10. februar 2022

Fremdrift i cyberrobustheden 2021

FSOR

FINANSIELT SEKTORFORUM FOR OPERATIONEL ROBUSTHED

Fremdrift i cyberrobustheden i 2021

I 2021 fyldte Finansielt Sektorforum for Operationel Robusthed fem år. Siden oprettelsen i 2016 har den finansielle sektor i et fælles samarbejdsforum arbejdet for at øge sektorens operationelle robusthed, herunder cyberrobustheden. FSOR-samarbejdet er et centralt forum, hvor sektoren med fælles viden og ressourcer kan adressere centrale risici. Blot de seneste år har cyberangreb mod eksempelvis SolarWinds og Microsoft Exchange vist, at ondsindede angreb, bl.a. via leverandører, kan være sofistikerede og ramme bredt.

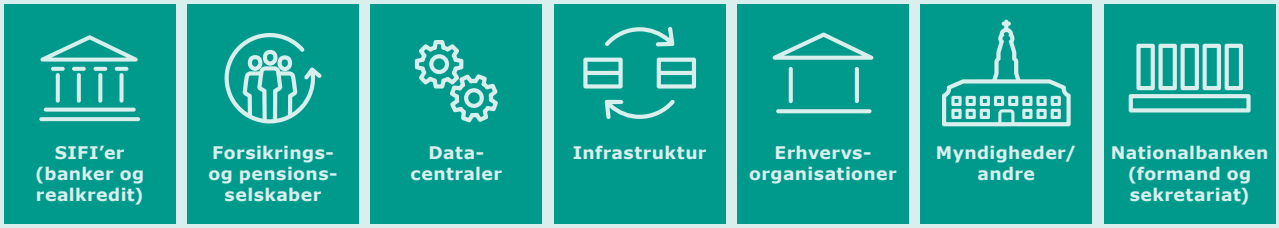
FSOR har i 2021 besluttet at udvide medlemskredsen med to nye medlemmer i form af Arbejdernes Landsbank og MasterCard. Endvidere er Peter Ejler Storgaard fra Danmarks Nationalbank tiltrådt som ny formand, efter at den tidligere formand fratrådte som led i et jobskifte.

I 2021 har FSOR haft særligt fokus på

- en risikoanalyse på sektorniveau, som opdateres halvårligt. To nye risici er tilføjet i løbet af 2021, og dermed er der nu identificeret 41 risici.
- at sætte rammerne for at identificere samfundskritisk data med det formål at forbedre sektorens databeskyttelse og evne til genopretning i tilfælde af en hændelse.
- at udarbejde et konkret værktøj, Baseline, til at evaluere cyberrobustheden i de enkelte organisationer og hos leverandører.
- at anvende resultaterne af en cyberundersøgelse til dels at vurdere den enkelte organisations status mod resten af den finansielle sektor, og dels at dele viden med hinanden.
- at teste sektorens kriseberedskab to gange og opdatere kriseberedskabsplanen kvartalsvist.
- at påbegynde en evaluering af rammerne for FSOR-samarbejdet via en besøgsrunde til de operationelle medlemmer.

Disse initiativer er bl.a. uddybet nedenfor. I tillæg hertil har Danmarks Nationalbank og den finansielle sektor fortsat arbejdet sammen om TIBER-programmet – også her med henblik på at styrke cyberrobustheden.

Vigtigheden af FSOR's arbejde med at øge den operationelle robusthed tydeliggøres af sofistikerede, ondsindede cyberangreb.



Finansielt Sektorforum for Operationel Robusthed

Den danske finansielle sektor gik i 2016 sammen i et privat-offentligt samarbejdsforum kaldet Finansielt Sektorforum for Operationel Robusthed, FSOR, for at øge sektorens operationelle robusthed over for bl.a. cyberangreb.

