BESLUT

Datum	Vår referens	Sida
2017-10-06	Dnr: 16-8986	1(6)

Nätsäkerhetsavdelningen
[redacted]

Tele2 Sverige AB
[redacted]

Endast via e-post

Tillsyn av åtgärder för skydd av behandlade uppgifter i butiks- och återförsäljarledet

Saken

Tillsyn av åtgärder enligt 5 – 7 och 9 §§ PTSFS 2014:1 för skydd av behandlade uppgifter i butiks- och återförsäljarledet.

Post- och Telestyrelsens beslut

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

Bakgrund

Den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst (tjänstetillhandahållare) ska vidta lämpliga åtgärder för att säkerställa att de uppgifter som överförs, lagras eller på annat sätt behandlas i samband med tillhandahållandet av tjänsten skyddas. 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.[1]

Tjänstetillhandahållare är således skyldiga att analysera riskerna för att integritetsincidenter inträffar och utifrån dessa vidta nödvändiga åtgärder för att skydda behandlade uppgifter. För att säkerställa ett visst minimiskydd har PTS föreskrivit om ett antal grundläggande åtgärder som tjänstetillhandahållare åtminstone ska vidta.[2]

[1] 6 kap. 3 § lagen (2003:389) om elektronisk kommunikation (LEK).
[2] Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter.

Post- och telestyrelsen

Postadress:
Box 5398
102 49 Stockholm

Besöksadress:
Valhallavägen 117 A
www.pts.se

Telefon: 08-678 55 00
Telefax: 08-678 55 05
pts@pts.se

Under 2015 och 2016 inträffade ett antal integritetsincidenter i butiks- och återförsäljarledet hos flera tillhandahållare av mobiltelefonitjänster. Till följd av detta beslutade PTS att inleda tillsyn mot de fyra största aktörerna som tillhandahåller dessa tjänster i egna butiker, hos återförsäljare eller bådadera för att granska deras åtgärder för skydd av behandlade uppgifter och om dessa åtgärder uppfyller föreskrivna krav.[3]

PTS beslutade att avgränsa tillsynen till en granskning av de grundläggande åtgärder som krävs enligt 5 – 7 och 9 §§ PTS föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter. De åtgärder som ska vidtas enligt dessa paragrafer avser åtkomsthantering, behörighetshantering, loggning och kryptering. Tjänstetillhandahållarnas eventuella ytterligare skyddsåtgärder – som krävs enligt 4 § PTSFS 2014:1 – faller således utanför tillsynen. PTS beslutade vidare att avgränsa tillsynen till att avse skyddsåtgärder för uppgifter som behandlas i tjänstetillhandahållarnas IT-system som används vid försäljning av mobiltelefonabonnemang i butiksmiljö (nedan kallat säljstödsystem). För varje tjänstetillhandahållare som ingick i tillsynen har PTS hållit möten och besökt en butik som antingen tillhört tjänstetillhandahållaren eller en återförsäljare.

Tele2 Sverige AB (Tele2) är en av de tjänstetillhandahållare som omfattas av den aktuella tillsynen. PTS inledde tillsynen mot bolaget den 29 augusti 2016. PTS har hållit möten med Tele2 hos PTS vid två tillfällen, den 26 september 2016 och den 10 oktober 2016. Den 2 november 2016 besökte PTS tillsammans med Tele2 en butik i Järfälla tillhörande Elgiganten, som är en av Tele2s återförsäljare.

Tele2 har vid dessa besök redogjort för bolagets skyddsåtgärder och förevisat säljstödsystemet. PTS granskning av Tele2s åtgärder för skydd av uppgifter som behandlas i bolagets säljstödsystem baseras på de iakttagelser och de muntliga uppgifter som framkommit i samband med tillsynsbesöken.

Iakttagelser och inhämtade uppgifter

Tele2s säljstöd utgörs i huvudsak av två olika system, men nedan beskrivs dessa som *säljstödsystemet*.

