Datum 2015-12-16 | Vår referens Dnr: 14-11117 | Aktbilaga 17

Nätsäkerhetsavdelningen
Peder Cristvall
08-6785529
peder.cristvall@pts.se

TeliaSonera Sverige AB

Säkerhetsbrister i kundplacerad utrustning

Saken

Tillsyn avseende vidtagande av lämpliga tekniska och organisatoriska åtgärder för att säkerställa skyddet av uppgifter som behandlas i samband med tillhandahållande av elektroniska kommunikationstjänster.

Post- och telestyrelsens avgörande

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

Bakgrund

Efter flera artiklar i media om sårbarheter i bredbandskunders modem beslutade PTS den 3 november 2014 att inleda en granskning av hur ett urval operatörer ser till att den utrustning de tillhandahåller till sina kunder är säker och att kundernas uppgifter är skyddade. Inom ramen för denna tillsyn begärde PTS den 4 november 2014 upplysningar angående den kundplacerade utrustning som tillhandahålls av TeliaSonera Sverige AB (TeliaSonera).

Den 9, 10 och 12 december inträffade störningar som drabbade TeliaSoneras tillhandahållande av Internetaccess (fast och mobil), IP-telefoni och IPTV. TeliaSonera lämnade den 11 respektive den 22 december 2014 in incidentrapporter med anledning av dessa störningar[1].

Den 11 december 2014 respektive den 27 mars 2015 har PTS begärt kompletterande upplysningar. PTS och TeliaSonera har härefter haft ett möte den 27 maj 2015 vid vilket TeliaSonera lämnat en utförligare redovisning av de

[1] I ärende Dnr 14-12684

svar som lämnats skriftligen samt visat upp och beskrivit viss kundutrustning och demonstrerat de tekniska system som används i samband med felsökning av kundplacerad utrustning.

Av inlämnade incidentrapporter framgår att störningarna som uppstått den 9, 10 och 12 december 2014 orsakats av intermittenta DDos-attacker. Attackerna utfördes via kundplacerad utrustning som kunnat kapas genom att man utnyttjat felaktiga inställningar i utrustningen. En del av de berörda kunderna hade bredbandsaccess från TeliaSonera och utrustningen användes för att skapa en förstärkt attack (amplification attack) genom att skicka DNS-förfrågningar gentemot vissa kunders domäner. Attackerna skapade en överbelastning i lastbalanserare i TeliaSoneras kommunikationsnätverk, vilket fick kommunikationstjänsterna att delvis sluta fungera.

Av incidentrapporterna framgår att TeliaSonera tillsatte extra resurser för att utarbeta en lösning för att komma till rätta med attackerna. Ett antal tekniska åtgärder vidtogs och vid förnyade attacker den 13-14 december 2014 orsakades inga kundstörningar, vilket enligt TeliaSoneras bedömning berodde på att vidtagna åtgärder haft effekt. Utöver vidtagna åtgärder identifierade TeliaSonera behovet av uppgradering av den kundplacerade utrustningen och behovet av information till kunderna om den aktuella typen av säkerhetsrisker och hur man ska skydda sig mot dessa.

På frågor från PTS har TeliaSonera sammanfattningsvis uppgett följande.

TeliaSonera tillhandahåller ett antal typer av kundplacerade utrustningar för access till bolagets bredbandsnät och till tjänster som tillhandahålls via dessa nät, t.ex. internet, telefoni och TV. Till dessa utrustningar hör CPE xDSL/Fiber (företagskunder), Bredbandsswitchar (privatkunder) och residental gateways (RGW) för surf, VoIP och IPTV. Utrustningarna behandlar uppgifter som behövs för anslutning mot respektive noder och tjänster i aktuella nät. RGW:er används av privatkunder och utgör den överväldigande majoriteten av aktuella kundplacerade utrustningar.

När det gäller riskanalyser i samband med tillhandahållande av kundplacerad utrustning så initieras en riskanalysprocess genom TeliaSoneras projektmodell som innehåller olika checkpunkter där identifierade risker ska hanteras. Dessa aktiviteter tillförsäkrar att säkerhetsspecialister, baserat på kända hot och attacker som TeliaSonera utsätts för, ger ett omdöme om teknisk lösning i utrustningen samt en rekommendation rörande säkerhetsaspekter i lösningen. Riskanalyser som genomförs för kundplacerad utrustning leder fram till detaljerade skyddsåtgärder som bland annat beskrivs i interna dokument.

