Datum	Vår referens	Aktbilaga
2016-08-17	Dnr: 14-11114	9

Nätsäkerhetsavdelningen

[redacted]

Bahnhof 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

Under hösten 2014 förekom uppgifter i media om att flera operatörers kundplacerade utrustningar var behäftade med säkerhetsbrister. Utrustningen, t.ex. modem, routrar och IP-telefonidosor (kundplacerad utrustning), hade i vissa fall en sårbarhet som innebar att obehöriga personer kunde få åtkomst till utrustningen och de uppgifter som behandlas i dessa.

Mot bakgrund av uppgifterna har PTS beslutat att inleda en granskning av hur ett urval operatörer tillgodoser skyddet av behandlade uppgifter när det gäller kundplacerad utrustning. Bahnhof AB (Bahnhof) har ingått i den aktuella tillsynen. Fokus för tillsynen är att granska operatörens arbete med åtkomst- och behörighetshantering, samt loggning. Fråga har även uppkommit i tillsynen om den kundplacerade utrustningen är en sådan tillgång som omfattas av reglerna om integritetsskydd i lagen (2003:389) om elektronisk kommunikation (LEK).

Inom ramen för tillsynen har PTS begärt upplysningar angående vilka typer av kundplacerad utrustning Bahnhof tillhandahåller abonnenterna och det

säkerhetsarbete som bolaget bedriver för att tillgodose att de uppgifter som behandlas i utrustningen skyddas. PTS har därvid efterfrågat t.ex. vilken behörighets- och åtkomsthantering som sker och vilken loggning som görs för de aktuella tillgångarna.

Bahnhof har i skriftliga svar till PTS redogjort för de av PTS ställda frågorna. Av svaren har bland annat framkommit vilken kundplacerad utrustning som företaget tillhandahåller sina kunder och vilka abonnemang som tillhandahålls. Bahnhof har även redogjort för behörighets- och åtkomsthanteringen samt vilken loggning som görs.

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) (föreskrifterna) framgår bland annat följande:

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.

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.

Utifrån de uppgifter Bahnhof har lämnat kan PTS konstatera att Bahnhof tillhandahåller sina kunder kundplacerad utrustning som en del i sitt erbjudande av vissa elektroniska 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 i vissa fall behörighet att ansluta till utrustningen via ett begränsat administrationsgränssnitt. På så vis kan kunderna anpassa utrustningen, till exempel genom att sätta egna lösenord.

Bahnhofs personal kan genomföra fjärrinloggning i samband med supportärenden. Detta innebär att Bahnhof har kontroll av delar av utrustningen som kunden inte råder över eller har möjlighet att påverka. Med hjälp av denna kontroll kan Bahnhof 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. I och med att Bahnhof har kontroll över vissa delar och kan göra ändringar i inställningarna får Bahnhof 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 Bahnhof 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).

Behörighets- och åtkomsthantering, samt loggning

Syftet med bestämmelserna i 5-6 §§ i föreskrifterna 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). Bestämmelserna är inte avsedda att reglera villkoren för abonnenternas användning av kundplacerad utrustning. Detta medför att bestämmelserna inte hindrar att abonnenter t.ex. ges möjlighet att ändra vissa inställningar i den kundplacerade utrustningen för att anpassa dessa till sina behov.

Enligt bestämmelserna ska tjänstetillhandahållaren säkerställa att åtkomst till behandlade uppgifter endast ges till den personal som behöver det för att utföra sina arbetsuppgifter. Vidare ska 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 hanteras, 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 Bahnhofs support- som driftsärenden kräver åtkomst till vissa av de uppgifter som behandlas i den kundplacerade utrustningen. Bahnhof har beskrivit att man tilldelar få arbetsgrupper behörighet att genomföra fjärrinloggning. Denna grupp av personal utgör en begränsad andel av Bahnhofs personal och tilldelas behörighet med utgångspunkt i behovet av att ta del av uppgifter för att kunna vidta nödvändiga åtgärder för drift och kundstöd.

PTS har 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. Utifrån de uppgifter Bahnhof lämnat gör PTS dock bedömningen att behörighet till åtkomst till den kundplacerade utrustningen endast ges till de som behöver det för att utföra sina arbetsuppgifter.

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 den kundplacerade utrustningen som genomförs av de arbetsgrupper som har behörighet till utrustningen omfattas av skyldigheten att logga utförda behandlingar. Utifrån de uppgifter som lämnats av Bahnhof kan PTS 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 Bahnhofs redovisning i ärendet och med de påpekanden PTS har gjort ovan, kan myndigheten konstatera att det saknas anledning att i dagsläget vidta ytterligare åtgärder i ärendet. Ärendet ska därför avskrivas från vidare handläggning.

Beslutet har fattats av enhetschefen Staffan Lindmark. I ärendets slutliga handläggning har även Peder Cristvall och Anders Lindell (föredragande) deltagit.

PTS

Beslutat av: Staffan Lindmark