FSOR

FINANSIELT SEKTORFORUM
FOR OPERATIONEL ROBUSTHED

3. MARTS 2017

Årsberetning 2016

I foråret 2016 tog Nationalbanken initiativ til at etablere et finansielt sektorforum for operationel robusthed – også kaldet FSOR.

Formålet med FSOR er at øge den operationelle robusthed i den finansielle sektor, herunder robustheden over for cyberangreb. Deltagerne i FSOR er de centrale spillere i den finansielle sektor, jf. boks.

Den danske finansielle sektor er en af verdens mest digitaliserede. Det er godt, men det betyder også, at landets penge- og realkreditinstitutter er knyttet tæt sammen via betalings- og afviklingssystemer, hvor der flyttes store værdier. Derudover benytter flere af institutterne de samme datacentraler, netværksleverandører mv. Det er derfor afgørende, at alle vigtige led i kæden er robuste og kan modstå og håndtere operationelle hændelser, herunder cyberangreb. Sikring af denne operationelle robusthed er kort fortalt det, som FSOR er sat i verden for at understøtte.

Der har i 2016 været afholdt to FSOR-møder. Et af de resultater, som jeg særligt vil fremhæve er, at vi i regi af FSOR har formuleret en "Vision for den finansielle sektors cybersikkerhed", nemlig, at den danske finansielle sektor i 2020 skal være "best in class i Europa til at imødegå truslen fra cyberkriminalitet". Visionen, der blev præsenteret på Finans Danmarks[1] årsmøde 5. december 2016, indeholder en række initiativer, som vi skal gennemføre de kommende år. Det kræver en dedikeret indsats fra alle involverede parter.

---

1 Finans Danmark hed Finansrådet, da årsmødet blev afholdt.

I 2016 har vi etableret et kriseberedskab, der skal sikre en effektiv og koordineret indsats på tværs i sektoren i tilfælde af en kritisk operationel forstyrrelse, fx et omfattende cyberangreb, og har også gennemført en test af beredskabet. Og endelig er der gennemført en undersøgelse af cyberrobustheden i den finansielle sektor. Alt det kan du læse mere om i denne beretning.

FSOR er kommet godt fra land. Alle har arbejdet dedikeret og konstruktivt. Det vil jeg gerne benytte lejligheden til at takke deltagerne i FSOR for. Med de opgaver der ligger foran os, er det nødvendigt, at vi holder dampen oppe. Det er jeg sikker på, vi kan. Jeg ser frem til det fortsatte samarbejde i 2017.

Karsten Biltoft
Vicedirektør i Nationalbanken
og formand for FSOR

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
Finans Danmark, Forsikring og Pension

Myndigheder
Center for Cybersikkerhed, Erhvervsministeriet, Finanstilsynet, Nationalbanken

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

Nationalbanken varetager formandskab og sekretariat for FSOR.

Vision for den finansielle sektors cybersikkerhed

Den 5. december 2016 offentliggjorde FSOR en 2020 vision for den finansielle sektors cybersikkerhed. Visionen er et vigtigt pejlemærke for FSOR's fremtidige arbejde. Ambitionsniveauet fastlægges af konkrete målsætninger og målepunkter, som arbejdet i FSOR skal understøtte og indfri.

Visionen er, at den danske finansielle sektor i 2020 skal være "best in class" i Europa til at imødegå truslen fra cyberkriminalitet. Derved bevares en sikker og effektiv infrastruktur, og danskernes tillid til den finansielle sektors digitale løsninger fastholdes. For at kunne måle, om visionen indfries har FSOR opstillet et foreløbigt bud på målepunkter:

1. At Danmark ligger i 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 på grund af cyberkriminalitet ligger i bund 5 i Europa.

I visionen er der også formuleret tre overordnede indsatsområder med en række tilknyttede aktiviteter:

- Styrket sektorsamarbejde og forbedrede handlemuligheder for de enkelte aktører.
- Stærkere samarbejde med relevante interessenter nationalt og internationalt.
- Øget opmærksomhed og viden om cybersikkerhed.

Et centralt initiativ i visionen er, at der skal sikres et fælles overblik over risici, der kan true robustheden i den finansielle infrastruktur. Den øgede digitalisering understøttes af komplekse it-systemer og digitale forretningsgange, der er forbundet på kryds og tværs i sektoren. Den øgede kompleksitet betyder, at der er behov for en detaljeret kortlægning af både de gensidige afhængigheder mellem systemerne og mellem aktørerne, for derved at kunne analysere, om der er sårbarheder i infrastrukturen, der skal adresseres.

