Datum	Vår referens	Aktbilaga
2015-08-12	Dnr: 15-2012	10

Nätsäkerhetsavdelningen
[redacted]

TeliaSonera AB
Stab Juridik
123 86 Farsta
[redacted]

Årlig tillsyn rörande incidentrapportering och inträffade driftstörningar och avbrott

Saken

Årlig tillsyn rörande incidentrapportering och inträffade incidenter; nu fråga om avskrivning.

Post- och telestyrelsens avgörande

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

Bakgrund

Under våren 2015 inledde PTS planlagda tillsyner över ett urval operatörer i syfte att dessa skulle redogöra för inträffade incidenter under 2014. Tillsynerna avsåg såväl driftstörningar som integritetsincidenter. Tillsynen kompletterades med en granskning av rutiner för att analysera riskerna för att integritetsincidenter inträffar i operatörens informationsbehandlingstillgångar.

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 driftsäkerhet i 5 kap. 6 b § 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 störningar och avbrott eller integritetsincidenter. Detta kan i sin tur utgöra underlag för PTS planlagda tillsynsinsatser och även bidra till myndighetens arbete med risk- och sårbarhetsanalyser för sektorn och till myndighetens arbete med robusthetshöjande åtgärder. Det är PTS avsikt att årligen

genomföra planlagda tillsyner över utvalda operatörer rörande incidentrapportering och inträffade incidenter.

Mot bakgrund av detta inledde PTS den 5 mars 2015 en planlagd tillsyn rörande incidentrapportering och inträffade driftstörningar och avbrott över TeliaSonera. Den 22 april respektive den 27 maj 2015 höll PTS tillsynsmöten med TeliaSonera.

Driftstörningar
Vid mötena redogjorde TeliaSonera för föregående års inträffade betydande störningar och avbrott, vilka har rapporterats in till PTS under 2014. Sammanlagt 11 olika driftstörningar diskuterades. Den vanligaste felorsaken vid inträffade störningar var någon typ av hårdvarufel i utrustning (4 fall), problem i samband med planerade arbeten/migrering (2 fall) samt storm/blixtnedslag (2 fall).

Vidare presenterade TeliaSonera de rutiner som tillämpas i samband med driftstörningar som drabbar verksamheten. Av rutinerna framgår att de har olika nivåer för störningar (minor, major, critical, emergency) beroende på hur många kunder som drabbats. Utifrån den inträffade störningen tas planer fram för hur trafik och tjänster ska återställas och hur framtida liknande störningar ska undvikas. I rutinerna ingår också att inrapportering av störningarna ska ske till PTS.

Vid mötena diskuterades också nätsamarbeten mellan operatörerna och TeliaSonera uppgav att rent praktiskt managerar TeliaSonera 3G-nätet för halva Sverige medan deras nätsamarbetspartner (Tele2) managerar den andra halvan. Både Tele2:s och TeliaSoneras kunder når det gemensamma nätet oavsett vem som managerar en viss del av nätet. En störning i februari 2015 drabbadeTele2:s nät. Erfarenheterna från denna störning har lett till att TeliaSonera har uppdaterat sina kontaktvägar och infört en rutin som innebär att de kan stänga ner sitt 3G-nät så fort det blir omfattande störningar. Stänger de ner 3G-nätet så går trafiken automatiskt över till 2G. Kunderna kan även göra detta manuellt i samband med störningar. De håller på att uppgradera sitt nät, vilket innebär att de kommer att ersätta äldre basstationer i delar av nätet med basstationer som hanterar 2G, 3G och 4G.

Integritetsincidenter
Vid mötena redogjorde TeliaSonera för de fyra integritetsincidenter som rapporterats in till PTS under föregående år och vilka åtgärder som vidtagits med anledning av dessa. TeliaSonera har även inkommit med sin förteckning över integritetsincidenter under 2014.

