BESLUT

Datum	Vår referens	Sida
2017-10-06	Dnr: 16-8985	1(5)

Nätsäkerhetsavdelningen
[redacted]

Hi3G Access 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.

Hi3G Access AB (Tre) är en av de tjänstetillhandahållare som omfattas av den aktuella tillsynen. PTS inledde tillsynen mot bolaget den 29 augusti 2016. PTS har besökt Tre vid två tillfällen, dels den 3 oktober 2016 på Tres kontor i Stockholm dels den 28 oktober 2016 i Tres egen butik i Sollentuna.

Tre har vid dessa besök redogjort för bolagets skyddsåtgärder och förevisat säljstödsystemet. PTS granskning av Tres 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

I Tres säljstödsystem behandlas inga uppgifter rörande befintliga kunder. Systemet kan endast användas för att teckna nya abonnemang åt kunder. Samtliga säljare i Tres egna butiker och hos återförsäljare har behörighet till systemet. Säljare som arbetar i Tres egna butiker kommer även åt CRM-systemet där det finns uppgifter om befintliga kunder och deras abonnemang.

Säljare i Tres egna butiker utbildas av Tres säkerhetschef och upplyses om tystnadsplikten i samband med anställning. I avtal med återförsäljare kräver Tre att säljare utbildas i bl.a. tystnadsplikt för att få behörighet till 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.

Tre har en process för att tilldela behörigheter till anställda och säljare hos återförsäljare. För återförsäljare är det en delegerad process där återförsäljaren själv administrerar behörigheter i säljstödsystemet.

Tre kan kontrollera att rätt behörigheter är tilldelade, samt ändra lösenord och spärra användare. Tre följer upp tilldelade behörigheter löpande.

Den besökta butiken är en av Tres egna butiker där de anställda utöver själva säljstödsystemet har tillgång till CRM-systemet som nås genom krypterad fjärruppkoppling som kräver personlig inloggning. Butikschefen har en egen bärbar dator som kräver tvåfaktorsautentisering för åtkomst till Tres system. Skulle ett konto inte ha använts efter 90 dagar stängs det.

Säljstödsystemets webbsida kräver personlig inloggning och nås med det krypterade protokollet HTTPS.

Tre har rutiner för att kunder alltid ska legitimera sig innan uppgifter hänförliga till kunden behandlas i säljstödsystemet. Tres butiker är dessutom utrustade med ett id-säkerhetssystem för att hindra identitetsbedrägerier. Systemet är dock inte tekniskt anslutet till säljstödsystemet utan för att komma åt en kunds uppgifter krävs att säljaren manuellt anger kundens personnummer i systemet.

Tre loggar all uppgiftsbehandling som sker i säljstödsystemet. Loggarna sparas i sex månader och kontrolleras dagligen. Systemet är utrustat med larm som reagerar på vissa sökbeteenden.

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 Tre har valt att utforma säljstödsystemet så inga uppgifter om abonnenter visas för återförsäljare.

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.

PTS vill 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 Tre 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.

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.