Datum	Vår referens	Aktbilaga
2016-04-29	Dnr: 14-11113	11

Nätsäkerhetsavdelningen

[redacted]

Alltele Allmänna Svenska Telefoniaktiebolag

[redacted]

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 avskriver ärendet från vidare handläggning.

Bakgrund

Post- och telestyrelsen (PTS) har uppmärksammat att det kan föreligga säkerhetsbrister i samband med tillhandahållande av elektroniska kommunikationstjänster som berör vissa typer av kundplacerad utrustning såsom modem, routrar och IP-telefonidosor (kundplacerad utrustning) som tillhandahålls abonnenter. Detta kan bland annat bero på hur denna utrustning har konfigurerats och uppgraderats. Vid en felaktig hantering av den kundplacerade utrustningen kan det uppstå en risk för att skyddet av behandlade uppgifter inte upprätthålls.

PTS har därför beslutat att inleda en granskning av hur ett urval operatörer tillgodoser skyddet av behandlade uppgifter när det gäller kundplacerad utrustning. Alltele Allmänna Svenska Telefoniaktiebolag (Alltele) har ingått i detta urval.

Inom ramen för tillsynen har PTS den 4 november 2014 begärt upplysningar angående vilka typer av kundplacerad utrustning Alltele tillhandahåller abonnenterna och det säkerhetsarbete som bolaget bedriver för att tillgodose att de uppgifter som behandlas i utrustningen skyddas. Alltele har inkommit med svar på PTS frågor den 24 november 2014. Härefter har PTS ställt kompletterande frågor den 11 december 2014, vilka besvarats av Alltele den 3 februari 2015.

Alltele har sammanfattningsvis lämnat följande upplysningar vad gäller den utrustningen som tillhandahålls privatkunder.

De flesta av Allteles kundplacerade utrustningar är relaterade till VoIP, ADSL och stadsnätsprodukter. Det innefattar ATA-boxar, IAD (Integrated Access Device) och RGW-enheter (Residential Gateway). Beroende på modell stöder de olika enheterna ADSL, Stadsnät, VoIP. De har även triple play abonnemang där de tillhandahåller IPTV med Stadsnät och VoIP.

När det gäller den information som lämnas till abonnenterna om kända risker i samband med att abonnenten konfigurerar den kundplacerade utrustningen anser Alltele att de inte behöver informera privatkunder om detta då dessa inte kan ändra inställningar på utrustningen. Kunderna ges dock, via inloggning med lösenord, begränsad tillgång till viss kundplacerad utrustning för att kunna ändra delar av tjänsten, såsom WiFi-lösenord och port forwarding.

När det gäller genomförande av riskanalyser uppger Alltele att riskanalyser genomförs inför inköp av specifik utrustning men att dessa även görs i den löpande verksamheten. Dessa analyser innefattar ett antal penetrationstester som genomförs på utrustningen, dels innan inköp på originalprogramvaran, dels efter installation av deras egen programvara. Testerna baseras på knowhow och i enlighet med rutiner på deras respektive tekniska avdelningar. Testerna är även baserade på aktuell information om sårbarheter som nyttjas. Alltele uppger vidare att dokumentation kring de riskanalyser som ska genomföras i enlighet med 4 § PTSFS 2014:1 saknas.

När det gäller säkerhetstester uppger Alltele att man genomför olika tester innan de sätter någon enhet i produktionen. Ett test är att enheterna kan kommunicera med deras provisioneringsservrar med hjälp av industristandarder. Vidare kontrolleras att enheterna har ett komplext lösenord och en mjukvara som anpassas för de parametrar som Alltele behöver. Vidare testas att webbaccessen begränsats m.m.

När det gäller den loggning som sker av åtkomst till olika funktioner och uppgifter i den kundplacerade utrustningen uppger Alltele att kundplacerad utrustning loggar vem som haft tillgång till enheten.

När det gäller krav på att tjänstetillhandahållaren ska ha dokumenterade rutiner för tilldelning av, ändring och uppföljning av behörighet har Alltele uppgett att all hantering av kundkritisk data är behörighetslåst i ett centralt CRM-system. Åtkomst till djupare tekniska data är begränsad för slutkunder och utökad behörighet ges enbart efter ett godkännande från CTO (Nätchef) eller motsvarande. Alltele har lämnat in en översiktlig schematisk beskrivning av hur kontroll av behörighet sker.

När det gäller dokumenterade rutiner för identifiering, intern rapportering, hantering och uppföljning av integritetsincidenter har Alltele uppgett att företaget har möjlighet att sätta upp trafiklarm kopplade till ett flertal olika parametrar och att övervakning sker dygnet runt. En riskbedömning görs i varje enskilt fall baserat på tidigare trafikmönster.

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 (PTSFS 2014:1)[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 § identifiera informationsbehandlings-tillgångar 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

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

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 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 aktuella tillsynen har föranletts av uppgifter i bland annat massmedia som beskrivit säkerhetsbrister som kan beröra vissa typer av kundplacerad utrustning såsom modem, routrar och IP-telefonidosor som tillhandahålls abonnenter.

