FSOR

FINANSIELT SEKTORFORUM
FOR OPERATIONEL ROBUSTHED

DECEMBER 2016

Cybersikkerhed i den finansielle sektor

VISION 2020

Den danske finansielle sektor skal være best in class i Europa til at imødegå truslen fra cyberkriminalitet, og derved

- **fortsat 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 samarbejdet med relevante interessenter nationalt og internationalt

Vi vil øge opmærksomheden og viden om cybersikkerhed

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 vurderer, at risikoen for cyberkriminalitet mod danske myndigheder og private virksomheder er meget høj.

Cybertruslen er stigende

I 2016 har tendensen i Danmark været, at de it-kriminelle går efter erhvervslivet. Senest har PwC i PwC Cybercrime Survey 2016 dokumenteret, at 69 pct. af adspurgte danske virksomheder har været ramt af et cyberangreb i det seneste regnskabsår. Direktørsvindel – også kendt som CEO Fraud – er en nyere angrebsmetode, som er på fremmarch. I årets første halvår er der blandt de danske banker kendskab til mindst 92 succesfulde angreb mod danske virksomheder med et samlet tab på over 60 mio. kr. til følge.

I nogle sager er der rigtigt store beløb på spil. Anklagemyndigheden kunne således i april 2016 berette om to sager, hvor svindlere narrede danske virksomheder til at overføre henholdsvis 100 og 40 millioner kroner. Også ransomware, hvor de it-kriminelle krypterer ofrenes computere for herefter at afkræve løsesum for at dekryptere computerne, har været i voldsom fremgang. En nylig analyse fra Trend Micro viser, at der internationalt har været en stigning på tæt på 200 pct. i forekomsten af ransomware-angreb i 1. halvår 2016 sammenlignet med 2015. Endelig har omfanget af phishing og smishing været stigende i den forgangne periode, hvilket bl.a. har bevirket, at Finansrådet har inkluderet denne type kriminalitet i statistikken over netbankindbrud fra og med 2016.

De it-kriminelles metoder ændrer sig løbende og bliver mere og mere avancerede. 2016 blev året, hvor det lykkedes for it-kriminelle gennem SWIFT-infrastrukturen at røve 81 mio. dollars fra Bangladesh' centralbank. SWIFT-systemet blev ikke selv kompromitteret, men en for svag it-sikkerhed i systemerne i Bangladesh' centralbank muliggjorde, at de it-kriminelle uautoriseret kunne anvende SWIFT-systemet til den kriminelle transaktion. Dette er et meget foruroligende og aktuelt eksempel på sårbarheden i vores sammenhængende systemer.

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 kundevendte 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. Og et 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 ved it-anvendelse på tværs i sektoren, herunder robustheden over for cyberangreb. FSOR har til opgave at:

- Sikre et fælles overblik over operationelle risici, der kan ramme på tværs af sektoren og potentielt kan 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 indenfor sektoren, mellem forskellige sektorer og internationalt.

Aktuelt er der i FSOR etableret fire arbejdsspor; etablering af et tværgående nationalt kriseberedskab for den finansielle sektor, afholdelse af en dansk cyberstresstest, kortlægning og risikovurdering af den finansielle infrastruktur og en generel stocktaking af nøgleaktørernes modstandsdygtighed over for cyberangreb. Arbejdet i FSOR adresserer operationel robusthed generelt, herunder med særlig fokus på cyberrobusthed.

FSOR finder, at ovenstående tiltag er oplagte, hensigtsmæssige og en god start, men vurderer samtidig, at der er behov for at formulere en fælles vision for finanssektorens modforholdsregler over for den tiltagende cyberkriminalitet.

Visionen skal samle og give fælles retning til FSOR's initiativer og det arbejde, der igangsættes i de enkelte penge- og realkreditinstitutter, datacentraler, betalings- og afviklingssystemer.