I säljstödsystemet behandlas vissa uppgifter, såsom samtalstider och förbrukad datamängd, samt uppgift om abonnemang. Det är inte möjligt att se kunders fakturor och samtalsspecifikationer.

Tele2 ger säljare i egna butiker och hos återförsäljare behörighet till säljstödsystemet. Administrationen är delegerad så att butikschefer ger sina säljare behörigheter i säljstödsystemet.

[3] 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.

Tele2 avtalar med återförsäljare om att återförsäljare ska utbilda sina säljare. Anställda i Tele2s egna butiker utbildas och upplyses om tystnadsplikten vid anställningstillfället, då behörighet till säljstödsystemet tilldelas.

Tele2 följer regelbundet upp tilldelade behörigheter. Konton som inte används under en period inaktiverats för att sedan även raderas om användaren inte meddelat att kontot behöver återaktiveras.

En säljare som har fått behörighet kan komma åt uppgifterna i säljstödsystemet genom de datorer som finns i butiken. Säljstödsystemets webbsida nås genom det krypterade protokollet HTTPS. I butiken som besöktes var datorernas skärmar försedda med insynsskydd.

Säljstödsystemet har en funktion med autentisering som används i de flesta egna butiker och hos återförsäljare men inte överallt. Funktionen innebär att det krävs ett personligt användarnamn och lösenord för att komma åt uppgifter i systemet. Tele2 har beslutat att funktionen med autentisering ska användas i alla egna butiker och hos återförsäljare innan årsskiftet 2017/2018.

Åtkomst till säljstödsystemet är möjlig inifrån Tele2s nät och från butikskedjornas nät, inte från internet i övrigt. Endast trafik från återförsäljares IP-adresser släpps in. Det finns dock en funktion med tvåfaktorsautentisering som används av ett antal säljare som har behov av att använda säljstödsystemet utanför nätverk till vilket systemet är låst. I dessa fall skickas ett extra lösenord via SMS.

Vid besöket i återförsäljarens butik observerades flera olåsta och obemannade datorer. Funktionen med autentisering till säljstödsystemet användes men användarnamn och lösenord var förifyllda på flera datorers webbläsare.

Den besökta butiken har rutiner för att kunder alltid ska legitimera sig innan uppgifter hänförliga till kunden behandlas i säljstödsystemet. Systemet kräver dock inte tekniskt detta utan säljaren anger manuellt kundens personnummer i systemet för att komma åt uppgifterna.

Tele2 loggar all uppgiftsbehandling som sker i säljstödsystemet. Loggningen är försedd med larm som löser ut vid vissa typer av avvikande beteende i systemet. Sådana larm föranleder sedan manuell undersökning.

Skäl för beslutet

Föreskrivna krav

Åtkomsthantering

Enligt 5 § PTSFS 2014:1 ska tjänstetillhandahållaren 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.

Enligt allmänna råd till 5 § bör en relevant utbildning innehålla information om när och hur behandlade uppgifter får hanteras, tecken på att en integritetsincident har inträffat, tänkbara konsekvenser av en inträffad integritetsincident för abonnenter och användare, hur rapportering av integritetsincidenter ska ske samt hur uppföljning av integritetsincidenter sker i organisationen.

Behörighetshantering

Enligt 6 § ska tjänstetillhandahållaren 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 ha system för identitets- och åtkomsthantering som säkerställer att åtkomst endast medges i enlighet med tilldelade behörigheter.

Loggning

Enligt 7 § ska tjänstetillhandahållaren 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.

Enligt allmänna råd till 7 § bör kontroll av loggar ske med den periodicitet som är lämplig med hänsyn till verksamhetens omfattning, antalet personer med behörighet, hur behörigheterna tilldelas och hur omfattande kontrollen är.

