Datum	Vår referens	Aktbilaga
2019-06-24	19-1561	8

Avdelningen för säker kommunikation

Telenor Sverige AB

Beslut – årlig tillsyn

Saken

Tillsyn enligt 7 kap. 1 § första stycket lagen (2003:389) om elektronisk kommunikation (LEK) över inrapporterade incidenter och rutiner för incidentrapportering.

Post- och telestyrelsens avgörande

Ärendet avskrivs.

Bakgrund

Post- och telestyrelsen (PTS) genomför årligen en planlagd tillsyn mot ett antal tillhandahållare av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster (tillhandahållare) för att granska och följa upp föregående års inträffade integritetsincidenter och störningar och avbrott av betydande omfattning, vilka tillhandahållarna är skyldiga att rapportera till PTS. I tillsynen granskas tillhandahållarnas arbete med att hantera, åtgärda och dra lärdomar av inträffade incidenter samt hur tillhandahållarnas rapportering av incidenter ser ut, mot bakgrund av reglerna i LEK med tillhörande föreskrifter och EU-förordning 611/2013[1]. Fokus i tillsynen ligger på uppföljning av tillhandahållarnas säkerhetsarbete mot bakgrund av de inträffade incidenterna.

[1] Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott.

Rapporterade incidenter

De incidenter som tas upp i årlig tillsyn är de som inrapporterats sedan föregående års årliga tillsyn och som inte omfattas av någon annan tidigare, pågående eller planerad tillsyn. För Telenor Sverige ABs (Telenor) del rör det sig om följande ärenden som granskats inom ramen för denna tillsyn:

Driftsäkerhetsincidenter med följande diarienummer hos PTS: 18-1357, 18-3224, 18-4072, 18-8035, 18-37208.

Integritetsincidenter med följande diarienummer hos PTS: 18-5815, 18-6660, 18-6942, 18-6970, 18-8040, 18-9210, 18-11235, 18-39598.

Skriftliga svar på frågor

I tillsynen har PTS begärt in skriftlig redogörelse från Telenor avseende hur de säkerställer att incidenter rapporteras i enlighet med regelverket samt hur de säkerställer att relevanta åtgärder vidtas med anledning av de incidenter som inträffat. Av de inkomna handlingarna framgår bl.a. att Telenor arbetar med incidenter enligt en modell för incidenthantering som baserar sig på ramverket ITIL. För incidenter som kräver uppföljning skapas ett problemärende vilket bl.a. innebär utredning av grundorsak, förebyggande åtgärder för att förhindra en liknande incident eller förbättrade möjligheter att bättra hantera en sådan incident i det fall den inte kan förhindras. Telenor har en intern modell för att prioritera incidenter och de med högre prioritet gås igenom veckovis vid ett särskilt forum. Incidenter och valda lösningar kan innebära risker och dessa rapporteras och hanteras via Telenors riskhanteringsprocess.

För rapportering av driftstörningar och avbrott är driftsledaren hos Security Operations Center (SOC) ansvarig. Alla skiftgående tekniker på SOC är instruerade i rutiner och rapporteringskrav vilket även finns dokumenterat i deras kunskapsdatabas. Vid omfattande störningar eller händelser där det varit medialt intresse rapporteras till PTS tjänsteman i beredskap. Information om en störning går även till kommunikationsavdelningen som kan kanalisera vidare till andra relevanta informationskanaler.

Telenor har även skickat in rutiner för att identifiera och internt rapportera integritetsincidenter. De har centrala styrande och stödjande dokument samt kompletterande lokala rutiner för vissa personalgrupper. Det uppmuntras internt att rapportera misstänkta integritetsincidenter antingen till sin närmaste chef eller via ett verktyg som finns på intranätet. Bedömningen av huruvida en händelse är en incident och vilken typ av incident det är görs av representanter från Telenors Legal/Regulatory och Telenors Privacy Office. Telenors Privacy

Officer ansvarar för rapportering till PTS i enlighet med Kommissionens förordning 611/2013.