Dessa dokumentet beskriver bland annat detaljerat testprocedurer som ska genomföras för kundaccesslösningar utifrån angrepp som setts över åren.

När det gäller den information som lämnas till abonnenterna om kända risker hänförliga till den kundplacerade utrustningen så uppger TeliaSonera att säkerhetsgranskning av produkter är en central aktivitet i produktutvecklingsprocessen. Om denna visar på risker relaterade till skyddet av de uppgifter som behandlas får inte produkten lanseras förrän detta är korrigerat. Med anledning av detta förekommer ingen information om risker för produkter som marknadsförs i dagsläget. Skulle det förekomma risker med anledning av föråldrad mjukvara m.m. i kundplacerad utrustning kontaktas dock kunderna på lämpligt sätt via exempelvis brev eller telefon med instruktion om hur risken kan åtgärdas.

När det gäller risker relaterade till att kunderna gör egna konfigurationer finns ingen specifik information vid konfigurationstillfället. Via TeliaSoneras webbplats lämnas dock utförlig information om säkerhet, t.ex. ges där beskrivningar av hur man kan ändra SSID och lösenord för att därigenom öka säkerheten. Utrustningen är förkonfigurerad med de inställningar som bedöms ge en bra kundupplevelse och lämplig nivå av säkerhet. En betydande majoritet av kunderna gör inga egna inställningar. De kunder som gör egna inställningar bedöms ha tillräckligt med kunskap för att kunna avgöra vad som är lämpligt.

När det gäller säkerhetstester inför tillhandahållandet av kundplacerad utrustning så är säkerhetskrav en viktig del av kravspecifikationen och vid val av leverantör av en viss produkt. TeliaSonera har en av världens största leverantörer av RGW:s och förlitar sig på deras säkerhetstester. Leverantören uppdaterar TeliaSonera med information angående säkerhetsbrister rörande utrustning TeliaSonera har, baserat på erfarenheter och återkoppling från alla leverantörens kunder. TeliaSonera begär också att få ta del av testresultat. Dessutom utförs interna tester av säkerhetstekniker med utgångspunkt i TeliaSoneras kunskap och erfarenhet samt utifrån testschema. Komponenter skannas för sårbarheter och testas utifrån tidigare identifierade problem. Då säkerhetsdefekter publiceras, som kan relateras till kundplacerad utrustning, tillfrågas den aktuella leverantören om säkerhetsdefekten. Verifiering sker även via egna tester. TeliaSonera följer även upp säkerhetspresentationer som ges på säkerhetskonferenser genom att göra egna tester. Information om sårbarheter bevakas av personal vid TS-CERT. Bland personalens uppgifter ingår att följa och analysera information från olika källor inom området.

När det gäller den kundplacerade utrustningens system för identitets- och åtkomsthantering kan anslutningsuppgifter aktiveras/modifieras av TeliaSoneras help-desk-personal som en del av felavhjälpningen. Även

abonnenten kan managera sin RGW via ett webbgränssnitt som kräver lösenord. Vidare kan uppdatering av mjukvara i kundutrustningarna initieras av TeliaSonera. Loggning sker av vissa av personalens åtgärder.

All ny berörd personal som ska använda systemet för managering av kundplacerade utrustning genomgår en lärarledd grundutbildning där de får relevant utbildning. Efter genomförd grundutbildning genomförs tester för att säkerställa att personalen har lärt sig det som krävs. Personalen får efter det löpande information om det sker förändringar i systemet via intranätet. Vid större förändringar genomförs även lärarledda informationstillfällen.

