Datum 2015-12-16
Vår referens Dnr: 14-11073
Aktbilaga 20

Nätsäkerhetsavdelningen
[redacted]

Com Hem 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

PTS uppmärksammades på att det kunde föreligga säkerhetsbrister i samband med tillhandahållande av elektroniska kommunikationstjänster i den verksamhet som Com Hem AB (Com Hem) bedriver. Enligt uppgifter i DN den 31 oktober 2014 skulle av Com Hem tillhandahållna modem vara behäftade med säkerhetsbrister vilka kunde möjliggöra att internetuppkopplingar kapades, vilket i sin tur skulle kunna möjliggöra avlyssning.

Mot bakgrund av denna och tillkommande information har PTS beslutat att inleda tillsyn mot Com Hem.

Inom ramen för tillsynen har PTS den 31 oktober 2014 begärt upplysningar angående de aktuella modemen och Com Hems pågående arbete med att komma tillrätta med eventuella säkerhetsbrister. PTS och Com Hem har härefter haft ett möte den 11 november 2014 vid vilket Com Hem lämnat en utförligare redovisning av sina bedömningar och vidtagna åtgärder för PTS. PTS har härefter begärt kompletterande upplysningar den 3 december 2014 respektive den 27 mars 2015. Den 20 april 2015 har Com Hem, vid möte med

PTS, visat upp och beskrivit en del av den aktuella kundutrustningen och demonstrerat de tekniska system som används i samband med felsökning i kundplacerad utrustning.

Com Hem har sammanfattningsvis anfört följande.

Com Hem tillhandahåller tio olika typer av kundplacerad utrustning av märkena Netgear, Compal, Cisco och Technicolor. Utrustningens funktion är att bland annat att omvandla digitala signaler som transporteras i kablarna till digitala signaler som konsumentprodukter såsom t.ex. PC och surfplattor kan hantera. Dessutom har flertalet utrustningar funktioner som trådlösa routers, dvs. de erbjuder trådlös access och ett lokalt hemmanät där all trafik som går ut på internet routas via modemet. De uppgifter som behandlas i utrustningen är bland annat inställningar av det trådlösa nätverket såsom Wifi-namn, trafikregler för IP-trafiken och om utrustningen ska vara bryggad eller om NAT (Network Address Translation) ska användas för att särskilja hemmanätet från internet eller inte.

I DN:s granskning uppmärksammades två problem i modem av typen Netgear CG3100, det första var relaterat till tillgången till modemets inställningar och det andra att det under specifika omständigheter var möjligt att ändra DNS-inställningar.

Den första säkerhetsbristen kom till Com Hems kännedom via ett meddelande till deras kundtjänst cirka 14 månader innan den uppmärksammades i media. Kundtjänsten informerade i enlighet med företagets rutiner till den tekniskt operativa expertisen för modemen inom Com Hem. Com Hem informerade leverantören om problemet som vid denna tidpunkt inte av Com Hem bedömdes vara ett allvarligt säkerhetsproblem. Leverantören tillhandahöll en mjukvara som testades och rullades ut i januari 2014. Den visade sig ha så allvarliga kvalitetsproblem att Com Hem fick en markant ökning av kundklagomål. Eftersom säkerhetsproblematiken hade klassats som ett mindre allvarligt fel fattades beslut att rulla tillbaka till den gamla mjukvaran. Under tiden därefter pågick arbetet med leverantören för att få ut en mjukvara som både åtgärdade säkerhetsproblemet såväl som andra kvalitetsproblem. I efterhand kan Com Hem konstatera att detta arbete gått för långsamt och med för låg intensitet vilket grundat sig i att problemet tidigare hade bedömts vara av mindre allvarlig karaktär. På grund av denna bedömning av problemets karaktär eskalerades problemet inte till någon ansvarig chef eller säkerhetsansvarig. Com Hem har inte haft en egen klassificering av säkerhetsrelaterade brister utan dessa har hanterats som vilket fel som helst, vilket man nu har förändrat.

När det gäller den allvarligaste säkerhetsbristen som berörde ovanstående modem, DNS-förändringen, blockerades den inom tolv timmar från det att Com Hem fått information om att det förelåg en potentiell säkerhetsbrist. De har även ändrat lösenord till betydligt svårare och okända, vilket försvårar intrång. Com Hem har också tagit fram en ny mjukvara som ska förhindra åtkomsten till modemen och stängt ner dolda konton på samtliga modem. Härutöver har man, efter sårbarhetsanalys, vidtagit ett antal tekniska åtgärder för ytterligare tre olika modemtyper som de tillhandahåller.

