Datum 2016-04-29

Vår referens Dnr: 16-1402

Nätsäkerhetsavdelningen

[redacted]

Tele2 Sverige AB

Årlig tillsyn över incidentrapportering och inträffade integritetsincidenter – Tele2 Sverige AB

Saken

Tillsyn över incidentrapportering och inträffade integritetsincidenter.

Post- och telestyrelsens avgörande

Post- och telestyrelsen (PTS) avskriver ärendet från vidare handläggning.

Bakgrund

PTS genomför årligen planlagd tillsyn över ett urval operatörer, bland annat i syfte att dessa ska redogöra för inträffade incidenter under föregående år. Tillsynen omfattar såväl driftstörningar som integritetsincidenter, vilka operatörerna är skyldiga att rapportera in till PTS.

Ett av huvudsyftena med inrapporteringsskyldigheten är att PTS ska kunna göra en bedömning av om det finns skäl att misstänka att bestämmelser i lagen (2003:389) om elektronisk kommunikation (LEK), t.ex. bestämmelsen om skydd av behandlade uppgifter i 6 kap. 3 § LEK, inte efterlevs. Även i de fall en incidentrapport till PTS inte ger upphov till direkta tillsynsåtgärder, kan incidentrapporten innehålla uppgifter som bidrar till myndighetens kunskap om vanliga orsaker till integritetsincidenter. Detta kan i sin tur utgöra underlag för PTS planlagda tillsynsinsatser.

PTS inledde den 17 februari 2016 den planlagda årliga tillsynen rörande incidentrapportering och inträffade integritetsincidenter över Tele2 Sverige AB (Tele2). Den 2 mars 2016 höll PTS ett tillsynsmöte med Tele2.

Vid mötet visade Tele2 sitt nya incidentrapporteringssystem, samt gick igenom de fyra incidenter som rapporterats in under föregående år och de åtgärder som vidtagits med anledning av dessa. Tele2 informerade också om att bolaget ger fortlöpande utbildning i incidenthantering till dem som berörs av detta.

Två av de aktuella incidenterna bestod i att A-nummer förväxlades, så att innehåll i meddelanden kom till fel mottagare. I det ena fallet orsakades detta av en driftstörning i nätet, i det andra fallet av ett mjukvarufel i samband med förändringsarbete. Tele2 valde bland annat att underrätta berörda abonnenter och användare om dessa båda incidenter i ett gemensamt pressmeddelande. Incidenterna rapporterades in den 23 februari och den 17 april, men pressmeddelandet kom först i början av juli 2015. Tele2 har uppgett att man har dragit lärdomar från detta och att bolaget alltjämt bedömer att media är en bra kanal för information vid större fel som detta där alla drabbade inte har kunnat identifieras. Tele2 uppgav vidare att en annan lärdom man dragit från incidenterna var att bolaget behöver involvera fler personer vid ändringar eller arbeten i den här typen av system för att ge större transparens internt.

En av de rapporterade incidenterna orsakades av en sårbarhet i ett system, vilken utnyttjats för bedrägeri. En annan incident orsakades av att personal i butik inte följde gällande rutiner och processer kring aktivering av SIM-kort. Genom förändringar av kraven vid inloggning uppgav Tele2 att man förbättrat kontrollen över säljare, både bolagets egna och hos återförsäljare. Tele2 redogjorde vid mötet också för en insats som genomförts för att medvetandegöra all berörd personal om vikten av att rutiner och processer följs och för att uppmuntra inrapportering av incidenter.

Skäl

Tillämpliga bestämmelser

PTS är enligt 2 § förordningen (2003:396) om elektronisk kommunikation tillsynsmyndighet enligt LEK. PTS ska enligt 7 kap. 1 § LEK utöva tillsyn över efterlevnaden av lagen och de beslut om skyldigheter eller villkor samt de föreskrifter som meddelats med stöd av lagen.

Enligt 6 kap. 3 § LEK ska den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas. Den som tillhandahåller ett allmänt kommunikationsnät ska vidta de åtgärder som är nödvändiga för att upprätthålla detta skydd i nätet. Åtgärderna ska vara ägnade att säkerställa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsincidenter.

Enligt 6 kap. 4 a § LEK ska den som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster utan onödigt dröjsmål underrätta tillsynsmyndigheten om integritetsincidenter. Om incidenten kan antas inverka negativt på de abonnenter eller användare som de behandlade uppgifterna berör, eller om tillsynsmyndigheten begär det, ska även dessa underrättas utan onödigt dröjsmål. När och hur rapportering ska ske framgår av Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott.

Av PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1) framgår bland annat följande:

Tjänstetillhandahållarens säkerhetsarbete avseende behandlade uppgifter ska enligt 3 § bedrivas långsiktigt, kontinuerligt och systematiskt och det ska finnas en tydlig rollfördelning med särskilt utpekade ansvariga. Rutiner, processer och rollfördelning ska dokumenteras.

