Datum 2015-06-16

Vår referens Dnr: 15-1621

Nätsäkerhetsavdelningen
Karin Lodin
08-678 56 04
karin.lodin@pts.se

Årlig tillsyn över incidentrapportering och inträffade incidenter – Hi3G Access AB

Saken

Tillsyn över incidentraportering och inträffade incidenter.

Post- och telestyrelsens avgörande

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

Bakgrund

PTS genomför årligen planlagda tillsyner 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.

Ett av huvudsyftena med inrapporteringsskyldigheten är att PTS ska kunna göra en bedömning av om det finns skäl att misstänka att bestämmelser i lagen (2003:389) om elektronisk kommunikation (LEK), t.ex. bestämmelsen om driftsäkerhet i 5 kap. 6 b § 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 störningar och avbrott eller integritetsincidenter. Detta kan i sin tur utgöra underlag för PTS planlagda tillsynsinsatser och även bidra till myndighetens arbete med risk- och sårbarhetsanalyser för sektorn och till myndighetens arbete med robusthetshöjande åtgärder.

PTS inledde den 20 februari 2015 den planlagda årliga tillsynen rörande incidentrapportering och inträffade incidenter över Hi3G Access AB (Tre). Den 23 mars 2015 höll PTS ett tillsynsmöte med Tre.

Vid mötet beskrev Tre sina rutiner för rapportering av integritetsincidenter och hur bolaget hanterar dessa. Tre redogjorde även för de fem integritetsincidenter som rapporterats in till PTS under föregående år och vilka åtgärder som hade vidtagits med anledning av dessa. Tre presenterade även sin förteckning över integritetsincidenter.

När det gäller vissa frågor som myndigheten ställde vid Tres redogörelse kunde bolaget inte svara direkt vid mötet, till viss del beroende på att en nyckelperson hos Tre hade avslutat sin anställning. Det rörde t.ex. frågor avseende utbildning av personal och vilka åtgärder som Tre hade vidtagit för att undvika att liknande incidenter inträffar igen. Den 1 april 2015 återkom Tre med den efterfrågade informationen.

Vid Tres redogörelse för en av integritetsincidenterna påtalade PTS att myndigheten inte hade fått del av någon kopia på underrättelse till berörda abonnenter och användare. Tre uppgav härvid att man muntligen hade haft en löpande kontakt med berörda kunder.

Vid mötet redogjorde Tre även för hur bolaget arbetar med riskanalyser på integritetsområdet, och hur status var för bolagets efterlevnad av PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1). Tre informerade vid mötet om att arbete med att identifiera informationsbehandlingstillgångar och kritiska system hade initierats, men att Tre inte ännu efterlevde föreskrifterna fullt ut, främst avseende genomförande av riskanalyser och vidtagande av efterföljande skyddsåtgärder.

När det gäller störningar och avbrott av betydande omfattning redogjorde Tre för sina rutiner för upptäckt och rapportering av dessa. Tre framförde att föregående år ur driftsäkerhetshänseende hade varit bra, då Tre endast haft att rapportera in två incidenter till PTS. Den ena incidenten hade drabbat Tres samarbetspartner. Tre uppgav att samarbetet mellan Tre och Tres partner fungerade väl och att man säkerställt att felet var mycket ovanligt och inte bör inträffa igen. PTS informerade Tre om att rapporteringen av incidenten inte var fullständig från början, vilket renderade i ett antal efterföljande frågor från myndighetens sida.

Den andra incidenten rörde störningar och avbrott till följd av stormen Egon, vid vilken Tre hade rapporterat information inkluderades kartor med drabbade områden och situationsbilder.

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.

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.

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.

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) framgår bl.a. vilka störningar och avbrott som ska rapporteras samt hur rapporteringen ska gå till.