Com Hem har gjort vad de anser är möjligt för att undersöka de potentiella risker som företagets kunder kan ha varit utsatta för. Man har gjort en scanning av modeminställningar för att få en bild av hur många modem som har fått ändrade inställningar och därmed teoretiskt har kunnat råka ut för en obehörig förändring. Detta visade sig vara omkring tio modem i den delen av nätet som DNS-förändringen var möjlig. Förändringen i dessa modem behöver dock inte betyda att modemen varit föremål för intrång. När det gäller den säkerhetsbrist som hade med tillgången till modemens inställningar att göra, så har man inte kunnat uppskatta problemets omfång. De har inte i något av fallen kunnat påvisa något fall av obehörigt utnyttjande.

Com Hem har informerat sina abonnenter om den inträffade incidenten och den uppgradering av mjukvaran som gjorts via företagets webbplats. I övrigt finns information i manualen som skickas ut till kund tillsammans med den kundplacerade utrustningen. Där återfinns bland annat råd om lösenordshantering. Vidare finns mer allmän information på ComHem.se.

På kompletterande frågor från PTS har Com Hem vidare bland annat anfört följande.

När det gäller rutiner avseende tilldelning av behörighet levereras kundplacerad utrustning med användar-ID och lösenord för kunds egen inloggning i utrustningen från kundsidan. Com Hem kan för supportärenden ges tillgång till utrustningen genom inloggning med administratörskonto. Den personal inom Com Hem som kan ges tillgång till administrationskonton i kundplacerad utrustning är supportpersonal i kundserviceorganisationen. Utöver detta kan ett fåtal personer inom drifts- respektive kundserviceorganisationen logga in i kundplacerad utrustning för avancerad felsökning och diagnosticering. Com Hem för logg över de arbeten som syftar till att införa ny mjukvara i kundplacerad utrustning. Vidare loggas åtgärder som har gjorts i supportärenden för enskild kund.

Vad gäller de säkerhetstester som genomförs innan ny mjuk- eller hårdvara införs, så går testerna ut på att utsätta kundplacerad utrustning för kända hot

och exploits. Tester sker därför av begränsningen av åtkomst, säkra inloggningsrutiner samt lösenordshantering. Tester kan t.ex. avse att modemet inte går att nå utifrån från okänd användare, att modemet inte går att hacka via det trådlösa nätverket och att krypteringen fungerar.

Com Hem har förbättrat sin test- och verifieringsprocess med anledning av det inträffade och har infört en säkerhetsklassificering av de buggar som utgör en sårbarhet och hot mot kundplacerad utrustning. Beroende på prioritet och baserat på resultat från riskanalysprocessen anpassas samarbetet med deras leverantörer vad gäller intensitet och frekvens på uppföljningsmöten för att så snart som möjligt få fram en lösning. De kommer också att införa ett godkännandeförfarande med en Change Advisory Board (CAB) bestående av involverade enheter (stakeholders) för att säkerställa att de tillhandahåller lösningar som adresserar uppkomna sårbarheter så snabbt som möjligt. Com Hem har infört en förbättrad riskhanteringsprocess, med vars hjälp de kan analysera uppkommen sårbarhet baserat på sannolikhets- och konsekvensbedömning. Com Hem kommer att använda riskanalysprocessen och agera efter den säkerhetsklassificering som en möjlig sårbarhet får. Man kommer också att förbättra sin omvärldsbevakning och uppdra åt externa säkerhetsresurser att utföra regelbundna kontroller av kundplacerad utrustning.

Com Hem har lämnat in en beskrivning av sin övergripande riskhanteringsprocess och exempel på en genomförd IT-säkerhetsriskanalys för 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 (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

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

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 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 föreliggande tillsynen har föranletts av brister som uppmärkammats avseende ett modem för fast bredband till slutkunder som tillhandahålls i Com Hems verksamhet. Det har funnits risk att de uppmärksammade bristerna skulle utnyttjas av obehöriga för att via ett administrationsgränssnitt ändra inställningar i modemen och därigenom kunnat ta del av innehållet och kunnat påverka den kommunikation som förmedlats. Com Hem har dock inte kunnat fastställa att bristerna har utnyttjats i något fall.

PTS kan konstatera att de aktuella modemen för abonnenten utgör en förutsättning för att kunna ta del av en eller flera av de tjänster som tillhandahålls av Com Hem. IP-telefoni ska enligt instruktionerna från Com Hem kopplas in via modemen. Via modemen tillhandahålls även trådbunden och trådlös internetuppkoppling. Användare har dessutom möjlighet att koppla in ytterligare utrustning i form av exempelvis egna routrar.

När det gäller inställningar och användningen av utrustningen 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.

