Vår referens: 21-4941 **Aktbilaga:** 24

Telenor Sverige AB
Org.nr. 556421-0309

Underrättelse om misstanke om bristande skyddsåtgärder i röstbrevlådesystem

Saken

Underrättelse enligt 7 kap. 4 § lagen (2003:389) om elektronisk kommunikation om misstanke om bristande skyddsåtgärder i röstbrevlådesystem.

Post- och telestyrelsens underrättelse

Telenor Sverige AB (Telenor) underrättas om Post-och telestyrelsens (PTS) misstanke om att Telenor brister i efterlevnad av 6 kap. 3 § lagen (2003:389) om elektronisk kommunikation (LEK) och 3 § första stycket samt 4 § andra stycket och tredje stycket första meningen i PTS föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter (föreskrifterna). Bristen består i att Telenor, i förhållande till de förekommande och identifierade riskerna, inte har vidtagit tillräckliga skyddsåtgärder för uppgifter i företagets röstbrevlådesystem.

För att efterleva ovan nämnda regler i LEK och föreskrifterna och därmed förhindra obehörigt intrång, samt underlätta avslöjanden om intrång i abonnentens röstbrevlådor ska Telenor:

- Införa en automatisk funktion som låser röstbrevlådan efter tre misslyckade inloggningsförsök.

- Löpande logga och övervaka misslyckade inloggningsförsök i syfte att avslöja och förhindra intrång i röstbrevlådor.

Post- och telestyrelsen
Postadress: Box 5398, 102 49 Stockholm
Besöksadress: Valhallavägen 117 A
Telefon: 08-678 55 00
E-post: pts@pts.se
www.pts.se

- Tekniskt övervaka systemen för att tidigt upptäcka avvikande trafikmönster mot röstbrevlådor samt ha en tydlig rutin och organisation för att vidta åtgärder baserat på vad övervakningen visar.

- I de fall ett abonnemangs röstbrevlåda har en initial lösenkod ska denna vara slumpmässigt genererad för varje enskild röstbrevlåda. Den initiala lösenkoden får inte utgöras av ett standardvärde eller kunna härledas ur annan data, t.ex. abonnentens PUK-kod.

- Abonnenten eller användaren ska kunna välja att ändra lösenkod till sin röstbrevlåda.

- Det ska finnas tekniska hinder mot att använda enkla lösenkoder, både initialt och när abonnent eller användare väljer lösenkod själv. Varken tillhandahållare eller abonnent ska kunna välja lösenkoder med för låg säkerhetsnivå. Det gäller åtminstone följande sekvenser: 1234, 9876, 1111, 2222, 3333, 4444, 5555, 6666, 7777, 8888, 9999, 0000 och 1212.

Åtgärderna ska vara genomförda **senast den 3 januari 2022.**

Telenor bereds tillfälle att yttra sig över denna underrättelse och tillämpningen av GSMA:s riktlinjer **senast den 1 september 2021.**

I yttrandet bör Telenor ange vilka åtgärder som företaget vidtagit eller avser att vidta med anledning av underrättelsen.

Om Telenor inte inkommer med yttrande kan PTS komma att fatta beslut på det underlag som står till myndighetens förfogande.

Bakgrund

I mars 2021 rapporterade Telenor en integritetsincident till PTS om omfattande intrång i ett röstbrevlådesystem. Incidenten visade säkerhetsbrister, som hade utnyttjats, i röstbrevlådesystemet. Inledningsvis rapporterades bristerna i ett röstbrevlådesystem, men Telenor har mot bakgrund av sin internutredning och den tillsyn som följt arbetat med ytterligare säkerhetsbrister av olika grad i alla bolagets röstbrevlådesystem.

Telenor fick kännedom om incidenten i början av februari och påbörjade en utredning för att identifiera vilka röstbrevlådor som berördes av incidenten. Telenor kunde konstatera att 800

röstbrevlådor under februari 2021 drabbades av incidenten. Incidenten rapporterades i mars 2021 till PTS.

Den 22 april 2021 beslutade PTS att inleda en tillsyn om Telenors arbete för att leva upp till kraven på skydd av uppgifter i röstbrevlådor.

PTS bedömning omfattar inte tjänsten visual voicemail.

Telenor har under tillsynen i huvudsak uppgett följande:

Telenor har fem olika system för röstbrevlådor. Telenor är medlem i branschorganisationen GSMA. Bolaget har i tillsynen uppgett att bolaget arbetar efter GSMA:s riktlinjer för tillhandahållare avseende säkerhetsåtgärder för röstbrevlådor i alla dessa fem system.

