**Vår referens:** 21-2291 **Aktbilaga:** 11

Finansiell ID-Teknik BID AB, org. nr. 556630-4928

# Avskrivningsbeslut: Tillsyn med anledning av driftstörningar i den betrodda tjänsten BankID

## Saken

Tillsyn enligt artikel 17.3 (b), 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

Finansiell ID-Teknik BID AB (FIDT) är en tillhandahållare av en betrodd tjänst enligt artikel 3.19, eIDAS-förordningen. En tillhandahållare av en betrodd tjänst ska enligt förordningen bl.a. vidta lämpliga åtgärder för att hantera säkerhetsrisker relaterade till den tjänst man tillhandahåller, samt rapportera in inträffade incidenter till tillsynsmyndigheten. PTS är tillsynsmyndighet över tillhandahållare av betrodda tjänster.

Den 24 februari 2021 inkom FIDT med en incidentrapport till PTS, avseende störningar som drabbade slutanvändare under kvällen den 23 februari 2021. Störningarna berodde på en överbelastningsattack mot BankID som varade mellan 19.30 till och med 22.30 den 23 februari.

Slutanvändare upplevde störningar i varierande grad främst mellan kl. 19.45 – 20.15 och kl. 21.45 – 22.10.

Mot bakgrund av denna incident inledde PTS tillsyn mot FIDT i syfte att granska huruvida bolaget vidtar lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos den betrodda tjänst som bolaget tillhandahåller.

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

Inom ramen för tillsynen har PTS skickat skriftliga frågor till FIDT om överbelastningsattacken, hanteringen av incidenten, hotbilden mot bolaget, samt bolagets säkerhetsarbete. PTS har därefter genomfört ett tillsynsmöte med representanter från FIDT, där FIDT ombetts svara på de frågor som PTS ställt.

FIDT har redogjort för omständigheterna kring överbelastningsattacken som resulterade i incidenten, sin hantering av incidenten under och efter attacken, sin bedömning av nuvarande hotbild mot tjänsten BankID, samt sina rutiner för incidenthantering, kommunikation med användare och riskanalys. Bolaget har vidare beskrivit vilka åtgärder som vidtagits med anledning av incidenten, samt vilka ytterligare utredningar som pågår för att säkerställa att säkerhetsarbetet står i proportion till graden av risk.

## Skäl

### Tillämpliga bestämmelser

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. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa att tillhandahållarens säkerhetsnivå står i proportion till graden av risk. I synnerhet ska åtgärder vidtas för att såväl förhindra eller minimera säkerhetsincidentens inverkan, som för att informera berörda parter om de negativa effekterna.

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

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

Tillsynsmyndigheten ska enligt 4 § lagen (2016:561) med kompletterande bestämmelser i EU:s förordning om elektronisk identifiering

1. fullgöra tillsynsorganets uppgifter enligt EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, samt

2. utöva tillsyn över efterlevnaden av denna lag och föreskrifter som har meddelats med stöd av denna lag.

**PTS bedömning**

Tjänsten BankID används i stor omfattning i Sverige, både inom privat och offentlig sektor. Den breda användningen innebär ett beroende som ökar i samhället, vilket blivit än tydligare under det senaste året då pandemin pågått. Det ökande beroendet till tjänsten innebär i sin tur att riskerna med tillhandahållandet ökar, eftersom störningar och avbrott kan få stora negativa konsekvenser.

Mot bakgrund av detta är det av stor vikt att tillhandahållare av betrodda tjänster ser till att höja säkerheten i takt med att beroendet till, och riskerna mot, tjänsten ökar.

Under tillsynsmötet kunde FIDT redogöra för sitt systematiska säkerhetsarbete och sin hantering och utvärdering av den inträffade incidenten. FIDT kunde utförligt beskriva de motåtgärder bolaget vidtog under attacken, samt de efterföljande åtgärder som vidtagits med anledning av den. Vidare upplyste FIDT om ytterligare utredningar som genomförs i bolaget för att bättre kunna motstå en liknande attack i framtiden. PTS bedömer att FIDT svarade utförligt och genomgående på de frågor som ställdes, samt gav fullgoda beskrivningar av sitt säkerhetsarbete.

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 eIDAS-förordningen.

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

---

Beslutet har fattats av enhetschef Karin Lodin. I ärendets slutliga handläggning har även handläggarna Anna Söyland (föredragande) och Åsa Gihl deltagit.