Datum	Vår referens	Aktbilaga
2020-06-25	19-5751	26

Telia Company AB, 556103-4249

Föreläggande att vidta skyddsåtgärder vid autentisering i kundtjänst

Saken

Föreläggande enligt 7 kap. 5 § lagen (2003:389) om elektronisk kommunikation (LEK); fråga om att vidta skyddsåtgärder vid autentisering i kundtjänst.

Post- och telestyrelsens avgörande

Post- och telestyrelsen (PTS) förelägger Telia Company AB (Telia) att senast den 31 mars 2021 införa en teknisk lösning som säkerställer att kunder som ringer in till kundtjänst är korrekt autentiserade innan kundtjänstmedarbetaren kan lämna ut uppgifter eller göra ändringar i abonnemang. En korrekt skyddsåtgärd ska omöjliggöra att information som behandlas i samband med tillhandahållandet av den elektroniska tjänsten kan avslöjas eller ändras på uppmaning av obehörig person via telefonkundtjänst. Den tekniska lösningen ska innebära att autentisering av kunder inte kan ske via en manuell bedömning av kundtjänstpersonal, utan avgörandet om autentiseringen blir godkänd eller ej ska ligga hos den tekniska lösningen. Det ska därmed inte heller vara möjligt att från- eller kringgå rutiner för autentisering.

Detta föreläggande gäller enligt 8 kap. 22 § LEK omedelbart.

Bakgrund

Under 2018 och 2019 har PTS tagit emot rapporter från flera tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster (tillhandahållare) om integritetsincidenter kopplade till kundtjänst. Dessa incidenter tyder på att medarbetare i tillhandahållarens kundtjänst brustit i sin autentisering av personer som ringer kundtjänst, vilket inneburit att obehörig person har kunnat

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

ändra eller komma åt uppgifter om en kunds abonnemang. Detta är en av de vanligaste integritetsincidenter som rapporteras till PTS. I och med att flera tillhandahållare rapporterat in liknande händelser har PTS funnit anledning att misstänka brister i tillhandahållares metod för att skydda behandlade uppgifter vid autentisering i kundtjänst.

PTS beslutade därför i maj 2019 att inom ramen för tillsyn granska ett antal tillhandahållare, däribland Telia, vad gäller företagets metod att autentisera personer som ringer till kundtjänsten för att få information om eller göra ändringar i en kunds abonnemang. Tillsynen avgränsades till kundtjänst som tillhandahålls via telefon.

PTS har begärt in dokumentation från Telia om rutinerna för autentisering av personer som ringer företagets kundtjänst samt även en övergripande beskrivning av hur Telia tillämpar dessa rutiner. PTS har vid möte med Telia gått igenom rutiner och processer och har ställt frågor till medarbetare i kundtjänst.

Telia har uppgett i huvudsak följande:

Telia har rutiner för identifiering som ska följas av personal i bolagets kundtjänst. Kundtjänst använder bl.a. följande säkerhetsåtgärder för identifiering av personer som ringer:

Vid enklare ärenden kan kundtjänstmedarbetaren använda kontrollfrågor angående detaljer kring kundens abonnemang som endast kunden kan känna till.

Mobilt BankID ska alltid användas vid ett antal ärenden där viktig information om kunden lämnas ut eller där ändringar i abonnemanget görs.

Brevutskick till folkbokföringsadress sker som bekräftelse vid ändring i abonnemang och vid de fall kunden inte har BankID så skickas skriftligt underlag.

Motringning används ofta i familjeabonnemang när felanmälan görs. Felanmälan tas emot och sedan kontaktas abonnemangsinnehavaren för hantering av ärendet.

Att hänvisa till butik är ett alternativ om kunden inte har BankID.

Om kundtjänstmedarbetaren tycker att något är misstänkt i samtalet, t.ex. om kunden ringer från ett annat nummer än sitt eget eller om kunden låter osäker på något annat sätt, så kan kundtjänstmedarbetaren använda BankID.

Telia har också uppgett att nyanställda kundtjänstmedarbetare får utbildning om bolagets rutiner för autentisering i kundtjänst.

