Datum 2017-04-21

Vår referens Dnr: 17-1299

Nätsäkerhetsavdelningen

[redacted]

Hi3G Access AB

Årlig tillsyn över incidentrapportering och inträffade incidenter – Hi3G Access AB

Saken

Årlig tillsyn över incidentrapportering och inträffade incidenter.

Post- och telestyrelsens avgörande

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

Bakgrund

PTS genomför årligen planlagd tillsyn över ett urval operatörer, bland annat i syfte att dessa ska redogöra för inträffade incidenter under föregående år. Tillsynerna omfattar såväl driftstörningar som integritetsincidenter, vilka operatörerna är skyldiga att rapportera in till PTS. I tillsynen granskas operatörernas arbete med att identifiera, hantera, åtgärda och dra lärdomar av inträffade incidenter, mot bakgrund av reglerna om integritetsskydd i lagen (2003:389) om elektronisk kommunikation (LEK) med tillhörande föreskrifter. Vidare granskas hur operatörerna följer kraven på rapportering av inträffade incidenter.

Ett av huvudsyftena med inrapporteringsskyldigheten är att PTS ska kunna göra en bedömning av om det finns skäl att misstänka att bestämmelser i LEK, t.ex. bestämmelserna om integritetsskydd i 6 kap. 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

Post- och telestyrelsen

Postadress: Box 5398 102 49 Stockholm

Besöksadress: Valhallavägen 117A www.pts.se

Telefon: 08-678 55 00 Telefax: 08-678 55 05 pts@pts.se

PTS planlagda tillsynsinsatser och även bidra till myndighetens arbete med risk- och sårbarhetsanalyser för sektorn.

PTS inledde den 16 februari 2017 den planlagda årliga tillsynen rörande incidentrapportering och inträffade incidenter över Hi3G Access AB (Tre). Den 15 mars 2017 höll PTS ett tillsynsmöte med Tre.

Vid mötet beskrev Tre sina rutiner för rapportering och upptäckt av integritetsincidenter och hur bolaget hanterar dessa, samt hur de underrättar de drabbade kunderna. Tre uppgav att det liksom förra året är många av incidenterna som upptäckts av kunder och att bolaget sedan fångar upp dem internt för vidare utredning. Det sker också kontinuerligt en utveckling av utbildningspaketet för personalen för att förbättra förutsättningarna för att upptäcka och rapportera incidenter.

Tre redogjorde också för de tjugofem integritetsincidenter som rapporterats in till PTS sedan den senaste årliga tillsynen och vilka åtgärder som vidtagits med anledning av dessa. Tre presenterade även sin förteckning över integritets-incidenter. De flesta incidenterna har även detta år inträffat hos under-leverantörer till Tre och i flera fall har det varit fråga om samma under-leverantör. Det har i en majoritet av fallen varit frågan om avvikelser från gällande rutiner, och många incidenter är identiska.

Skäl

Tillämpliga bestämmelser

PTS är enligt 2 § förordningen (2003:396) om elektronisk kommunikation tillsynsmyndighet enligt LEK. PTS ska enligt 7 kap. 1 § LEK utöva tillsyn över efterlevnaden av lagen och de beslut om skyldigheter eller villkor samt de föreskrifter som meddelats med stöd av lagen.

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.

Enligt 6 kap. 4 a § LEK ska den som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster utan onödigt dröjsmål underrätta tillsynsmyndigheten om 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 ska ske framgår av Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott (förordningen).

Av PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1) framgår bland annat följande:

Tjänstetillhandahållarens säkerhetsarbete avseende behandlade uppgifter ska enligt 3 § bedrivas långsiktigt, kontinuerligt och systematiskt och det ska finnas en tydlig rollfördelning med särskilt utpekade ansvariga. Rutiner, processer och rollfördelning ska dokumenteras.

Tjänstetillhandahållaren ska enligt 4 § bland annat identifiera informationsbehandlingstillgångar och föra en förteckning över dessa samt analysera riskerna för att integritetsincidenter inträffar för de identifierade informationsbehandlingstillgångarna. Vidtagna skyddsåtgärder samt tjänstetillhandahållarens bedömningar av lämplig nivå ska dokumenteras och följas upp årligen och vid behov.

Tjänstetillhandahållaren ska enligt 10 § 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 § lagen (2003:389) om elektronisk kommunikation,
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.

Enligt 6 kap. 4 b § LEK ska tjänstetillhandahållaren löpande föra en förteckning över integritetsincidenter. Vad förteckningen närmare ska innehålla framgår av 11 § i de ovannämnda föreskrifterna.

PTS bedömning

Tre har rapporterat in tjugofem integritetsincidenter sedan den förra årliga tillsynen. PTS ser positivt på att Tre rapporterar in allt fler incidenter till PTS, då detta talar för att Tre har bra rutiner för upptäckt och rapportering. PTS ser också positivt på att Tre fortsätter att utbilda personal om integritetsincidenter och hur dessa ska rapporteras internt så att så många incidenter som möjligt fångas upp.

Det har också skett förbättringar från tidigare år gällande innehållet i rapporteringen till PTS, där de konkreta uppgifterna i underrättelsen till kunderna numera finns med. Det framgår nu även av underrättelsen till kunderna att de drabbade själva kan behöva fundera över vilka åtgärder de måste vidta på grund av incidenten för att begränsa eventuella negativa konsekvenser. Mot bakgrund av detta lämnar PTS denna del av tillsynen utan åtgärd.

PTS kan konstatera att Tres förteckning över integritetsincidenter innehåller de uppgifter som enligt 11 § i föreskrifterna måste finnas med i förteckningen, och PTS har därför inget att erinra i den delen av tillsynen.

När det gäller orsakerna till de inrapporterade integritetsincidenterna kan PTS konstatera att det stora flertalet av incidenterna har orsakats av en och samma underleverantör till Tre. Det finns mot denna bakgrund anledning att ifrågasätta Tres förmåga att t.ex. genom avtal och uppföljning av dessa säkerställa att underleverantörer lever upp till de krav på rutiner och säkerhetsåtgärder som lagen kräver. Detta tyder på en brist i det grundläggande säkerhetsarbetet hos Tre och PTS kommer att granska dessa förhållanden närmare i ett särskilt tillsynsärende. PTS lämnar därför även denna del av den årliga tillsynen utan åtgärd.

Skäl att fortsätta den årliga tillsynen mot Tre föreligger inte, varför ärendet avskrivs från vidare handläggning.

Beslutet har fattats av enhetschefen Staffan Lindmark. I ärendets slutliga handläggning har även juristerna Ulrika de la Iglesia och Anders Lindell (föredragande) deltagit.