Nätsäkerhetsavdelning

[redacted]

Genomförd tillsyn avseende säker och konfidentiell kommunikation under 2016

PTS arbete med tillsyn 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 konfidentialitet och personlig integritet. Målet med PTS arbete inom området är att alla i Sverige ska kunna kommunicera elektroniskt utan att riskera att informationen kommer på avvägar eller används på ett oönskat sätt.

Lagen (2003:389) om elektronisk kommunikation (LEK) innehåller regler om konfidentiell kommunikation och integritetsskydd som gäller tillhandahållare av elektroniska kommunikationsnät och -tjänster. Bland annat finns regler om under vilka förutsättningar och hur länge trafik- och lokaliseringsuppgifter får behandlas, 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. [1]

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

[1] Post- och telestyrelsens föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter, PTSFS 2014:1
[2] Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott

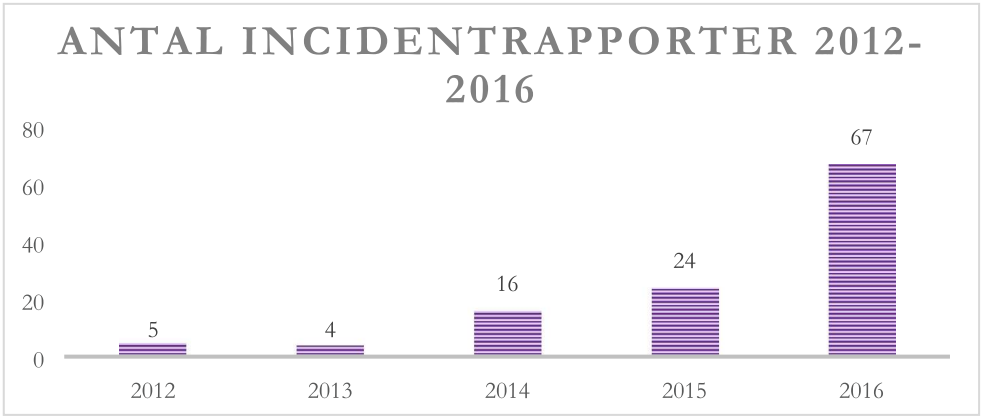
Rapporterna kan även ge PTS anledning att misstänka att bestämmelserna om integritetsskydd inte efterlevs och i sådana fall bedriva tillsyn.

Närmare om PTS tillsynsarbete under 2016

PTS granskar löpande de rapporter om integritetsincidenter som inkommer. PTS bedriver även egen omvärldsbevakning vad gäller inträffade incidenter. I händelse av mer omfattande eller principiellt intressanta incidenter kan PTS komma att inleda händelsestyrd tillsyn, som regel inriktad på att granska orsakerna till den inträffade händelsen och tillhandahållarens arbete för att förebygga att liknande händelser inträffar igen. Under 2016 har PTS fått in 67 rapporter om integritetsincidenter. PTS har under 2016 beslutat att inleda tillsyn i anslutning till sex av de inrapporterade incidenterna. En av dessa tillsyner har avsett fyra olika inrapporterade incidenter.

Inom ramen för PTS långsiktiga arbete följer PTS upp de större tillhandahållarnas arbete med att hantera och dra lärdomar av inträffade incidenter genom en planlagd årlig tillsyn. Tillsynen omfattar samtliga integritetsincidenter som inträffat för berörda tjänstetillhandahållare under i första hand föregående år och som inte redan har granskats inom ramen för händelsestyrd tillsyn. Under 2016 har PTS genomfört årlig tillsyn som omfattat de fem största tjänstetillhandahållarna.

PTS har tagit fram tillsynsplaner för myndighetens tillsynsarbete under 2016-2018[3]. De aktiviteter som genomförts under 2016 i enlighet med tillsynsplanen har avsett hur tjänstetillhandahållarna kartlägger och förtecknar sina informationsbehandlingstillgångar där behandlade uppgifter förekommer samt genomför riskanalyser för att tillgångarna drabbas av integritetsincidenter. Denna tillsyn har omfattat sex tjänstetillhandahållare.



[3] Se ”Plan för PTS integritetstillsyn 2016-2017”, Dnr 15–11631 och ”Plan för PTS tillsyn avseende säker och konfidentiell kommunikation 2017-2018”, Dnr 16-12018.

Årlig tillsyn avseende inrapporterade incidenter under 2016

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 redogjort för innehållet i sina förteckningar över integritetsincidenter samt redovisat de åtgärder de vidtagit med anledning av inträffade incidenter.

PTS har kunnat konstatera att samtliga tillhandahållare för 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 upplysningar om inträffade incidenter vilket har försämrat PTS möjligheter att bedöma behovet av åtgärder från myndighetens sida.

