FOLKETINGET
RIGSREVISIONEN

Juni 2023

Rigsrevisionens notat om

tilrettelæggelsen af en større undersøgelse af Finanstilsynets tilsyn med finansielle virksomheders it-sikkerhed

Tilrettelæggelsen af en større undersøgelse af Finanstilsynets tilsyn med finansielle virksomheders it-sikkerhed

8. juni 2023

RN 1113/23

I. Indledning

1. Statsrevisorerne anmodede på deres møde den 24. april 2023 om en undersøgelse af Finanstilsynets tilsyn med finansielle virksomheders it-sikkerhed, jf. rigsrevisorlovens § 8, stk. 1. Dette notat beskriver, hvordan en eventuel større undersøgelse vil kunne tilrettelægges.

Undersøgelsen kan gennemføres, så Rigsrevisionen kan afgive en beretning til Statsrevisorerne i foråret 2024.

II. Baggrund

2. Baggrunden for Statsrevisorernes anmodning er, at Folketingets Udvalg for Digitalisering og It har anmodet Statsrevisorerne om revisionsmæssig bistand til en undersøgelse. Fokus for undersøgelsen er omfanget og kvaliteten af Finanstilsynets it-tilsyn og inspektioner af finansielle virksomheders styring af deres it-sikkerhed og it-risici.

Finansielle virksomheder
Finansielle virksomheder omfatter penge- og realkreditinstitutter, pensions- og forsikringsselskaber, investeringsselskaber, fondsmæglere mfl.

It-sikkerhed i den finansielle sektor

3. It-sikkerhed i den finansielle sektor er vigtig af flere grunde. For det første kan længerevarende it-nedbrud true den finansielle stabilitet og tilliden til den finansielle sektor, ikke mindst fordi langt de fleste betalinger foregår digitalt i Danmark. Det fremgår af "Strategi for den finansielle sektors cyber- og informationssikkerhed 2022-2025". For det andet står den danske finanssektor ifølge trusselsvurderingen fra Center for Cybersikkerhed over for et meget højt trusselsniveau fra cyberkriminalitet. For det tredje har Finanstilsynet gennem flere år gennemført en spørgeskemaundersøgelse, der viser, at it-relaterede risici topper listen over risici, som de finansielle virksomheder er mest bekymrede for, og at cybersikkerhed er den risiko, virksomhederne finder mest udfordrende at håndtere.

Finanstilsynet

4. Finanstilsynets opgave er at medvirke til finansiel stabilitet og tillid til den finansielle sektor hos borgere og virksomheder i ind- og udland. Opgaven løses ved, at Finanstilsynet:

- fører tilsyn med de finansielle virksomheder og markeder
- udarbejder regler på det finansielle område
- belyser udviklingen i den finansielle sektor i Danmark gennem statistik og løbende information.

Finanstilsynet er finansieret af afgifter fra de virksomheder, der er underlagt tilsynet.

Systemisk vigtige finansielle institutter
Systemisk vigtige finansielle institutter er institutter, der er så store og vigtige, at det kan få store konsekvenser for hele samfundsøkonomien, hvis de kommer i problemer.

De systemisk vigtige finansielle institutter i Danmark er: Danske Bank A/S, Nykredit Realkredit A/S, Jyske Bank A/S, Nordea Kredit Realkreditaktieselskab, Sydbank A/S, Spar Nord Bank A/S, DLR Kredit A/S og A/S Arbejdernes Landsbank.

5. Finanstilsynet skal ifølge loven tilrettelægge tilsynsvirksomheden ud fra et væsentlighedshensyn, hvor den tilsynsmæssige indsats står i forhold til de potentielle risici eller skadevirkninger. Dette indebærer bl.a., at Finanstilsynet skal føre et intensiveret tilsyn med de systemisk vigtige finansielle institutter. Tilsynet foregår dels ved inspektioner, dels på grundlag af de løbende indberetninger af it-sikkerhedshændelser fra virksomhederne.

Tilsynet med finansielle virksomheders it-sikkerhedsstyring

6. Ifølge lov om finansiel virksomhed skal finansielle virksomheder have betryggende kontrol- og sikringsforanstaltninger på it-området. Finanstilsynet har i loven hjemmel til at fastlægge, hvilke foranstaltninger en finansiel virksomhed skal træffe for at have effektive former for virksomhedsstyring på it-området. Dette har Finanstilsynet gjort i bekendtgørelse om finansielle virksomheders ledelse og styring, jf. boks 1.

Indberetning af it-sikkerhedshændelser
Finansielle virksomheder, der er omfattet af krav til it-sikkerhed, skal indberette kritiske hændelser til Finanstilsynet. Derudover skal finansielle virksomheder, der udbyder betalingstjenester, underrette Finanstilsynet om større hændelser, der kan påvirke sikkerheden eller driften. Endelig skal finansielle virksomheder, der er operatører af væsentlige tjenester, underrette Finanstilsynet og Center for Cybersikkerhed om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer.

Boks 1

Krav til finansielle virksomheders it-sikkerhedsstyring

Kravene fastlægger bestyrelsens og direktionens opgaver og ansvar i forhold til it-sikkerhed.

