Datum	Vår referens	Aktbilaga
2016-12-13	Dnr: 15-7027	18

Nätsäkerhetsavdelningen
Anders Lindell
08-6785541
anders.lindell@pts.se

Telenor Sverige AB

Tillsyn av säkerheten i system som innehåller kunduppgifter

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

I april 2015 inkom Telenor med en inledande och en kompletterande incidentrapport till PTS. Av rapporterna framgår att Telenor, efter underrättelse från en utomstående person, i mars 2015 fått kännedom om en integritetsincident som ska ha inträffat redan i maj 2012. Incidenten bestod i att en tidigare anställd olovligen kopierat en kunddatabas som sedan använts i eget försäljningssyfte. Kunddatabasen innehöll ett stort antal uppgifter som omfattat både kunduppgifter som namn, personnummer och telefonnummer men även uppgifter om kundens abonnemang i form av start- och slutdatum på abonnemang och abonnemangsform.

PTS har utifrån denna händelse inlett tillsyn. Tillsynen har främst varit inriktad på granskning av Telenors rutiner för åtkomst- och behörighetshantering, samt granskning av operatörens rutiner för loggning.

På begäran av PTS har Telenor inkommit med skriftliga svar på de frågor PTS har ställt, samt vid ett möte med myndigheten presenterat företagets arbete med anledning av incidenten och de åtgärder som vidtagits. Telenor har härvid beskrivit det generella säkerhetsarbete som bolaget bedriver när det gäller

hanteringen av uppgifter som behandlas i samband med tillhandahållande av elektroniska kommunikationstjänster. Det har bland annat varit frågan om de övergripande rutiner och processer som finns på plats, samt den rollfördelning som finns inom organisationen. Telenor har även beskrivit sina rutiner för åtkomst- och behörighetshantering, samt sina rutiner för loggning och kontroll av loggar.

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) som trädde ikraft den 1 september 2014 framgår bland annat följande:

Tjänstetillhandahållarens säkerhetsarbete avseende behandlade uppgifter ska enligt 3 § bedrivas långsiktigt, kontinuerligt och systematiskt och det ska finnas en tydlig rollfördelning med särskilt utpekade ansvariga. Rutiner, processer och rollfördelning ska dokumenteras.

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. Vid misstanke om att en integritetsincident har inträffat ska relevanta loggar alltid kontrolleras.
Tjänstetillhandahållaren ska ha dokumenterade rutiner för kontroll av loggar.

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.

PTS bedömning

Åtkomst och behörighet

I den aktuella tillsynen har en nu före detta anställd hos Telenor haft tillgång till och kopierat ett stort antal uppgifter om abonnenter och deras abonnemang från en kunddatabas. Telenor har härvid uppgivit att denna person hade tilldelats den åtkomst och behörighet till kunddatabasen som krävdes för gärningen, eftersom personen behövde detta för sitt arbete.

Inom ramen för tillsynen har Telenor beskrivit sin åtkomsthantering till olika system och de behörigheter som finns till dessa. Telenor har även redogjort för den översyn av åtkomst- och behörighetshanteringen som genomförts efter att incidenten upptäcktes. Översynen har lett till att ett flertal behörigheter har tagits bort eller begränsats.

Av Telenors redogörelser framgår, enligt PTS bedömning, att kunddatabasen och liknande system som innehåller behandlade uppgifter skyddas mot obehörig åtkomst av rutiner som säkerställer att endast de med godkänd behörighet ges tillgång till systemen. Enligt PTS bedömning finns det inget som tyder på att den person som orsakat incidenten skulle ha haft en snävare behörighet än vad som var fallet. Telenors rutiner innefattar instruktioner om hur de rollbaserade behörigheterna tilldelas i olika nivåer samt hur de kan ändras eller tas bort. I den utsträckning som PTS har granskat Telenors rutiner för åtkomst- och behörighetshantering, bedömer PTS att Telenor uppfyller kraven i föreskrifterna.

Att operatören även har genomfört en övergripande översyn och begränsat sina behörigheter tyder vidare på att Telenor, enligt PTS bedömning, har dragit

lärdomar från den inträffade incidenten och vidtagit åtgärder för att minska risken för att en incident inträffar som orsakats av obehörig åtkomst.

Enligt PTS bedömning behöver operatören även i framtiden kontinuerligt arbeta med att säkerställa att rutinerna för åtkomst- och behörighet följs, och tillse att behörigheterna löpande följs upp för att bland annat säkerställa att dessa är på lämplig nivå, samt att gamla behörigheter tas bort om en anställd slutar eller byter tjänst. Att detta arbete kontinuerligt prioriteras i verksamheten kan PTS komma att följa upp i framtida tillsyn. Med detta påpekande lämnar PTS denna del av tillsynen utan ytterligare åtgärd.

Loggning

I det övergripande säkerhetsarbetet ska Telenor analysera riskerna för att integritetsincidenter inträffar i de aktuella systemen och utifrån detta ska lämpliga skyddsåtgärder vidtas, däribland loggning. Syftet med kravet på loggning är bland annat att operatören ska kunna kontrollera vilka som varit inne i systemen och se vad de gjort samt vid vilken tidpunkt. För att uppnå detta är det viktigt att det finns bra loggar. Det är också viktigt att dessa loggar kontrolleras systematiskt och återkommande, samt att det finns rutiner för hur kontrollen ska utföras och att kontrollen dokumenteras. Vid en misstanke om att en integritetsincident har inträffat ska relevanta loggar alltid kontrolleras.

Telenor har beskrivit den loggning som sker av åtkomst och aktiviteter i det berörda systemet. Telenor har också uppgivit att man tagit fram rutiner för kontroll av loggar som bland annat innebär kontroll av viss typ av aktivitet och avvikande mönster i användningen. Enligt uppgift från Telenor görs kontinuerliga kontroller av loggar, vilka nu också dokumenteras. Telenor har vidare uppgivit att man förbättrar de verktyg som används för granskningen av loggar och det arbetet bedöms vara klar**t** under 2017.

PTS konstaterar att det har tagit lång tid för Telenor att upptäcka incidenten, samt att det faktum att bolaget blivit varse om det inträffade först efter tips från utomstående kan hänföras till brister i Telenors rutiner för kontroll av loggar. Även vad som loggas bör kontinuerligt ses över samt behovet av automatiska varningar som aktiveras vid avvikande beteenden för att snabbt kunna detektera potentiella incidenter. Detta ska bland annat göras med grund i de risker som analyserats för att en integritetsincident kan inträffa.

PTS förutsätter att en förbättring av kontroller av loggar som de nya förbättrade verktygen medför kommer att innebära en minskad risk för att integritetsincidenter inträffar eller att det åtminstone går snabbare att upptäcka dem och därmed kunna begränsa skadan.

PTS vill i detta sammanhang betona vikten av kontinuerliga kontroller av loggarna samt att med jämna mellanrum se över de parametrar som kontrolleras, som stora slagningar eller andra avvikande beteenden. En utökad och systematiserad kontroll av loggarna behövs och PTS kan komma att granska detta då de nya rutinerna och systemen är implementerade. Med detta lämnar PTS även denna del av tillsynen utan ytterligare åtgärd i dagsläget.

Sammantaget gör PTS bedömningen att det saknas skäl att vidta ytterligare åtgärder i ärendet. PTS beslutar därför att skriva av ärendet från vidare handläggning.

Beslutet har fattats av enhetschefen Patrik Bystedt. I ärendets slutliga handläggning har även Karin Lodin och Anders Lindell (föredragande) deltagit.