Derfor har FSOR i 2016 indledt en omfattende kortlægning af de mest kritiske forretningsaktiviteter, processer, systemer og aktører i den finansielle sektor. En kortlægning, der skal bidrage til at belyse de gensidige afhængigheder mellem aktørerne og i sidste ende danne grundlag for en egentlig risikovurdering af infrastrukturen set under et.

"Forbundetheden, og dermed den gensidige afhængighed mellem snart sagt alle aktørerne i sektoren betyder, at deling af viden og samarbejde er helt afgørende for at dæmme op for de angreb, der givet vil komme i fremtiden"

Nationalbankdirektør Lars Rohde, Finans Danmarks årsmøde

Test af krise-beredskabet

FSOR etablerede i 2016 den finansielle sektors kriseberedskab, som skal håndtere alvorlige operationelle hændelser, herunder cyberangreb. Formålet med beredskabet er at sikre en koordineret indsats på tværs af sektoren, så krisens omfang og konsekvenser kan minimeres mest muligt. Beredskabet er en udvidelse af det krisekommunikationsberedskab, der blev etableret tilbage i 2008.

Der blev i november 2016 gennemført en test af det nye krise-beredskab, da der i FSOR er bred enighed om, at uanset, hvor gode kriseberedskaber man i teorien har, er det først, når de testes og udsættes for stress, at man finder ud af, om de også holder i praksis. Testen, der løb over to dage og blev ledet af et anerkendt konsulenthus, var en såkaldt skrivebordsøvelse, der simulerede flere cyberangreb mod centrale dele af den finansielle infrastruktur. Deltagerne i beredskabet skulle så vise, om de kunne håndtere angrebene via samarbejde og koordinering af indsatsen på tværs af sektoren.

Konsulenterne har udarbejdet en rapport med observationer, konklusioner og anbefalinger.

Rapportens hovedkonklusion

”Det er vores konklusion, at den gennemførte sektor-test fuldt ud, og på tilfredsstillende vis fik afprøvet det nyetablerede kriseberedskab, herunder beredskabets aktivering og evne til at håndtere et kritisk cyberangreb. Det er vores vurdering, at testen havde stor læringsmæs-sig værdi for kriseberedskabsgruppen, og at den påviste en række styringsmæssige, organisatoriske og praktiske forbedringspunkter, som kan styrke kriseberedskabets mulighed for effektivt at håndtere et reelt cyberangreb i fremtiden. Det er ligeledes vores vurdering, at krisese-kretariatet overordnet set fungerede tilfredsstillende og arbejdede professionelt, støttet af en yderst samarbejds-villig og professionel kriseberedskabsgruppe.”

Alt i alt har det været en lærerig test, der vil blive fulgt op af en ny test i 2017 og flere test i de kommende år. Link

Cyberrobustheden i den finansielle sektor

Nationalbanken og Finanstilsynet gennemførte i 2016 en spørgeskemaundersøgelse, hvis formål var at give et billede af cyberrobustheden i den finansielle sektor i Danmark. 15 finansielle kerneaktører, der også er medlemmer af FSOR, deltog i spørgeskemaundersøgelsen.

Hovedkonklusion fra undersøgelsen

"Kerneaktørerne i den finansielle sektor i Danmark har et betydeligt fokus på cybersikkerhed, men der er plads til forbedring."

En væsentlig observation fra undersøgelsen var, at der er størst fokus på cybersikkerhed blandt de finansielle aktører, der har en bestyrelsesgodkendt strategi for cybersikkerhed, som er kendt bredt i organisationen. Det vil sige, at både topledelsen, andre ledelsesniveauer og medarbejderne er involveret. Disse aktører har generelt også et højere niveau for cybersikkerhed på flere områder.

Derudover viste undersøgelsen, at der hos nogle aktører er plads til forbedringer på følgende områder:

- Risikostyring er en løbende proces til identificering, vurdering og håndtering af risici. Som led i god it-sikkerhed og som grundlag for at kunne lægge en effektiv strategi for styring af cyberrisiko, er det nødvendigt at arbejde struktureret med kortlægning af kritiske forretningsområder og de systemer og processer, som understøtter disse.
- Alle medarbejdere skal trænes i cybersikkerhed med særligt fokus på medarbejdere med forretningskritiske funktioner og adgange. Organisationen kan derfor med fordel give sidstnævnte ekstra træning i cybersikkerhed.
- Beredskabsplaner kan med fordel testes mod cyberhændelser, da disse kan have særlige karakteristika i forhold til andre operationelle hændelser.

Link