FSOR er et frivilligt, men forpligtende, samarbejdsforum, og medlemmerne er den finansielle sektors mest centrale deltagere. Medlemmerne i FSOR er:

- De største og systemisk vigtige finansielle institutioner, SIFI'er, og repræsentanter for forsikrings- og pensionsselskaber.
- Datacentraler, som drifter kritiske systemer og opbevarer og håndterer dele af sektorens data.
- De virksomheder, som ejer infrastrukturen – herunder platforme til finansielle transaktioner.
- Finansielle erhvervsorganisationer.
- Centrale myndigheder. Danmarks Nationalbank er formand for FSOR og varetager sekretariatsfunktionen.

FSOR har fokus på de systemiske risici, der kan true den finansielle stabilitet og realøkonomien, og sætter i dag dagsordenen for det fælles arbejde med operationel robusthed i den danske finansielle sektor.

FSOR-samarbejdet udbygges med to nye medlemmer

FSOR-kredsen vurderer mindst en gang årligt, om alle relevante aktører er repræsenteret i forummet. Arbejdernes Landsbank er blevet identificeret som ny SIFI efter overtagelsen af aktiemajoriteten i Vestjysk Bank, og MasterCard har overtaget driften af detailclearingerne fra Nets. Begge organisationer indbydes derfor i FSOR-samarbejdet.

Risikoanalyse sætter retning for de fælles tiltag i FSOR

FSOR samarbejder om at identificere og adressere operationelle risici, der kan ramme på tværs af sektoren og potentielt true den finansielle stabilitet. Centralt for arbejdet er en systematisk risikoanalyse, der bidrager til at identificere risici, og som giver et struktureret grundlag for at prioritere tiltag til at reducere risici. Risikoanalysen inddrager en række kilder til at identificere de risici, som den finansielle sektor står over for. Det omfatter bl.a. kortlægning af centrale forretningsprocesser og systemmæssige afhængigheder, tidligere hændelser, trusselsvurderinger og input fra FSOR-medlemmerne, herunder input fra den årlige undersøgelse af FSOR-medlemmernes største bekymringer i relation til operationel robusthed. Nationalbanken har offentliggjort risikoanalysens metode på Danmarks Nationalbanks hjemmeside (*link*).

Risikoanalysen opdateres halvårligt. Ved opdateringerne i 2021 er der identificeret to nye risici, og der er nu identificeret 41 risici i alt. Vurderingen af de eksisterende risici er genbesøgt i forhold til sandsynlighed og konsekvens. I 2021 har FSOR haft særlig fokus på risici i relation til beskyttelsen af kritisk data og reetablering af data efter et eventuelt cyberangreb.

Risici i den centrale infrastruktur behandles mere detaljeret i Risikoforum for Gensidige Afhængigheder, RGA, som er et samarbejdsforum med deltagelse af Euronext Securities Copenhagen, Finans Danmark, e-nettet og Danmarks Nationalbank. RGA har til formål at identificere og håndtere risici og hændelser som følge af gensidige afhængigheder mellem systemerne bag værdipapirafviklingen, detailbetalingssystemerne og Kronos2. RGA arbejder bl.a. med fælles nedluknings- og genåbningsscenarier samt køreplaner og test for kontrolleret nedlukning af den kritiske infrastruktur i tilfælde af operationelle hændelser. Risikoarbejdet i RGA og FSOR koordineres løbende.

FSOR har identificeret 41 risici, som potentielt kan true finansiel stabilitet, og arbejder i fællesskab på at mitigere de centrale risici

FSOR sætter strategisk fokus på databeskyttelse og recovery

Risikoanalysen har som nævnt identificeret flere risici, som omhandler databeskyttelse og recovery. Derfor har FSOR sat fokus på disse områder.

Et af de centrale initiativer er at identificere samfundskritisk data. Det er fundamentet for det videre arbejde, at der er kendskab til, hvilke data der ud fra et samfundsperspektiv særligt skal passes på, og hvad der skal have fokus i en genetableringssituation. FSOR-RISK og RGA har i 2021 påbegyndt arbejdet med i fællesskab at identificere kritisk data, herunder at få fastlagt en fælles forståelse for, hvad samfundskritisk data er, og en fælles model for at klassificere data.

