ERHVERVSMINISTERIET

**Folketingets Erhvervsudvalg**

**ERHVERVSMINISTEREN**

3. februar 2023

**ERHVERVSMINISTERIET**

Slotsholmsgade 10-12
1216 København K

Tlf. 33 92 33 50
Fax. 33 12 37 78
CVR-nr. 10092485
EAN nr. 5798000026001
em@em.dk
www.em.dk

**Besvarelse af spørgsmål 27 alm. del stillet af udvalget den 19. januar 2023.**

**Spørgsmål:**
Vil ministeren kommentere det internt omdelt materiale om bedre IT-sikkerhed i finanssektoren, jf. ERU alm. del – bilag 26 (internt bilag)?

**Svar:**
Jeg har forelagt spørgsmålet for Finanstilsynet, der har oplyst følgende, som jeg kan henholde mig til:

"Finanstilsynet fører et risikobaseret tilsyn med overholdelsen af reglerne om IT-sikkerhed for finansielle virksomheder m.v. med henblik på at sikre finansiel stabilitet og tilliden til den finansielle sektor hos borgere og virksomheder. Det er vigtigt, at fx bankkunder kan være trygge ved at have deres penge i banken.

Den risikobaserede tilgang indebærer, at omfanget og dybden af IT-tilsynsaktiviteter tilrettelægges og prioriteres med udgangspunkt i virksomhedernes systemiske vigtighed og en vurdering af IT-risikoen blandt de ca. 450 væsentligste finansielle virksomheder, datacentraler, udbydere af betalingstjenester m.v. under IT-tilsyn. En vurdering af IT-risikoen sker bl.a. med afsæt i en vurdering af de systemiske og samfundsmæssige konsekvenser ved brud på IT-sikkerhed i de enkelte virksomheder.

I den forbindelse er det væsentligt at bemærke, at den systemiske IT-risiko på bankområdet primært er koncentreret hos nogle få pengeinstitutter og fællesejede datacentraler. Det skyldes, at kun få pengeinstitutter drifter deres egen IT, mens de fællesejede datacentraler varetager IT-driften for de øvrige, og dermed for størstedelen af de danske pengeinstitutter. Derfor er Finanstilsynets største tilsynsindsats også rettet mod disse virksomheder.

Finanstilsynet gennemfører derfor særskilte IT-inspektioner i de systemisk vigtige virksomheder, datacentraler og finansielle infrastrukturselskaber. For de ikke-systemiske finansielle virksomheder indgår IT-sikkerhed som et element i det generelle tilsyn og inspektioner i disse virksomheder.

På baggrund af den stigende IT-afhængighed samt udviklingen i trusselsbilledet har Finanstilsynet gennem de seneste år øget fokusset på IT-sikkerhed og udvidet antallet af medarbejdere, som specifikt har med IT-tilsyn

at gøre. Finanstilsynet oprettede i efteråret 2021 et separat kontor for tilsyn med IT-sikkerhed for at styrke tilsynet på området. Kontoret varetager bl.a. tilsyn med IT-sikkerhed i de systemisk virksomheder og er ekspertisecenter for Finanstilsynets arbejde med IT-sikkerhed i den finansielle sektor. Afdelingen består på nuværende tidspunkt 11 medarbejdere, hvoraf to er dedikeret til arbejde med sektorstrategien for cyber- og informationssikkerhed mv.

Siden 2020 er der gennemført 10 IT-inspektioner hos systemiske virksomheder, hvoraf redegørelserne fremgår på Finanstilsynets hjemmeside.

Finanstilsynets inspektioner afsluttes med en inspektionsredegørelse, som offentliggøres på virksomhedernes og Finanstilsynets hjemmeside. Tilsynsreaktioner såsom påbud, vil fremgå af redegørelserne. Det enten som en del af en særskilt redegørelse fsva. inspektioner i de systemiske virksomheder eller som en del af en samlet redegørelse fra en generel inspektion fsva. de øvrige virksomheder. Offentliggørelsen sikrer transparens for omverdenen om situationen i de enkelte virksomheder.

