10].

En övervägande del av integritetsincidenterna beror på handhavandefel i kundtjänst eller hos återförsäljare, och drabbar normalt endast en eller ett par abonnenter. Typexempel är att fel mejladress skrivs in i ett kundtjänst ärende, eller att två kunder förväxlas, vilket leder till att abonnemangsbekräftelse eller faktura skickas fel. En mindre del av incidentrapporterna beror dock på att obehöriga får ut information eller ändrar i abonnemang, vilket är allvarligt och kan leda till stor integritetskränkning.

[9] Se Brottsförebyggande rådets kartläggning i rapport (2016:9) Bedrägeribrottsligheten i Sverige, kartläggning och åtgärdsförslag

[10] Se avsnittet i denna rapport om planerad tillsyn, samt tillsyn under 2017 flera operatörers förmåga att identifiera och internt rapportera integritetsincidenter, Dnr: 17–10175, 17–10176 och 17–10177.

# Genomförd tillsyn under 2020

I det här avsnittet beskrivs de tillsynsinsatser som genomförts under 2020. De korta beskrivningarna för varje tillsyn ger information om vilken sorts tillsyn det varit, när den inleddes och avslutades, samt bakgrunden till tillsynen och anledningen eller syftet med den samt hur den avslutades.

Under året har totalt åtta tillsynsinsatser genomförts och avslutats - Den återkommande årliga tillsynen, två stycken händelsestyrda som initierades efter driftssäkerhetsincidenter, fyra stycken som rörde konfidentiell kommunikation och en som avsåg både driftssäkerhet och konfidentiell kommunikation.

Flertalet tillsynsinsatser har avslutats efter dialog, då operatörerna förbättrat sina säkerhetsåtgärder i enlighet med PTS krav. Den tillsyn som gällde autentisering i kundtjänst ledde dock till förelägganden mot fyra operatörer. Ett av dessa förelägganden har överklagats.

## Den återkommande årliga tillsynen

Granskningen omfattade 2020 Tele2, Telenor, Telia och Tre och avsåg alla rapporterade incidenter från dessa operatörer 2019, som inte har behandlats i annan tillsyn. Tillsynen syftade till att kontrollera att operatörerna vidtagit åtgärder och dragit lärdomar av fjolårets inträffade incidenter. Den årliga tillsynen avslutades efter konstaterande av att operatörerna uppdaterat processer och rutiner för att hantera incidenter, att de genomfört de åtgärder de angett i incidentrapportering, och att de därmed har förutsättningar att hantera incidenterna i enlighet med regelverket.

**Tillsyn inledd:** 2020-02-06
**Tillsyn avslutad:** 2020-05-05

## Tillsyn av driftsäkerhet

Under år 2020 genomfördes två tillsynsinsatser som inleddes efter driftstörningsincidenter. Båda var händelsestyrda och har alltså inte ingått i tidigare tillsynsplanering. Här beskrivs kort omständigheterna kring dessa två tillsynsinsatser.

**Driftstörningar hos Tele2 i juni 2019**

Händelsestyrd tillsyn.

Under ett par dagar i juni 2019 drabbades Tele2 av driftsstörningar som gjorde att privatpersoner och företag i hela landet hade stora problem med att ringa och ta emot samtal. PTS inledde en granskning som visade att orsaken till störningarna var ett programvarufel i noder i Tele2:s nät. Noderna, som ska dirigera trafik, överbelastades på grund av felet. Driftstörningen avhjälptes genom att Tele2 uppgraderade programvaran till en senare version. Efter att störningen var avhjälpt vidtog Tele2 åtgärder för att minska risken för framtida störningar och inledde ett närmare samarbete med leverantören av den aktuella utrustningen. PTS bedömde åtgärderna som tillräckliga och avslutade granskningen.

**Tillsyn inledd:** 2019-07-05
**Tillsyn avslutad:** 2020-02-26

**Driftsstörningar som gjorde det omöjligt att nå 112, 1177 och 90 000 via Telenors ip-telefonitjänst**

Händelsestyrd tillsyn.

Under en vecka i december 2019 pågick driftstörningar som påverkade Telenors abonnenter med ip-telefoni i hela landet. Abonnenter som ringde 112, 1177 eller 90 000 fick endast upptagetton. Telenor anmälde incidenten till PTS, som sedan i tillsyn granskade varför driftstörningarna hade inträffat och vad Telenor gjorde för att lösa problemen och för att det inte ska inträffa igen. Telenor vidtog flera åtgärder avseende planerade förändringar, övervakning och beredskap för att stärka driftsäkerheten. Myndigheten bedömer att Telenors åtgärder uppfyller rimliga krav på driftsäkerhet vid planerade förändringar som kan påverka de samhällsnyttiga numren 112, 1177 och 90 000, varför tillsynen avslutats.

