Datum 2019-02-28
Vår referens Dnr: 18-5043
Aktbilaga 9

Nätsäkerhetsavdelningen

Telenor Sverige AB

Beslut om avskrivning av tillsyn gällande tjänstetillhandahållares förmåga att upptäcka och hantera sårbarheter i signaleringssystem nummer 7 (SS7)

Saken

Tillsyn gällande tjänstetillhandahållares förmåga att upptäcka och hantera sårbarheter i signaleringssystem nummer 7 (SS7).

Post- och telestyrelsens avgörande

Post- och telestyrelsen avskriver ärendet från vidare handläggning.

Bakgrund

SS7 består av en uppsättning protokoll som möjliggör tillgång till ett flertal tjänster för både fasta och mobila nätverk. Det har sedan en tid tillbaka varit känt att SS7 innehåller sårbarheter som innebär att aktörer exempelvis kan spåra mobiler, avlyssna samtal och läsa sms. Sådana former av attacker kan utgöra en integritetsincident vilket kan innebära ett hot mot tilltron till elektroniska kommunikationstjänster.

PTS har tidigare tillsammans med andra nordiska regulatoriska myndigheter utarbetat rekommendationer kring möjliga och lämpliga åtgärder för att upptäcka och motverka vissa hot som utnyttjar SS7. Rekommendationerna är inte bindande men innehåller ett flertal åtgärder som kan vara motiverade att genomföra för att hantera SS7-relaterade hot.

Mot bakgrund av de kända sårbarheterna i SS7 har PTS granskat vilka skyddsåtgärder Telenor Sverige AB (Telenor) har vidtagit i syfte att hantera sårbarheterna. Inom ramen för tillsynen har Telenor besvarat ett antal skriftliga

frågor. Bolaget har förevisat och demonstrerat de tekniska verktyg som används för att upptäcka och hantera SS7-relaterade hot i samband med ett möte varvid Telenor också redogjorde för bolagets rutiner och processer kring säkerhetsfrågor rörande SS7.

Telenor har sammanfattningsvis anfört följande.

De har arbetat med säkerhetsåtgärder gällande SS7-relaterade hot sedan 2014. De har vidtagit ett antal åtgärder i enlighet med rekommendationer och best practice. De loggar och analyserar signaleringstrafik i syfte att upptäcka illasinnad signalering. De har arbetsmetoder och processer för att kunna hantera säkerhetsincidenter. De har upprättat en intern struktur för omvärldsbevakning och deltar exempelvis vid möten inom olika fora såsom säkerhetskonferenser.

Skäl

Tillämpliga bestämmelser

Enligt definitionen i 6 kap. 1 § LEK är en integritetsincident en händelse som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring, eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster.

Enligt 6 kap. 3 § 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 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.

Av Post- och telestyrelsens (PTS) föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1), nedan benämnda föreskrifterna, framgår bland annat krav på att tjänstetillhandahållaren identifierar de informationsbehandlingstillgångar där behandlade uppgifter förekommer och för en förteckning över dessa. Av 4 § andra stycket föreskrifterna framgår att tjänstetillhandahållaren ska analysera riskerna för att integritetsincidenter inträffar för de informationsbehandlingstillgångar som tjänstetillhandahållaren identifierat. Av 4 § tredje stycket framgår att tjänstetillhandahållarna ska vidta de skyddsåtgärder som föreskrivs i 6-9 §§ samt andra nödvändiga skyddsåtgärder på den nivå som är lämplig för att hantera de risker som har identifierats.

Enligt 7 kap. 1 § LEK ska tillsynsmyndigheten bl.a. ha tillsyn över efterlevnaden av lagen och de föreskrifter som har meddelats med stöd av lagen. Enligt 2 §

förordningen (2003:396) om elektronisk kommunikation är PTS tillsynsmyndighet enligt LEK.

PTS bedömning

Genom bestämmelserna i LEK kompletterade med PTS föreskrifter finns ett skydd för behandling av uppgifter vid tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster. Detta ställer krav på de aktörer som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster att de vidtar åtgärder för att upprätthålla ett sådant skydd.

PTS kan konstatera att Telenor har uppmärksammat de sårbarheter som är förknippade med SS7 och att bolaget har vidtagit ett antal åtgärder i linje med gällande rekommendationer. Signaleringstrafiken övervakas i syfte att upptäcka illasinnad signalering. Uppenbart felaktiga SS7-meddelanden blockeras. Telenor har dessutom arbetsmetoder och processer på plats för att kunna hantera säkerhetsincidenter och har en aktiv omvärldsbevakning genom att bland annat delta i olika fora där sårbarheter och motåtgärder för att åtgärda dessa diskuteras.

PTS kan vidare konstatera att Telenor planerar för ett antal kommande aktiviteter inom området.

Mot bakgrund av vad som framkommit i ärendet bedömer PTS att skäl saknas att fortsätta granska Telenors åtgärder för att komma till rätta med sårbarheterna förknippade med SS7 i detta ärende. PTS vill dock poängtera att ett aktivt säkerhetsarbete förutsätter en kontinuerlig bevakning av nät och tjänster samt ett fortsatt vidtagande av adekvata säkerhetsåtgärder. PTS avser också att i kommande tillsyn granska operatörernas fortsatta arbete för att komma tillrätta med sårbarheter förknippade med såväl SS7 som med nyare signaleringssystem.

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

PTS

Beslutat av: Staffan Lindmark