Definitionen av vad som utgör en integritetsincident är vid och PTS har i samband med de årliga tillsynsmötena förklarat att myndigheten bedömer det som sannolikt att det hos många tillhandahållare kan finnas fler integritetsincidenter än de som rapporterats till myndigheten under det gångna året. PTS har redogjort för att myndigheten därför ser positivt på det intensifierade arbete tillhandahållarna bedriver för att utbilda personal i sina organisationer och skapa en medvetenhet om integritetsincidenter för att dessa ska rapporteras snabbt både internt och till PTS. Det är bland annat mot bakgrund av vikten att på ett tidigt stadie kunna upptäcka och rapportera incidenter som PTS inlett en särskild planlagd tillsyn rörande upptäckt och intern rapportering under 2017.

Ett antal av de incidenter som drabbat tillhandahållarna har berott på felorsaker 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.

Händelsestyrda tillsynsinsatser och slutsatser av dessa

Nedan återges en kort sammanfattning av de händelsestyrda tillsynsinsatser som avslutats under 2016.

I juni 2015 inleddes en tillsyn 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 en tidigare anställd olovligen kopierat en kunddatabas som sedan använts i eget försäljningssyfte.

Kunddatabasen innehöll ett stort antal uppgifter som omfattat både kunduppgifter som namn, personnummer och telefonnummer men även uppgifter om kundens abonnemang i form av start- och slutdatum på abonnemang och abonnemangsform.

Inom ramen för tillsynen beskrev tjänsteleverantören sina system för åtkomst- och behörighetshantering samt den översyn som genomförts av dessa efter den inträffade incidenten. PTS påpekade vikten av att kontinuerligt arbeta med att säkerställa att rutinerna för åtkomst- och behörighetshantering löpande följs upp för att bland annat säkerställa att dessa är på lämplig nivå, samt att gamla behörigheter tas bort om en anställd slutar eller byter tjänst. PTS konstaterade vidare att det tagit lång tid för tjänsteleverantören att upptäcka incidenten, samt att man blivit varse om det inträffade först efter tips från utomstående. Detta har kunnat hänföras till brister i tjänsteleverantörens rutiner för kontroll av loggar. Tjänsteleverantören uppgav att man tagit fram rutiner för kontroll av loggar som bland annat innebär kontroll av viss typ av aktivitet och avvikande mönster i användningen. Vidare genomfördes kontinuerliga kontroller av loggar, vilka också dokumenterades. Tjänsteleverantören uppgav vidare att man förbättrar de verktyg som används för granskningen av loggar och det arbetet bedöms vara klart under 2017. Med påpekandet att PTS kan komma att granska de nya rutinerna och systemen efter att dessa implementerats i verksamheten avskrevs ärendet i december 2016.

I mars 2016 inleddes, efter anmälan, en tillsyn avseende behandling av trafikuppgifter för vissa ändamål utan att den som uppgifterna berört hade samtyckt innan behandlingen skedde. I det aktuella ärendet hade tjänstetillhandahållaren i samband med abonnentupplysning per telefon tagit del av den uppringandes telefonnummer trots att abonnenten begärt att numret skulle vara hemligt. Anmälaren reagerade på att tjänstetillhandahållaren i samband med abonnentupplysning erbjöd att skicka svaret på nummerförfrågan till anmälaren per sms, trots att denne hade hemligt nummer. Den aktuella tjänstetillhandahållaren bedriver nummerupplysningsverksamhet men är även anmäld till PTS såsom tillhandahållare av elektroniska kommunikationstjänster och hade i den sistnämnda egenskapen möjlighet att ta del av de nummer som förmedlas i näten, bland annat den uppringandes telefonnummer (s.k. A-nummer). PTS bedömde att tillhandahållande av abonnentupplysning inte är en elektronisk kommunikationstjänst och att behandling av A-nummer för detta ändamål därmed fordrade samtycke enligt 6 kap. 6 § LEK. Den behandling som skedde genom att A-numret gjorts tillgängligt för användning i abonnentupplysningsverksamheten bedömdes, i avsaknad av samtycke, stå i strid med reglerna i 6 kap. 5-7 §§ LEK. Efter att tjänstetillhandahållaren genomfört tekniska förändringar så att företagets telefonister inte längre kan se uppringarens nummer eller skicka sms till numret, i de fall abonnentens samtycke saknades, avskrevs ärendet från vidare handläggning i april 2017.

PTS inledde i juni 2016 en tillsyn gällande krav på underrättelser till abonnenter och enskilda personer som berörts av en integritetsincident. PTS kunde i det

aktuella ärendet konstatera att den berörda tjänstetillhandahållaren till viss del brustit i underrättelser till berörda abonnenter och användare, såväl vad gällde bedömningen av vilka personer som skulle underrättas, tiden för underrättelse samt innehållet i den information som lämnats till berörda abonnenter. Tjänsteleverantören ändrade under tillsynen sina rutiner för att säkerställa att rätt information skulle ges i rätt tid och att man på rätt sätt skulle kunna bedöma i vilken kanal berörda skulle underrättas. Efter att ha tagit del av tjänsteleverantörens rutiner har PTS avskrivit ärendet i september 2016.