**Tillsyn inledd:** 2020-02-13
**Tillsyn avslutad:** 2020-05-22

## Tillsyn av konfidentiell kommunikation

Under år 2020 gjordes fyra tillsynsinsatser på området konfidentiell kommunikation. En av tillsynsinsatserna var planerad. Tre av dem var händelsestyrda och har alltså inte ingått i tidigare tillsynsplanering. Här beskrivs kort omständigheterna kring dessa.

**Teknisk säker autentisering av inringande kund i kundtjänst hos de fyra största operatörerna, Telia, Tele2, Telenor och Tre**

Planerad tillsyn.

Under åren 2018 och 2019 var en av de vanligaste typerna av inrapporterade incidenter att obehöriga personer hade fått ut integritetskänslig information om kunder och hade kunnat ändra kunders abonnemang. Konsekvenserna för kunderna visade sig kunna bli allvarliga och verkade ofta bero på att kundtjänstpersonal bröt mot rutiner för arbetet. Tillsyn inleddes därför mot de fyra största operatörerna. Granskningen visade att en teknisk skyddsåtgärd behövs för att förhindra att obehöriga får ut/ändrar information. Tillsynsinsatserna avslutades med förelägganden för operatörerna om att införa en teknisk lösning för autentisering/legitimering av kunder som ringer in till kundtjänst. Lösningen innebär att avgörandet av om kunden är autentiserad/legitimerad ligger hos den tekniska lösningen. En manuell bedömning av autentiseringsfrågan ska inte kunna göras. De fyra operatörerna ska ha infört den säkra tekniska lösningen senast sista mars 2021. En av de fyra operatörerna har överklagat föreläggandet till förvaltningsrätten.

**Tillsyn inledd:** 2019-05-17
**Tillsyn avslutad:** 2020-06-25 (en operatör har överklagat föreläggandet)

**Sårbarhet i röstbrevlådan hos Tele2**

Händelsestyrd tillsyn. Konfidentiell kommunikation.

Genom medieuppgifter år 2019 fick PTS veta att obehöriga hade kunnat lyssna av röstmeddelanden och ändra inställningar i röstbrevlådor hos Tele2. Trots att operatören vidtog vissa åtgärder kvarstod denna sårbarhet i delar av nätet. PTS inledde därför en tillsyn och granskade om operatören levde upp till kraven på skydd av uppgifter samt rutiner för loggning. Tele2 vidtog då flera nya åtgärder som stärker skyddet för uppgifter i kundernas röstbrevlådor. Tele2 uppdaterade också sina riskanalyser. Tele2 följer nu riktlinjer för säkerhet i röstbrevlådor och följer etablerad standard och praxis för skyddsåtgärder på detta område. Därmed minskade risken för att liknande incidenter ska inträffa igen varför PTS har valt att avsluta tillsynen.

**Tillsyn inledd:** 2019-12-18
**Tillsyn avslutad:** 2020-05-07

**Obehörigt intrång i säljstödsystem hos Telenor och Tele2**

Händelstyrd tillsyn.

Integritetsincidentrapporter som inkom till PTS under 2019 visade att abonnentuppgifter hade hamnat i orätta händer på grund av att obehöriga tagit sig in

i Telenors och Tele2:s säljstödsystem. Det hade kunnat ske genom att obehöriga kom åt användarkonton i operatörernas säljstödsystem. I dessa fanns åtkomst till abonnentuppgifter. PTS inledde tillsyn och granskade hur operatörerna levde upp till kraven om skydd av uppgifter, och tittade särskilt på rutinerna för åtkomst, behörighet samt loggning. Båda operatörerna vidtog flera nya skyddsåtgärder för sina åtkomst- och behörighetsprocesser och införde nya rutiner för kontroll och uppföljning av loggar. PTS avslutade tillsynen med bedömningen att dessa åtgärder bidrar till ett stärkt skydd och att åtgärderna minskar risken för att liknande incidenter inträffar igen.

**Tillsyn inledd:** 2019-10-28
**Tillsyn avslutad:** 2020-02-20

#### Brister i Telias rapportering av integritetsincidenter

Händelsestyrd tillsyn.

