Nätsäkerhetsavdelningen
Enheten för säker och
konfidentiell kommunikation

Hi3G Access AB
[redacted]

Endast via e-post

Årlig tillsyn av rapportering och vidtagna åtgärder med anledning av inträffade integritetsincidenter

Saken

Årlig tillsyn av rapportering och vidtagna åtgärder med anledning av inträffade integritetsincidenter.

Post- och telestyrelsens avgörande

Post- och telestyrelsen (PTS) avskriver ärendet från vidare handläggning.

Bakgrund

PTS genomför årligen en planlagd tillsyn mot ett antal tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster (tjänstetillhandahållare) för att granska och följa upp föregående års inträffade integritetsincidenter, vilka tjänstetillhandahållarna är skyldiga att rapportera till PTS. I tillsynen granskas tjänstetillhandahållarnas arbete med att hantera, åtgärda och dra lärdomar av inträffade incidenter samt hur tjänsteleverantörernas rapportering av integritetsincidenterna ser ut, mot bakgrund av reglerna i lagen (2003:389)

om elektronisk kommunikation (LEK) med tillhörande föreskrifter och EU-förordning 611/2013[1].

Ett av huvudsyftena med rapporteringsskyldigheten är att PTS ska kunna göra en bedömning av om det finns skäl att misstänka att bestämmelser i LEK, t.ex. bestämmelsen om skydd av behandlade uppgifter i 6 kap. 3 § LEK, inte efterlevs. Även i de fall en incidentrapport till PTS inte ger upphov till direkta tillsynsåtgärder, kan incidentrapporten innehålla uppgifter som bidrar till myndighetens kunskap om vanliga orsaker till integritetsincidenter. Detta kan i sin tur utgöra underlag för PTS planlagda tillsynsinsatser.

PTS inledde den 31 januari 2018 den planlagda årliga tillsynen rörande incidentrapportering och inträffade incidenter över Hi3G Access AB (Tre). Den 15 mars 2018 höll PTS ett tillsynsmöte med Tre. Tre har därutöver inkommit med bolagets förteckning över integritetsincidenter.

PTS granskning av Tres rapportering och åtgärder med anledning av inträffade integritetsincidenter baseras på de inskickade incidentrapporterna och förteckningen över integritetsincidenter samt de muntliga upplysningar som lämnats av Tre i samband med tillsynsmötet.

Vid tillsynsmötet redogjorde Tre för händelseförlopp och orsak till de integritetsincidenter som granskats i samband med den årliga tillsynen samt för de långsiktiga åtgärder som vidtagits och de lärdomar som dragits med anledning av dessa incidenter. Under tillsynsmötet beskrev Tre även hur bolaget fortlöpande utbildar personalen kring vad som kan utgöra en integritetsincident och hur sådana incidenter identifieras och hanteras.

Ett flertal av de inrapporterade incidenterna har uppkommit i samband med avvikelser från befintliga rutiner, exempelvis underlåtelse att inhämta fullmakt. Tre uppgav att de arbetar med att ta fram långsiktiga lösningar i form av tekniska begränsningar som syftar till att minska denna typ av incidenter.

Skäl

Tillämpliga bestämmelser

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

[1] Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation.

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.

Vidare bestämmelser om dessa tekniska och organisatoriska åtgärder 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 integritetsincidenter. Rutinerna ska säkerställa

1. att samtliga uppgifter i 11 § förs in i den förteckning som tjänstetillhandahållaren ska föra enligt 6 kap. 4 b § LEK,
2. att inträffade integritetsincidenter och dess orsaker beaktas vid genomgång av riskanalyser i enlighet med 4 §, och
3. 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.

Enligt 6 kap. 4 b § första stycket LEK ska den som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster löpande föra en förteckning över integritetsincidenter. Vilka uppgifter som företeckningen ska innehålla framgår av 11 § i PTSFS 2014:1.

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.

PTS bedömning

Tre har under tillsynsmötet gett en god bild av de inträffade integritetsincidenterna samt av de åtgärder som vidtagits och de lärdomar som dragits med anledning av dessa incidenter. PTS ser vidare positivt på att Tre kontinuerligt utbildar personalen kring hur integritetsincidenter kan identifieras och hanteras.

PTS anser att Tres rapporter och underrättelser av integritetsincidenter samt förteckningen över integritetsincidenter innehåller den information som krävs enligt gällande bestämmelser. PTS anser vidare att Tres incidentrapporter är tydliga och kan konstatera att de har inkommit i rätt tid.

PTS har generellt inom ramen för den årliga tillsynen noterat att integritetsincidenter många gånger orsakas av den mänskliga faktorn. Det kan t.ex. bero på bristande IT-stöd, slarv, avvikelse från befintliga rutiner, okunskap samt manuell hantering av handlingar. PTS kan konstatera att flera av de av Tre inrapporterade incidenterna har uppkommit i samband med avvikelser från befintliga rutiner. PTS vill därför understryka vikten av att ständigt dra lärdomar av inträffade incidenter och vidta lämpliga åtgärder. Tre har även uppgett att de har påbörjat ett arbete som syftar till att minska denna typ av incidenter. I sammanhanget kan PTS nämna att myndigheten har för avsikt att i en kommande tillsyn granska tillhandahållarnas åtgärder för att säkerställa identitet och behörighet vid kontakt med kundtjänst. Tre kan komma att omfattas av denna tillsyn.

PTS har sammanfattningsvis inte kunnat se några uppenbara brister i Tres hantering av inträffade integritetsincidenter.

Skäl att fortsätta den årliga tillsynen av rapportering och åtgärder med anledning av inträffade integritetsincidenter föreligger inte, varför ärendet avskrivs från vidare handläggning.

Beslutet har fattats av enhetschefen Staffan Lindmark. I ärendets slutliga handläggning har även Erika Hersaeus, Marie Wahlin Tideklev och Isabelle Westerlund (föredragande) deltagit.

Beslutat av: Staffan Lindmark