Datum	Vår referens	Aktbilaga
2020-03-11	Dnr: 18-39492	29

Hi3G Access AB

Beslut – tillsyn av riskanalysarbete

Saken

Tillsyn enligt 7 kap. 1 § första stycket lagen (2003:389) om elektronisk kommunikation (LEK) över skyldigheten att analysera riskerna för störningar, avbrott och integritetsincidenter; nu fråga om avskrivning.

Post- och telestyrelsens avgörande

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

Bakgrund

PTS inledde den 20 december 2018 en planlagd tillsyn för att kontrollera att Hi3G Access AB (Hi3G) tillämpar en godtagbar metod för att efterleva skyldigheten att analysera

1. risken för att dokumenterade tillgångar och förbindelser orsakar störningar eller avbrott i kommunikationsnät och kommunikations-tjänster, samt
2. risken för att integritetsincidenter inträffar för identifierade informationsbehandlingstillgångar.

Inom ramen för tillsynen har Hi3G redogjort för sina processer för bolagets arbete med riskanalyser avseende riskerna för störningar och avbrott respektive integritetsincidenter för sina tillgångar, förbindelser och informationsbehandlingstillgångar.

Av denna redogörelse framkom bl.a. att de har en process för sitt arbete med riskanalyser i sin driftsorganisation och en annan process för att genomföra analyser av riskerna för integritetsincidenter. Processerna innehåller moment

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

för att identifiera och bedöma risker för företagets tillgångar. Vad gäller integritetsriskanalyserna bedrivs de i så stor utsträckning som möjligt i arbetsgruppsmöten där sammansättningen av deltagare ska vara representativt för att belysa alla relevanta hot och risker. Hi3G uppger att de genomför riskanalyser årligen och vid behov t.ex. vid tidpunkter då de bedömer att riskbilden förväntas ändras. Riskanalyser sker även vid planerat underhåll- och ändringsarbeten inom ramen för deras förändringshanteringsprocess.

Hi3G uppgav vidare att samtliga nättillgångar omfattades av någon riskanalys. Även de informationsbehandlingstillgångar som utgörs av en fysisk tillgång i Tre:s kommunikationsnät omfattades av riskanalyser. Vad gäller övriga informationsbehandlingstillgångar uppgav Hi3G att merparten av dessa tillgångar saknade riskanalyser utifrån LEK och PTS föreskrifter, t.ex. så saknades riskanalys avseende Tre:s röstbrevlådefunkton. Med anledning av detta underrättade PTS i juli 2019 Hi3G om myndighetens misstanke om att bolaget därmed inte uppfyllde regelverket. I enlighet med underrättelsen skulle Hi3G senast den 31 december 2019 ha genomfört och dokumenterat riskanalyser avseende risken för att integritetsincidenter inträffar för samtliga identifierade informationsbehandlingstillgångar.

Den 19 december 2019 meddelade Hi3G att de nu hade färdigställt samtliga riskanalyser. PTS önskade därefter ta del av Hi3G:s riskanalys för funktionen röstbrevlåda. Denna presenterades vid ett möte den 21 februari 2020. De risker som bolaget tagit upp för de olika objekt som utgör tillgången hade de identifierat med hjälp av workshops och de har utifrån fastställda skalor bedömt identifierade risker. Efter att analysen genomförts tar deras riskhanteringsprocess vid.

Skäl

Tillämpliga bestämmelser

Av 5 kap. 6 b § lagen (2003:389) om elektronisk kommunikation (LEK) framgår 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. De åtgärder som vidtas ska vara ägnade att skapa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för störningar och avbrott.

PTS har tagit fram föreskrifter om krav på driftsäkerhet (PTSFS 2015:2) för att förtydliga lagens krav på driftsäkerhetsarbetet. Av 4 § i föreskrifterna framgår att tillhandahållaren ska dokumentera samtliga sina tillgångar och förbindelser och av 5 § framgår att tillhandahållaren minst en gång per år ska analysera

risken för att dokumenterade tillgångar och förbindelser orsakar störningar eller avbrott i kommunikationsnäten eller kommunikationstjänsterna.

Enligt bestämmelsen ska tillhandahållares riskanalyser innefatta följande delar:

1. Identifiering av samtliga relevanta hot mot den aktuella tillgången eller förbindelsen. Hot relaterade till väder samt intrång och annan yttre påverkan ska alltid analyseras.
2. Kvalificerad bedömning av konsekvenser i händelse av att identifierade hot inträffar.
3. Kvalificerad bedömning av sannolikheten för att identifierade hot inträffar.
4. Kvalificerad sammanvägd bedömning av sannolikheten för att identifierade hot inträffar och de konsekvenser det kan medföra om de inträffar (riskbedömning).

