FOLKETINGET
RIGSREVISIONEN

September 2024

Rigsrevisionens notat om
beretning om

Finanstilsynets it-tilsyn

Vedrører:

Statsrevisorernes beretning nr. 14/2023 om Finanstilsynets it-tilsyn

Erhvervsministerens redegørelse af 15. august 2024

11. september 2024

RN 1112/24

1. Rigsrevisionen gennemgår i dette notat de initiativer, som erhvervsministeren vil iværksætte som følge af Statsrevisorernes bemærkninger og beretningens konklusioner. Dette sker med henblik på at vurdere, om Erhvervsministeriets initiativer adresserer den kritik, der fremgår af Statsrevisorernes bemærkninger og Rigsrevisionens beretning.

Konklusion

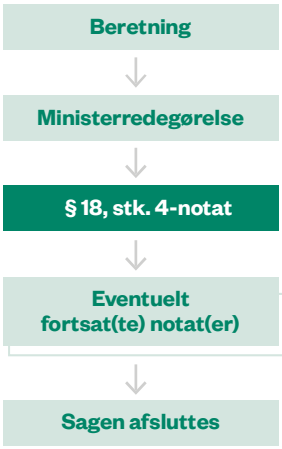
Rigsrevisionen finder, at erhvervsministeren har redegjort for, hvordan ministeriet og Finanstilsynet vil følge op på de væsentligste kritikpunkter i beretningen og Statsrevisorernes bemærkninger.

Erhvervsministeren tager beretningen til efterretning og oplyser, at en række kommende tiltag vil adressere beretningens konklusioner og anbefalinger. I forhold til beretningens konklusioner om at styrke tilrettelæggelsen og gennemførelsen af it-tilsynet henviser ministeren til, at Erhvervsministeriet er ved at implementere en ny EU-forordning, DORA, som indebærer ændringer af it-tilsynet. Rigsrevisionen vil, når det nye it-tilsyn foreligger, vurdere, om Finanstilsynet har taget højde for Statsrevisorernes bemærkninger og beretningens konklusioner for så vidt angår tilrettelæggelsen og gennemførelsen af it-tilsynet.

Erhvervsministeren oplyser også, at Finanstilsynet vil genoverveje sin praksis for anvendelse af sanktioner over for virksomheder, der ikke efterlever lovkravene til it-sikkerhed eller overskrider fristerne for efterlevelse af påbud. Finanstilsynet vil desuden vurdere muligheden for at tydeliggøre konsekvenserne for kunderne, når de offentliggør påbud i redegørelserne.

Alle 3 initiativer forventes gennemført 1. kvartal 2025.

Sagsforløb for en større undersøgelse



Du kan læse mere om forløbet og de enkelte step på www.rigsrevisionen.dk

DORA-forordningen

Formålet med DORA-forordningen er at styrke og harmonisere it-tilsynet med den finansielle sektor på tværs af virksomhedstyper i hele EU. Erhvervsministeriet er p.t. ved at implementere forordningen i dansk lovgivning.

Rigsrevisionen vil følge udviklingen og orientere Statsrevisorerne om:

- Finanstilsynets arbejde med at styrke it-tilsynet inden for rammerne af DORA-forordningen
- Finanstilsynets arbejde med at sanktionere virksomheder, der ikke efterlever lovkravene til it-sikkerhed eller overskrider fristerne for efterlevelse af påbud
- Finanstilsynets arbejde med at tydeliggøre konsekvenserne af de konstaterede mangler i virksomhedernes it-sikkerhed for kunderne.

I. Baggrund

2. Rigsrevisionen afgav i maj 2024 en beretning om Finanstilsynets it-tilsyn. Beretningen handlede om Finanstilsynets tilsyn med finansielle virksomheders it-sikkerhed.

3. Da Statsrevisorerne behandlede beretningen, fandt de Finanstilsynets tilsyn med finansielle virksomheders it-sikkerhed utilfredsstillende. Statsrevisorerne fandt, at det utilfredsstillende tilsyn øger risikoen for it-nedbrud, økonomiske tab og tab af tillid fra kunder og omverden.

4. Hele sagen kan følges på www.rigsrevisionen.dk og på www.ft.dk/Statsrevisorerne.

5. Bilag 1 viser Folketingets behandling af beretningen.

Systemisk vigtige virksomheder
Virksomheder, der i kraft af deres størrelse eller karakteren af deres ydelser er så væsentlige for den finansielle sektor, at brud på it-sikkerheden vil kunne true den samlede finansielle stabilitet.

Investeringsforvaltningsselskaber
Investeringsforvaltningsselskaber forvalter og administrerer danske investeringsforeninger, fx selskabet Formuepleje.

E-penge- og betalingsinstitutter
E-penge- og betalingsinstitutter (fx Nets og Forbrugsforeningen) er virksomheder, der formidler elektroniske betalinger mellem 2 parter.

II. Gennemgang af ministerens redegørelse

Tilrettelæggelse og gennemførelse af it-tilsynet

6. Statsrevisorerne fandt det bekymrende, at Finanstilsynet ikke havde inspiceret it-sikkerheden i en tredjedel af de systemisk vigtige virksomheder inden for det 4-årige interval, som de skal ifølge deres retningslinjer. På områder som fx adgangsstyring og fysisk sikkerhed havde Finanstilsynet ikke gennemført it-inspektioner i flere år, selv om Finanstilsynet selv vurderer, at en del virksomheder har høje risici på områderne.

