Nätsäkerhetsavdelningen

Genomförd tillsyn avseende säker och konfidentiell kommunikation under 2017

Inledning

Denna rapport har i syfte att sammanfatta PTS genomförda tillsynsinsatser inom området säker och konfidentiell kommunikation under 2017. Rapporten beskriver tillsynsinsatser som har genomförts sedan den förra tillsynsrapporten, publicerad i juni 2017[1], till och med juni 2018.

Rapporten beskriver syftet med genomförda tillsynsinsatser, hur tillsynsinsatserna har genomförts samt resultatet och vilka slutsatser som PTS har dragit av tillsynerna.

Inledningsvis redogörs kortfattat för PTS tillsynsarbete inom området säker och konfidentiell kommunikation och personlig integritet utifrån PTS mandat. Därefter sammanfattas PTS genomförda planlagda samt händelsestyrda tillsynsinsatser.

PTS arbete med tillsyn över regler i lagen om elektronisk kommunikation inom området säker och konfidentiell kommunikation och personlig integritet

Ett av PTS övergripande mål är att främja tillgången till säker elektronisk kommunikation. En viktig säkerhetsfråga är skyddet av den personliga integriteten. Målet med PTS integritetsskyddsarbete är att alla i Sverige ska kunna kommunicera förtroligt och att information inte används på ett sätt som hotar den enskildes integritet.

Lagen (2003:389) om elektronisk kommunikation (LEK) innehåller regler om integritetsskydd som gäller tillhandahållare av elektroniska kommunikationsnät

[1] Se PTS ärende dnr 17-7513

Post- och telestyrelsen

Postadress:
Box 5398
102 49 Stockholm

Besöksadress:
Valhallavägen 117 A
www.pts.se

Telefon: 08-678 55 00
Telefax: 08-678 55 05
pts@pts.se

och -tjänster. Bland annat finns regler om under vilka förutsättningar och hur länge trafik- och lokaliseringsuppgifter får behandlas och krav på att vidta tekniska och organisatoriska säkerhetsåtgärder för att skydda de uppgifter som behandlas. Reglerna i LEK kompletteras av PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1).

Enligt bestämmelser i LEK, kompletterade av en direkt tillämplig EU-förordning[2], är tjänstetillhandahållare även skyldiga att rapportera inträffade integritetsincidenter till PTS och till berörda abonnenter eller enskilda personer samt att föra en förteckning över inträffade incidenter. Incidentrapporterna ger PTS underlag om de viktigare orsakerna till integritetsincidenter, och hur tillhandahållarna arbetar för att förebygga och hantera inträffade händelser. Rapporterna kan även ge PTS anledning att misstänka att bestämmelserna om integritetsskydd inte efterlevs och i sådana fall bedriva tillsyn.

Närmare om PTS tillsynsarbete under 2017

PTS granskar löpande de rapporter om integritetsincidenter som inkommer. PTS bedriver även egen omvärldsbevakning för att få kännedom om inträffade incidenter. I händelse av mer omfattande eller principiellt intressanta incidenter kan PTS komma att inleda *händelsestyrd tillsyn*, som regel är inriktad på att granska orsakerna till den inträffade händelsen och tillhandahållarens arbete för att förebygga att liknande händelser inträffar igen.

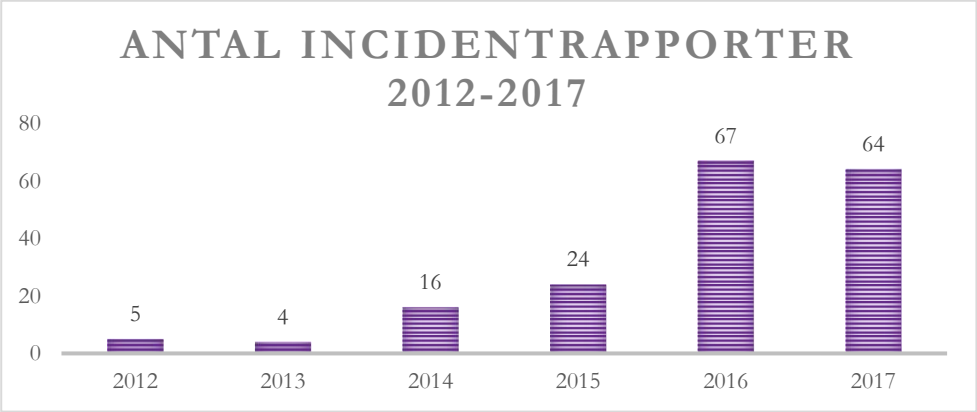
Under 2017 har PTS fått in 64 rapporter om integritetsincidenter. Det är i samma storleksordning som under 2016. PTS har tidigare gjort bedömningen att det finns ett mörkertal av integritetsincidenter som inte rapporteras till myndigheten, varför myndigheten under 2017-2018 har genomfört en planlagd tillsyn av de största tillhandahållarnas förmåga att identifiera och internt rapportera integritetsincidenter. Slutsatserna från den tillsynen beskrivs senare i denna rapport.

