FSOR
FINANSIELT SEKTORFORUM
FOR OPERATIONEL ROBUSTHED

ÅRSBERETNING 2018

2018 var et begivenhedsrigt år i Finansielt Sektorforum for Operationel Robusthed, FSOR. Og kulminationen var i min optik, da Nationalbanken den 18. december – som nogle af de allerførste i Europa – kunne offentliggøre implementeringsguiden for TIBER-DK, Threat Intelligence Based Ethical Red-teaming. TIBER-DK skal de kommende år sikre, at de mest kritiske finansielle institutioner i Danmark gennemgår et ambitiøst red team-testprogram, som skal øge cyberrobustheden hos deltagerne.

TIBER-DK er et program, som Nationalbanken er myndighed på. Enigheden om at etablere programmet blev opnået i FSOR i februar 2018. Her kom værdien af det gode samarbejde, der har været med sektoren siden etableringen af FSOR i 2016, i høj grad til udtryk. FSOR-deltagerne var alle enige om, at hvis man skal leve op til FSOR's vision om at være best in class, så skal Danmark have et TIBER-program.

Også på andre områder har vi fortsat arbejdet med at højne cyberrobustheden. Det gælder både i forhold til at forbedre og udvikle FSOR's kriseberedskab og i forhold til at følge op på anbefalingerne i analysen fra 2017 om tværgående operationelle risici i den danske finansielle infrastruktur.

Vi har i 2018 igen haft fokus på vidensdeling. Det kom blandt andet til udtryk i en velbesøgt workshop, der kom i kølvandet på en cyberrobusthedsundersøgelse, som Nationalbanken gennemførte i løbet af året. Og vores finske centralbankkolleger gennemførte i efteråret en nordisk cyberkonference, der fulgte op på den cyberkonference, som Nationalbanken tog initiativ til i 2017.
I årsrapporten for 2017 fremhævede jeg, at en af mine ambitioner for 2018 var at inddrage og samarbejde med aktører både uden og inden for den finansielle sektor. Den målsætning er vi godt i gang med at opfylde.

Spar Nord er som ny SIFI-bank blevet medlem af FSOR, og på workshoppen om cyberrobusthed udvidede vi kredsen af inviterede til også at omfatte virksomheder, der har tæt tilknytning til den finansielle sektor. Vi har også taget første skridt i forhold til at samarbejde tættere med de kritiske leverandører, som vi identificerede i forbindelse med analysen om tværgående operationelle risici.

Sidst, men ikke mindst, blev det sidst på året – i fællesskab med Forsikring & Pension – besluttet, at forsikrings- og pensionssektoren fremadrettet skal være en mere integreret del af FSOR, så FSOR i endnu højere grad omfatter hele den finansielle sektor.

Verden omkring os står ikke stille. I 2018 blev cybertruslen ikke mindre, snarere tværtimod. Regeringen lancerede i foråret 2018 en ambitiøs national cyberstrategi og udpegede i den forbindelse seks kritiske sektorer – herunder selvfølgelig også den finansielle sektor – hvor der skal gøres en særlig indsats for at højne cyberrobustheden. Jeg er helt enig i ambitionerne, og fra Nationalbankens side er vi klar til at fortsætte det gode samarbejde, både i FSOR ogpå tværs af de kritiske sektorer.

Afslutningsvist vil jeg benytte lejligheden til at takke FSOR-deltagerne for deres konstruktive bidrag til FSOR's dagsordener. Selv om FSOR har eksisteret i 3 år, sporer jeg en fortsat lyst til at dele viden og højne cyberrobustheden i sektoren i bevidsthed om, at en større cyberrobusthed er til gavn for alle.

Karsten Biltoft, formand for FSOR og vicedirektør i Nationalbanken

TIBER-DK

I februar 2018 blev der i FSOR opnået principiel enighed om at etablere et dansk "intelligence"-baseret red team-testprogram. Herefter har en arbejdsgruppe i løbet af 2018 udarbejdet en tilpasning af det europæiske TIBER-EU-rammeværk til danske forhold. Tilpasningen har udmøntet sig i et dansk rammeværk kaldet TIBER-DK, der blev offentliggjort af Nationalbanken i december 2018. Offentliggørelsen var samtidig startskuddet på testforløbet, hvor de første test finder sted i 2019, og de øvrige test følger i løbet af 2020 og 2021.

TIBER står for Threat Intelligence Based Ethical Red-teaming, og programmet er udviklet af Den Europæiske Centralbank. TIBER sætter en ny, fælleseuropæisk standard for test af cybersikkerheden i de samfundskritiske dele af den finansielle sektor.