Endvidere er databeskyttelse og recovery inddraget i udformningen af værktøjet Baseline, som er nævnt nedenfor. FSOR har også kortlagt de få eksisterende fællesskabsløsninger om databeskyttelse og recovery, der findes i andre lande til inspiration for det videre arbejde. Derudover er der afholdt en workshop om databeskyttelse. Endelig har Nationalbanken inddraget databeskyttelse som et fokusområde i de kommende TIBER-test (*link*).

Værktøjet baseline vil øge sektorens cybermodenhed

På baggrund af risikoanalysens konklusioner påbegyndte FSOR i 2020 et projekt, der skulle lede frem til et såkaldt Baselineværktøj. Baseline skal – med udgangspunkt i gældende lov og kendte internationale standarder – formulere konkrete og målbare anbefalinger til arbejdet med cyberrobusthed på forskellige områder, fx databeskyttelse eller governance. Baseline bliver en it-platform, hvor den enkelte organisation på frivillig basis kan "måle" sin aktuelle cyberrobusthed og få specificeret konkrete tiltag, som kan iværksættes for at opnå et ønsket niveau. Baseline kan anvendes af alle aktører i den finansielle sektor og deres leverandører. Arbejdsgruppen, der udformer Baseline, har i 2021 arbejdet intenst på at færdiggøre værktøjet, som er blevet lanceret i begyndelsen af 2022.

Undersøgelse af cyberrobustheden viser en højere grad af robusthed i 2020 end i 2018

I 2020 foretog Nationalbanken den tredje spørgeskemaundersøgelse om cyberrobusthed blandt FSOR-medlemmerne. Undersøgelsen er en selvevaluering af det aktuelle niveau for cyberrobusthed. Resultaterne er blevet delt med hver enkelt organisation, på en måde hvor de har fået indsigt i, hvor deres organisation er sammenlignet med de øvrige aktører i den finansielle sektor. Derudover er de samlede resultater drøftet på et FSOR-møde.

Resultaterne fra undersøgelsen anvendes også som input til FSOR-risikoanalysen og bidrager dermed til FSOR's beslutninger om, hvilke fælles initiativer der skal tages for at adressere de væsentligste cyberrisici i sektoren.

Desuden har FSOR på baggrund af undersøgelsen afholdt to best practice-workshops om henholdsvis databeskyttelse og detektion. De aktører, der er best in class på hver af disse områder, har delt viden og erfaringer med resten af FSOR-medlemmerne.

I september 2021 udgav Nationalbanken artiklen "Hvor cyberrobust er den finansielle sektor i Danmark?" (*link*). Her gives et overblik over resultaterne af undersøgelsen på et aggregeret niveau.

I analysen vurderer Danmarks Nationalbank, at den finansielle sektor samlet set står stærkt i forhold til evnen til at beskytte systemer og netværk og detektere udefrakommende angreb – og stærkere end i 2018. Samtidig stiger cybertruslen primært fra ransomware-angreb, og de teknikker og taktikker, som cyberkriminelle benytter sig af, bliver løbende mere specialiserede og sofistikerede. Risikoen for, at avancerede hackergrupper bryder igennem det ydre forsvar, kan ikke elimineres. Det er vigtigt, at udviklingen i trusselsbilledet løbende modsvares med passende sikkerhedsforanstaltninger, herunder med særligt fokus på arbejdet med databeskyttelse og sikker genopretning efter et cyberangreb.

I FSOR har de bedste aktører indenfor databeskyttelse og detektion delt ud af deres viden og erfaring

Kriseberedskabet sikrer koordinering på tværs af sektoren i tilfælde af en krise

Til trods for gode forebyggende tiltag vil operationelle hændelser forekomme. FSOR har derfor udarbejdet en detaljeret kriseberedskabsplan til at sikre en koordineret indsats på tværs af den finansielle sektor i tilfælde af en systemisk krise. Den supplerer medlemmernes egne kriseplaner og det nationale kriseberedskab, NOST.