Under hösten 2019 och våren 2020 lade PTS märke till att Telias incidentrapportering inte alltid nådde upp till kraven. PTS inledde tillsyn i två delar[11]. Granskningen ledde till att Telia har vidtagit åtgärder för att säkerställa fungerande rutiner för incidentrapportering. PTS avslutade tillsynen efter att Telia nu har förutsättningar att framöver hantera incidentrapporteringen i enlighet med regelverket.

**Tillsyn inledd:** 2020-07-08
**Tillsyn avslutad:** 2020-11-20

### Tillsyn av både driftsäkerhet och konfidentiell kommunikation

#### Tillsyn av metoder och genomföranden av riskanalyser hos Telia, Telenor, Tre och Com Hem

Planerad tillsyn.

PTS inledde 2018 tillsyn mot Telia, Telenor, Tre och Com Hem om deras metoder och genomföranden av riskanalyser, både för driftsäkerhet och för konfidentiell kommunikation. Riskanalyser utgör en grund för säkerhetsarbetet, och är nödvändiga för att rätt säkerhetsåtgärder ska kunna vidtas. Tillsynen inleddes då PTS fått tydliga indikationer på brister i operatörernas processer för riskanalyser, samt att riskanalyser ibland saknades helt. Syftet med tillsynen var att säkerställa att operatörerna tillämpar en acceptabel metod för sina riskanalyser och att de faktiskt genomfört riskanalyser för sina tillgångar och förbindelser. Tillsynsärendena mot Telia och Telenor kunde efter skriftväxling och tillsynsmöten skrivas av från vidare

[11] Se information om den tidigare tillsynen mot Telia i PTS sammanställning av tillsyn 2019, dnr 20-8548.

handläggning under 2019 då de två operatörerna redovisat rimliga metoder för genomförande av riskanalyser och lämnat exempel på sådana riskanalyser. Tillsynsinsatserna mot Com Hem och Tre avslutades 2020, då operatörerna rättat sig efter underrättelse om uppmärksammad brist.

**Tillsyn inledd:** 2018-12-20
**Tillsyn avslutad:** 2020-03-11

# Tillsyn under 2021 och 2022

I det här avsnittet beskrivs de tillsynsinsatser som pågår i nuläget (januari 2021) och de som planeras att genomföras under 2021-22. Planeringen kan komma att ändras eftersom erfarenheten visar att det årligen behöver utföras händelsestyrda tillsynsinsatser. I planeringen finns därför visst utrymme för händelsestyrd tillsyn. Blir dessa händelsestyrda tillsynsinsatser många kan det förändra en redan beslutad tillsynsplanering. Det görs i så fall för att resurserna ska räcka till.

## Pågående tillsyn

För närvarande (januari 2021) pågår tre tillsynsinsatser. Två avser driftsäkerhet och en både driftsäkerhet och konfidentiell kommunikation. I dagsläget pågår inte några händelsestyrda tillsynsinsatser.

#### Säkerhetsåtgärder för att minska risker i Border Gateway Protocol (BGP)

Planerad tillsyn. Driftsäkerhet och konfidentiell kommunikation.

PTS inledde i oktober 2020 tillsyn av ett antal av de större internetoperatörerna i syfte att utreda om de har tillräcklig kunskap och vidtar åtgärder för kända sårbarheter i BGP. Protokollet är en central del av internet och används av bland annat internet- och knutpunktsleverantörer för att vidarebefordra trafik över världen. Det finns kända sårbarheter i BGP som har uppmärksammats internationellt de senaste åren. Dessa kan leda till såväl driftstörningar som integritetsincidenter. Farorna kan vara avsiktliga attacker eller oavsiktlig felkonfiguration. PTS har hittills mottagit en incidentrapport avseende oavsiktlig felkonfiguration av BGP. Incidenten ledde till ett omfattande avbrott i kommunikationstjänster. PTS avser att slutföra tillsynen under första kvartalet 2021.

**Tillsyn inledd:** 2020-10-01

#### Efterlevnad av föreskrifter om reservkraft för operatörers tillgångar

Planerad tillsyn.

