Datum	Vår referens	Aktbilaga
2019-06-24	19-1560	10

Avdelningen för säker kommunikation

Hi3G Access AB

Beslut – årlig tillsyn

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

Tillsynen 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. Fokus i tillsynen ligger på uppföljning av tillhandahållarnas säkerhetsarbete mot bakgrund av de inträffade incidenterna.

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 Hi3G Access AB:s (Tre) del rör det sig om följande ärenden som granskats inom ramen för denna tillsyn:

Tres ärendenr	PTS diarienummer
2018-001	18-364
2018-007	18-2134
2018-012	18-3118
2018-030	18-9249
20180823-01	18-9796
20181227-01	18-39612
2018-018	18-6938
2018-019	18-7203
20181102-01	18-28265
20181106-01	18-33729
20190129-01	19-966 och 19-1020
20190129-02	19-967
20190125-01	19-838
20181022-01	18-12352
20181119-01	18-38339
2018-017	18-5816
20181024-01	18-12421
20190118-01	19-571
2018-009	18-2405
2018-016	18-4224
20190109-01	19-330
20180903-01	18-10183
20181030-01	18-25508
20181108-01	18-33663
20181211-01	18-39236
20190110-01	19-331
20190124-01	19-776
20181129-01	18-38677
20181129-02	18-38709
20181217-01	18-39392

I tillsynen har PTS begärt in skriftlig redogörelse från Tre avseende hur bolaget säkerställer att incidenter rapporteras i enlighet med regelverket samt hur bolaget säkerställer att relevanta åtgärder vidtas med anledning av de incidenter som inträffat.

Av de inkomna handlingarna framgår bl.a. att Tre sedan januari 2018 har tagit fram och implementerat en ny process för identifiering, intern rapportering, hantering och uppföljning av personuppgifts- och integritetsincidenter. För varje avdelning finns en utsedd roll, s.k. Privacy Officer, PO, som ansvarar för att integritetsincidenter blir utredda, rapporterade och att upphovet till incidenten blir åtgärdat. Inrapporterade integritetsincidenter följs upp, minst en gång per år. Förteckningen över beslutade åtgärder gås igenom och status och progress stäms av med berörda. De erfarenheter som dragits i samband med inträffade integritetsincidenter samt dess orsaker utgör ett underlag för Tres riskanalysarbete.

Vidare framgår av dessa handlingar att Tre har en incidenthanteringsprocess för driftstörning och avbrott för att säkerställa att relevanta åtgärder vidtas vid driftstörningar. Tres driftorganisation består nästintill uteslutande av egen personal och Tre arbetar med enhetliga driftprocesser inom alla teknikområden, med en hög grad av verktygsstöd vilket väsentligen försvårar möjligheten att avvika från arbetsrutiner. Samtliga händelser under en störning loggas och alla incidenter är sökbara. I samband med allvarligare störningar och avbrott genomförs en förnyad riskanalys. Tres nätövervakning har tillgång till ett flertal analysmetoder, för att kunna avgöra om en störning faller inom rapporterings-skyldigheten.

Den 14 mars 2019 genomfördes ett tillsynsmöte med representanter från PTS och Tre. Vid detta möte behandlades samtliga inträffade incidenter och det framkom bl.a. följande.

Tre redogjorde för händelseförlopp och orsak till de integritetsincidenter som granskats i samband med den årliga tillsynen. Händelseförloppen stämde i stort sett överens med beskrivningen i inlämnade incidentrapporter. Vidare redogjorde Tre för de direkta och långsiktiga åtgärder som vidtagits och de lärdomar som dragits med anledning av dessa incidenter.

Under tillsynsmötet beskrev Tre även att bolaget upptäcker många incidenter tack vare sin nya process som involverar hela organisationen. Processen började gälla från och med årsskiftet 2018/19.

Vidare uppgav Tre att personalen informeras och utbildas fortlöpande kring rutiner samt hantering och identifiering av incidenter. Tre har tagit fram ett nytt utbildningsverktyg för personalen. Införandet av BankID vid autentisering av kunder har haft stor betydelse för Tres arbete med skydd för behandlade uppgifter.