Tjänstetillhandahållaren ska enligt 4 § bland annat identifiera informations-behandlingstillgångar och föra en förteckning över dessa samt analysera riskerna för att integritetsincidenter inträffar för de identifierade informationsbehandlingstillgångarna. Vidtagna skyddsåtgärder samt tjänstetillhandahållarens bedömningar av lämplig nivå för hantering av riskerna ska dokumenteras och följas upp årligen och vid behov.

Tjänstetillhandahållaren ska enligt 10 § ha dokumenterade rutiner för identifiering, intern rapportering, hantering och uppföljning av integritetsincidenter. Rutinerna ska säkerställa

1. att samtliga uppgifter i 11 § förs in i den förteckning som tjänstetillhandahållaren ska föra enligt 6 kap. 4 b § lagen (2003:389) om elektronisk kommunikation,
2. att inträffade integritetsincidenter och dess orsaker beaktas vid genomgång av riskanalyser i enlighet med 4 §, och
3. att skyddsåtgärder vidtas för att undvika liknande integritetsincidenter.

Enligt 6 kap. 4 b § LEK ska tjänstetillhandahållaren löpande föra en förteckning över integritetsincidenter. Vad förteckningen närmare ska innehålla framgår av 11 § i de ovannämnda föreskrifterna.

PTS bedömning

Inledningsvis kan PTS konstatera att Tele2 hade förberett sig väl inför tillsyns-mötet den 2 mars 2016. PTS bedömer att Tele2:s förberedelser inför mötet förkortar tiden för tillsyn och underlättar för myndigheten att bedöma om t.ex. rutiner för incidenthantering och säkerhetsarbetet i övrigt uppfyller lagens krav.

PTS konstaterar också att Tele2 under året rapporterat in fyra incidenter till PTS, vilket är samma antal som året dessförinnan. Definitionen av vad som utgör en integritetsincident är mycket vid, och PTS bedömer det som sannolikt att det inträffar integritetsincidenter i Tele2:s verksamhet som inte upptäcks eller rapporteras till PTS. PTS ser positivt på det arbete Tele2 gör för att utbilda berörd personal om upptäckt och rapportering av integritetsincidenter och förväntar att dessa förändringar medför att fler incidenter kan upptäckas och rapporteras till myndigheten. Under 2016 har PTS planlagt en tillsynsinsats för att kontrollera tillhandahållares förmåga att upptäcka och rapportera integritets-incidenter. Denna fråga kan således komma att bli föremål för en framtida granskning under 2016. Med dessa påpekanden lämnar PTS denna del av tillsynen utan åtgärd.

Avseende Tele2:s underrättelser till berörda abonnenter och användare kan PTS konstatera att ett pressmeddelande kan utgöra en del av informationen kring en incident för att nå ut till alla berörda. Enligt art 3 p. 6 i förordningen ska kommunikationen ges på ett sätt som säkerställer att informationen snabbt kan mottas. Informationen ska enligt samma punkt enbart omfatta uppgifter om det aktuella personuppgiftsbrottet, och inte innehålla uppgifter om något annat ämne. Att dock endast lämna informationen genom ett pressmeddelande kan enligt PTS uppfattning inte anses följa kraven i förordningen. Det är inte en metod som säkerställer att informationen snabbt kan mottas, då det är svårt att förutse spridningen i media, och då informationen inte tydligt riktar sig direkt till de berörda. Inte heller är det lämpligt att slå samman information om två incidenter i samma kommunikation. Det är också viktigt att informationen innehåller alla de uppgifter som krävs enligt bilaga II till förordningen. I pressmeddelandet saknas främst information om de förmodade konsekvenserna av personuppgiftsbrottet för den berörda abonnenten eller enskilda personen. För det fallet att berörda abonnenter och användare inte kan identifieras och nås individuellt ska enligt art. 3 punkten 7 i förordningen annonsering ske i större nationella eller regionala medier. Underrättelsen ska också göras utan onödigt dröjsmål och att det dröjde över fyra månader efter den första incidenten innan Tele2 gick ut med pressmeddelandet anser PTS vara anmärkningsvärt och får anses klart överskrida denna tidsfrist. PTS har dock valt att inte gå vidare i denna del men förutsätter att Tele2 i framtiden säkerställer att gällande regler om underrättelse till berörda användare eller enskilda följs. Med detta påpekande lämnar PTS saken utan ytterligare åtgärd.

Två av de aktuella incidenterna hänför sig till bristande säkerhet i återförsäljar-ledet. PTS förutsätter att Tele2:s åtgärder för att göra berörd personal medveten om vikten av att följa rutiner och processer ska öka säkerheten i denna del. PTS har planlagt en tillsynsinsats under 2016 vad gäller skyddsåtgärder vid åtkomst till uppgifter i butiker och hos underleverantörer. En sådan tillsyn kan komma

att omfatta Tele2. Med detta påpekande lämnar PTS även denna del av tillsynen utan åtgärd i dagsläget.

Skäl att fortsätta tillsynen föreligger därför inte, varför ärendet avskrivs från vidare handläggning.

Beslutet har fattats av enhetschefen Patrik Bystedt. I ärendets slutliga handläggning har även juristerna Anders Lindell (föredragande) och Karin Lodin deltagit.