PTS har under 2017 i ett fall beslutat att inleda *händelsestyrd* tillsyn i anslutning till inrapporterade integritetsincidenter. Tillsynen avser en granskning av operatörens åtgärder för att hantera återkommande incidenter hos underleverantörer.

Inom ramen för PTS långsiktiga arbete följer myndigheten även upp de större tillhandahållarnas arbete med att hantera och dra lärdomar av inträffade incidenter genom en planlagd *årlig tillsyn* som omfattar samtliga de integritetsincidenter som inträffat för berörda tjänstetillhandahållare under i första hand föregående år och som inte redan har granskats inom ramen för händelsestyrd tillsyn. Under 2017 har PTS genomfört årlig tillsyn som omfattat de fem största tjänstetillhandahållarna.

[2] Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott

Mot bakgrund av tidigare års inrapportering av integritetsincidenter och PTS erfarenheter i övrigt har PTS tagit fram tillsynsplaner som styr PTS långsiktiga tillsynsinsatser under 2017-2019[3]. De aktiviteter som genomförts under 2017 i enlighet med tillsynsplanen har avsett tjänstetillhandahållarnas förmåga att upptäcka och internt rapportera incidenter samt tillhandahållares behandling och gallring av uppgifter. Dessa redogörs för i avsnittet om ”Planlagda tillsynsinsatser och slutsatser av dessa”.



Årlig tillsyn avseende inrapporterade incidenter under 2017

Den årliga tillsynen har främst avsett tjänstetillhandahållarnas incidentrapportering till PTS, deras arbete med incidenthantering och deras utveckling av sitt informationssäkerhetsarbete.

Vid möten har tjänstetillhandahållarna redogjort för sina rutiner, verktyg och utbildningsinsatser som används för att kunna upptäcka och rapportera integritetsincidenter. Vidare har tjänstetillhandahållarna redovisat innehållet i sina förteckningar över integritetsincidenter samt redovisat de åtgärder de vidtagit med anledning av inträffade incidenter.

PTS kan konstatera att samtliga tillhandahållare rapporterat integritetsincidenter i enlighet med gällande regelverk; dvs. rapporterna har inkommit i tid och innehåller de uppgifter som krävs, på en tillräckligt detaljerad nivå för att kunna bedöma tillhandahållarens säkerhetsarbete.

PTS har dessutom kunnat konstatera att samtliga tillhandahållare fört förteckning över integritetsincidenter. Några tillhandahållare har dock fått anmärkning vad gäller de uppgifter som ska finnas i förteckningen. I dessa fall har det bland annat varit svårt att utläsa vilka konsekvenser det inträffade kunnat få för drabbade användare. I något fall har PTS fått bristfälliga

[3] Plan för PTS tillsyn avseende säker och konfidentiell kommunikation 2017-2018, dnr 16-12018, och Plan för PTS tillsyn avseende konfidentiell kommunikation 2018-2019, dnr 17-11870

upplysningar om inträffade incidenter vilket har försämrat PTS möjligheter att bedöma behovet av åtgärder från myndighetens sida.

Tillhandahållarna har gett en god bild av de inträffade incidenterna samt vidtagna kortsiktiga och långsiktiga åtgärder i syfte att undvika dem igen. PTS har generellt inom ramen för den årliga tillsynen noterat att integritetsincidenter, som rapporterats till PTS, många gånger orsakas av den mänskliga faktorn. Det kan bero på bristande it-stöd, slarv och okunskap samt manuell hantering av handlingar.

Ett antal av de integritetsincidenter som har drabbat tillhandahållarna kan hänföras till tillhandahållarnas webbtjänster riktade till användarna. Orsakerna till dessa incidenter har exempelvis varit bristande säkerhet i hantering av webbsessioner och användning av felaktig sökmotorindexering, som gjort abonnentuppgifter tillgängliga och sökbara för obehöriga.

Andra incidenter har berott på fel hänförliga till underleverantörer. PTS har i detta sammanhang noterat vikten av att genom avtal och uppföljning av dessa säkerställa att underleverantörerna lever upp till de krav på rutiner och säkerhetsåtgärder som följer av lag och föreskrifter samt att utbildning och kontroll sker av berörd personal.