PTS kan konstatera att Alltele tillhandahåller sina kunder kundplacerad utrustning som en del i sitt erbjudande av vissa kommunikationstjänster. Via utrustningen tillhandahålls t.ex. 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 utrustningen kan konstateras att kunderna får behörighet och möjlighet att ansluta till det av utrustningen tillhandahållna trådlösa nätverket och vidare ges behörighet att ansluta till utrustningen via ett begränsat administrationsgränssnitt. På så vis kan kunderna anpassa utrustningen, till exempel genom att sätta egna lösenord.

Allteles personal kan genomföra fjärrinloggning i samband med supportärenden. Detta innebär att Alltele har kontroll av delar av utrustningen som kunden inte råder över eller har möjlighet att påverka. Med hjälp av denna kontroll kan Alltele 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. En fråga i detta ärende är hur långt detta ansvar sträcker sig när det gäller kundplacerad utrustning. Som framgår ovan förutsätts kunderna i normalfallet använda den aktuella kundplacerade utrustningen för åtkomst till vissa av Allteles kommunikationstjänster. Alltele har dessutom uteslutande kontroll vad gäller hanteringen av väsentliga inställningar. I och med att det endast är Alltele som kan göra ändringar i dessa inställningar får Alltele anses förfoga över den kundplacerade utrustningen i dessa delar. Mot bakgrund av dessa omständigheter bedömer PTS att den aktuella utrustningen utgör en tillgång som används av Alltele 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 Allteles åtgärder beträffande den aktuella kundplacerade utrustningen i förhållande till vissa 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.

PTS betonar i detta sammanhang vikten av ett kontinuerligt förebyggande säkerhetsarbete för att så långt som möjligt undvika att incidenter inträffar 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. PTS kan konstatera att Allteles säkerhetsarbete även omfattar kundplacerad utrustning och att bolaget arbetar aktivt med tekniskt inriktade säkerhetsfrågor relaterade till den kundplacerade utrustningen. PTS vill betona att det är viktigt att ha organisatoriskt ansvariga utpekade och tillämpliga rutiner som hanterar krav i samband med införskaffande och åtgärder för kontinuerlig uppföljning av den kundplacerade utrustningen.

Med detta påpekande lämnar PTS frågan hur Alltele efterlever den aktuella bestämmelsen utan vidare åtgärd i nuläget. PTS kan dock återkomma till frågan i kommande tillsynsarbete.

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

PTS har ovan konstaterat att kundplacerad utrustning 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 startat en särskild tillsyn som avser dokumentation av informationsbehandlingstillgångar[2].

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.

PTS kan konstatera att Alltele genomför en teknisk analys som är inriktad mot risker hänförliga till de modem företaget tillhandahåller. 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.

Det är också viktigt att ha en löpande omvärldsbevakning för att få kännedom om eventuella nya sårbarheter så att en bedömning kan göras om det finns behov av förnyade riskanalyser eller andra åtgärder.

PTS kan konstatera att det ovan beskrivna arbetet delvis står i överensstämmelse med PTS föreskrifter. Av Allteles beskrivning framgår att Alltele primärt genomfört analyser med inriktning mot att förhindra manipulation av utrustningen. PTS anser att även en övergripande, mer generell riskanalys, är nödvändig för att beakta eventuella risker som inte är direkt relaterade till modemen 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 i den kundplacerade utrustningen.

Av 4 § PTSFS följer vidare att genomförda riskanalyser ska dokumenteras. PTS kan konstatera att Alltele uppgett att dokumentation inte sker av de riskanalyser som genomförts. Enligt PTS bedömning är dokumentation av genomförda riskanalyser en grundläggande förutsättning för att kunna bedriva ett kontinuerligt arbete som syftar till att upprätthålla ett skydd av behandlade uppgifter. I avsaknad av dokumenterad riskanalys kan inte heller en

[2] Inledningsvis har PTS inlett tillsyn mot två större operatörer i ärende 16-3656 och 16-3657.

ändamålsenlig uppföljning av tidigare genomförda riskanalyser ske. PTS förutsätter därför att Alltele fortsättningsvis prioriterar arbetet med att dokumentera genomförda riskanalyser.

Med detta påpekande lämnar PTS frågan hur Alltele efterlever den aktuella bestämmelsen utan vidare åtgärd i nuläget. PTS kan dock återkomma till frågan i kommande tillsynsarbete.

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 inträffade incidenter 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.

PTS kan konstatera att såväl support- som driftsärenden kräver åtkomst till vissa av de uppgifter som behandlas i modemen. Alltele har uppgett att man tilldelar teknisk personal i drift-/utvecklingsorganisationen behörighet att genomföra fjärrinloggning. Denna kategori av personal utgör en begränsad andel av Allteles 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 Alltele lämnat gör PTS bedömningen att behörighet till åtkomst till modemen 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 vidare 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. modem för att anpassa dessa till 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 drift/utvecklingsorganisationen omfattas av skyldigheten att logga utförda behandlingar. PTS kan konstatera att loggning sker vad gäller tillgång till kundplacerad utrustning. PTS har dock inte särskilt granskat loggar eller utförda kontroller av dessa i detta ärende.

Samlad bedömning

Mot bakgrund av Allteles redovisning i ärendet 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.