När ett nytt mobilabonnemang tecknas hos Telenor ingår även en röstbrevlåda. Röstbrevlådan aktiveras i samband med att abonnemanget aktiveras. Röstbrevlådan tilldelas en initial lösenkod av Telenor. Före incidenten tillämpade och tillät Telenor lösenkoder med låg säkerhetsnivå för röstbrevlådor. Den säkerhetsbristen utnyttjades av obehörig vid incidenten.

Vid tidpunkten då Telenor mottog information om försök till intrång i röstbrevlådor kunde bolaget inte i det angripna systemet, genom övervakning eller loggning upptäcka incidenter av det här slaget, fastställa när angreppen började, eller hur många abonnenter som drabbats. Telenor startade då en intern utredning och började också spara mer uppgifter från det systemet.

Telenor har i tillsynen angett vilka säkerhetsåtgärder som bolaget efter incidenten vidtar, utvecklar eller utreder i alla sina röstbrevlådesystem. Telenors uppfattning är att bolaget genom dessa åtgärder uppfyller ett tillräckligt skydd i alla röstbrevlådesystemen.

Telenor har i vissa av sina röstbrevlådesystem infört säkrare lösenkoder och i ett par system spärrar mot enkla lösenkoder, eller spärrar mot ett fåtal enkla koder. I ett par system tvingas nu abonnenten att välja en ny lösenkod med högre säkerhetsnivå än innan incidenten. Telenor inför också i ett röstbrevlådesystem spärr vid misslyckade inloggningsförsök, och utreder det i ett annat system. I alla röstbrevlådesystem där det inte fanns tidigare, utvecklar nu Telenor förbättrade rutiner för övervakning. Loggning av misslyckade inloggningsförsök utvecklas i majoriteten av systemen.

Skäl

Tillämpliga bestämmelser

Av 7 kap. 4 § LEK framgår att om PTS finner skäl att misstänka att den som bedriver verksamhet enligt denna lag inte efterlever lagen eller de beslut om skyldigheter eller villkor eller de föreskrifter som har meddelats med stöd av lagen, ska myndigheten underrätta den som bedriver verksamheten om detta förhållande och ge denne möjlighet att yttra sig inom skälig tid.

Enligt 6 kap. 3 § LEK ska den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst vidta lämpliga tekniska och organisatoriska 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.

Enligt 3 § första stycket i föreskrifterna ska tjänstetillhandahållaren ha ett säkerhetsarbete avseende behandlade uppgifter som är långsiktigt, kontinuerligt och systematiskt.

Enligt 4 § andra och tredje styckena i föreskrifterna ska tillhandahållaren analysera riskerna för att integritetsincidenter inträffar för de identifierade informationsbehandlingstillgångarna, samt vidta de skyddsåtgärder som är nödvändiga, på den nivå som är lämplig för att hantera de identifierade riskerna.

Enligt det allmänna rådet till 4 § bör tillhandahållarens vidtagna skyddsåtgärder följa etablerade standarder, normer och praxis.

PTS har i sin bedömning av vad som är lämpliga och nödvändiga åtgärder lagt vikt vid GSMA:s riktlinjer: GSMA | SG.20 Voicemail Security Guidelines - Security (se länk eller bilaga 1).

PTS bedömning

PTS finner skäl att misstänka att Telenor inte har vidtagit nödvändiga skyddsåtgärder på den nivå som är lämplig och nödvändig för att hantera riskerna i enlighet med kraven i 6 kap. 3 § LEK och 3 § första stycket samt 4 § andra stycket och tredje stycket första meningen i föreskrifterna.

Vid tidpunkten för de aktuella intrången använde Telenor inte tillräckligt säkra lösenkoder i det angripna röstbrevlådesystemet. Det fanns inte någon spärr vid upprepade misslyckade inloggningsförsök i röstbrevlådesystemet som angreps. Det saknades också sådan

övervakning och loggning som gjorde att Telenor självt kunde upptäcka, förhindra eller begränsa integritetsincidenten.

Det var säkerhetsbristerna i det angripna röstbrevlådesystemet som möjliggjorde att obehörig kunde ta del av innehåll i röstbrevlådorna, och som också möjliggjorde det stora antalet intrång utan att Telenor upptäckte det. På grund av de bristande skyddsåtgärderna har det inte heller helt kunnat utredas hur många abonnenter som totalt har drabbats av incidenten, eftersom Telenor inte inledningsvis hade tillräckliga uppgifter för att på egen hand upptäcka incidenten.

