VISION

Cybersikkerhed i den finansielle sektor

FSOR

FINANSIELT SEKTORFORUM FOR OPERATIONEL ROBUSTHED

Vision

Den danske finansielle sektor skal kunne imødegå den foranderlige trussel fra cyberkriminalitet og derved til enhver tid kunne

- **levere en sikker og effektiv infrastruktur**
- **fastholde danskernes tillid til de digitale løsninger i den danske finansielle sektor.**

Vi vil styrke sektorsamarbejdet og forbedre handle-mulighederne for de enkelte aktører

Vi vil styrke samarbej-det med relevante interessenter nationalt og internationalt

Vi vil øge opmærksomheden og viden om cybersikkerhed

September 2022

Cybersikkerhed i den finansielle sektor

Over hele verden bliver den finansielle sektor og andre kritiske samfundssektorers it-systemer angrebet af både kriminelle og statssponsorerede aktører. Danmark er et af de mest digitaliserede samfund i verden. Dette, sammenholdt med at store værdier håndteres, gør finanssektoren i Danmark til et mål for cyberkriminalitet. Center for Cybersikkerhed har i en række år vurderet, at risikoen for cyberkriminalitet mod den danske finansielle sektor er meget høj.

Cyberangreb er en potentiel trussel mod finansiel stabilitet

Den finansielle sektor er afhængig af komplekse it-systemer for at fungere, og samtidig er penge- og realkreditinstitutterne forbundet på tværs af sektoren via datacentraler, betalings- og afviklingssystemer.

Et stabilt finansielt system beror bl.a. på tilliden til, at der sker korrekt og fortrolig registrering af transaktioner, at afviklingen af betalinger og værdipapirhandler sker rettidigt, og at systemer er sikre og tilgængelige. Gentagne cyberangreb på virksomheder og systemer i den finansielle sektor kan – selv om det enkelte angreb ikke umiddelbart har samfundsmæssige konsekvenser – svække tilliden til det finansielle system. Enkeltstående, men omfattende cyberangreb, der kompromitterer kritiske systemer, har potentiale til at sætte hele eller væsentlige dele af sektoren ud af drift i en periode. Cyberangreb i det finansielle system er dermed en potentiel trussel mod finansiel stabilitet.

De enkelte aktører i den finansielle sektor har stor fokus på it-sikkerhed, herunder på at gøre deres systemer robuste over for cybertruslen. Forbundetheden i den finansielle sektor betyder imidlertid, at der er behov for en fælles og koordineret indsats mod den tiltagende cyberkriminalitet. Nationalbanken satte emnet på Det Systemiske Risikoråds dagsorden i december 2015, og ved opfølgende drøftelser med den finansielle sektor var der bred enighed om det hensigtsmæssige i at etablere et formaliseret sektorsamarbejde. På den baggrund blev FSOR, Finansielt Sektorforum for Operationel Robusthed, nedsat. FSOR havde sit første møde i juni 2016.

Finansielt Sektorforum for Operationel Robusthed

FSOR er et samarbejdsforum mellem myndigheder og vigtige aktører i den finansielle sektor, som har til formål at øge den operationelle robusthed på tværs af sektoren, herunder robustheden over for cyberangreb. FSOR har til opgave[1] at:

- sikre et fælles overblik over operationelle risici, der kan ramme på tværs af sektoren og potentielt true den finansielle stabilitet i Danmark

- beslutte og sikre gennemførelsen af fælles tiltag til at sikre den finansielle sektors robusthed over for store operationelle hændelser, herunder cyberangreb

- skabe rammer for samarbejde og videndeling, både inden for sektoren, mellem forskellige sektorer og internationalt.

FSOR opdaterer jævnligt en risikoanalyse på sektorniveau[2], som udgør omdrejningspunktet for FSOR's og Danmarks Nationalbanks initiativer til at øge cyberrobustheden. Risikoanalysen identificerer for det første risici, der kan true finansiel stabilitet i Danmark, og giver for det andet et struktureret grundlag for at prioritere mellem tiltag, der kan reducere risici.

En række kilder inddrages i risikoanalysen til at identificere de risici, som den finansielle sektor står over for. Det omfatter bl.a. kortlægning af centrale forretningsprocesser, kortlægning af systemmæssige afhængigheder, tidligere hændelser, trusselsvurderinger og input fra FSOR-medlemmerne, herunder input fra en årlig undersøgelse af FSOR-medlemmernes største bekymringer i relation til operationel robusthed. Blandt de centrale initiativer, der er taget på baggrund af risikoanalysen, er:

- En detaljeret kriseberedskabsplan på sektorniveau til at sikre en koordineret indsats på tværs af den finansielle sektor i tilfælde af en systemisk krise. Beredskabsplanen supplerer medlemmernes egne kriseplaner og det nationale kriseberedskab, NOST. Det er essentielt med beredskabsplaner på forskellige niveauer, da operationelle hændelser vil forekomme til trods for gode forebyggende tiltag. Til illustration kan nævnes, at kriseberedskabet under covid-19 videreformidlede viden om situationsbilledet på tværs af den finansielle sektor på baggrund af de enkelte organisationers indrapporteringer til beredskabet. Kriseberedskabsplanen bliver testet løbende og opdateres og forbedres på baggrund af de opsamlede erfaringer.

