Datum	Vår referens	Aktbilaga
2020-04-29	Dnr: 20-992	17

Avdelningen för säker kommunikation

Hi3G Access AB

Beslut – årlig tillsyn

Saken

Tillsyn enligt 7 kap. 1 § första stycket lagen om elektronisk kommunikation (2003:389), 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.

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

De incidenter som behandlas i årlig tillsyn är de incidenter som inrapporterats till PTS sedan föregående års årliga tillsyn och som inte omfattas av någon annan tidigare, pågående, planerad eller händelsestyrd tillsyn. Hi3G har endast rapporterat in integritetsincidenter föregående år.

För Hi3G Access AB (Hi3G) har ett antal rapporterade integritetsincidenter med liknande grundorsaker granskats övergripande:

PTS referens	Hi3Gs referens
19-11094	20190925-02
19-13138	29101128-01
19-12904	20191121-01
19-12795	2019115-01
19-11489	20191004-01
19-11561	20191009-01
19-11473	20191004-02
19-11251	20190927-01
19-10924	20190920-02
19-10638	20190913-03
19-1373	20190211-01
19-9546	20190801-04
19-9493	20190731-01
19-9307	20190719-02
19-9306	20190719-01
19-8628	20190628-01

19-2435	20190315-01
19-2736	20190321-01
19-8873	20190704
19-13604	20191213-01
19-12932	20191121-02
19-1407	20190212-01
19-1357	20190205-01
19-966	20190129-01
19-967	20190129-02
19-3244	20190329-01
19-7591	20190604-01
19-8066	20190611-01
19-9006	20190708-01
19-10166	20190829-01
19-10423	20190902-01
19-10636	20190913-01
19-11987	20191025-01
19-12061	20191029-01
19-5298	20190507-02
19-5380	20190509-01
19-7934	20190612-01

I incidentrapporterna ges en beskrivning av integritetsincidenterna, vid vilka tidpunkter de inträffat och i förekommande fall vad de har fått för konsekvenser för slutanvändare. Vidare anges åtgärder som Hi3G vidtagit eller har för avsikt att vidta för att mildra effekterna av incidenterna och för att förhindra att liknande incidenter ska inträffa igen.

PTS har begärt in en skriftlig redogörelse för rapporterade incidenter som granskats övergripande. Avsikten har varit att klargöra huruvida vidtagna åtgärder har haft avsedd verkan för de ofta förekommande liknande fallen eller om ytterligare åtgärder varit påkallade.

Hi3G har inkommit med svar på PTS frågor den 9 mars 2020 och den 14 april 2020. Tillsynsmöte som PTS kallat till den 20 mars 2020 blev inställt pga av Covid-19 pandemi.

Hi3G har i de skriftliga svaren beskrivit ändringar som genomförts i processer och rutiner för att undvika att integritetsincidenter av samma slag upprepas.

Skäl

Tillämpliga bestämmelser

Integritet

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 integritetsincidenter. 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 artikel 2.2 första stycket denna förordning ska anmälan ha inkommit till PTS senast 24 timmar efter att personuppgiftsbrottet upptäckts (eng. *detection*). Av tredje stycket samma artikel framgår att ett personuppgiftsbrott ska anses ha upptäckts om leverantören har varit tillräckligt medveten om att en säkerhetsincident har inträffat som ledde till att personuppgifter äventyrats, för att göra en anmälan i enlighet med förordningen.

Tillsyn

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 ska myndigheten underrätta den som bedriver verksamheten om detta förhållande och ge denne möjlighet att yttra sig inom skälig tid.

PTS bedömning

Organisation för incidenthantering och rapportering

PTS konstaterar att Hi3G endast har rapporterat in integritetsincidenter under det gångna året. De underlag som Hi3G inkommit med visar enligt PTS bedömning att Hi3G har etablerade rutiner, utpekade personer och en organisation för såväl intern hantering som rapportering till PTS av integritetsincidenter.

Vidtagande av skyddsåtgärder

När det gäller de incidenter som PTS har granskat översiktligt framgår det att Hi3G har vidtagit åtgärder i syfte att avhjälpa problemen.

PTS kan konstatera att det av de skriftliga svar Hi3G lämnat på frågorna i myndighetens begäran om uppgifter framgår att de planerade åtgärder som finns angivna i incidentrapporterna och som tagits upp i efterföljande kommunikation har genomförts.

PTS bedömer att Hi3G har uppdaterat processer och rutiner för integritetsincidenter på ett lämpligt sätt.

PTS har en pågående tillsyn autentisering i kundtjänst som avgränsats till kundtjänst per telefon (PTS ärende nr 19-5730) och PTS har förväntningar på att en tillfredsställande teknisk lösning i detta ärende ska tas fram som kan tillämpas i samtliga kanaler. I avvaktan på beslut det ärendet ser vi inte skäl att fortsätta handläggningen i denna del inom ramen för årlig tillsyn.

Annat har inte framkommit genom de aktuella incidentrapporterna och den ytterligare skriftliga information som lämnats inom ramen för tillsynsärendet än att Hi3G har vidtagit skyddsåtgärder som är lämpliga för att avhjälpa och hantera identifierade brister i enlighet med 6 kap. 3 § LEK 10 § PTSFS 2014:1.

Sammanfattningsvis bedömer PTS att Hi3G har förutsättning att framöver hantera incidenter i enlighet med regelverket och det finns därmed inte skäl att fortsätta tillsynen.

Ärendet avskrivs därför från vidare handläggning.

Beslutet har fattats av enhetschefen Anna Montelius. I ärendets slutliga handläggning har även Linus Kilander Xu och Åsa Gihl (föredragande) deltagit.

PTS Beslutat av: Anna Montelius