Några åtgärder som tillhandahållarna har vidtagit med anledning av de inträffade incidenterna är utbildning av medarbetare, översyn av riskanalysmodeller inklusive mallar och rutiner, förtydligande och utökande av testning av egenframtagna webbtjänster, utökad kravställning mot tredjepartsleverantörer av testning och översyn av systemberoenden. Ytterligare åtgärder som har vidtagits är elektronisk identifiering av abonnenter vid kontakt med kundtjänst samt vidareutveckling av system och av tekniska begräsningar för att motverka att personal kan frångå rutiner.

Händelsestyrda tillsynsinsatser och slutsatser av dessa

Nedan återges en kort sammanfattning av de fyra *händelsestyrda* tillsynsinsatser som genomförts sedan föregående tillsynsrapport. De fyra insatserna har avsett fem ärenden.

Åtgärder för förbättrad testmiljö efter sms-incident

I mars 2016 genomförde en operatör en planerad uppdatering i sitt mobilnät. Uppdateringen, som genomfördes i bolagets SMSC (Short Messages Service Center), resulterade i ett fel som innebar att samtliga inkommande sms till operatörens kunder från andra operatörer hamnade hos fel mottagare i den egna operatörens nät.

I och med att incidenten innebar att uppgifter, som förmedlats i samband med tillhandahållande av tjänsten, har avslöjats för obehöriga rapporterades händelsen till PTS som en integritetsincident. Med anledning av det inträffade inledde PTS tillsyn i mars 2016.

Orsaken till den inträffade incidenten var att uppgraderingen innehöll en ny funktionalitet, som inte skulle aktiveras vid det planerade arbetet. Funktionen visade sig vara aktiverad av misstag och innehöll defekt mjukvara som orsakade problemet.

PTS kunde konstatera att operatören återställde den tekniska produktionsmiljön i samband med felavhjälpningen av den icke framgångsrika uppgraderingen. Därefter har sms-plattformen fungerat felfritt. Myndigheten höll dock tillsynsärendet öppet för att följa upp operatörens långsiktiga arbete med att införa en förbättrad testmiljö då en förbättrad testmiljö bedöms öka möjligheterna att undvika en liknande incident.

Operatören har inom ramen för tillsynen uppgett att en erfarenhet är att den testspecifikation som använts i testmiljön inför och vid utförandet av det planerade arbetet i detta fall inte fångade upp grundproblemet. Sett till de identifierade bristerna i testspecifikationen har operatören identifierat åtgärder som ingår i det fortsatta långsiktiga arbetet för att undvika liknande incidenter. Åtgärderna handlar om att utöka interna testspecifikationer med fler testfall och att uppdatera rutinerna för implementation av ny mjukvara i SMSC:n. Dessutom ställer operatören tydligare krav på underleverantörer avseende vilka tester de ska genomföra innan produktionssättning av mjukvaruuppdateringar. Genom ytterligare vidareutveckling av testmiljön kommer operatören erhålla möjlighet att styra testtrafik till testmiljön på ett sätt som kommer att öka likheten till deras produktionsmiljö.

Operatören har vidare inom ramen för tillsynen uppgett att testmiljön för andra typer av tester finns på plats och att den nya testmiljön för mer utökade tester enligt planeringen ska färdigställas under hösten 2018. Utöver ovanstående har operatören uppgett att de moderniseringar som utförts i företagets kommunikationsnät under 2018 kommer att åtgärda en del av de problem som uppgraderingen den 1 mars 2016 syftade till att lösa.

Mot bakgrund av de åtgärder som operatören vidtagit, avskrevs ärendet från vidare handläggning i april 2018. PTS noterade dock att myndigheten kan komma att återkomma till operatörens fortsatta arbete med färdigställandet av den utökade testmiljön i ett fortsatt tillsynsarbete.

Införande av identitetskontroll vid aktivering av SIM-kort via kundtjänst

I oktober 2016 inledde PTS en tillsyn mot en operatör gällande vidtagande av lämpliga tekniska och organisatoriska åtgärder för att säkerställa skyddet av uppgifter som behandlas i samband med tillhandahållande av elektroniska kommunikationstjänster. Tillsynen föranleddes av att två olika anställda i operatörens kundtjänst på uppmaning av en inringande person hade flyttat över mobilabonnemang till nya SIM-kort. Abonnemangen tillhörde i inget av fallen den person som hade kontaktat kundtjänsten.