Det fremgår af præsentationen til Erhvervsudvalget, at der ikke er opgjort nogle påbud for IT-tilsyn. Dette beror på en misforståelse. For at se, hvilke tilsynsreaktioner, herunder påbud, Finanstilsynet har uddelt skal man kigge under *Inspektionsredegørelser*. I 2022 offentliggjorde Finanstilsynet seks særskilte IT-inspektionsredegørelser.

Når Finanstilsynet har givet påbud og påpeget forbedringsprojekter hos virksomhederne, følger Finanstilsynet op på, at virksomhederne får adresseret de centrale IT-risici som påbuddene skal håndtere. Derudover har Finanstilsynet flere andre tilsynsaktiviteter med virksomhederne som gennemføres som led i det løbende tilsyn og risikoafdækning af systemiske virksomheder. Det indebærer eksempelvis regelmæssige IT-risikomøder, og overvågning af større IT-sikkerhedshændelser.

Som led i en væsentlig styrkelse af indsatsen i forhold til cyber- og informationssikkerhed blev Finanstilsynet, som led i den nationale strategi på området, i 2018 udpeget som decentral enhed for cyber- og informationssikkerhed for finanssektoren (DCIS). Finanstilsynet har i kraft af sin rolle som DCIS ansvaret for den tværgående indsats for cyber- og informationssikkerhed på det finansielle område og samarbejder med de øvrige samfundskritiske sektorer, herunder energi og tele. Herudover samarbejder DCIS'en med en række enheder, herunder det offentlig/private samarbejdsforum Finansielt Sektorforum for Operationel Robusthed (FSOR) ledet af Nationalbanken, om at styrke cybersikkerheden i den finansielle sektor. Der er desuden et omfattende samarbejde på IT- og cybersikkerhedsområ-

det mellem Finanstilsynet og Nationalbanken, som overvåger, at de systemisk vigtige betalings- og afviklingssystemer og de vigtigste betalingsløsninger er sikre og effektive.

For at styrke robustheden i den finansielle sektor og styrke de systemisk vigtige virksomheders evne til at genoprette driften efter et eventuelt alvorligt nedbrud har Finanstilsynet iværksat et program om styrket operationel robusthed. Programmet skal gennem cyberstresstest kortlægge, hvad der vil ske i tilfælde af omfattende IT-nedbrud i sektoren. Finanstilsynet understøtter, at de enkelte virksomheder forebygger og reducerer konsekvenserne af et nedbrud.

I takt med udviklingen i trusselsbilledet på IT-sikkerhedsområdet er reguleringen og kravene til IT-sikkerhed i den finansielle sektor ligeledes løbende blevet udbygget. Kravene til IT-sikkerhed fremgår af ledelsesbekendtgørelsens bilag 5. Det dækker eksempelvis over IT-risikostyring, adgangsstyring og logning, beredskabsstyring og fysisk sikkerhed. Virksomhederne skal bl.a. sikre, at fysiske sikringsforanstaltninger bliver defineret, dokumenteret og implementeret for at beskytte ejendomme, datacentre og følsomme områder mod uautoriseret adgang og mod klima- og miljøfarer. Endvidere skal virksomheden etablere overvågning og foranstaltninger for at kunne opdage og rapportere fysisk eller logisk indtrængen. Finanstilsynet fører tilsyn med virksomhedernes overholdelse af disse regler.

Senest er der på EU-niveau vedtaget en ny forordning om digital operationel modstandsdygtighed (DORA), der bl.a. har til formål at styrke robustheden mod cyberangreb. DORA-forordningen er trådt i kraft den 16. januar 2023 og vil finde anvendelse for alle finansielle virksomheder fra den 17. januar 2025. De kommende regler vil stille en række nye krav til finansielle virksomheders risikostyring og beredskab i forhold til cybersikkerhed. De nye regler vil desuden betyde en yderligere forøgelse af IT-tilsynets omfang.

Lovgivningen er således løbende blevet strammet og opdateret i takt med den øgede IT-anvendelse og risiko i den finansielle sektor, ligesom tilsynsindsats er øget."

Med venlig hilsen

Morten Bødskov