Vid mötena efterfrågade PTS även en redogörelse för hur integritetsincidenter hanteras i organisationen, allt från upptäckt till vidarerapportering såväl internt som till PTS. TeliaSonera uppgav att man inte tidigare haft föreskriften som utgångspunkt i sitt arbete men att den nu används som ett stöd för hur incidenter ska upptäckas och rapporteras. De är ofta händelsestyrda och kunderna upptäcker en del fel själva. Det ingår dock även i utbildningen för kundtjänstpersonalen att de ska upptäcka när något inte är som det ska vara. För att säkerställa att kunskapen fortlever inom organisationen så genomför de en privacy-utbildning och informerar även personalen om tystnadsplikten och vilka uppgifter som får lämnas ut m.m. Uppföljning sker regelbundet av personalens utbildning. Personalen ska ha kunskap om gällande policies. De har ändrat sin tidigare modell som innebar att systemägaren hade ansvar för uppföljning av incidenter till en modell som innebär att säkerhetsgrupperingen för Sverige har ansvar att följa upp incidenter och se till att åtgärder vidtas. De använder sig av nyckeltal och allmänna mätetal för att kunna följa upp hanteringen av incidenter. TeliaSonera lämnade vidare in rutinbeskrivningar avseende underrättelse i samband med incidenter och hantering av incidenter.

När det gäller dokumentation av tillgångar så har de system för att dokumentera stödsystem och nätobjekt. I dessa system framgår i vilken mån riskanalys genomförts eller ej för de berörda tillgångarna. TeliaSonera har vidare presenterat ett exempel på en riskanalys som avser två olika affärssystem. I modellen beaktas hot, svagheter och sannolikheten för att en viss händelse ska inträffa. Riskskalan går från 0-3. Modellen fungerar bäst för större system och måste anpassas till TeliaSoneras olika system. Tanken är att denna modell ska implementeras i verksamheten. Dokumentation i samband med riskanalyser är krävande och drar mycket resurser. De ser till att få riskanalyser avseende nyinköpta system och när de gör inköp har de säkerhetskrav på sina underleverantörer som innebär att de ska uppfylla de krav som framgår av PTS föreskrifter.

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.

Av 5 kap. 6 b § LEK framgår bl.a. att den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ska vidta lämpliga tekniska och organisatoriska

åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet.

Av 5 kap. 6 c § första stycket LEK framgår att den som tillhandahåller ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst utan onödigt dröjsmål ska rapportera störningar eller avbrott av betydande omfattning till tillsynsmyndigheten.

Av PTS föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning (PTSFS 2012:2) framgår bl.a. vilka störningar och avbrott som ska rapporteras samt hur rapporteringen ska gå till.

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 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.

Tillsynsmyndigheten ska enligt 7 kap. 1 § LEK utöva tillsyn över bland annat efterlevnaden av lagen.

PTS bedömning

TeliaSonera kunde redogöra för såväl orsaker till avbrott och störningar som för vidtagna åtgärder för de driftstörningsincidenter som rapporterats under 2014.

Det finns enligt PTS bedömning inte skäl att ytterligare granska någon av de inrapporterade incidenterna, utan myndigheten konstaterar att TeliaSonera i hanteringen av incidenterna får anses ha uppfyllt sina skyldigheter avseende driftsäkerhet så som de framgår av 5 kap. 6b§ LEK.

När det gäller nätsamarbeten konstaterar PTS att det är TeliaSoneras ansvar att minska riskerna för att driftstörningar uppkommer för bolagets abonnenter. Detta kan t.ex. ske genom kravställning i avtal och genom att aktivt efterfråga testresultat m.m. från samarbetspartners/leverantörer.

I övrigt lämnar PTS denna del av tillsynen utan ytterligare åtgärd.

När det gäller integritetsincidenter och processer för upptäckt inrapportering av integritetsincidenter bedömer PTS att processer för att hantera uppkomna incidenter finns dokumenterade och tillämpas i verksamheten på olika nivåer. Jämfört med föregående år har antalet inrapporterade incidenter ökat från två till fyra.

När det gäller implementationen av de krav som framkommer av PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1) bedömer PTS att dessa ännu inte fullt ut tillämpas av TeliaSonera. Detta gäller framförallt dokumentation av informationsbehandlingstillgångar och analys av risker. PTS ser allvarligt på detta och förutsätter att TeliaSonera prioriterar detta arbete och kommer att vidta de åtgärder som är nödvändiga för att efterleva skyldigheterna i föreskrifterna. PTS kommer att följa upp att detta sker i en kommande planlagd tillsyn. PTS lämnar med denna erinran denna del av tillsynen utan ytterligare åtgärd.

Skäl att fortsätta tillsynen i detta ärende föreligger därför inte. Ärendet avskrivs därför från vidare handläggning.

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

Beslutat av: Patrik Bystedt