Enligt föreskrifter från PTS måste operatörerna från juni 2020 ha reservkraft för sina tillgångar i enlighet med kraven Samhällets beroende av elektronisk kommunikation och internetuppkoppling växer. Kraven ökar då också på att tjänsterna ska fungera. För att minska sårbarheten i näten har PTS därför infört krav på reservkraft för

operatörernas tillgångar[12] för det fall det uppstår strömavbrott. Vilka reservkraftskrav som gäller bestäms genom en klassificering. Generellt sett kan man säga att ju fler aktiva anslutningar en tillgång har desto längre reservkraftstid krävs. Operatörer av mobila kommunikationsnät och mobila kommunikationstjänster har utöver det också ett särskilt krav på reservkraft.

PTS inledde i september 2020 en granskning av åtta större tillhandahållare av fasta och mobila nät och tjänster för att genom stickprov kontrollera att de följer kraven på reservkraft [13]. PTS avser att slutföra granskningen under andra kvartalet 2021.

**Tillsyn inledd:** 2020-09-18

#### Driftsäkerhet vid förläggning av sjökablar

Planerad tillsyn.

Tillsynsinsatser som utförts av myndigheterna i Norge och Finland har visat att det fanns brister i skyddet av sjökablar i dessa båda länder, särskilt för den delen av sjökabeln som går från stranden till kopplingspunkten på land. Mot den bakgrunden beslutade PTS att inleda tillsyn mot två operatörer avseende bolagens skydd av sjökablar i svenskt territorialvatten samt insjöarna Mälaren, Vänern och Vättern. Tillsynen innefattar även att granska riskanalyser och skyddsåtgärder och PTS har inspekterat sjökablar fysiskt på två platser hittills. PTS avser att avsluta granskningen under första kvartalet 2021.

**Tillsyn inledd:** 2020-05-25

## Planerad tillsyn

Under år 2021 och 2022 planerar PTS att utföra tillsyn över operatörers förmåga att med tekniska lösningar upptäcka integritetsincidenter, hur operatörerna arbetar med autentisering av kunder vid flytt av nummer till ett annat SIM-kort och över säkerhetsbrister i operatörers användarportaler. Vidare planeras tillsyn av hur operatörerna efterlever nya säkerhetskrav och ny lagstiftning.

---

[12] En tillgång är en funktion som utgörs av en avgränsad del av ett kommunikationsnät eller kommunikationstjänst och som är nödvändig för tillhandahållande av sådant nät eller tjänst samt används för att sända, motta, bearbeta eller lagra information (PTSFS 2015:2).

[13] (PTSFS 2015:2)

### Årlig tillsyn

I den årliga tillsynen, som varit en återkommande och planerad tillsynsinsats, granskas ett urval av operatörer. Hittills har PTS valt de största operatörerna. I den årliga tillsynen tittar PTS på föregående års inrapporterade incidenter, som inte tagits om hand genom händelsestyrd tillsyn

Syftet med den årliga tillsynen är se till att de fyra största operatörerna har fungerande rutiner för rapportering av incidenter på de båda områdena. De ska följa upp inträffade incidenter och lära sig av det inträffade.

PTS avser under 2021 att göra en utvärdering av den årliga tillsynen och eventuellt förändra arbetet för ökad effektivitet och nytta.

### Skärpta säkerhetskrav för operatörer inför upphandling av utrustning eller tjänster

Planerad tillsyn. Driftsäkerhet.

Tillsyn av hur ändringar i driftsäkerhetsföreskrifterna[14] följs. Ändringarna innebär bl.a. att tillhandahållare ska genomföra riskanalyser inför upphandling, krav att tillhandahållare beaktar ytterligare hot i riskanalysen, ökade dokumentationskrav och förtydliganden kring åtkomst och behörighet.

Mot bakgrund av dessa nya krav planerar PTS att under 2021 inleda en tillsyn över ett urval av de större operatörerna i syfte att granska om dessa efterlever de nya kraven.

**Planerad inledning:** 2021

### Granskning av operatörers förmåga att upptäcka integritetsincidenter med hjälp av tekniska lösningar

Planerad tillsyn. Konfidentiell kommunikation.

PTS avser att undersöka vilken förmåga operatörerna har att med tekniska metoder förebygga och upptäcka integritetsincidenter. Tillsynen omfattar ett urval av större operatörer och ett urval av metoder (t.ex. behörighetsspärrar och automatiserad logganalys).

**Planerad inledning: 2021**

[14] (PTSFS 2015:2, ändrade genom PTSFS 2020:1)

**Tillsyn av autentisering i samband med s.k. SIM-swapping**

Planerad tillsyn. Konfidentiell kommunikation.