Planlagda tillsynsinsatser och slutsatser av dessa

Tillsyn av kartläggning och förteckning av informations-behandlingstillgångar

PTS inledde i april 2016 en granskning för att kontrollera om ett urval operatörer följer myndighetens föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter. Syftet har varit att säkerställa att operatörerna skyddar abonnenters och användares integritet i samband med tillhandahållande av tjänsterna. Inledningsvis valde PTS att kontrollera att operatörerna har identifierat och dokumenterat de system, databaser och fysiska tillgångar som används för informationsbehandling.

Efter att PTS genomfört tillsynsmöten med samtliga tillsynsobjekt som omfattats av tillsynen har PTS kunnat konstatera att det återkommande hade förelegat vissa generella brister hos tillsynsobjekten. Dessa brister har främst varit relaterade till tolkningen av vissa för tillsynen relevanta begrepp, såsom begreppet ”informationsbehandlingstillgång”. PTS bedömning är att denna typ av tillgång inte bara behandlar trafikuppgifter, abonnentuppgifter och lokaliseringsuppgifter – utan även uppgiftskategorin *uppgifter i ett elektroniskt meddelande* (innehåll). Detta innebär att berörda tjänstetillhandahållares förteckningar och övriga säkerhetsarbete även gäller för de informationsbehandlingstillgångar som används i samband med överföring av innehållet i elektroniska meddelanden.

Alla fysiska tillgångar som används för informationsbehandling, dvs. behandlar uppgifter, ska dokumenteras. Som exempel på fysiska tillgångar som typiskt sett behandlar uppgifter kan anges routrar, switchar, servrar, aktiva fysiska förbindelser och media converters. Till stöd för bedömningen av vilka tillgångar som omfattas bör operatören, enligt PTS bedömning, utreda vilka tillgångar som skulle kunna drabbas av en integritetsincident, genom att t.ex. ställa sig frågan om den fysiska tillgången på något sätt, oavsiktligt eller otillåtet, kan vara föremål för utplåning, förlust, ändring, avslöjande eller åtkomst till behandlade uppgifter.

Det andra begreppet där flera operatörer inte har haft samma tolkning som PTS är *uppgifter som behandlas i samband med tillhandahållandet av tjänsten*. Begreppet återfinns både i föreskrifterna och i 6 kap. 3 § LEK.

Det finns, enligt PTS bedömning, ingen begränsning i de tillämpliga reglerna avseende vilka uppgifter som omfattas av begreppet, utan i vart fall samtliga uppgiftskategorier som omnämns i 6 kap. LEK omfattas. Dessa kategorier utgörs åtminstone av

- uppgifter i ett elektroniskt meddelande (innehåll) (t.ex. 6 kap. 17 § LEK),
- uppgifter om abonnemang (6 kap. 20 § LEK),
- lokaliseringsuppgifter (t.ex. 6 kap. 9 § LEK) och
- trafikuppgifter (t.ex. 6 kap. 5 § LEK).

Den kategori som PTS genom tillsynen har kunnat konstatera att operatörer generellt har haft okunskap rörande har varit ”uppgifter i elektroniska meddelanden”, dvs. meddelandens innehåll. Enligt PTS bedömning utgör denna kategori ofta den mest integritetskänsliga av de kategorier som omfattas av uttrycket ”uppgifter som behandlas vid tillhandahållandet av tjänsten”.

PTS har vidare inom ramen för tillsynen konstaterat att flera av operatörerna i sin förteckning endast har angett en kategori av uppgifter och att den ofta har kallats ”personuppgifter”. Även om t.ex. trafikuppgifter mycket väl kan utgöra personuppgifter skyddas i LEK inte bara personuppgifter utan även t.ex. uppgifter om företag och själva konfidentialiteten i kommunikationen, oavsett om den går att härleda till en viss person eller inte.

När det gäller den information som en godtagbar förteckning bör innehålla konstaterar PTS att förteckningen bör vara ändamålsenlig för de efterföljande kraven i föreskrifterna. Förteckningen bör således kunna användas som underlag till de riskanalyser som ska genomföras för samtliga informationsbehandlingstillgångar, samt för de skyddsåtgärder som ska vidtas efter riskanalyserna. Enligt PTS bedömning är det mot bakgrund av detta lämpligt att i sin förteckning inkludera information om
- vilken eller vilka uppgifter som en specifik tillgång behandlar,
- namn på tillgången och dess funktion,
- placering (fysiska tillgångar),
- vem som ansvarar för den, samt
- en hänvisning till den riskanalys, eller de riskanalyser, som genomförts för tillgången.

Slutligen har PTS kunnat konstatera att det i flera fall har förelegat vissa tveksamheter gällande hur ofta förteckningen över informationsbehandlings-tillgångar uppdateras. Flera operatörer har uppgivit att detta sker årligen inom ramen för en befintlig process. Kravet i föreskrifterna är dock att förteckningen, utöver årlig revision, ska ses över ”vid behov”.

Även om flera operatörer har uppgivit att man även ser över förteckningen vid anskaffning av nya tillgångar eller vid avveckling, har det förekommit att operatörer har saknat en process som säkerställer att förteckningen även uppdateras t.ex. vid förändringar av befintliga tillgångar.

Tillsynen av kartläggning och förteckning av informationsbehandlingstillgångar avslutades i februari 2017.