När det gäller möjligheterna att upptäcka enskilda fall där säkerhetsbrister utnyttjats, tillämpar TeliaSonera standardiserade processer enligt ITIL (IT Infrastructure Library) för att upptäcka och hantera obehöriga intrång i bland annat kundplacerad utrustning. Det innebär att det finns en funktion för felavhjälpning som alltid är bemannad. Vid behov av djupare kompetens och specialister finns en andra och tredje nivå att lämna över ärendet till. På nätter och helger jobbar dessa funktioner under beredskap. För integritets-, säkerhets- och missbruksrelaterade ärenden finns en specialiserad enhet som hanterar dessa.

TeliaSonera har inkommit med dokumentation som beskriver hanterade roller och ansvar i samband med en sårbarhetsincident och rutinbeskrivning av hur bolaget underrättar PTS och berörda kunder i samband med integritetsincidenter. Vid möte har TeliaSonera visat upp exempel på en riskanalys som berör kundplacerad utrustning.

Skäl

Tillämpliga bestämmelser

Enligt 6 kap. 3 § i lagen (2003:389) om elektronisk kommunikation (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 tillhandahållande 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.

Av PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter[2] 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 § identifiera informationsbehandlingstillgångar där behandlade uppgifter förekommer och föra en förteckning över dessa. Tjänstetillhandahållaren ska analysera riskerna för att integritetsincidenter inträffar för de identifierade informationsbehandlingstillgångarna. Riskanalyserna ska dokumenteras och följas upp årligen och vid behov. Tjänstetillhandahållaren ska vidta föreskrivna skyddsåtgärder samt andra nödvändiga skyddsåtgärder, på den nivå som är lämplig för att hantera de identifierade riskerna. Vidtagna skyddsåtgärder samt tjänstetillhandahållarens bedömningar av lämplig nivå ska dokumenteras och följas upp årligen och vid behov.

Tjänstetillhandahållaren ska enligt 5 § säkerställa att åtkomst till behandlade uppgifter endast ges till den som
1. behöver det för att utföra sina arbetsuppgifter,
2. har relevant utbildning med hänsyn till de uppgifter denne hanterar,
3. har upplysts om tystnadsplikten i 6 kap. 20 – 21 §§ lagen (2003:389) om elektronisk kommunikation.

Tjänstetillhandahållaren ska enligt 6 § tilldela behörighet i enlighet med vad som föreskrivs i 5 §. Tjänstetillhandahållaren ska ha dokumenterade rutiner för tilldelning, ändring och uppföljning av behörigheter. Uppföljning av tilldelade behörigheter ska ske årligen.

Tjänstetillhandahållaren ska vidare ha system för identitets- och åtkomsthantering som säkerställer att åtkomst endast medges i enlighet med tilldelade behörigheter.

Tjänstetillhandahållaren ska enligt 7 § dokumentera (logga) all läsning, kopiering, ändring och utplåning av behandlade uppgifter samt åtkomst till de system som används för behandling av sådana uppgifter. Loggning ska ske på ett sådant sätt att det går att se vem som har vidtagit vilken åtgärd med vilka uppgifter och vid vilken tidpunkt. Tjänstetillhandahållaren ska systematiskt och

[2] Post- och telestyrelsens föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter, PTSFS 2014:1.

återkommande kontrollera loggarna. Kontrollerna får avgränsas till att omfatta utvalda behandlingar under begränsade tidsperioder, om kostnaderna för kontrollen motiverar en sådan avgränsning. Tjänstetillhandahållaren ska dokumentera genomförda kontroller av loggar. Vid misstanke om att en integritetsincident har inträffat ska relevanta loggar alltid kontrolleras. Tjänstetillhandahållaren ska ha dokumenterade rutiner för kontroll av loggar.

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

Den föreliggande tillsynen har föranletts av att PTS uppmärksammat att det kan föreligga generella säkerhetsbrister i samband med tillhandahållande av elektroniska kommunikationstjänster som berör vissa typer av kundplacerad utrustning såsom modem, routrar och IP-telefonidosor. Inom ramen för den pågående tillsynen har PTS också granskat brister avseende sådan kundutrustning som omfattas av den incident TeliaSonera rapporterat in till PTS i ärende 14-12684.