Telias inställning

PTS har den 3 februari 2020, i enlighet med 7 kap. 4 § LEK, underrättat Telia om att myndigheten finner skäl att misstänka att Telia inte efterlever 6 kap. 3 § LEK och 4 § i PTS föreskrifter (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter, genom att inte vidta tillräckliga skyddsåtgärder i samband med autentisering vid telefonsamtal med företagets kundtjänst. Telia har i yttrande daterat den 28 februari 2020 och vid möte den 25 mars 2020 sammanfattningsvis framfört följande:

Telia anser att det är av yttersta vikt att deras kunder har förtroende för att Telia hanterar deras personuppgifter på ett säkert och korrekt sätt. Telia ser kontinuerligt över sina rutiner och hur de efterlevs i ljuset av bl. a. inträffade incidenter, teknikutveckling m.m. för att säkerställa att uppgifter om kunderna inte lämnas till och utnyttjas av obehöriga. Telia utvecklar och förbättrar identifieringsmetoderna för allt fler ärenden i kundtjänsten men det kvarstår fortfarande problemet att personalen i vissa fall inte följder rutinerna. Det måste därför bli svårare att göra fel och enklare att göra rätt.

Telia avser i detta syfte att genomföra ett flertal tekniska åtgärder och en kartläggning och mappning av aktiviteter mot autentiseringsbehov. Första steget att utföra tekniska åtgärder är att införa bank-id i talsvar. När kartläggningen är klar ska tekniska åtgärder för korrekt autentisering införas. Telia har anfört att de kan vara klara med både steg 1 och steg 2 till årsskiftet 2020/2021.

Skäl

Tillämpliga bestämmelser

I 7 kap. 4 § LEK anges 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, inte efterlever en genomförandeåtgärd som avses i 1 § andra stycket eller inte använder en radiosändare i den utsträckning som villkoren medger, ska myndigheten underrätta den som bedriver verksamheten om detta förhållande och ge denne möjlighet att yttra sig inom skälig tid.

Enligt 7 kap. 5 § LEK får tillsynsmyndigheten meddela de förelägganden och förbud som behövs för rättelse av en överträdelse som avses i 4 § ska ske omedelbart eller inom skälig tid. Följs inte föreläggandet, får tillsynsmyndigheten, efter utgången av den tid som angetts i underrättelsen enligt 4 §, meddela de ytterligare förelägganden eller förbud som behövs för efterlevnaden. Enligt fjärde stycket får förelägganden och förbud förenas med vite.

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 4 § Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter ska tillhandahållaren vidta de skyddsåtgärder som anges i föreskrifterna samt andra nödvändiga skyddsåtgärder, på den nivå som är lämplig för att hantera de identifierade riskerna.

PTS bedömning

Den som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster har ett ansvar att skydda uppgifter som behandlas i samband med tillhandahållandet. Integritetsincidenter som kan uppstå när sådana uppgifter inte skyddas kan leda till allvarliga konsekvenser för enskilda användare, såsom ekonomisk skada, allvarlig personlig kränkning eller till och med fara för liv och hälsa om en obehörig får tillgång till information. Dessutom kan integritetsincidenter försvaga allmänhetens tillit till elektroniska kommunikationstjänster.

PTS har i sin tillsyn av Telia och andra tillhandahållare av elektroniska kommunikationstjänster funnit att rutiner för att använda skyddsåtgärder vid autentisering av inringande kund inte alltid följs. Detta leder typiskt sett till att information om kunden delas med obehörig person eller att en obehörig person kan göra ändringar i en kunds abonnemang. Detta utgör en brist i åtgärderna för att skydda uppgifter som behandlas i samband med tillhandahållande av den elektroniska kommunikationstjänsten.

Antalet anmälda incidenter skiljer sig åt mellan de tillhandahållare som PTS granskat men metoderna för autentisering skiljer sig inte åt i någon större utsträckning. PTS bedömer därför att brister i autentiseringen av personer som ringer till kundtjänst är ett generellt problem hos alla tillhandahållare som ingår i tillsynen.