- Et TIBER-testforløb for de vigtigste aktører i den finansielle sektor, som Danmarks Nationalbank og aktørerne i samarbejde har etableret. TIBER står for Threat Intelligence Based Ethical Red-teaming, og den danske implementeringsguide for udførelsen af testene tager udgangspunkt i et rammeværk, der er overordnet udviklet af Den Europæiske Centralbank. I en test skal testdeltagere identificere såkaldte etiske hackerangreb og stoppe/forhindre angreb fra at gøre

1 Se Kommissorium for FSOR for uddybning (*link).*
2 Se "Metodehåndbog for FSOR's risikoanalyse" (*link).*

skade. Nationalbanken er myndighed for TIBER-DK[3] og understøtter udførelsen af testene.

- Regelmæssig undersøgelse af cyberrobustheden i den finansielle sektor, herunder identifikation af generelle problemstillinger på tværs af sektoren koblet med videndeling og individuelle tilbagemeldinger til deltagerne foretaget af Danmarks Nationalbank.

- Udvikling af en fælles baseline for cyberrobusthed, som kan anvendes på frivillig basis af organisationer i den finansielle sektor. Baseline har til formål at give konkrete og målbare anbefalinger omkring cyberrobusthed på forskellige områder, fx databeskyttelse og governance.

- Fælles fokus på at øge niveauet af databeskyttelse for sektorkritiske data og evnen til at sikre en sikker og effektiv genopretning efter et cyberangreb.

- Inddragelse af kritiske leverandører i FSOR-arbejdet med det formål at bringe leverandørerne tættere på sektorens aktører.

FSOR har desuden et tæt samarbejde med Risikoforum for Gensidige Afhængigheder (RGA)[4], der arbejder på at øge den operationelle robusthed mellem de centrale systemer i infrastrukturen. Risici, som identificeres i RGA, men som ikke kan mitigeres i regi heraf, løftes til FSOR.

FSOR's vision om at imødegå den foranderlige trussel fra cyberkriminalitet er retningsgivende for FSOR's initiativer som de ovennævnte og det arbejde, der igangsættes i de enkelte penge- og realkreditinstitutter, datacentraler, betalings- og afviklingssystemer. Derved skal arbejdet i FSOR bidrage til at sikre, at den finansielle sektor til enhver tid kan

- levere en sikker og effektiv infrastruktur og

- fastholde danskernes tillid til de digitale løsninger i den danske finansielle sektor.

Det er afgørende, at den finansielle sektors kunder har tillid til sektoren og til de digitale løsninger, som sektoren anvender. Tilliden er en forudsætning for at kunne indfri det vækst- og innovationspotentiale, som digitaliseringen af samfundet medfører.

3 TIBER-DK var et af de første TIBER-programmer i Europa. Se Nationalbankens hjemmeside for yderligere information om TIBER-DK (*link).*

4 Se Danmarks Nationalbanks hjemmeside for yderligere information om RGA (*link).*

Indsatsområder

For at realisere visionen har FSOR gennemført en række initiativer inden for tre overordnede indsatsområder:

Styrket sektorsamarbejde og forbedrede handlemuligheder for de enkelte aktører

FSOR skal danne ramme om et styrket sektorsamarbejde og forbedre sektorens handlemuligheder i forhold til cyber- og it-sikkerhedstrusler. Et stærkere sektorsamarbejde skal bidrage til at styrke de enkelte aktørers muligheder for at håndtere cyber- og it-sikkerhedstrusler.

Stærkere samarbejde med relevante interessenter nationalt og internationalt

FSOR skal styrke samarbejdet med relevante interessenter både nationalt og internationalt med henblik på at dele erfaringer og best practice for imødegåelse af cyberkriminalitet. Dette for at forbedre både FSOR-medlemmernes og interessenternes konkrete handlemuligheder.

Øget opmærksomhed og viden om cybersikkerhed

FSOR skal bidrage til at sikre, at alle aktører i den finansielle sektor har den nødvendige viden, kompetencer og muligheder for at beskytte sig imod cyber- og it-sikkerhedstrusler. Arbejdet i FSOR skal samtidig bidrage til at styrke de enkelte aktørers indsats i relation til deres kunders opmærksomhed og kompetencer vedrørende cybersikkerhed.

Deltagere i FSOR

Penge- og realkreditinstitutter

Betaling- og afviklingssystemer

Datacentraler

Brancheorganisationer

Myndigheder

Forsikrings- og pensionsselskaber

Andre relevante organisationer

Nationalbanken varetager formandskab og sekretariat for FSOR.