Testprogrammet er "intelligence-led", hvilket betyder, at testscenarierne er baseret på efterretninger om aktuelle og konkrete trusler imod den danske finansielle sektor og specifikt imod den enkelte testdeltager. Dermed sikrer programmet en virkelighedstro test, hvor testdeltageren får erfaring med at forsvare sigimod de metoder og taktikker, som benyttes af de virkelige trusselsaktører.

Myndigheders koordination på tværs af landegrænser er en integreret del af TIBER-rammen. Det tværgående samarbejde er en fordel, da flere testdeltagere opererer i Norden, og flere nordiske lande barsler med deres egen version af TIBER-programmet.

Den danske sektor bliver, sammen med den belgiske, den første til at benytte det færdige TIBER-program, og det understøtter FSOR's vision om at være best in class i Europa til at imødegå truslen fra cyberkriminalitet. Se mere her:

http://www.nationalbanken.dk/da/finansielstabilitet/fsor/Sider/TIBER-DK.aspx

TVÆRGÅENDE RISICI

I 2018 fortsatte arbejdet med at følge op på de 13 anbefalinger fra 2017, som var resultatet af FSOR's analyse af tværgående operationelle risici i den danske finansielle infrastruktur. Der er bl.a. etableret et løbende og formaliseret samarbejde om at styre de risici, der opstår i samspillet mellem kernesystemerne i infrastrukturen, eller som kan ramme flere systemer samtidig. Og risici ved brug af fælles kritiske netværk og centrale driftsleverandører er adresseret, ligesom der er taget de første skridt til en fælles dialog med de kritiske leverandører om, hvordan robustheden i infrastrukturen i fællesskab kan øges.

Der er også gennemført en analyse af, om forholdsreglerne til at opdage og forhindre kriminelle transaktioner er tilstrækkelige. Dette arbejde har til formål at mindske risikoen for, at it-kriminelle vil kunne føre et stort kronebeløb ud af det finansielle system, som det tidligere er set i bl.a. Bangladesh, hvor det i 2016 lykkedes kriminelle at føre 100 mio. amerikanske dollar ud af landet.

FSOR'S KRISEBEREDSKAB

Vedligeholdelsen og udviklingen af FSOR's kriseberedskab er en topprioritet. Derfor arbejdes der løbende på at optimere beredskabet. I 2018 har der særligt været fokus på at implementere de forbedringspunkter, som testen af kriseberedskabet i 2017 gav anledning til. Derudover har der også været fokus på valg af kommunikationsværktøj, der kan bidrage til en smidigere kommunikation i en krisesituation.

FSOR fik også præsenteret en detaljeret testplan for de kommende år, som skal bidrage til, at beredskabet kontinuerligt skærpes og udvikles.

UNDERSØGELSE AF CYBERROBUSTHEDEN

Nationalbanken og Finanstilsynet gennemførte i foråret 2018 en spørgeskemaundersøgelse af cyberrobustheden hos 16 kerneaktører i den finansielle sektor.

Undersøgelsen viste, at de fleste aktører vurderer, at de har løftet deres cyberrobusthedsniveau siden den første undersøgelse i 2016. De fleste respondenter angav, at de nu har en bestyrelsesgodkendt cyberstrategi. Det er en positiv udvikling. Undersøgelsen viser nemlig en klar tendens til, at aktører med en bestyrelsesgodkendt strategi har et højere niveau af cyberrobusthed på andre områder. Ledelsen kan således via strategien fremme arbejdet med cybersikkerhed, da strategien indeholder krav og forventninger til, hvordan virksomheden identificerer, styrer og håndterer cyberrisici.

Undersøgelsen viste også, at der er plads til forbedringer. Få aktører har ikke forbedret deres niveau siden undersøgelsen i 2016, og de bør opprioritere cyberindsatsen. De øvrige aktører har også fortsat områder, der kan forbedres. Fx kan de fleste øge systematikken og grundigheden i arbejdet med cyberrobusthed. Samtidig stiger kapaciteten hos cyberkriminelle hele tiden. Det betyder, at det kræver en kontinuerlig indsats at bevare et højt cyberrobusthedsniveau.

De overordnede konklusioner fra undersøgelsen er offentliggjort (link), og Nationalbanken har givet individuelle tilbagemeldinger til brug for de enkelte aktørers videre arbejde med at øge cyberrobustheden. Der er endvidere afholdt en best practice-workshop, hvor aktører, der var best in class på forskellige områder, delte ud af deres erfaringer.