Ett flertal av de inrapporterade incidenterna har uppkommit i samband med avvikelser från befintliga rutiner. Tre uppgav härvid att många av Tres anställda arbetar med åtkomst till uppgifter under en kort tid.

Tre bekräftade att det inte har uppstått några rapporteringspliktiga störningar eller avbrott under tidsperioden. Avbrotten i samband med stormen Alfrida är den enda störningen sedan lång tid tillbaka, vilken omhändertas inom ramen för en annan tillsyn.

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 PTS föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning 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 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 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

PTS kan konstatera att Tre har rapporterat in integritetsincidenter under det gångna året. Tre har en rutin för rapportering av såväl integritetsincidenter som driftstörningar och avbrott. Det finns utpekade personer som sköter rapporteringen och det finns interna mallar och rutiner för incident-rapporteringen. PTS kan konstatera att Tres rapportering av incidenter i huvudsak sker i enlighet med fastställda tidsfrister och att rapporterna till övervägande del innehåller de uppgifter som efterfrågas. PTS ser positivt på att Tre kontinuerligt utbildar personalen kring hur integritetsincidenter kan förhindras, identifieras och hanteras. PTS bedömer att Tre har förutsättningar att även fortsättningsvis hantera incidentrapportering av integritetsincidenter i enlighet med 6 kap. 4 a § första stycket LEK och förordningen EU 611/2013.

Tre har inte haft någon incident avseende störningar eller avbrott, förutom avbrott i samband med stormen Alfrida, vilket har granskats närmare inom ramen för ett annat tillsynsärende. Av Tres inlämnade handlingar framgår emellertid att Tre har en incidenthanteringsprocess för störningar och avbrott för att säkerställa att relevanta åtgärder vidtas vid driftstörningar. PTS bedömer således att Tre har förutsättningar att hantera incidentrapportering av störningar eller avbrott i enlighet med 5 kap. 6 c § första stycket LEK och PTSFS 2018:4.

Vidtagna skyddsåtgärder

PTS kan konstatera att Tre under den granskade perioden har haft ett stort antal integritetsincidenter. Vid genomgång av ärendena framkom att incidenterna framförallt beror på att personal och underleverantörer har frångått befintliga rutiner. Tre har vid tillsynsmötet uppgett att de vidtagit åtgärder för att förhindra att rapporterade incidenter eller liknande händelser inträffar igen. Tre uppger att de har ett nytt utbildningsverktyg för personal. Vidare har Tre infört inloggning med BankID för kunder, för att Tre ska kunna behandla vissa uppgifter utan manuell hantering av Tres personal.

Av de granskade ärendena framgår att Tre, i samband med att incidenter har inträffat, har vidtagit åtgärder för att komma till rätta med vissa problem. De åtgärder som vidtagits framstår som relevanta åtgärder och PTS bedömer därför att Tre hanterat dessa i enlighet med 6 kap. 3 § LEK samt 10 § PTSFS 2014:1. PTS förutsätter att de vidtagna åtgärderna kommer att leda till att antalet integritetsincidenter minskar framöver.

PTS vill dock framhålla vikten av att Tre, i sin utredning och analys av inträffade integritetsincidenter, identifierar och vidtar ytterligare långsiktiga skyddsåtgärder för behandlade uppgifter, då ett stort antal av de inrapporterade integritetsincidenterna är likartade och med relativt enkla medel, såsom bättre kontroll vid autentisering och ytterligare utbildning av personalen, hade kunnat undvikas. Även om flertalet av de inrapporterade incidenterna inte har drabbat särskilt många enskilda så finns alltid en risk att varje inträffad incident får stora konsekvenser för enskilda individer.

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

Beslutet har fattats av t.f. enhetschefen Anna Montelius. I ärendets slutliga handläggning har Petra Nilsson (föredragande) deltagit.