Datum	Vår referens	Aktbilaga
2019-12-18	Dnr: 19-8763	10

Avdelningen för säker kommunikation

Finansiell ID-Teknik BID AB

Beslut – tillsyn efter störningar och avbrott i en betrodd tjänst

Saken

Tillsyn enligt Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS-förordningen).

Post- och telestyrelsens avgörande

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

Bakgrund

PTS inledde i juli 2019 tillsyn av Finansiell ID-teknik BID AB (Finansiell ID-teknik) efter att bolaget inkommit med en incidentrapport avseende en incident som i betydande omfattning påverkat den betrodda tjänst de tillhandahåller, dvs. den del av Bank-ID som utgörs av tjänsten för avancerad elektronisk underskrift (nedan Bank-ID).

Inom ramen för tillsynen har PTS haft ett tillsynsmöte med representanter från Finansiell ID-teknik, samt tagit del av skriftliga svar på kompletterande frågor. Av dessa redogörelser har bl.a. följande framkommit.

Under natten till den 2 maj 2019 drabbades tjänsten Bank-ID av intermittenta störningar under cirka 50 minuter. Under arbetet med att felsöka och åtgärda felet blev tjänsten helt otillgänglig i ungefär en timme. Det tolkades som att störningen uppstått till följd av fel i en hårdvarukomponent, vilket även var det som rapporterades till PTS den 2 maj samt i den komplettering som inkom den 24 maj (dnr 19-6439).

Efter att tjänsten återställts fortsatte bolaget analysen av komponenten för att hitta grundorsaken till felet för att slutgiltigt kunna åtgärda detta. Under detta arbete uppstod samma problem igen, men det gick denna gång att hantera utan att det fick någon påverkan på tjänsten. Finansiell ID-teknik förstod i samband med denna händelse att orsaken till felet var ett annat än de först trott; istället för ett hårdvarufel rörde det sig om ett fel i en drivrutin till en applikation som de tidigare under året börjat använda. Inför införandet av aktuell applikation hade bolaget genomfört testning under en sexmånadersperiod, men detta fel hade inte uppmärksammats. Finansiell ID-teknik inledde omedelbart ett arbete med att åtgärda felet. Analys samt testning av lösningen av felet tog 12 dagar och slutgiltig åtgärd i skarpt system gjordes den 22 maj. Finansiell ID-teknik bedömer att det därmed inte är troligt att felet ska kunna uppstå igen. Fortsatt analys och arbete har dock vidtagits för att ytterligare analysera applikationen för att säkerställa funktionen även vid fel liknande det som inträffade i maj.

Sedan det inträffade har bolaget också justerat vissa av sina rutiner avseende bl.a. felsökning samt förtydligande kring den externa kommunikation som sker vid driftsstopp.

Vidare redogjorde Finansiell ID-teknik för sitt säkerhetsarbete. De presenterade bl.a. sitt ledningssystem för informationssäkerhet vilket enligt uppgift från bolaget utgår ifrån ISO 27001. Detta innebär, enligt Finansiell ID-teknik, bl.a. att de har en systematik för att genomföra riskanalyser och hotbildsanalyser, samt att det finns utpekade roller med ansvar för detta arbete. Vidare uppgav bolaget att de har en kontinuerlig översyn av sitt ledningssystem genom bl.a. internrevision.

Bolaget presenterade även hur de arbetar med leverantörsstyrning av de externa parter de anlitar. De uppgav att de har detaljerade krav- och servicenivåer samt skriftliga processbeskrivningar, tjänstebeskrivningar och instruktioner. De arbetar enligt ITIL och har ett antal huvudprocesser avseende drift, t.ex. service request, change och incident. Inom ramen för detta arbete har de två gånger i veckan CAB (change advisory board) och kan vid behov sammankalla E-CAB (emergency change advisory board).

Vidare presenterade Finansiell ID-teknik hur de arbetar med revision och tester av underleverantörer. De ställer krav på att leverantörerna granskar sig själva men utöver detta genomför både Finansiell ID-teknik externa oberoende granskare kontroll av leverantörerna. Dessa granskningar resulterar i åtgärdslistor som Finansiell ID-teknik sedan följer upp och säkerställer att åtgärder vidtas.