Under tillsynens gång inkom operatören med skriftliga svar på frågor PTS ställt och deltog även vid ett tillsynsmöte. Operatören redogjorde då för hur deras organisation är uppbyggd när det gäller kundtjänst och orsakerna till de två incidenterna. Operatören redogjorde dessutom för att de först införde en behörighetsbegränsning för personal i kundtjänst. Därefter infördes en mer permanent lösning som innebär att personer som ringer in till kundtjänst ska legitimera sig via bank-ID för att få överföra abonnemang till ett annat SIM-kort.

PTS bedömde därmed att operatören vidtagit en sådan lämplig teknisk och organisatorisk åtgärd som krävs för att skydda uppgifter som behandlas i samband med tillhandahållande av en mobiltelefonitjänst och för att minska risken för att incidenter av aktuellt slag uppstår. Ärendet avskrevs därför från vidare handläggning i april 2018.

Genomförande av riskanalyser för samtliga tillgångar

I juni 2017 inledde PTS en tillsyn mot en operatör avseende de analyser som operatören genomfört när det gäller riskerna för integritetsincidenter för identifierade informationsbehandlingstillgångar. Tillsynen föranleddes av att det i en tidigare tillsyn mot operatören framkommit att denne endast hade genomfört riskanalyser för en begränsad del av bolagets informationsbehandlingstillgångar. Syftet med tillsynen var att granska operatörens arbete med att genomföra riskanalyser för bolagets samtliga informationsbehandlingstillgångar. Detta är ett krav enligt 4 § andra stycket PTSFS 2014:1.

Under tillsynens gång begärde PTS månatligen in en redovisning avseende hur arbetet med genomförande av riskanalyser fortskred. Därutöver hölls tillsynsmöten med operatören varvid det bland annat redogjordes för det särskilda projekt som tillsats i syfte att genomföra riskanalyser för samtliga identifierade informationsbehandlingstillgångar. Operatören redogjorde också för hur riskanalyserna genomförts enligt en standardiserad modell och att analyserna justeras kontinuerligt och i samband med integritetsincidenter.

PTS bedömde därefter att operatören uppfyller kravet om att tjänstetillhandahållare ska analysera risken för integritetsincidenter för de informationsbehandlingstillgångar som identifierats. Ärendet avskrevs från vidare handläggning i juni 2018.

Behandling av trafikuppgifter och innehåll i datatrafiken för att kunna särskilja trafik till vissa tjänster på internet

Flera teleoperatörer har erbjudanden som innebär att abonnenterna kan nyttja sociala medier eller vissa musiktjänster utan att användningen belastar surfpotten.

PTS inledde tillsyn mot en operatör 2015 genom att fråga på vilket sätt företaget identifierar och särskiljer viss typ av trafik. PTS frågade också hur företaget informerar användarna och om de inhämtar samtycke från

användarna för denna behandling i enlighet med reglerna i 6 kap LEK med anledning av bolagets erbjudande. I juli 2017 beslutade PTS att inleda en tillsyn mot ytterligare en operatör som har liknande erbjudanden.

PTS har granskat hur de båda operatörerna identifierar vilken datatrafik som ska belasta användarnas surfpotter och vilken som inte ska göra det. Att behandla innehållet i användarnas trafik, utan deras samtycke, strider mot reglerna om konfidentiell kommunikation i LEK.

PTS anser att en av operatörerna följer reglerna och har därför avslutat tillsynen mot denna i januari 2018. Myndigheten anser däremot att den andra operatören behöver inhämta användarnas samtycke för att få fortsätta sortera användarnas datatrafik på det sätt som sker. Anledningen till att PTS gör olika bedömningar är att den första operatören endast behandlar information om vilka ip-adresser som genererar datatrafiken, medan den andra även behandlar innehållet i användarnas datatrafik. PTS har därför underrättat denna operatör om att de senast den 1 juli 2018 ska ha hämtat in samtycke från de användare som har erbjudandet fri surf. Alternativt kan bolaget välja att sluta behandla innehållet i datatrafiken.

Planlagda tillsynsinsatser och slutsatser av dessa

Detta avsnitt redogör i korthet för de två *planlagda* tillsynsinsatser som PTS har genomfört sedan föregående tillsynsrapport. De två insatserna har avsett sex ärenden.

Lagring och gallring av trafikuppgifter

Trafikuppgifter är uppgifter som behandlas för att kunna överföra information i ett elektroniskt kommunikationsnät eller för att fakturera sådan överföring. Med trafikuppgifter avses alltså inte själva innehållet som överförs, utan uppgifter som beskriver överföringen, t.ex. uppgift om vilka telefonnummer som kommunicerat med varandra och när detta skett. Tillhandahållare av elektroniska kommunikationsnät- och tjänster behandlar normalt en stor mängd trafikuppgifter i sina verksamheter.