FSOR's kriseberedskab er testet to gange i 2021 for at sikre, at kriseplanen fungerer i praksis i tilfælde af en alvorlig hændelse i sektoren. Den 15. juni 2021 blev der gennemført en partiel test af FSOR-kriseberedskabsplanen med det formål at øve en uvarslet aktivering af FSOR-kriseberedskabet. Den 23. november 2021 gennemførte FSOR-kriseberedskabet en test med særligt fokus på de faser af beredskabsplanen, som har fokus på at begrænse skaden, fjerne angrebet, genoprette forretningsaktiviteter og deaktivere kriseberedskabet. I 2021 har bl.a. kriseberedskabstest givet anledning til opdateringer til FSOR-kriseberedskabsplanen, som nu foreligger i version 4.0.

Som i 2020 har pandemien også i 2021 medført perioder af nedlukning og øget brug af hjemmearbejde. Den finansielle sektor har ikke i perioden været operationelt udfordret i forhold til at kunne varetage de samfundskritiske funktioner.

Besøgsrundtur tager temperaturen på FSOR-samarbejdet

FSOR-sekretariatet har i 2021 været på besøg hos de operationelle FSOR-medlemmer. Formålet har været dels at drøfte samarbejdet i FSOR, dels at vende næste skridt i forhold til arbejdet med beskyttelse af sektorkritisk data. Input fra besøgsrunden peger på, at samarbejdet giver værdi på tværs af sektoren, og at der er god tillid og fælles forståelse blandt medlemmerne. Input fra besøgsrunden giver endvidere anledning til en forventningsafstemning om det fremtidige ressourceforbrug.

FSOR afholder to årlige medlemsmøder, som fungerer som drøftelses- og beslutningsforum. Udvikling og produktion af konkrete FSOR-initiativer foregår i nedsatte arbejdsgrupper. Der er p.t. nedsat tre arbejdsgrupper under FSOR, og en fjerde er ved at blive oprettet. Endvidere afholdes ad hoc-temamøder med det formål at dele viden på konkrete områder. I 2021 er der afholdt tre temamøder om hhv. databeskyttelse, detektion og trusselslandskabet.

Cybersamarbejde og fortsat fokus på at øge robustheden i 2022

Cyberrobusthed er højt på dagsordenen i hele samfundet
Udover de initiativer, der er søsat i den finansielle sektor i regi af FSOR, arbejdes der med cyberrobusthed bredt i samfundet.

Regeringen offentliggjorde i slutningen af 2021 en ny national strategi for cyber- og informationssikkerhed, der dækker perioden 2022-2024. Strategien ligger i forlængelse af den forrige strategi for 2018-2021 og har ambition om at løfte den digitale sikkerhed på tværs af samfundet gennem 34 initiativer. Initiativerne bygger videre på allerede gennemførte tiltag og introducerer også nye (*link*). Den udvides bl.a. fra at omfatte de seks nuværende samfundskritiske sektorer til også at omfatte en bredere kreds af ministerområder med ansvar for samfundsvigtige funktioner.

For hver af de samfundskritiske sektorer er der etableret en decentral enhed for cyber- og informationssikkerhed, DCIS, samt en sektorstrategi for arbejdet. Finanstilsynet varetager funktionen som DCIS for finanssektoren og er tovholder på den finansielle sektors cyberstrategi, hvori flere af FSOR's ovennævnte indsatser indgår.

Den finansielle sektors cyberstrategi løb frem til 2021, og en ny sektorstrategi forventes at blive lanceret i første halvår af 2022 på baggrund af den nye nationale strategi.