Som en uppföljning av PTS tillsyn avseende autentisering i kundtjänst avser myndigheten att granska om operatörerna har infört tekniska lösningar som säkerställer att fel person inte ges tillgång till uppgifter eller har möjligheter att ändra abonnemang. Tillsynen ska fokusera på flytt av nummer till nytt SIM-kort, och bör gälla alla kanaler där människor vänder sig till operatörernas kundtjänst. Eventuellt ska detta ske i samarbete med polisen.

**Planerad inledning:** andra halvåret 2021

**Brister i skydd av uppgifter i ”Mina sidor” hos operatörer**

Planerad tillsyn. Konfidentiell kommunikation.

Det har kommit in incidentrapporter som visar på brister i säkerheten för operatörers användarportaler såsom ”Mina sidor”. PTS planerar tillsyn för att granska att uppgifter om användare och kommunikation skyddas i enlighet med regelverket.

**Planerad inledning:** 2022

**Ny lag om elektronisk kommunikation**

Planerad tillsyn. Driftsäkerhet och konfidentiell kommunikation.

Den nya lagen kan komma att innebära förändrade krav gentemot operatörer. PTS planerar att genomföra tillsyn med utgångspunkt i någon eller några av de nya kraven, i syfte att granska om operatörerna efterlever regelverket. Tillsynen kommer sannolikt att bedrivas genom skriftlig informationsinhämtning i kombination med tillsynsmöten.

**Planerad inledning:** 2022

## Framåtblick

PTS tillsynsarbete bedrivs för att säkerställa att operatörerna lever upp till kraven på ett rimligt säkerhetsarbete för driftsäkerhet och konfidentiell kommunikation. Nästa tillsynsrapport kommer att publiceras i januari 2022. Den kommer att omfatta rapport över genomfört arbete med incidenthantering och tillsyn år 2021, och en plan för åren 2022-2023. Planen är tvåårig men uppdateras varje år. Det pågående arbetet med nya föreskrifter till den kommande nya lagen om elektronisk kommunikation fortsätter under 2021.

## BILAGA 1

**Sammanställning av vissa tillämpliga regler om driftsäkerhet, regler vid incidentrapportering, tillsynsverksamhet, och anpassning av verksamhet för att lämna ut uppgifter till brottsbekämpande myndigheter**

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[15].

**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[16].

**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

[15] 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.

[16] 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).

**Regler om anpassning av verksamhet för att kunna tillhandahålla uppgifter till brottsbekämpande myndigheter**

I 6 kap. 3 a § LEK finns särskilda regler som gäller skydd för uppgifter som lagras för brottsbekämpande ändamål med stöd av 6 kap. 16 a §.

Dessa preciseras av PTS föreskrifter och allmänna råd om skyddsåtgärder i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål (PTSFS 2012:4).

Enligt 6 kap. 19 § LEK är tillhandahållare av allmänna kommunikationsnät, samt tillhandahållare av fasta och mobila telefoni- och internettjänster skyldiga att bedriva verksamheten så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs. Innehållet i och uppgifter om avlyssnade eller övervakade meddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand.

Enligt 6 kap. 20 § första stycket 1 LEK har operatörerna tystnadsplikt för uppgift om abonnemang. Men tystnadsplikten för uppgift om abonnemang bryts enligt 6 kap. 22 § första stycket 2 LEK när det gäller misstanke om brott och begäran har kommit in från åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet.

**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 som störningen eller avbrottet pågått parallellt med störningens eller avbrottets uppskattade omfattning.

**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**<br>**≥ 15 000 km² sammanhängande berört område eller**<br>**≥ 50 % kapacitetsbortfall** |
| **≥ 2 timmar** | **≥ 30 000 abonnenter eller**<br>**≥ 5 000 km² sammanhängande berört område eller**<br>**≥ 30 % kapacitetsbortfall** |
| **≥ 6 timmar** | **≥ 5 000 abonnenter eller**<br>**≥ 2 500 km² sammanhängande berört område eller**<br>**≥ 20 % kapacitetsbortfall** |
| **≥ 24 timmar** | **≥ 2000 abonnenter eller**<br>**≥ 1 000 km² sammanhängande berört område eller**<br>**≥ 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.

## BILAGA 2

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

EU:s dataskyddsförordning (GDPR) är direkt tillämplig i svensk rätt med vissa tillägg, 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 Datainspektionen (DI).

**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 DI enligt GDPR; dubbel rapportering av samma incident är inte nödvändig.