Tillsynsmöte

Den 19 mars 2019 genomfördes ett tillsynsmöte med representanter från Telenor och PTS. Vid detta möte gicks samtliga incidenter igenom och Telenor redogjorde för händelseförlopp och orsak till dessa. Vidare redogjorde Telenor för de åtgärder som vidtagits, på kort och på lång sikt, med anledning av händelserna. Det framkom bl.a. följande.

Med anledning av händelseförloppet vid två driftsincidenter har de sett behov av att förtydliga rutinerna kring larm och bl.a. vilka händelser som ska föranleda vilken allvarlighetsgrad av larm. Telenor uppger att de nu förbättrat detta.

Vidare har Telenor haft en avgrävning av en kabel som lett till ett rapporteringspliktigt avbrott. De ser avgrävningar som ett stort problem och har därför anslutit sig till initiativet Grävallvar, ett forum för dialog mellan operatörer och grävare där de bl.a. uppmuntrar till användning av Ledningskollen.

Vad gäller integritetsincidenter så har Telenor haft flera incidenter med anledning av designfel och mjukvarubuggar. Åtgärder som de vidtagit är bl.a. utökad testning och att de förbättrat sina testscenarier. De har också haft incidenter vid manuell hantering av uppgifter. Telenor uppgav att de ser manuell hantering som ett riskmoment och att de försöker att minimera antalet manuella steg. På längre sikt vill de i större utsträckning använda Customer relationship management, CRM-system och mer reglerade gränssnitt. Åtgärder som Telenor vidtagit med anledning av incidenterna är bl.a. att de informerat berörda medarbetare om aktuella rutiner och i vissa delar förtydligat instruktionen. För tre huvudleverantörer har de infört systembaserade gränssnitt med endast viss manuell hantering och de har också påbörjat ett arbete med att i huvudsak använda sig av digitala avtal.

Vid mötet tog PTS upp vikten av att incidentrapporter avseende störningar och avbrott innehåller de uppgifter som framgick av PTS föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning PTSFS 2012:2 och som numera återfinns i PTSFS 2018:4. PTS framhöll även de tidsgränser för rapportering av integritetsincidenter som framgår av reglerna i Kommissionens förordning (EU) nr 611/2013.

Skäl

Tillämpliga bestämmelser

Av 5 kap. 6 b § LEK framgår bl.a. att den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet.

Bestämmelsen förtydligas genom PTS föreskrifter om krav på driftsäkerhet, PTSFS 2015:2.

Enligt 3 § PTSFS 2015:2 ska tillhandahållarens driftsäkerhetsarbete bl.a. bedrivas långsiktigt, kontinuerligt och systematiskt. Arbetet ska omfatta såväl normala driftsförhållanden som extraordinära händelser. Tillhandahållaren ska i driftsäkerhetsarbetet ha en tydlig rollfördelning med särskilt utpekade ansvariga för arbetet.

Enligt 7 § PTSFS 2015:2 ska tillhandahållaren bl.a. säkerställa att 1. inträffade incidenter rapporteras internt, 2. åtgärder vidtas skyndsamt för att hantera en uppkommen incident, 3. åtgärder vidtas för att undvika liknande incidenter, och 4. att erfarenheter från inträffade incidenter beaktas vid genomförande av riskanalyser enligt 5 §.

Av 5 kap. 6 c § första stycket LEK framgår att den som tillhandahåller ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst utan onödigt dröjsmål ska rapportera störningar eller avbrott av betydande omfattning till tillsynsmyndigheten.

Av PTSFS 2012:2, som gällde vid tidpunkten då granskade incidenter rapporterades, framgår bland annat vilka störningar och avbrott som ska rapporteras samt hur rapporteringen ska gå till. Regler om detta finns numera i PTSFS 2018:4.

Enligt 6 kap. 3 § 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. 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.

Närmare bestämmelser om vilka tekniska och organisatoriska åtgärder som tjänstetillhandahållare ska vidta finns i PTS föreskrifter och allmänna råd PTSFS 2014:1 om skyddsåtgärder för behandlade uppgifter.

Enligt 10 § PTSFS 2014:1 ska tjänstetillhandahållaren ha dokumenterade rutiner för identifiering, intern rapportering, hantering och uppföljning av integritets-incidenter. Rutinerna ska bl.a. säkerställa att skyddsåtgärder vidtas för att undvika liknande integritetsincidenter.