Nordisk cybersamarbejde
Der afholdes årlige cyberkonferencer blandt de nordiske lande. Her deltager aktører fra den finansielle sektor og myndigheder, hvor formålet er at øge viden om cybersikkerhed på tværs af den nordiske finansielle sektor. I november 2021 var Norges Bank vært for den fjerde af slagsen med temaet "cyber security in complex value chains" (*link*). Her blev der sat fokus på cyberrisici i relation til leverandører.

I 2022 afholdes konferencen af Islands centralbank, Seðlabanki.

Internationalt samarbejde – CIISI-EU
Danmarks Nationalbank har i 2021 deltaget på alle møder i et offentlig-privat samarbejde mellem de vigtigste europæiske finansielle aktører kaldet Euro Cyber Resilience Board, ECRB (*link*).

ECRB, der blev etableret efter beslutning af ECB i 2017, vedtog i begyndelsen af 2020 et såkaldt "Cyber Information and Intelligence Sharing Initiative", CIISI-EU, hvor der blev oprettet en fælles platform for videndeling på strategisk, taktisk og operationelt niveau mellem de vigtigste finansielle aktører i EU (*link*).

Nationalbanken er formelt medlem af CIISI-EU og bidrager blandt andet med erfaring fra FSOR, som i forhold til samarbejde og sektorinitiativer er blandt frontløberne i international sammenhæng. Omvendt modtager Nationalbanken løbende operationelle informationer og beretninger via CIISI-EU, som bruges til at berige det aktuelle trusselslandskab og håndtere aktuelle sager. I løbet af 2022 vil fokus være på, hvordan denne information kan udveksles til gavn for flere, herunder hvordan informationer fra denne kreds kan bidrage til FSOR's øvrige arbejdsspor.

TIBER–programmet sætter fokus på databeskyttelse
Siden begyndelsen af 2019 har Nationalbanken koordineret test af cyberrobustheden i den finansielle sektor under et program kaldet TIBER-DK. En særlig enhed i Nationalbanken understøtter disse test og faciliterer videndeling blandt deltagere i programmet. I TIBER-test simuleres avancerede angreb fra organiserede kriminelle cybergrupper eller statssponsorerede grupper i faktiske produktionsmiljøer. På baggrund af efterretningsbaseret trusselsinformation tager testene udgangspunkt i virkelige taktikker, teknikker og procedurer. Målet er at identificere styrker og svagheder i cyberforsvaret. Ved at adressere svaghederne øges cyberrobustheden.

Med udgangspunkt i gode erfaringer med TIBER-DK besluttede Nationalbanken og de enkelte deltagere i foråret 2021 at fortsætte testene fremadrettet.

I fremtidige TIBER-test ønsker Nationalbanken yderligere fokus på databeskyttelse med henblik på at øge indsatsen på dette område. Derfor vil alle test i næste runde som udgangspunkt indeholde et angrebsscenarie med særligt fokus på databeskyttelse. Scenariet kan give læring om, hvorvidt det er muligt at få adgang til at læse, ændre eller slette følsomme data, hvorvidt det bliver opdaget, når følsomme data forlader organisationen, samt om det i tilfælde af et angreb er muligt at tilgå backupdata. Desuden arbejdes der hen imod særskilte og mere målrettede test af centrale, kritiske leverandører i den finansielle infrastruktur.

Testene følger fortsat TIBER-DK-rammeværket, som i 2021 er opdateret med input fra TIBER-deltagerne og ECB på baggrund af de hidtil opnåede erfaringer med TIBER. Opdateringen giver plads til det nye fokus på databeskyttelse og giver deltagerne et endnu stærkere læringsgrundlag. Endelig blev der i slutningen af 2021 udformet den årlige trusselslandskabsrapport til brug for TIBER-testene. Rapporten er udarbejdet af NFCERT med involvering af relevante parter.

Ny hjemmeside offentliggøres i 2022

FSOR-sekretariatet har i 2021 arbejdet på at opdatere FSOR's hjemmeside. Den nye hjemmeside forventes lanceret i begyndelsen af 2022 med det formål, at det bliver lettere at tilgå information om FSOR.