I ärendet aktualiseras i första hand två olika typer av kundplacerad utrustning. För det första aktualiseras den utrustning som TeliaSonera förser abonnenterna med i samband med erbjudande om öppet fiber, bredbandsswitchar. TeliaSonera äger utrustningen och via utrustningen kan ytterligare utrustning anslutas för att nå TeliaSoneras eller andra operatörers utbud av elektroniska kommunikationstjänster. Denna utrustning får anses utgöra en del i TeliaSoneras kommunikationsnät- och tjänster och omfattas således av reglerna i LEK.

För det andra aktualiseras TeliaSoneras kundplacerade utrustning i form av t.ex. RGW:er som kan användas för att ta del av TeliaSoneras egna utbud av kommunikationstjänster. PTS kan konstatera att den aktuella utrustningen för abonnenten utgör en förutsättning för att kunna ta del av en eller flera av de

tjänster som tillhandahålls av TeliaSonera, t.ex. IP-telefoni. Via denna tillhandahålls även trådbunden eller trådlös internetuppkoppling. Användare har dessutom möjlighet att koppla in ytterligare utrustning i form av t.ex. egna routrar.

När det gäller inställningar och användningen av RGW:n kan konstateras att kunderna får behörighet och möjlighet att ansluta till utrustningen via ett begränsat administrationsgränssnitt. Genom anslutningen ges kunderna möjlighet att i viss grad anpassa utrustningen, till exempel genom att sätta egna lösenord.

TeliaSoneras personal kan genomföra fjärrinloggning via bolagets administrativa supportnät. Sådan behörighet tilldelas TeliaSoneras olika kategorier av help-desk-personal. Vidare tilldelas behörighet för att genomföra bland annat teknisk konfigurering, uppdateringar och omstarter till teknisk personal i drift/utvecklingsorganisationen. Detta innebär att TeliaSonera har kontroll av delar utrustningen som kunden inte råder över eller har möjlighet att påverka. Med hjälp av denna kontroll kan TeliaSonera genomföra nödvändiga uppgraderingar och stödja sina kunder i samband med problem relaterade till den aktuella utrustningen.

Av 6 kap 3 § LEK följer att den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas *i samband med* tillhandahållandet av tjänsten skyddas. Frågan i detta ärende är hur långt detta ansvar sträcker sig när det gäller kundplacerad utrustning, t.ex. RGW:er. Som framgår ovan förutsätts abonnenterna i normalfallet använda den aktuella utrustningen för åtkomst till TeliaSoneras kommunikationstjänster. TeliaSonera har dessutom uteslutande kontroll vad gäller hanteringen av väsentliga inställningar. I och med att det endast är TeliaSonera som kan göra ändringar i dessa inställningar får TeliaSonera anses förfoga över RGW:erna i dessa delar. Mot bakgrund av dessa omständigheter bedömer PTS att den aktuella utrustningen utgör en tillgång som används av TeliaSonera för att tillhandahålla elektroniska kommunikationstjänster. Den omfattas därmed av bestämmelsen i 6 kap 3 § LEK. Eftersom utrustningen innehåller uppgifter knutna till vissa abonnemang och därtill används för att förmedla abonnenternas trafik får den anses utgöra en sådan informationsbehandlingstillgång som regleras i PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1)

Nedan följer de bedömningar PTS gör vad gäller TeliaSoneras åtgärder beträffande den kundplacerade utrustningen i förhållande till tillämpliga krav som de framgår av PTS föreskrifter.

Säkerhetsarbete i enlighet med 3 § i PTSFS 2014:1

Kravet i 3 § föreskrifterna på säkerhetsarbete syftar bland annat till att minimera risker för otillåtna ingrepp i abonnenters och användares personliga integritet och att öka verksamhetens förmåga att upptäcka och hantera de incidenter som inträffar.