PTS inledde 2013 en planlagd tillsyn mot en tillhandahållare för att särskilt granska de trafikuppgifter som genereras och behandlas vid tillhandahållandet av mobila kommunikationstjänster.

Trafikuppgifter kan innehålla information som av användarna av elektroniska kommunikationstjänster betraktas som mycket känslig. PTS såg därför ett behov av utreda vilka trafikuppgifter som behandlas och hur länge och med vilken rättslig grund lagring av uppgifterna sker samt hur uppgifterna raderas (gallras).

Operatören har under tillsynens gång vid ett flertal tillfällen, på myndighetens begäran, lämnat uppgifter skriftligen till PTS och i samband med möten lämnat kompletterande upplysningar. Operatören har även demonstrerat de tekniska

system som används vid lagring av trafikuppgifter för kommersiella ändamål. Operatören har redogjort för vilka trafikuppgifter bolaget behandlar, för vilka ändamål de behandlas, på vilket sätt och hur länge uppgifterna lagras, samt för hur och när de gallras. PTS har valt att härvid i synnerhet granska den lagring och gallring av trafikuppgifter som operatören uppgivit att man gör för följande ändamål:

- Lagring och gallring av uppgifter för överföring av elektronisk kommunikation
- Avslöjande av obehörig användning (anti fraud)
- Avräkning av samtrafikavgifter (Interconnect)
- Fakturering och prissättning
- Affärs- och kundanalys samt marknadsföring (Business Intelligence)
- Felsökning

Vidare granskade PTS hur uppgifter används, lagras och gallras i ett särskilt system (medieringssystem), där uppgifterna lagras i rådataformat.

PTS kunde konstatera att den berörda operatören hade stöd för de behandlingar som utfördes och de gallringsfrister som tillämpades, antingen direkt i enlighet med bestämmelserna i 6 kap. LEK eller med stöd av inhämtat samtycke varför tillsynen avslutades.

Tillsyn av tillhandahållarnas förmåga att identifiera och internt rapportera integritetsincidenter

Tjänstetillhandahållare är skyldiga att rapportera integritetsincidenter till PTS. PTS inledde under 2017 en särskild tillsyn av de fem största tjänstetillhandahållarnas förmåga att identifiera och internt rapportera integritetsincidenter. Myndigheten inledde granskningen utifrån bedömningen att det troligen inträffar betydligt fler integritetsincidenter än de som rapporteras.

Tillsynen tog sin utgångspunkt i kravet i 10 § PTSFS 2014:1 om att tjänstetillhandahållare ska ha dokumenterade rutiner för att identifiera och internt rapportera integritetsincidenter. I tillsynen granskades förmågan hos tjänstetillhandahållarens medarbetare och uppdragstagare att identifiera och förstå när en händelse utgör en integritetsincident. Tillsynen omfattade inte tjänstetillhandahållarens tekniska åtgärder, såsom loggning eller övervakning, för att upptäcka en incident.

Tillsynen avslutades i juni 2018. PTS anser att operatörernas rutiner nu är ändamålsenliga och att samtliga har ett systematiskt arbetssätt för att rapportera integritetsincidenter internt. Myndigheten anser dock att det finns utrymme för operatörerna att utveckla sin förmåga att identifiera integritetsincidenter.

PTS har generellt inom ramen för tillsynen noterat att de integritetsincidenter som fångas upp och rapporteras av tjänstetillhandahållare framför allt är sådana

som har uppmärksammats av kunder och rör händelser där obehöriga har kommit åt uppgifter till följd av bristande skydd. Detta till skillnad från incidenter som t.ex. ännu inte har uppmärksammats av kunder eller som till sin natur är sådana att kunder kan ha svårt att upptäcka dem på egen hand, t.ex. händelser där uppgifter gått förlorade eller ändrats till följd av bristande skydd. Det skulle kunna bero på att andra delar än kundtjänst inte identifierar de händelser som rapporteras i organisationen som integritetsincidenter eller att det inte proaktivt kontrolleras om integritetsincidenter har inträffat. PTS tror därför fortfarande att det sannolikt inträffar händelser som inte identifieras som integritetsincidenter, och som aldrig rapporteras internt hos tillhandahållaren, och därmed inte heller till PTS.

Efter en helhetsbedömning av tjänstetillhandahållarnas åtgärder har dock att myndigheten beslutat att avsluta sin granskning.