Datum 2015-06-18
Vår referens Dnr: 15-1713
Aktbilaga 6

Nätsäkerhetsavdelningen

[redacted]

Com Hem AB

Årlig tillsyn rörande incidentrapportering och inträffade incidenter

Saken

Årlig tillsyn rörande incidentrapportering 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. Det är PTS avsikt att årligen genomföra planlagda tillsyner över utvalda operatörer rörande incidentrapportering och inträffade incidenter.

PTS inledde den 25 februari 2015 den planlagda årliga tillsynen rörande incidentrapportering och inträffade incidenter över Com Hem AB (Com Hem). Den 14 april 2015 höll PTS ett tillsynsmöte med Com Hem. Därefter har ytterligare skriftväxling skett.

Vid mötet redogjorde Com Hem för föregående års inträffade störningar och avbrott, vilka har rapporterats in till PTS under 2014 samt för inträffade integritetsincidenter och status för långsiktiga åtgärder. Vid genomgången av incidenterna angav Com Hem att felet i flera fall låg hos leverantören och inte hos dem, men framförde att leverantörsavtal ses över kontinuerligt.

Com Hem redogjorde även för deras nya arbetssätt vad gäller tester, både vad gäller integritets- och driftstörningsområdena. De har infört ett helhets-perspektiv med s.k. end to end-tester, dvs. tester av helheten. Detta görs för att säkerställa kvaliteten i de tjänster som de levererar. De har även infört ett nytt system för att hantera incidenter. Systemet innebär bl.a. kortare ledtider, tydligare ansvarsfördelning och ett större helhetsperspektiv, vilket gör att de kommer att kunna agera mer proaktivt.

Vid mötet efterfrågade PTS även en redogörelse för hur integritetsincidenter hanteras i organisationen, inklusive beskrivning av rutiner för såväl upptäckt av integritetsincidenter som vidarerapportering av dessa internt och till PTS. Com Hem framförde härvid att bolaget ser en utmaning i arbetet med integritets-incidenter eftersom det är 500 personer som arbetar i kundtjänst och personalomsättningen är relativt hög där. Personalen i kundtjänst får en utbildning när de är nyanställda men ingen uppföljning av utbildningen görs i dagsläget, vilket Com Hem uppgav skulle kunna vara en förbättringsmöjlighet vad gäller att upptäcka integritetsincidenter. PTS efterfrågade även en beskrivning av Com Hems säkerhetsorganisation och beskrivning av dess ansvarsförhållanden, vilka Com Hem inkom med den 20 maj 2015.

Mötet omfattade också en redogörelse för Com Hems arbete med att efterleva de krav som föreskrivs i PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS2014:1). Enligt uppgift från Com Hem framgick det vid mötet att arbetet med att identifiera informationsbehandlings-tillgångar och kritiska system hade initierats, men att Com Hem inte ännu efterlevde föreskrifterna fullt ut, främst avseende genomförande av riskanalyser och vidtagande av efterföljande skyddsåtgärder.

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.

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.

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. 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.

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. En integritetsincident definieras i 6 kap. 1 § LEK som en händelse som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring, eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster

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.

PTS bedömning

Inledningsvis kan PTS konstatera att Com Hem hade förberett sig inför tillsynsmötet den 14 april 2015, vid vilket 5 incidenter gicks igenom. De incidenter som föranlett att PTS inleder händelsestyrd tillsyn behandlas inte inom ramen för den årliga tillsynen, utan behandlas särskilt i den händelsestyrda tillsynen . Vid genomgången av tillsynsinsatserna saknade PTS dock en tydlig redogörelse för vilka åtgärder som vidtagits för respektive incident och att samtliga åtgärder slutförts. Detta är något som kommer att efterfrågas av myndigheten till kommande års årliga tillsyner.

Förändringar har skett i Com Hems organisation under året. Vad gäller integritetsområdet anser PTS att Com Hem har beskrivit hur deras nya säkerhetsorganisation är utformad, med en särskilt utpekad ansvarig. Såvitt framgått har en och samma person utsetts med många olika ansvarsområden. Rutiner, processer och rollfördelning ska enligt gällande föreskrifter vara dokumenterade som ett led i att säkerhetsarbetet avseende behandlade uppgifter ska bedrivas långsiktigt, kontinuerligt och systematiskt. Eftersom Com Hem har en stor verksamhet och erbjuder många tjänster vill PTS påtala vikten av att den dagliga verksamheten organiseras på ett sådant sätt att ansvaret för informationssäkerhetsfrågorna och regelefterlevnaden säkerställs.

PTS har i tidigare tillsynser över Com Hem (PTS dnr 14-12617, tillsyn efter inträffad incident i e-postplattform) bland annat påtalat brister kring det förebyggande riskanalysarbetet och arbetet med att implementera PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter

(PTSFS 2014:1). PTS anser att Com Hem måste intensifiera sitt arbete gällande detta.

Com Hem har uppgett att de alltid har gjort riskanalyser men inte ur ett integritetsperspektiv. PTS kan således konstatera att det föreligger betydande brister i Com Hems arbete med att implementera de krav som framkommer av PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1). PTS ser allvarligt på dessa brister och förutsätter att Com Hem 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 Com Hem inte vid uppföljningen vidtagit nödvändiga åtgärder för att efterleva föreskrifterna kan PTS komma att förelägga Com Hem att vidta åtgärder. Med detta påpekande lämnar PTS denna del av tillsynen utan åtgärd i dagsläget.

PTS anser att Com Hem även måste intensifiera sitt arbete med att hålla personalen i kundtjänst informerade om vilka regler som finns att följa i syfte att upptäcka och hantera integritetsincidenter. En utbildning av personalen i ett initialt skede ses inte som tillräckligt, av myndigheten, utan Com Hem behöver se till att det görs kontinuerliga utbildningsinsatser.

Com Hem har, vid genomgången av föregående års incidenter, flera gånger hänvisat till att felet ligger hos leverantören, oavsett om det är en integritet- eller driftincident. En brist hos en underleverantör eller samarbetspartner kan mycket väl utgöra en brist i det grundläggande säkerhetsarbetet hos Com Hem. PTS anser att det är Com Hems ansvar att genom avtal, kravställning och genom att aktivt efterfråga testresultat från leverantören minska risken för att incidenter uppkommer, såväl inom driftsäkerhet och integritet. PTS lämnar med detta påpekande denna del av tillsynen utan ytterligare åtgärd.

PTS ser positivt på att Com Hem har tagit ett helhetsperspektiv på sin incidenthanteringsprocess och sitt testarbete. PTS förhoppning är att Com Hem på så sätt tar ett större ansvar för sina tjänster och att det innebär en större systematik i att dra lärdom av inträffade incidenter och på så sätt agera proaktivt. Flertalet av de störningar som Com Hem har haft vad gäller driftsäkerhet har under året pågått under lång tid. Om det nya systemet och arbetssättet kan leda till kortare tider för återställning är det positivt och detta är ett område som PTS kommer att återkomma till i kommande tillsynsinsatser.

Skäl att fortsätta den årliga tillsynen av incidentrapportering och inträffande störningar och avbrott av betydande omfattning föreligger därför inte, varför ärendet avskrivs från vidare handläggning.

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