Av 6 kap. 4 a § första stycket LEK framgår att den som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster utan onödigt dröjsmål ska underrätta tillsynsmyndigheten om inträffade integritetsincidenter. Om incidenten kan antas inverka negativt på de abonnenter eller användare som de behandlade uppgifterna berör, eller om tillsynsmyndigheten begär det, ska även dessa underrättas utan onödigt dröjsmål.

När och hur rapportering av integritetsincidenter ska ske och vad rapporterna ska innehålla framgår av Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott.

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.

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

PTS bedömning

Rutiner för incidentrapportering

Telenor har rapporterat in såväl driftsäkerhets- som integritetsincidenter under det gångna året. De har rutiner för att upptäcka och rapportera både drift-säkerhetsincidenter och integritetsincidenter och har utpekade personer som sköter rapporteringen vilket PTS bedömer ger förutsättningar att hantera inträffade incidenter i enlighet med bestämmelserna i 5 kap. 6 c § första stycket LEK och 6 kap. 4 a § första stycket LEK.

PTS kan konstatera att Telenors inledande rapportering av integritetsincidenter i huvudsak sker i enlighet med fastställda tidsfrister men att kompletterande uppgifter vid flera tillfällen inte inkommit inom de tidsgränser som framgår av förordningen EU 611/2013. Vid tillsynsmötet poängterades vikten av att rapportering sker inom de uppställda tidsramarna. Om hanteringen av incidenten inte är helt färdigställd vid tidpunkten då komplettering ska ske kan ytterligare kompletteringar skickas till PTS därefter allteftersom arbetet fortskrider. PTS förutsätter att Telenor förbättrar sin hantering i detta avseende och ser inte anledning att fortsätta granskningen i denna del men PTS kan komma att följa upp detta.

Vad gäller rapporteringen av driftsäkerhetsincidenter har inledande rapport oftast inkommit i enlighet med tidsgränserna som gällde vid tidpunkten för incidenterna i PTSFS 2012:2. PTS kan konstatera att rapporterna vid flera tillfällen inte varit kompletta och PTS har fått ställa kompletterande frågor. Vid flera tillfällen har PTS dessutom fått påminna Telenor om att komma in med svar på dessa frågor. Detta togs upp vid tillsynsmötet och PTS förutsätter att Telenor förbättrar sin hantering även i detta avseende. PTS ser dock inte heller här anledning att granska detta närmare men kan komma att följa upp även denna del.

Vidtagna skyddsåtgärder

PTS har i granskningen av inträffade incidenter inte sett annat än att Telenor hanterar inträffade incidenter och vidtar åtgärder för att de inte ska inträffa igen i enlighet med 5 kap. 6 b § LEK och 7 § PTSFS 2015:2 samt 6 kap. 3 § LEK och 10 § PTSFS 2014:1. Telenor har bl.a. uppgett att de förbättrat sin larm-funktion vad gäller driftstörningar och infört systembaserade gränssnitt för vissa leverantörer för att minska risken för att personuppgifter skickas fel vilket är åtgärder som PTS bedömer som lämpliga. PTS vill dock framhålla vikten av att Telenor i sin utredning och analys av inträffade incidenter även identifierar långsiktiga åtgärder som kan vidtas för att liknande händelser inte ska inträffa. PTS kan t.ex. konstatera att det uppstått flera incidenter som beror på designfel och mjukvarubuggar som inte uppmärksammats vid testning. Även om de fel som konstaterats har avhjälpts och av Telenor bedömts inte kunna uppstå igen vill PTS uppmana Telenor att i större utsträckning identifiera och rapportera åtgärder som kan vidtas för att undvika att liknande händelser inträffar.

Sammanfattningsvis bedömer PTS att Telenor har förutsättningar att framöver hantera incidenter och incidentrapporteringen i enlighet med regelverket och det finns därmed inte skäl att fortsätta tillsynen och ärendet avskrivs därför.

Beslutet har fattats av t.f. enhetschefen Anna Montelius. I ärendets slutliga handläggning har även Mikael Ejner, Petra Nilsson och Caroline Sundholm (föredragande) deltagit.