Det er bestyrelsens opgave at beslutte en it-sikkerhedspolitik ud fra den ønskede risikoprofil på området. Bekendtgørelsen oplister en lang række forhold, som det fx kan være relevant at tage stilling til, bl.a. risikovurdering, beskyttelse af systemer, overholdelse af relevant lovgivning og fastsættelse af forholdsregler i tilfælde af brud på it-sikkerhedsregler.

Direktionens opgave er at udarbejde procedurer, der sikrer, at politikken efterleves. Procedurerne skal bl.a. understøtte ansvar, kontrol, dokumentation, tests, adgangskontrol/fysisk sikkerhed samt udarbejdelse og afprøvning af en beredskabsplan.

Kilde: Bekendtgørelse nr. 1026 af 30. juni 2016, bilag 5 med senere ændringer, og bekendtgørelse nr. 1723 af 16. december 2015, bilag 4 med senere ændringer.

Ifølge Finanstilsynets oplysninger er der i alt 332 finansielle virksomheder og fælles datacentraler, der skal leve op til kravene vedrørende it-sikkerhed. Hvis tilsynet viser, at der er mangler i de finansielle virksomheders it-sikkerhed, kan Finanstilsynet give påbud eller bøder.

Fælles datacentraler
Fælles datacentraler er virksomheder, hvis primære aktivitet er at varetage it-driftsopgaver eller it-udviklingsopgaver for flere finansielle virksomheder. Datacentralerne er overvejende ejet af finansielle virksomheder.

Statsrevisorernes spørgsmål

7. Statsrevisorerne har anmodet Rigsrevisionen om at besvare følgende spørgsmål:

- Hvor mange it-tilsyn og it-inspektioner af finansielle virksomheder har Finanstilsynet gennemført i perioden 2017-2022?
- Hvor mange og hvilke påbud har Finanstilsynet udstedt i den forbindelse, og hvilken virkning har de haft?
- Hvilke muligheder har Finanstilsynet for at føre tilsyn med banker i Danmark, som har adresse/hovedsæde i andre lande, men hvor en stor del af deres kritiske finansielle infrastruktur er placeret i Danmark?
- Har Finanstilsynets it-tilsyn og inspektioner været tilfredsstillende i perioden, bl.a. i forhold til tilsynsfrekvens, rammer for tilsynet, risici og lovens hovedformål?
- Hvilke muligheder har kunderne for at blive orienteret om eventuelle it-sikkerhedsmæssige risici og påbud fra Finanstilsynet i deres pengeinstitut?

8. Vi forventer i hovedsagen at kunne besvare Statsrevisorernes spørgsmål.

III. Tilrettelæggelsen af undersøgelsen

9. Det overordnede formål med undersøgelsen er at vurdere, om Finanstilsynets tilsyn med finansielle virksomheders styring af deres it-sikkerhed er tilfredsstillende. Dette besvarer Statsrevisorernes spørgsmål 4.

Undersøgelsen vil bestå af 3 dele, herunder en undersøgelse af Finanstilsynets planlægning af it-tilsynet, en undersøgelse af Finanstilsynets gennemførelse af tilsynet og en undersøgelse af Finanstilsynets opfølgning på tilsynet.

Er Finanstilsynets planlægning af it-tilsynet tilfredsstillende?

Vi vil undersøge, om Finanstilsynet har etableret et tilstrækkeligt videngrundlag og på baggrund heraf udarbejdet en analyse, så Finanstilsynet kan fokusere indsatsen på de vigtigste risici og på de virksomheder, hvor konsekvenserne af eventuelle sikkerhedsbrister er størst. Desuden vil vi besvare Statsrevisorernes spørgsmål 3 om muligheden for at føre tilsyn med banker, som har hovedsæde i andre lande.

Er Finanstilsynets gennemførelse af it-tilsynet tilfredsstillende?

10. Vi vil undersøge omfanget af Finanstilsynets it-tilsyn, herunder Finanstilsynets overvågning af indberetninger og revisionsprotokollater, it-inspektioner og det eventuelle tilsyn med it-sikkerheden, der indgår i det almindelige tilsyn med de finansielle virksomheder/pengeinstitutter. Vi vil desuden undersøge, om Finanstilsynet gennemfører tilsynet på en måde, så eventuelle svagheder i virksomhedernes it-sikkerhedsstyring kan identificeres. Endelig vil vi undersøge, hvor mange påbud Finanstilsynet har givet. Vi besvarer hermed Statsrevisorernes spørgsmål 1 og 2.

Er Finanstilsynets opfølgning på it-tilsynet tilfredsstillende?

11. Vi vil undersøge, om og hvordan Finanstilsynet følger op på, om virksomhederne efterlever påbuddene. Hvis dette er tilfældet, vil vi også undersøge, hvad opfølgningen viser. Resultaterne heraf vil udgøre vores svar på Statsrevisorernes spørgsmål 2 vedrørende virkningen af tilsynet, da vi ikke vil være i stand til at undersøge, om tilsynet direkte resulterer i bedre it-sikkerhed i finansielle virksomheder. Endelig vil vi besvare Statsrevisorernes spørgsmål 5 om, hvorvidt kunderne har mulighed for at blive orienteret om eventuelle it-sikkerhedsmæssige risici og påbud i deres respektive pengeinstitutter.

12. Undersøgelsen omfatter som udgangspunkt perioden 2017-2022.

13. Rigsrevisionen skal for god ordens skyld understrege, at der undervejs vil kunne ske ændringer i forhold til det skitserede oplæg.

Birgitte Hansen