Vår referens: Dnr 20–14733, **Aktbilaga:** 11

Scrive AB, org. nr. 556816-6804

Beslut – tillsyn med anledning av driftstörning i den betrodda tjänsten som Scrive AB tillhandahåller

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) avslutar ärendet från vidare handläggning.

Bakgrund

Scrive AB (Scrive) är en tillhandahållare av en betrodd tjänst enligt artikel 3.16 a eIDAS-förordningen.

Enligt artikel 19.1 i eIDAS-förordningen ska tillhandahållare av betrodda tjänster vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster som de tillhandahåller. Viktiga organisatoriska säkerhetsåtgärder kan vara att ha fastställda och dokumenterade riskhanteringsprocesser vid förändringsarbete samt incidenthanteringsprocesser.

Den 5 maj 2021 inkom Scrive med en incidentrapport[1] enligt artikel 19 i eIDAS-förordningen. Incidenten berodde på ett förändringsarbete som Scrive utförde i syfte att rensa i sin databas. Förändringen ledde till en överbelastning som i sin tur i betydande omfattning påverkade

[1] PTS Dnr. 21-5778

Post- och telestyrelsen
Postadress: Box 5398, 102 49 Stockholm
Besöksadress: Valhallavägen 117 A
Telefon: 08-678 55 00
E-post: pts@pts.se
www.pts.se

Scrives betrodda tjänst, e-Signature Service. Incidenten innebar att Scrives tjänst för elektroniska underskrifter samt alla system som använde tjänsten, var nedsatta eller helt otillgängliga under tiden för incidenten. Den 11 maj inkom Scrive vidare med en kompletterande incidentrapport. I rapporten uppgav Scrive att de utfört tester som visar att samma mängd belastning som orsakade incidenten inte längre överbelastar systemet. Av rapporten framkom vidare de genomförda och planerade åtgärderna för att undvika liknande incidenter.

Inom ramen för tillsynen har PTS haft ett tillsynsmöte med representanter från Scrive samt tagit del av skriftliga svar på kompletterande frågor. Vid mötet och i de skriftliga svaren har Scrive redogjort för sina processer för riskhantering vid förändringsarbete samt och incidenthantering samt de åtgärder Scrive vidtagit för att säkerställa att alla i organisationen följer dessa. Scrive har även förtydligat flertal planerade åtgärder samt åtgärder för att minska risken för att en liknande incident inträffar igen.

Skäl

Tillämpliga bestämmelser

Enligt artikel 17.1 i eIDAS förordningen ska det i varje medlemsstat utses ett tillsynsorgan.

PTS är, enligt 4 § förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, tillsynsmyndighet enligt lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Tillsynsmyndigheten ska enligt artikel 17.3 b eIDAS-förordningen vid behov vidta åtgärder avseende icke-kvalificerade tillhandahållare av betrodda tjänster om de tar del av påståenden att dessa icke-kvalificerade tillhandahållare av betrodda tjänster eller de betrodda tjänster som de tillhandahåller inte uppfyller kraven i förordningen.

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

PTS bedömning

Fel i samband med förändringar utgör en stor risk för säkerheten i betrodda tjänster och är en vanlig orsak till incidenter. Enligt PTS bedömning är det en förutsättning för att en tillhandahållare ska anses kunna bedriva ett godtagbart säkerhetsarbete enligt eIDAS-förordningen, att tillhandahållaren tillämpar ändamålsenliga processer för incidenthantering och riskhantering vid genomförande av förändringar.

Inom ramen för tillsynen har Scrive redogjort för hur de hanterar den här typen av incidenter samt klarlagt vilka åtgärder som vidtagits för att liknande incidenter inte ska inträffa igen. Bland annat har Scrive uppgett att de planerar att använda en annan lösning än den nuvarande för att lagra data, då tjänsten växt så pass mycket att Scrive behöver se över hur de lagrar data och då främst vilken data som ska lagras i databasen och vilken data som ska lagras på annat sätt. Scrive har vidare förstärkt sin kompetens kring databaser och utökat personal som arbetar med förändringshantering

Inom ramen för tillsynen har Scrive redogjort för sin process för riskhantering vid förändringsarbete och sin process för incidenthantering. Scrive har även uppgett att de är certifierade enligt ISO 27001. Utifrån Scrives redogörelse för sin process vid förändringsarbete, samt de åtgärder som har vidtagits och planeras att vidtas för att undvika liknande incidenter, bedömer PTS att Scrive uppfyller kraven i artikel 19 i eIDAS-förordningen.

PTS bedömer att Scrive vid tidpunkten för tillsynen visat att de bedriver ett systematiskt säkerhetsarbete där de kan identifiera risker vid förändringsarbete. PTS bedömer vidare att Scrive vid tidpunkten för tillsynen påvisat att de har en godtagbar process för incidenthantering. Sammantaget bedömer PTS att Scrive vid tidpunkten för tillsynen vidtar relevanta åtgärder i enlighet med artikel 19.1 eIDAS-förordningen.

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

Beslutet har fattats av enhetschef Karin Lodin. I ärendets slutliga handläggning har även handläggarna Bahare Sadeghi Gazani (föredragande), Åsa Gihl och Björn Scharin deltagit.