Com Hems personal kan genomföra fjärrinloggning via bolagets administrativa supportnät. Sådan behörighet tilldelas supportpersonalen i kundservice. Vidare tilldelas behörighet för att genomföra bland annat teknisk konfigurering, uppdateringar och omstarter till teknisk personal i drift/utvecklingsorganisationen. Detta innebär att Com Hem har kontroll av delar av utrustningen som kunden inte råder över eller har möjlighet att påverka. Med hjälp av denna kontroll kan Com Hem genomföra nödvändiga

ändringar 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. Som framgår ovan förutsätts kunderna i normalfallet använda den aktuella kundplacerade utrustningen för åtkomst till vissa av Com Hems kommunikationstjänster. Com Hem har dessutom uteslutande kontroll vad gäller hanteringen av väsentliga inställningar. I och med att det endast är Com Hem som kan göra ändringar i dessa inställningar får Com Hem anses förfoga över modemen i dessa delar. Mot bakgrund av dessa omständigheter bedömer PTS att den aktuella utrustningen utgör en tillgång som används av Com Hem 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 Com Hems åtgärder beträffande de aktuella modemen i förhållande till tillämpliga krav som de framgår av PTS föreskrifter.

Säkerhetsarbete i enlighet med 3 § i PTSFS 2014:1

I föreliggande ärende framgår att Com Hem uppmärksammades på de aktuella sårbarheterna under hösten 2013 via ett e-postmeddelande till Com Hems kundtjänst. Härefter testades och implementerades en mjukvaruuppgradering som visade sig vålla kvalitetsproblem, vilket föranledde Com Hem att återinstallera tidigare mjukvara under tiden leverantören ombads ta fram en korrigerad mjukvara. Com Hem har själv konstaterat att detta arbete gått för långsamt och bedrivits med för låg intensitet, vilket grundat sig på att problemet tidigare bedömts vara av mindre allvarlig karaktär och därmed inte eskalerats till ansvarig chef eller säkerhetsansvarig. Först i samband med tidningsartiklar den 31 oktober 2014 vidtogs mer aktivt åtgärder. Mot bakgrund av de allvarliga konsekvenser ett utnyttjande av den aktuella sårbarheten skulle kunnat få för Com Hems abonnenter finner PTS det anmärkningsvärt att Com Hem inte agerat skyndsammare. PTS kan dock konstatera att Com Hem dragit lärdom av det inträffade och har infört en säkerhetsklassificering av säkerhetsbrister som utgör sårbarhet och hot mot kundplacerad utrustning. Arbetet med prioritering av bland annat mjukvaruuppgraderingar styrs numera av resultatet av

genomförda riskanalyser och bedömd hotbild. Vidare har Com Hem inrättat ett godkännandeförfarande för att på ett mer skyndsamt sätt kunna godkänna mjukvaruuppgraderingar.

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. Com Hem har beskrivit sitt övergripande säkerhetsarbete i detta ärende i samband med möte med PTS. Av Com Hems redogörelse framgår att det finns en utpekat ansvarig för att ställa säkerhetskrav på bland annat kundplacerad utrustning och för att löpande hantera säkerhetsfrågor relaterade till denna utrustning. Vidare har de beskrivit sitt arbete med att lista informationsbehandlingstillgångar och hur de arbetar med riskanalyser avseende dessa. För större risker har de en genomgång med en särskilt sammansatt grupp som bland annat består av CTO (Chief Technical Officer) och chefen för den juridiska avdelningen.

Com Hem har också beskrivit ett antal åtgärder som vidtagits för att informera kunderna och för att uppgradera mjukvaran m.m. med anledning av uppmärksammade sårbarheter. PTS noterar att säkerhetsarbetet huvudsakligen varit av reaktiv karaktär med anledning av de säkerhetsbrister som uppmärksammats i detta ärende och vill i detta sammanhang betona 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 Com Hem 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 modem 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.

PTS kan konstatera att Com Hem genomför en teknisk analys som är inriktad mot risker hänförliga till de olika typer av modem som tillhandahålls. 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 eventuella nya sårbarheter så att en bedömning kan göras om det finns behov av förnyade riskanalyser eller andra åtgärder. Com Hem har i ärendet beskrivit sitt arbete med omvärldsbevakning och att det finns en särskilt utpekad med ansvar för detta.

PTS kan konstatera att det ovan beskrivna arbetet huvudsakligen står i överensstämmelse med PTS föreskrifter. PTS anser dock 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 modemen.

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. Com Hem har beskrivit att man tilldelar supportpersonal i kundserviceorganisationen behörighet att genomföra fjärrinloggning för att kunna logga in och kontrollera enheternas status och inställningar i samband med felsökning. Vidare tilldelas teknisk personal i drifts- respektive kundserviceorganisationen behörighet att genomföra fjärrinloggning via administrationsgränssnitt för teknisk avancerad felsökning och diagnosticering. Båda kategorierna av personal utgör en begränsad andel av Com Hems 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 Com Hem 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 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 Com Hem loggar den egna personalens åtgärder. PTS har dock inte särskilt granskat Com Hems loggar eller utförda kontroller i detta ärende.

Samlad bedömning

Mot bakgrund av de åtgärder Com Hem har genomfört och redovisat i ärendet för att komma till rätta med de uppmärksammade 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