

Kort fortalt

Finanstilsynets it-tilsyn

Konklusion

Finanstilsynets tilsyn med finansielle virksomheders it-sikkerhed er ikke tilfredsstillende. Konsekvensen er, at der er risiko for, at virksomhedernes it-sikkerhed ikke er tilstrækkelig til at forhindre brud på it-sikkerheden til skade for kunderne og samfundet.

Statsrevisorerne udtaler

”Statsrevisorerne finder Finanstilsynets tilsyn med finansielle virksomheders it-sikkerhed utilfredsstillende. Det utilfredsstillende tilsyn øger risikoen for it-nedbrud, økonomiske tab og tab af tillid fra kunder og omverden.

Statsrevisorerne finder det bekymrende, at Finanstilsynet ikke har inspiceret it-sikkerheden i en tredjedel af de systemisk vigtige finansielle virksomheder inden for det 4-årige interval, som de skal ifølge deres retningslinjer. Der er i gennemsnit gået 4½ år mellem inspektionerne, og for nogle af virksomhederne er der gået over 7 år”.

Væsentligste resultater af undersøgelsen

- Finanstilsynet har årligt risikovurderet it-sikkerheden i de finansielle virksomheder, der er så væsentlige, at nedbrud vil kunne true den finansielle stabilitet. Men de mangler at risikovurdere en del af de øvrige finansielle virksomheders it-sikkerhed.
- Finanstilsynet har ikke inspiceret it-sikkerheden i en tredjedel af de væsentligste virksomheder så ofte, som de skulle. Finanstilsynet har fastsat en minimumsfrekvens for inspektionerne på 4 år, men for nogle af virksomhederne er der gået over 7 år mellem inspektionerne.
- Der er risikofyldte områder som fx adgangsstyring og fysisk sikkerhed, der ikke er blevet inspiceret i flere år.
- Finanstilsynet har givet hovedparten af de væsentligste virksomheder påbud om at forbedre deres it-sikkerhed og har fulgt op på, om de efterlever påbudene. Virksomhederne har dog overskredet fristerne for efterlevelse af påbud med ca. 2 år i gennemsnit. Finanstilsynet har ikke udstedt bøder eller politianmeldt virksomheder i den periode, vi har undersøgt.

Baggrund og formål med undersøgelsen

Formålet med undersøgelsen er at vurdere, om Finanstilsynet har ført et tilfredsstillende tilsyn med finansielle virksomheders it-sikkerhed. Undersøgelsen vedrører perioden 2017-2023.

Da næsten alle økonomiske aktiviteter foregår digitalt i Danmark, er det vigtigt, at finansielle virksomheders it-sikkerhed er tilstrækkelig til at forhindre it-nedbrud. Samtidig vurderer Finanstilsynet, at it-sikkerheden er en af de væsentligste risikofaktorer for den finansielle sektor, og Center for Cybersikkerhed vurderer, at trusselsniveauet mod den finansielle sektor er højt.

Det er Finanstilsynets opgave at føre tilsyn med, om finansielle virksomheder har betryggende kontrol- og sikringsforanstaltninger på it-området. Finanstilsynet skal løbende risikovurdere virksomhedernes it-sikkerhed og inspicere it-sikkerheden i de væsentligste og mest risikofyldte virksomheder. Finanstilsynet har vurderet, at konsekvenserne af eventuelle it-nedbrud i de væsentligste virksomheder er så store, at de skal inspiceres mindst hvert fjerde år.

Tabellen viser, hvor mange år der er gået mellem Finanstilsynets it-inspektioner i de væsentligste virksomheder.

Antal år mellem Finanstilsynets it-inspektioner

Interval mellem inspektioner	Antal virksomheder
Mindre end 4 år mellem inspektioner	6
4-5 år mellem inspektioner	5
5-6 år mellem inspektioner	3
6-7 år mellem inspektioner	0
7 år eller derover mellem inspektioner	3

Note: Perioden er regnet fra tidspunktet for gennemførelsen af den forrige it-inspektion til tidspunktet for gennemførelsen af den næste inspektion.