Enligt bestämmelsen ska tillhandahållaren också ha en plan som visar vid vilka tidpunkter och i vilka situationer företaget kommer att genomföra riskanalyser. Att planen ska dokumenteras framgår av 3 § i föreskrifterna.

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.

PTS har tagit fram föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1) för att förtydliga lagens krav på integritetsskydd. 4 § första stycket i de föreskrifterna uppställer krav på att tjänstetillhandahållaren identifierar de informationsbehandlingstillgångar där behandlade uppgifter förekommer och för en förteckning över dessa. Av 4 § andra stycket framgår att tjänstetillhandahållaren ska analysera riskerna för att integritetsincidenter inträffar för de informationsbehandlingstillgångar som tjänstetillhandahållaren identifierat.

Riskanalyserna ska dokumenteras och följas upp årligen och vid behov på sätt som framgår av respektive bestämmelse i de båda föreskrifterna.

PTS bedömning

Att löpande genomföra ändamålsenliga riskanalyser är en förutsättning för att operatörer ska kunna bedriva ett långsiktigt, systematiskt och kontinuerligt

säkerhetsarbete i enlighet med PTS föreskrifter. Riskanalyserna ska t.ex. ligga till grund för bedömningen av vilka säkerhetsåtgärder som är relevanta för att skydda tillgångar, förbindelser och informationsbehandlingstillgångar.

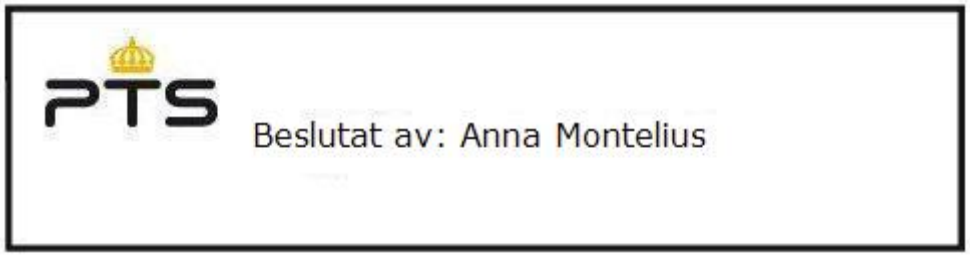
Av PTS föreskrifter om krav på driftsäkerhet framgår att riskanalyserna ska innefatta åtminstone följande moment: identifiera hot, bedöma sannolikheten för och konsekvenserna av att hoten inträffar samt en sammanvägd bedömning av dem, s.k. riskbedömning.

PTS kan konstatera att Hi3G genomför riskanalyser och att de numera har riskanalyser för samtliga identifierade tillgångar. Processerna för att genomföra riskanalyser ser något olika ut beroende på om analyserna avser risken för integritetsincidenter respektive risken för driftstörningar och avbrott men på respektive område genomförs de enligt en fastställd metod. Av redogörelsen från Hi3Gs, samt utifrån det exempel som bolaget redovisat, framgår att de har processer för att identifiera relevanta hot mot den tillgång som analyseras. Vissa hot analyseras, i enlighet med kraven i PTSFS 2015:2, alltid t.ex. risker för att väderrelaterade händelser skulle leda till störning eller avbrott av betydande omfattning. Vidare bedömer de vilka konsekvenser ett realiserat hot kan få och sannolikheten för att detta skulle inträffa samt gör utifrån dessa bedömningar en samlad riskbedömning avseende tillgången. PTS bedömer därmed att Hi3Gs genomför riskanalyser utifrån en metod som är i enlighet med föreskrifternas krav.

Hi3G har uppgett att de genomför riskanalyser löpande och vid vissa fastställda händelser, t.ex. efter störningar, avbrott eller incidenter. Riskanalys kan också genomföras om de ser behov av det t.ex. vid organisationsförändringar. PTS bedömer därför även att bolagets har en godtagbar plan för vid vilka tidpunkter och i vilka situationer bolaget genomför de riskanalyser som regelverket kräver.

Sammanfattningsvis bedömer PTS att Hi3G lever upp till kraven på att genomföra riskanalyser enligt PTSFS 2014:1 och PTSFS 2015:2 och ärendet avskrivs därför från vidare handläggning.

Beslutet har fattats av t.f. enhetschefen Anna Montelius. I ärendets slutliga handläggning har även juristen Caroline Sundholm (föredragande) deltagit.


PTS
Beslutat av: Anna Montelius