Vision for den finansielle sektors cybersikkerhed

Den danske finansielle sektor skal være best in class i Europa til at imødegå truslen fra cyberkriminalitet, og derved

- fortsat 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.

Målepunkter

For at kunne måle, om visionen indfris, opstilles tre målepunkter for visionsperioden med tilhørende indikatorer. Et foreløbigt bud på målepunkter er:

1. At Danmark ligger top 5 i internationale benchmarks på cybersikkerhedsområdet for finansielle virksomheder i Europa.
2. At der blandt danske borgere og virksomheder fortsat er stor tillid til sektorens digitale løsninger.
3. At sektorens tab pga. cyberkriminalitet ligger i bund 5 i Europa.

Indikatorerne er p.t. under afklaring.

Indsatsområder

For at realisere visionen skal der gennemføres 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. Vi skal være best in class i Europa i forhold til at optimere og teste den operationelle robusthed på tværs i sektoren. Et stærkere sektorsamarbejde skal samtidig 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.

Initiativer i de kommende år

Nedenfor beskrives de væsentligste initiativer i 2016 og de kommende år.

2016

I 2016 har der primært været fokus på målsætningen om styrket sektorsamarbejde og handlemuligheder.

- Etablering af tværgående kriseberedskab til håndtering af alvorlige operationelle hændelser, herunder cyberangreb.
- Gennemførelse af cyberstresstest af det fælles kriseberedskab.
- Identifikation af kritiske aktører og kernefunktionalitet.
- Kortlægning af infrastrukturen og de gensidige afhængigheder ml. forskellige aktører.
- Stocktaking af nøgleaktørernes robusthed over for cyberangreb.
- Deltagere i FSOR afsøger muligheden for at oprette en Nordisk FinansCSIRT.

2017-20

- Identificere og vurdere operationelle risici, der kan ramme på tværs af sektoren og potentielt true den finansielle stabilitet.
- Udarbejde en handleplan bl.a. på baggrund af FSOR-aktiviteter fra 2016, herunder:
  - Initiativer på baggrund af risikovurderingen.
  - Initiativer som følge af stocktaking.
  - Initiativer som opfølgning på cyberstresstest.
- Gennemføre jævnlige test af det fælles kriseberedskab og på den baggrund forbedre/videreudvikle beredskabet.
- I relevant omfang indarbejde IOSCO-anbefalinger om cybersikkerhed i forvaltningen af de danske betalings- og afviklingssystemer.

- Sikre koordination mellem FSOR's arbejde og en kommende opdateret national cyberstrategi.
- Etablere samarbejde med relevante fora svarende til FSOR i andre lande.
- Etablere samarbejde med en kommende Nordisk FinansCSIRT.
- Afdække mulighederne for at intensivere samarbejdet med nordiske finanstilsyn, nationalbanker og cybersikkerhedsansvarlige myndigheder.

Styrket sektor-samarbejde og handlemuligheder

Stærkere sam-arbejde med andre interessenter

- Identificere international best practice for cybersikkerhed.
- Skabe en ramme for at invitere international viden til DK.
- Dele viden om indsatsen i forskellige dele af sektoren i forhold til borgeres og virksomheders viden om it-sikkerhed og kompetencer til bedre at sikre sig mod cyberkriminalitet.

Øget opmærksomhed på og viden om cybersikkerhed

Deltagere i FSOR

Penge- og realkreditinstitutter
Danske Bank, DLR Kredit, Jyske Bank, Nordea, Nykredit, Sydbank

Betaling- og afviklingssystemer
Nets, VP Securities

Datacentraler
Bankdata, BEC, JN Data, SDC

Brancheorganisationer
Finansrådet, Forsikring og Pension, Realkreditrådet

Myndigheder
Center for Cybersikkerhed, Erhvervsministeriet, Finanstilsynet, Nationalbanken

Øvrige
e-nettet, Finansiel Stabilitet A/S, Nasdaq

Nationalbanken varetager formandskab og sekretariat for FSOR.