Datum 2015-06-16
Vår referens Dnr: 15-1627

Nätsäkerhetsavdelningen
Karin Lodin
08-678 56 04
karin.lodin@pts.se

Årlig tillsyn över incidentrapportering och inträffade integritetsincidenter – Tele2 Sverige AB

Saken

Tillsyn över incidentraportering och inträffade integritetsincidenter.

Post- och telestyrelsens avgörande

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

Bakgrund

PTS genomför årligen planlagda tillsyner över ett urval operatörer, bland annat i syfte att dessa ska redogöra för inträffade incidenter under föregående år. Tillsynerna 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 20 februari 2015 den planlagda årliga tillsynen rörande incidentrapportering och inträffade integritetsincidenter över Tele2 Sverige AB (Tele2). Den 30 mars 2015 höll PTS ett tillsynsmöte med Tele2.

Vid mötet beskrev Tele2 sina rutiner för rapportering av integritetsincidenter och hur bolaget hanterar dessa. Tele2 informerade bland annat om att bolaget har information och utbildning om intern rapportering av integritetsincidenter på sitt intranät. Samtliga anställda, och även bolagets samarbetspartners, har tillgång till Tele2s incidentrapporteringssystem.

Tele2 redogjorde även för de fyra integritetsincidenter som rapporterats in till PTS under föregående år och vilka åtgärder som hade vidtagits med anledning av dessa. Tele2 presenterade även sin förteckning över integritetsincidenter, som liksom föregående år utgörs av ett system där man för att få fram underliggande information behöver klicka sig vidare från listan med incidenter.

Vid mötet redogjorde Tele2 även för sina underrättelser om inträffade integritetsincidenter till berörda abonnenter och användare. När det gäller två incidenter hade en underrättelse gått ut till berörda abonnenter och användare i vilka Tele2 informerade om att man hade vidtagit ”alla nödvändiga åtgärder”, utan att ange vilka dessa åtgärder var. I dessa två underrättelser fanns vidare ingen information om rekommenderade åtgärder för abonnenter och användare att vidta för att mildra den tänkbara menliga inverkan av incidenterna.

Vid mötet redogjorde Tele2 även för hur bolaget arbetar med riskanalyser på integritetsområdet, och status för bolagets efterlevnad av PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1). Enligt uppgift från Tele2 vid mötet hade ett arbete med att efterleva föreskrifterna initierats, men bolaget efterlevde ännu inte föreskrifterna fullt ut, främst avseende genomförande av riskanalyser och vidtagande av efterföljande skyddsåtgärder. Tele2 uppgav härvid att man definierat ett antal åtgärdspunkter och tillsatt ett projekt för att uppfylla kraven. Inom ramen för detta har ett inventeringsarbete genomförts där samtliga system som hanterar uppgifter enligt föreskrifterna har markerats inför kommande skyddsåtgärder.

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 informationsbehandlingstillgångar 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 under det föregående året har rapporterat in fyra integritetsincidenter till PTS, vilket är lika många som föregående år. Mot bakgrund av att definitionen av vad som utgör en integritetsincident är så vid bedömer PTS att det inte kan uteslutas att det inträffar integritetsincidenter i Tele2s verksamhet som inte upptäcks och rapporteras till PTS. Tele2 har dock byggt upp en plattform för intern rapportering av integritetsincidenter och genomför utbildningar för personalen, vilket PTS ser positivt på. PTS bedömer dock att arbetet med att säkerställa att processerna för upptäckt och intern rapportering också följs och uppdateras över tid är ett kontinuerligt arbete som Tele2 uppmanas att utveckla och förbättra, i syfte att bland annat öka möjligheten att upptäcka och rapportera integritetsincidenter till PTS. Med detta påpekande lämnar PTS denna del av tillsynen utan åtgärd.

När det gäller Tele2s förteckning över integritetsincidenter upprepar PTS sin uppmaning från föregående år, dvs. att Tele2 vid presentation för PTS bör tillhandahålla en förteckning som visar samtliga uppgifter som enligt 11 § i föreskrifterna måste finnas med i förteckningen, utan att PTS måste efterfråga kompletterande information. För Tele2s interna bruk är det godtagbart att ha ett system som kräver att man klickar vidare på en viss incident för att få tillgång till efterfrågad information. Vid presentation för PTS är det dock viktigt att myndigheten ges tillgång till all information, så att en bedömning kan göras huruvida förteckningen följer kraven enligt föreskrifterna. PTS lämnar med ovannämnda uppmaning denna del av tillsynen utan ytterligare åtgärd.

Avseende Tele2s underrättelser till berörda abonnenter och användare kan PTS konstatera att det förelegat vissa brister i informationen som skickats, i och med att underrättelserna inte fullt ut följt kraven enligt förordningen (se lista på vad underrättelserna ska innehålla i förordningens Bilaga 2). Tele2 har i underrättelserna inte tillräckligt utförligt beskrivit vilka åtgärder som bolaget har vidtagit med anledning av incidenterna och har inte heller angett vilka, om några, åtgärder som de berörda abonnenterna och användarna kan vidta för att minska den negativa effekten av incidenterna. Utan utförligare information om vilka åtgärder som har vidtagits av Tele2 eller kan vidtas av berörda abonnenter och användare kan de som drabbats inte fullt ut bedöma potentiella konsekvenser av incidenterna och vilka eventuella åtgärder som den enskilde kan vidta för att begränsa sin negativa påverkan. PTS förutsätter att Tele2 vid

kommande underrättelse ser till att samtlig information som måste inkluderas i underrättelserna skickas till berörda abonnenter och användare. Med detta lämnar PTS även denna del av tillsynen utan åtgärd.

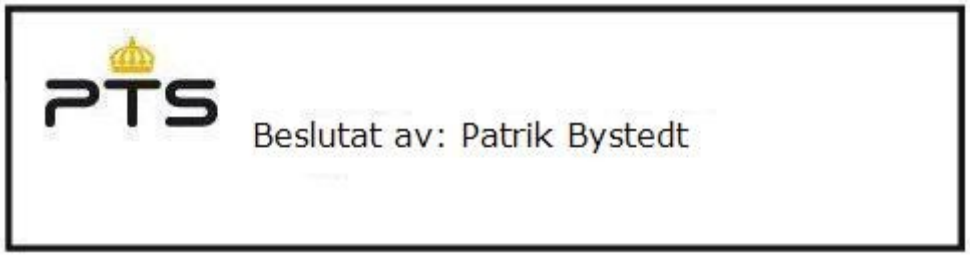
Vid Tele2s redogörelse för status i arbetet med efterlevnad av föreskrifterna om skyddsåtgärder för behandlade uppgifter kan PTS konstatera att det föreligger betydande brister i Tele2s säkerhetsarbete. Tele2 har endast initierat ett arbete med att efterleva föreskrifterna. PTS ser allvarligt på dessa brister, med tanke på att föreskrifterna trädde i kraft den 1 september 2014. PTS förutsätter att Tele2 nu kommer att vidta de åtgärder som är nödvändiga för att efterleva skyldigheterna i föreskrifterna. PTS kommer att följa upp att detta sker. För det fall att Tele2 inte vid uppföljningen vidtagit nödvändiga åtgärder för att efterleva föreskrifterna kan PTS komma att förelägga Tele2 att vidta åtgärder. Med detta påpekande lämnar PTS också denna del av tillsynen utan åtgärd i dagsläget.

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

Underrättelse om överklagande

Beslutet kan inte överklagas.

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


PTS
Beslutat av: Patrik Bystedt