TeliaSonera har upptäckt de inträffade incidenterna och vidtagit ett antal tekniska åtgärder för att minimera effekterna under pågående händelse. Bolaget har underrättat PTS om incidenterna i enlighet med vad som följer av 5 kap 6c § LEK. Vidare har bolaget utrett orsaken till vad som orsakat incidenterna och har identifierat ett antal åtgärder för att så långt möjligt undvika liknande incidenter. PTS kan konstatera att incidenterna medfört problem relaterade till driftsäkerheten i TeliaSoneras kommunikationsnät men att de också inneburit risker för otillåtna ingrepp i abonnenters och användares personliga integritet. Av det genomförda arbetet med anledning av inträffade incidenter och den redovisning som lämnats i detta ärende framgår att TeliaSonera tillämpar rutiner för upptäckt av integritetsincidenter och att man har en organisation som styrs av en intern policy med särskilt utpekade ansvariga för att kunna upptäcka och hantera inträffade integritetsincidenter. PTS noterar att säkerhetsarbetet huvudsakligen varit av reaktiv karaktär med anledning av de säkerhetsbrister som uppmärksammats och betonar vikten av ett kontinuerligt förebyggande säkerhetsarbete för att så långt som möjligt undvika incidenter och för att kunna hantera risker på ett tidigt stadium. Den kundplacerade utrustningen utgör sådana informationsbehandlingstillgångar som regleras i PTS föreskrifter och det är viktigt att det övergripande säkerhetsarbetet även omfattar dessa.

Med detta påpekande lämnar PTS frågan hur TeliaSonera efterlever den aktuella bestämmelsen utan vidare åtgärd. PTS kan dock återkomma till frågan i framtida tillsynsärenden.

Identifikation av informationsbehandlingstillgångar, genomförande av riskanalyser och vidtagande av skyddsåtgärder i enlighet med 4§ PTSFS 2014:1

PTS har ovan konstaterat att RGW:er får anses utgöra sådana informationsbehandlingstillgångar som omfattas av kraven i PTSFS 2014:1. Av 4 § framgår att tjänstetillhandahållaren ska *identifiera sina informationsbehandlingstillgångar och föra en förteckning över dessa*. En grundläggande förutsättning för att en tjänstetillhandahållare ska kunna vidta lämpliga åtgärder, upprätthålla en lämplig skyddsnivå och följa upp sitt säkerhetsarbete är att denne har en samlad bild över de informationsbehandlingstillgångar där uppgifter behandlas i samband med tillhandahållande av elektroniska kommunikationstjänster.

PTS föreskrifter reglerar inte särskilt i vilken form förteckningen av informationsbehandlingstillgångar ska föras. Syftet med förteckningen är dock att tjänstetillhandahållaren bland annat ska få en överblick och kunna planera sitt arbete med t.ex. riskanalyser. I samband med upptäckta sårbarheter eller inträffade incidenter kan förteckningen också användas för att t.ex. underlätta programuppdateringar i kundutrustningen och för att kontakta de abonnenter som är berörda.

PTS har valt att inom ramen för denna tillsyn inte närmare granska hur förteckningen förs eller dess innehåll. PTS har dock för avsikt att återkomma till frågan om förteckningen över informationsbehandlingstillgångar i kommande tillsynsarbete.

PTS föreskrifter anger vidare att en kartläggning ska ske av riskerna för att integritetsincidenter inträffar för identifierade informationsbehandlings-tillgångar eller grupper av tillgångar. Den genomförda riskanalysen styr omfattningen av de skyddsåtgärder som vidtas beträffande de aktuella informationsbehandlingstillgångarna. En sådan analys ska dokumenteras, liksom de säkerhetsåtgärder som behöver vidtas för att hantera de identifierade riskerna.

Av utredningen framgår att TeliaSonera genomför riskanalyser i samband med tillhandahållande av kundplacerad utrustning. Eftersom nya sårbarheter kan uppkomma eller upptäckas efterhand är regelbundna riskanalyser nödvändiga för att kunna hantera nya och förändrade risker. Enligt föreskrifterna ska genomförda riskanalyser följas upp minst en gång per år.

PTS kan konstatera att det av TeliaSonera beskrivna arbetet med riskanalyser står i överensstämmelse med PTS föreskrifter. PTS vill i detta sammanhang peka på att även en övergripande, mer generell riskanalys, kan vara nödvändig för att beakta eventuella risker som inte är direkt relaterade till modem/RGW:er och deras hård- och mjukvara. En sådan analys skulle t.ex. kunna omfatta hanteringen av lösenord och överväganden vad gäller abonnenternas möjligheter att göra egna inställningar.