PTS bedömning

Inledningsvis kan PTS konstatera att Tre under det föregående året har rapporterat in fem integritetsincidenter. Året innan hade bolaget inte rapporterat in någon integritetsincident till PTS. PTS gör därför bedömningen att Tres rutiner för upptäckt och rapportering av integritetsincidenter har förbättrats sedan den förra årliga tillsynen. PTS ser positivt på denna utveckling och uppmanar Tre att, i enlighet med PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter, kontinuerligt utbilda personal om integritetsincidenter och hur dessa ska rapporteras internt i syfte att säkerställa att rapporteringen till PTS alltjämt förbättras framöver.

När det gäller redogörelsen av incidenterna kunde Tre inte vid mötet redogöra för samtliga omständigheter som myndigheten efterfrågade. Även om Tre uppgav att man arbetade för att inte vara personberoende bedömer PTS att det faktum att det vid mötet vid flera tillfällen hänvisades till en person som avslutat sin anställning innebär att Tre inte fullt ut har lyckats säkerställa att kompetens och kunskap om inträffade incidenter överförs vid personalomsättning. PTS uppmanar därför Tre att fortsätta arbetet med att säkerställa att flera personer inom företaget har kontinuerlig kunskap om incidenter, genom att tillse att det finns dokumenterade rutiner, processer och

rollfördelningar för detta, i enlighet med 3 § i PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter.

När det gäller en integritetsincident påtalade PTS att myndigheten inte fått del av den kopia på underrättelse som ska tillsändas myndigheten enligt lagen. Det faktum att berörda abonnenter och användare har fått del av den information som de har rätt till från Tre innebär inte att bolaget uppfyllt sin skyldighet att informera PTS om innehållet i underrättelsen. Utan att PTS får del av en kopia av underrättelsen kan myndigheten inte bedöma huruvida berörda kunder har fått del av den information om inträffade incidenter som de har rätt till. PTS förutsätter därför att Tre i framtiden säkerställer att kopia av underrättelse även tillsänds PTS.

Vid Tres redogörelse för status i arbete med efterlevnad av föreskrifterna om skyddsåtgärder för behandlade uppgifter kan PTS konstatera att det föreligger betydande brister i Tres säkerhetsarbete. Den riskanalys som presenterats för PTS är alltför rudimentär för att kunna utgöra ett relevant underlag till efterföljande skyddsåtgärder. Tre har även endast initierat ett arbete med att identifiera behandlade informationsbehandlingstillgångar. PTS ser allvarligt på dessa brister med tanke på att föreskrifterna trädde i kraft den 1 september 2014. PTS förutsätter att Tre nu kommer att vidta de åtgärder som är nödvändiga för att efterleva skyldigheterna i föreskrifterna. PTS kommer att följa upp att detta sker. För det fall att Tre inte vid uppföljningen vidtagit nödvändiga åtgärder för att efterleva föreskrifterna kan PTS komma att förelägga Tre att vidta åtgärder. Med detta påpekande lämnar PTS denna del av tillsynen utan åtgärd i dagsläget.

När det gäller Tres rutiner för rapportering av störningar och avbrott av betydande omfattning anser PTS att Tre vid den första störningen hade kunnat vara utförligare i sin rapportering i syfte att undvika efterföljande kompletterande frågor från myndigheten, vilket drar ut på ärendets handläggningstid och riskerar att leda till att PTS inleder tillsyn för att få in den information som krävs för att PTS ska kunna avgöra om det föreligger brister. När det gäller rapportering av stormen Egon har PTS inget att erinra utan kan konstatera att Tre väl har uppfyllt inrapporteringsskyldigheten. PTS lämnar därför även denna del av tillsynen utan ytterligare åtgärd. Det finns enligt PTS bedömning heller inte skäl att ytterligare granska själva hanteringen av incidenterna, utan myndigheten kan konstatera att Tre vad gäller detta har uppfyllt sina skyldigheter avseende driftsäkerhet enligt 5 kap. 6 b § LEK.

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

Underrättelse om överklagande

Beslutet kan inte överklagas.

Beslutet har fattats av enhetschefen Patrik Bystedt. I ärendets slutliga handläggning har även Karin Lodin (föredragande) och Anna Wibom deltagit.

PTS Beslutat av: Patrik Bystedt