PTS anser att det stora antalet incidenter som rapporterats in av flera tillhandahållare till PTS stödjer bedömningen att risken för att personuppgifter som behandlas i samband med tillhandahållandet av den elektroniska kommunikationstjänsten lämnas ut till obehörig person är hög. Kunder ringer även in till operatörens kundtjänst för att få hjälp med att göra ändringar i sitt abonnemang och sker inte en korrekt autentisering av kunden finns risk att det är en obehörig person som gör ändringar i kundens abonnemang. Om inte de skriftliga eller muntliga rutinerna följs av kundtjänstmedarbetaren är risken stor att ett otillåtet avslöjande eller en otillåten ändring görs av kundens personuppgifter och abonnemang.

För att hantera risken för att obehöriga får tillgång till kunders personuppgifter eller kan göra ändringar i abonnemang anser PTS att det krävs en teknisk skyddsåtgärd som hindrar detta. Den tekniska skyddsåtgärden ska säkerställa att kunden är korrekt autentiserad innan information om kunden lämnas ut eller förändring av kundens abonnemang eller av kundens uppgifter görs. Det ska därmed inte vara möjligt att kringgå rutinerna för autentisering.

Telia ska därför föreläggas att införa en teknisk lösning som säkerställer att kunder som ringer in till kundtjänst är korrekt autentiserade innan kundtjänstmedarbetaren kan lämna ut uppgifter eller göra ändringar i abonnemang. En korrekt skyddsåtgärd ska omöjliggöra att information som behandlas i samband med tillhandahållandet av den elektroniska tjänsten kan avslöjas eller ändras på uppmaning av obehörig person via telefonkundtjänst. Den tekniska lösningen ska innebära att autentisering av kunder inte kan ske via en manuell bedömning av kundtjänstpersonal, utan avgörandet om autentiseringen blir godkänd eller ej ska ligga hos den tekniska lösningen. Det ska därmed inte heller vara möjligt att från- eller kringgå rutiner för autentisering. Telia kan exempelvis uppfylla detta krav genom att införa de tekniska lösningar som beskrivits i Telias kompletterande yttrande i PTS tillsyn daterat den 28 februari 2020 vilka har förtydligats vid möte den 25 mars 2020 och i skrivelse daterat den 2 april 2020.

Tid för rättelse

PTS anser att den tid som Telia uppgett för färdigställande av funktionaliteten är rimlig med hänsyn till utvecklingens omfattning och art, samt behovet av noggranna tester, utbildning och information till kunder. Vidare är det viktigt att den tekniska skyddsåtgärden är en väl genomtänkt lösning. Det föreligger inga hinder för Telia att vidta tekniska säkerhetsåtgärder för autentisering av kunder som ringer in till kundtjänst.

Tiden för rättelse sätts därför till den 31 mars 2021.

Underrättelse om överklagande

Om ni vill överklaga detta beslut ska ni skriva till Förvaltningsrätten i Stockholm. Brevet ska dock sändas till Post- och telestyrelsen, Box 5398, 102 49 Stockholm, alternativt till pts@pts.se.

Tala om i brevet vilket beslut ni överklagar genom att ange beslutets nummer. Tala också om vilken ändring av beslutet ni vill ha.

Brevet med överklagandet ska innehålla: ert person-/organisationsnummer, postadress, e-postadress och telefonnummer till bostaden och mobiltelefon. Adress och telefonnummer till er arbetsplats ska också anges samt eventuell annan adress där ni kan nås för delgivning. Om ni anlitar ett ombud, ska ombudets namn, postadress, e-postadress, telefonnummer till arbetsplatsen och mobiltelefonnummer anges.

PTS måste ha fått ert överklagande inom tre veckor från den dag ni fått del av beslutet. Annars kan överklagandet inte prövas.

PTS sänder överklagandet vidare till Förvaltningsrätten i Stockholm för prövning.

Om något är oklart kan ni vända er till PTS.

Beslutet har fattats av enhetschefen Anna Montelius. I ärendets slutliga handläggning har även Åsa Gihl (föredragande), Frida Ekengren, verksjuristen Julia Pistol, enhetscheferna Katarina Holmqvist och Åsa Möller samt chefsjuristen Karolina Asp deltagit.