Åtkomst till uppgifter i enlighet med 5 § och tilldelning av behörighet i enlighet med 6 § PTSFS 2014:1

Syftet med bestämmelserna är att tillgodose skyddet av behandlade uppgifter genom att förhindra obehörig användning eller åtkomst till behandlade uppgifter genom regler för åtkomst- och behörighetshantering.

Bestämmelserna gäller enligt PTS bedömning för tjänstetillhandahållarnas egen personal (och personal hos underleverantörer). Genom bestämmelserna begränsas åtkomstmöjligheterna till känsliga uppgifter, så att endast den

personal som behöver dessa för att utföra sina arbetsuppgifter får tillgång till uppgifterna. Vidare bör tillförsäkras att personalen har god kännedom om reglerna om tystnadsplikt och har en relevant utbildning så att den vet när och hur behandlade uppgifter får behandlas, kan se tecken på att incident har inträffat och kan bedöma tänkbara konsekvenser av inträffadeincidenter m.m. Av det allmänna rådet till 5 § föreskrifterna framgår att en relevant utbildning bör innefatta information som ger personalen kunskap att upptäcka, bedöma och rapportera integritetsincidenter. TeliaSonera har i ärendet redogjort för att all ny berörd personal genomgår en lärarledd grundutbildning för systemet som används för managering av kundplacerad utrustning. Inom ramen för utbildningen bör säkerställas att personalen får kunskaper så att de kan hantera integritetsincidenter på ett lämpligt sätt.

PTS kan konstatera att såväl support- som driftsärenden kräver åtkomst till vissa av de uppgifter som behandlas i RGW:n. TeliaSonera har beskrivit att man tilldelar supportpersonal i kundservice behörighet att genomföra fjärrinloggning för att kunna logga in och kontrollera enheternas status och inställningar i samband med felsökning. Vidare tilldelas teknisk personal i drift/utvecklingsorganisationen behörighet att genomföra fjärrinloggning via administrationsgränssnitt för teknisk konfigurering, uppdateringar och omstarter. Båda kategorierna av personal utgör en begränsad andel av TeliaSoneras personal och tilldelas behörighet med utgångspunkt i behovet av att ta del av uppgifter för att kunna vidta nödvändiga åtgärder för drift och kundstöd.

Utifrån de uppgifter TeliaSonera lämnat i ärendet gör PTS bedömningen att behörighet till åtkomst till kundplacerad utrustning endast ges till de som behöver det för att utföra sina arbetsuppgifter. PTS har dock inte inom ramen för detta tillsynsärende närmare granskat de system för identitets- och åtkomsthantering som är nödvändiga för att säkerställa att åtkomst endast medges i enlighet med tilldelade behörigheter.

PTS gör bedömningen att bestämmelserna inte är avsedda att reglera villkoren för abonnenternas användning av kundplacerad utrustning. Detta medför att bestämmelserna inte hindrar att abonnenter ges möjlighet att ändra vissa inställningar i t.ex. RGW:er för att anpassa dessa efter sina behov.

7 § loggning
Av 7 § framgår att tjänstetillhandahållare ska logga all behandling som sker av uppgifter i och åtkomst till system som används för behandling av uppgifter. Loggarna ska återkommande kontrolleras och dokumentation ska ske av genomförda kontroller.

PTS gör bedömningen att de åtgärder med modemen som genomförs av supportpersonal i kundservice och av teknisk personal i driftsorganisationen omfattas av skyldigheten att logga utförda behandlingar. PTS kan konstatera att TeliaSonera loggar den egna personalens åtgärder. PTS har dock inte särskilt granskat TeliaSoneras loggar eller utförda kontroller i detta ärende.

Samlad bedömning

Mot bakgrund av de åtgärder TeliaSonera har genomfört och redovisat i ärendet för att komma till rätta med de aktuella säkerhetsbristerna och med de påpekanden PTS har gjort ovan, kan myndigheten konstatera att det saknas anledning att vidta ytterligare åtgärder i ärendet. Ärendet ska därför avskrivas från vidare handläggning.

Beslutet har fattats av enhetschefen Patrik Bystedt. Föredragande har varit juristen Peder Cristvall.

PTS Beslutat av: Patrik Bystedt