Statsrevisorerne bemærkede også, at Finanstilsynet stort set ikke havde risikovurderet it-sikkerheden for investeringsforvaltningsselskaberne og heller ikke for de e-penge- og betalingsinstitutter og datacentraler, der ikke er systemisk vigtige. Desuden havde Finanstilsynet kun i meget begrænset omfang inspiceret investeringsforvaltningsselskaberne samt e-penge- og betalingsinstitutterne. Den begrænsede inspektion var dermed sket uden foregående risikovurdering af it-sikkerheden i virksomhederne, og Finanstilsynet havde ikke haft et grundlag for at vide, om fravalget af tilsyn med it-sikkerheden var hensigtsmæssigt.

7. Erhvervsministeren oplyser, at Erhvervsministeriet er ved at implementere DORA-forordningen i dansk lovgivning, og at Finanstilsynet er i gang med at tilpasse it-tilsynet til de nye regler i DORA-forordningen. Finanstilsynet er i den forbindelse ved at opdatere metoderne for tilrettelæggelse og gennemførelse af tilsynet. Arbejdet forventes implementeret ved udgangen af 1. kvartal 2025. Rigsrevisionen vil, når det nye it-tilsyn foreligger, vurdere, om Finanstilsynet i det nye tilsyn har taget højde for Statsrevisorernes bemærkninger og beretningens konklusioner for så vidt angår tilrettelæggelsen og gennemførelsen af it-tilsynet.

8. Rigsrevisionen vil følge Finanstilsynets arbejde med at styrke it-tilsynet inden for rammerne af DORA-forordningen.

Anvendelse af sanktioner

9. Statsrevisorerne bemærkede, at Finanstilsynet aldrig havde anvendt deres hjemmel til at sanktionere virksomheder, der ikke overholdt Finanstilsynets frister for efterlevelse af påbud, selv om virksomhederne i gennemsnit havde overskredet fristerne med 2 år.

Frister for efterlevelse af påbud
Når Finanstilsynet afslutter deres inspektioner fastsætter de en frist for, hvornår virksomheden skal efterleve eventuelle påbud om at rette op på mangler i deres it-sikkerhed.

Statsrevisorerne bemærkede også, at Finanstilsynet ikke havde udstedt administrative bødeforlæg til virksomhederne, fordi de vurderede, at bødesatserne var så små, at bøderne kun kunne gives for overtrædelser, der kunne karakteriseres som bagatelagtige. Statsrevisorerne anbefalede i den forbindelse, at Finanstilsynet skærper deres praksis for anvendelse af sanktioner over for virksomheder, der ikke efterlever lovkravene til it-sikkerhed eller overskrider fristerne for efterlevelse af påbud.

10. Det fremgår af erhvervsministerens redegørelse, at Finanstilsynet vil genoverveje sin praksis for anvendelse af sanktioner over for virksomheder, der ikke efterlever lovkravene til it-sikkerhed eller overskrider fristerne for efterlevelse af påbud. Ministeren oplyser desuden, at der vil blive anlagt en bred tilgang, og at der kan blive tale om øget anvendelse af såvel tilsynsreaktioner som kapitaltillæg og bøder. Ministeren forventer, at en ny tilgang vil være på plads 1. kvartal 2025.

Rigsrevisionen vil følge Erhvervsministeriets arbejde med at sanktionere virksomheder, der ikke efterlever lovkravene til it-sikkerhed eller overskrider fristerne for efterlevelse af påbud.

Tydeliggørelse af konsekvenserne af manglende it-sikkerhed

11. Rigsrevisionens undersøgelse viste, at det ikke fremgik af de offentliggjorte redegørelser, hvilke konsekvenser den manglende it-sikkerhed, som Finanstilsynet havde påbudt virksomhederne at følge op på, kunne få for virksomhedernes kunder.

Offentliggørelse af påbud
I henhold til lov om finansiel sikkerhed skal Finanstilsynet efter hver inspektion sende en redegørelse til virksomheden med de påbud, Finanstilsynet har givet. Både Finanstilsynet og virksomheden skal herefter offentliggøre redegørelsen.

Rigsrevisionen anbefalede derfor, at Finanstilsynet overvejede at supplere påbuddene med en vurdering af, hvilke konsekvenser virksomhedernes utilstrækkelige it-sikkerhed kan have for kunderne, så de kan se det i de offentliggjorte redegørelser. Statsrevisorerne tilsluttede sig Rigsrevisionens anbefaling.

Det fremgår af erhvervsministerens redegørelse, at Finanstilsynet vil vurdere muligheden for at tydeliggøre konsekvenserne for kunderne, når de offentliggør påbud i redegørelserne. Ministeren oplyser i den forbindelse, at det skal vurderes, om konsekvenserne kan tydeliggøres på en måde, så det giver reel merværdi for kunderne inden for rammerne af den direktivfastsatte tavshedspligt. Vurderingen forventes at foreligge senest 1. kvartal 2025.

Rigsrevisionen vil følge Erhvervsministeriets arbejde med at tydeliggøre konsekvenserne af de konstaterede mangler i virksomhedernes it-sikkerhed for kunderne.

Birgitte Hansen

Bilag 1. Folketingets behandling af beretningen

Beretning (nr.), dato for Statsrevisorernes mødebehandling og ministerredegørelse(r)	Behandlet i udvalg	Teknisk gennemgang ved Statsrevisorerne og Rigsrevisionen	Udvalgsspørgsmål (nr.)	Indkaldt til samråd	Statsrevisorerne har holdt møde med ministeren	§ 20-spørgsmål
Finanstilsynets it-tilsyn (nr. 14/2023) 13-05-2024 **Ministerredegørelse:** Erhvervsministeren: 15-08-2024	Finansudvalget: 23-05-2024					