Telenor har uppgett att bolaget arbetar efter GSMA:s riktlinjer för tillhandahållare avseende säkerhetsåtgärder för röstbrevlådor i alla bolagets röstbrevlådesystem. PTS bedömning är att riktlinjerna ger en bra grund för ett tillräckligt säkerhetsarbete i linje med tillämpliga regler. Telenor har i tillsynen redogjort för en rad åtgärder som införs, utreds och planeras. Dessa åtgärder skiljer sig åt för de fem olika systemen. Åtgärderna når endast delvis upp till de rekommendationer som finns i GSMA:s riktlinjer.

Riskerna för allvarliga integritetsincidenter genom obehörigt intrång i röstbrevlådor är hög. Det är känt inom telekombranschen. Därför behövs de åtgärder som PTS beskrivit i denna underrättelse.

Kostnaderna för dessa lämpliga och nödvändiga åtgärder bedöms av PTS som proportionerliga med beaktande av de kände riskerna, det sagda i denna underrättelse, och med beaktande av tillgänglig teknik.

Dessa åtgärder, som PTS således bedömer som lämpliga och nödvändiga, ska dels markant förbättra säkerhetsnivån i röstbrevlådesystemen i syfte att förhindra obehöriga att olovligen tränga in i röstbrevlådor, dels säkerställa att Telenor kontinuerligt och systematiskt arbetar för att få kännedom om avvikande trafikmönster i röstbrevlådesystemen för att på så vis kunna avslöja och förhindra olovliga intrång i abonnenters röstbrevlådor.

Mot bakgrund av ovanstående bedömer PTS att Telenors befintliga och planerade åtgärder är otillräckliga för att uppnå det skydd för uppgifter som reglerna och riskerna kräver. Det är inte tillräckligt att införa några av säkerhetsåtgärderna, utan samtliga uppräknade åtgärder ska införas för samtliga röstbrevlådor i samtliga röstbrevlådesystem.

Tid för rättelse

Åtgärderna ska vara genomförda senast **den 3 januari 2022.**

Telenor får tillfälle att yttra sig

PTS finner sammanfattningsvis att myndigheten enligt 7 kap. 4 § LEK ska underrätta Telenor om att myndigheten misstänker att Telenor agerar i strid med 6 kap. 3 § LEK och 3 § första stycket samt 4 § andra stycket och tredje stycket första meningen i föreskrifterna.

Telenor ges tillfälle att senast **den 1 september 2021** yttra sig över denna underrättelse och tillämpningen av GSMA:s riktlinjer (se länk ovan eller bilaga 1).

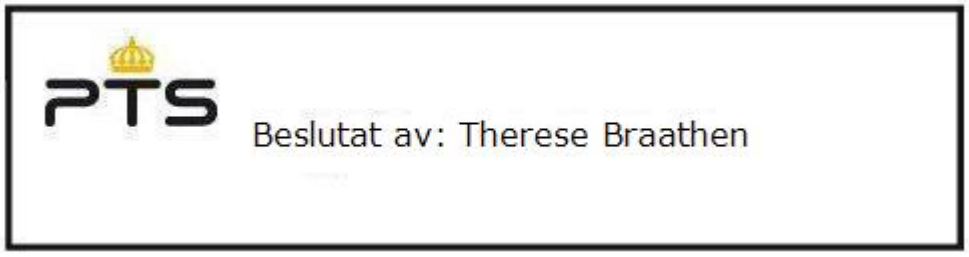
När tiden för att inkomma med yttrande har löpt ut kan PTS med stöd av 7 kap. 5 § LEK komma att meddela de förelägganden som behövs för att Telenor ska vidta nödvändiga åtgärder för rättelse. Eventuella förelägganden kan komma att förenas med vite. Om Telenor inte alls hörs av kan PTS ändå komma att fatta beslut på det underlag som står till myndighetens förfogande.

Överklagandehänvisning

Ett beslut om underrättelse enligt 7 kap. 4 § LEK får enligt 8 kap. 21 § samma lag inte överklagas.

Therese Braathen

Underrättelsen har beslutats av tf enhetschefen Therese Braathen. Föredragande har varit Anna Montelius. I ärendets slutliga handläggning har även Karina Ekdahl, Frida Ekengren samt verksjuristen Louise Steengrafe och tf chefsjuristen Katarina Holmqvist deltagit.


PTS
Beslutat av: Therese Braathen