Skäl

Tillämpliga bestämmelser

Enligt artikel 17.1 i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS-förordningen) ska det i varje medlemsstat utses ett tillsynsorgan. Av 4 § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering framgår att den myndighet som regeringen bestämmer ska fullgöra tillsynsorganets uppgifter enligt förordningen och utöva tillsyn. Av 4 § punkt 14 förordningen (2007:951) med instruktion för Post- och telestyrelsen framgår att PTS utsetts till tillsynsmyndighet.

Vidare framgår av artikel 17.3 b. i eIDAS-förordningen att tillsynsorganets roll bl.a. är att vid behov vidta åtgärder avseende icke-kvalificerade tillhandahållare av betrodda tjänster genom tillsynsverksamhet i efterhand om de tar del av påståendet att en icke-kvalificerad tillhandahållare av betrodda tjänster eller de betrodda tjänster som de tillhandahåller inte uppfyller kraven i denna förordning.

Av artikel 19.1 i eIDAS-förordningen framgår bl.a. att tillhandahållare av betrodda tjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster de tillhandahåller.

Vidare följer av artikel 19.2 att tillhandahållare inom 24 timmar ska underrätta tillsynsorganet om alla säkerhetsincidenter som i betydande omfattning påverkar den betrodda tjänst som tillhandahålls. Vad en rapport bör innehålla har beskrivits närmare i PTS vägledning för betrodda tjänster i Sverige (dnr 17-4465) och det framgår där bl.a. att incidentrapporten ska innehålla en beskrivning av incidenten samt såväl grundorsak som andra underliggande orsaker. Det ska även framgå vilka åtgärder som vidtagits för att hantera incidenten och vilka åtgärder som vidtagits för att undvika att motsvarande incident inträffar igen.

PTS bedömning

PTS bedömer att Finansiell ID-teknik i de delar som PTS granskat har ett systematiskt och långsiktigt säkerhetsarbete. Detta arbete utgår från etablerad standard och de har metoder för riskanalys och hantering av inträffade incidenter.

Vidare bedömer PTS att Finansiell ID-teknik i de delar som PTS tillsyn omfattat har vidtagit lämpliga tekniska och organisatoriska åtgärder, i enlighet med artikel 19.1 i eIDAS-förordningen, för att hantera det fel som ledde till att den avancerade underskriftstjänsten blev otillgänglig. Det har enligt PTS

bedömning inte framgått annat än att Finansiell ID-teknik har vidtagit åtgärder för att problemet inte ska uppstå igen samt att de dragit lärdom av det inträffade på så sätt att de t.ex. justerat vissa rutiner efter incidenten.

PTS bedömer sammantaget att bolaget vid tidpunkten för tillsynen visat att de bedriver ett systematiskt säkerhetsarbete där de kan identifiera risker och vidta relevanta åtgärder i enlighet med artikel 19.1 i eIDAS-förordningen.

När det gäller incidentrapportering vill PTS dock framhålla vikten av att de incidentrapporter som inkommer till myndigheten behöver vara tillräckligt detaljerade för att myndigheten ska kunna lägga dessa till grund för bedömningen av behov av vidare åtgärder. PTS kan konstatera att Finansiell ID-teknik visserligen inkommit med en incidentrapport inom den föreskrivna tidsramen enligt artikel 19.2 i eIDAS-förordningen men att den var mycket kortfattad. Inte heller efter det att PTS efterfrågat kompletterande information framgick klart t.ex. orsak till incidenten och vidtagna åtgärder. Finansiell ID-teknik uppgav även i denna kompletterande skrivelse att det troligen rörde sig om ett hårdvarufel, trots att de vid denna tidpunkt fanns uppgift om att felet var ett annat. PTS vill poängtera att det är mycket viktigt att den information som lämnas är korrekt och att en komplettering bör lämnas till PTS om det framkommer att tidigare lämnad information inte stämmer. PTS framförde vid tillsynsmötet bl.a. att Finansiell ID-teknik måste vara mer utförliga i sin rapportering och PTS förutsätter därmed att Finansiell ID-teknik framöver kommer vara mer omsorgsfulla i sin incidentrapportering och beskriva t.ex. orsaker och vidtagna åtgärder mer ingående.

PTS bedömer därmed att det inte finns skäl att fortsätta tillsynen och avskriver ärendet från vidare handläggning.

Beslutet har fattats av t.f. enhetschefen Karin Lodin. I ärendets slutliga handläggning har även samordnaren Emelie Björkegren Näslund och handläggaren Björn Hesthamar deltagit. Juristen Caroline Sundholm har varit föredragande.

Beslutat av: Karin Lodin