Kryptering

Enligt 9 § ska behandlade uppgifter som överförs via internet skyddas genom kryptering. Detta gäller inte vid överföring till berörd abonnent eller användare om denne vid det enskilda tillfället har samtyckt till att överföringen sker utan kryptering. Kryptering ska ske med en allmänt erkänd krypteringsmetod med tillräcklig nyckellängd. Krypteringsnycklar ska hanteras på ett säkert sätt. Tjänstetillhandahållaren ska ha dokumenterade rutiner för kryptering och hantering av krypteringsnycklar.

PTS bedömning

PTS ser positivt på att Tele2 begränsar mängden uppgifter säljare har åtkomst till, t.ex. genom att inte låta säljare ta del av kunders samtalsspecifikationer i säljstödsystemet. PTS vill dock i sammanhanget framhålla vikten av att fortlöpande arbeta med att anpassa säljarnas behörigheter för att säkerställa att åtkomst till behandlade uppgifter begränsas till de uppgifter en säljare behöver för att utföra sina arbetsuppgifter.

Förbindelsen mellan webbläsaren och säljstödsystemet använder HTTPS vilket innebär att den är krypterad och därmed torde uppfylla kraven enligt 9 § PTSFS 2014:1, under förutsättning att nycklarna är tillräckligt långa och hanteras säkert samt att rutinerna för detta dokumenteras.

Tele2 är skyldigt att säkerställa att åtkomst till behandlade uppgifter endast ges till den som behöver det för att utföra sina arbetsuppgifter samt att kunna se vilken säljare som har vidtagit vilken åtgärd med vilken uppgift och vid vilken tidpunkt. För att säkerställa detta förutsätts det personlig inloggning samt att dessa personliga inloggningsuppgifter inte är förifyllda i systemet. PTS noterar att Tele2 inte säkerställer detta i dagsläget men ser positivt på att bolaget har beslutat att personlig inloggning ska vara införd innan årsskiftet 2017/2018. PTS lämnar denna del av tillsynen utan åtgärd, men kan komma att följa upp den angivna tidplanen och hur den personliga inloggningen tillämpas i praktiken.

PTS vill även framhålla vikten av att fortlöpande arbeta med att säkerställa att endast behöriga får del av uppgifter i säljstödsystemet. Detta har både en intern och en extern dimension, dvs. det innefattar både att säljare endast kommer åt uppgifter om de kunder som de faktiskt betjänar och att obehöriga butiksbesökare inte ges åtkomst till behandlade uppgifter i säljstödsystemet. Det är Tele2 som är skyldigt att analysera riskerna för att integritetsincidenter inträffar och utifrån dessa vidta de åtgärder som är lämpliga för att hantera de identifierade riskerna.

Riskanalyserna ska regelbundet följas upp och vid behov justeras, t.ex. i ljuset av incidenter som inträffar. Om analyserna visar att det finns risk för bedrägerier och att säljare bryter mot tystnadsplikten kan det därför finnas anledning att ytterligare begränsa åtkomsten till uppgifter i säljstödsystemet. T.ex. kan det finnas anledning att överväga om åtkomsten till uppgifter i säljstödsystemet bör begränsas så att det endast är möjligt att få åtkomst till kunduppgifter efter att systemet automatiskt läst av den aktuella kundens id-handling, och därmed ta bort möjligheten att manuellt ange en kunds personnummer och därmed få åtkomst till kunduppgifterna. Det kan även finnas anledning att överväga om ytterligare fysiska hinder, såsom automatisk låsning eller utloggning vid inaktivitet, skulle kunna vara åtgärder som i ytterligare utsträckning skulle kunna förhindra obehörig – och därmed otillåten – åtkomst till behandlade uppgifter.

Skäl att fortsätta tillsynen av avseende skyddsåtgärder för behandlade uppgifter i butiks- och återförsäljarledet finns inte, varför ärendet avskrivs från vidare handläggning.

Beslutet har fattats av enhetschefen Staffan Lindmark. I ärendets slutliga handläggning har även Camilla Östlund och Mikael Ejner (föredragande) deltagit.