19. januar 2021

Årsberetning 2020

FSOR

FINANSIELT SEKTORFORUM FOR OPERATIONEL ROBUSTHED

Årsberetning 2020

Corona har i 2020 præget samtalen både i det offentlige rum, på arbejdspladsen og hjemme ved spisebordet – og har krævet fokus hos myndigheder, virksomheder og hos den enkelte. Derved har corona naturligt nok også taget fokus fra andre vigtige dagsordener – herunder bl.a. cybersikkerhed. Inden udbruddet af corona var cyberangreb en af de største bekymringer for stabiliteten i den finansielle sektor, og det er det fortsat. Under coronapandemien er der, jf. Center for Cybersikkerhed, bl.a. blevet sendt flere phisning-mails til danske myndigheder og virksomheder end normalt. Derfor er det vigtigt – til trods for de nuværende udfordringer med coronavirus – fortsat at holde skarpt fokus på de centrale risici i sektoren.

Medlemmerne af Finansielt Sektorforum for Operationel Robusthed, FSOR, har i 2020 formået både at have fokus på at håndtere den særlige situation under udbruddet af coronavirus og samtidig drive dagsordenen om operationel robusthed fremad.

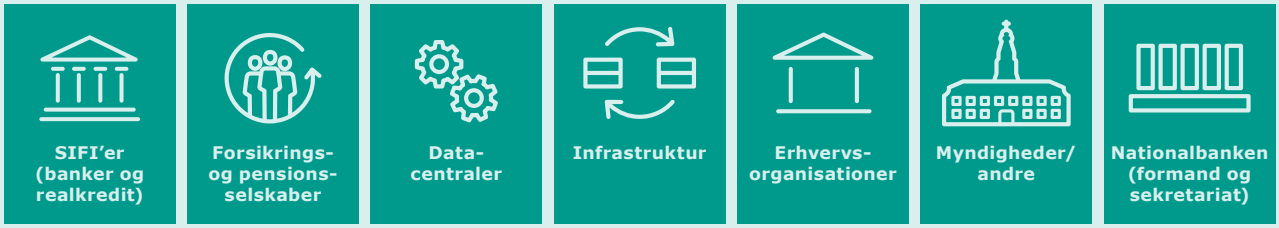
I løbet af 2020 er FSOR's risikoanalyse opdateret to gange, og risikoanalysens metode er blevet publiceret. Med udgangspunkt i analysens resultater er der igangsat nye tiltag, herunder at udforme en fælles baseline for håndtering af cyberrisici, som vil bidrage til at øge modenhedsniveauet på tværs af sektoren. Forsikrings- og pensionsbranchen har også gennemført en risikoanalyse af branchens operationelle risici. Således er den samlede finansielle sektor nu dækket af en risikoanalyse.

I 2020 har Nationalbanken undersøgt cyberrobustheden i den finansielle sektor på baggrund af organisationernes selvevaluering. Undersøgelsen giver de enkelte organisationer mulighed for at benchmarke sig mod resten af sektoren. Endvidere er testningen af forsvarsværn over for cyberangreb fortsat i de enkelte organisationer via trusselsbaserede red team-test inden for rammen af TIBER-DK.

Kriseberedskabet har i 2020 på baggrund af indmeldinger fra sektoren løbende dannet situationsoverblik i forbindelse med udbruddet af coronavirus, og sektorens kritiske funktioner har ikke været påvirket heraf. Samtidig er kriseberedskabsplanen blevet testet to gange, herunder for første gang som en del af en tværgående kriseøvelse orkestreret af Center for Cybersikkerhed og med deltagelse af Danmarks seks kritiske sektorer.

FSOR-medlemmerne er repræsenteret i en række fora, hvor vidensdeling er et centralt element. Det gælder inden for sektoren,

FSOR har i 2020 formået både at håndtere den særlige situation under udbruddet af coronavirus og samtidig drive dagsordenen om operationel robusthed fremad.



Finansiel 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 25 mest centrale deltagere. Medlemmerne i FSOR er:

- De største og systemisk vigtige finansielle institutioner, SIFI'er, og 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.

hvor NFCERT spiller en central rolle i forhold til vidensdeling om hændelser og trusselsvurderinger. Det gælder også mellem de seks kritiske sektorer i Danmark i regi af Center for Cybersikkerhed. Og endelig internationalt, fx i regi af nordisk samarbejde og samarbejde i Den Europæiske Centralbank, ECB.

Udbruddet af coronavirus har ikke påvirket de kritiske funktioner i sektoren

FSOR's medlemmer har med udbruddet af coronavirus i begyndelsen af 2020 haft fokus på at sikre bemanding af de kritiske opgaver, som sektoren løser. Generelt har sektoren ikke været udfordret i forhold til at kunne varetage de samfundskritiske funktioner. På den baggrund har kriseberedskabet heller ikke været aktiveret under pandemien, men situationen er blevet fulgt tæt. Sektoren har indrapporteret det løbende situationsbillede til FSOR Kriseberedskabssekretariatet, som har struktureret information om situationsbilledet på tværs af den finansielle sektor. Denne information er delt med det nationale kriseberedskab, NOST.

Risikoanalysen sætter dagsordenen for de fælles tiltag i FSOR

Sektoren samarbejder om at identificere og adressere systemiske risici på et struktureret grundlag. Centralt for dette samarbejde er udformning af en risikoanalyse, som bidrager til at afdække de operationelle risici, der potentielt kan true stabiliteten i det finansielle system, og som giver et struktureret grundlag for at prioritere tiltag til at reducere disse risici.

Risikoanalysen anvender en række kilder til at identificere de risici, som den finansielle sektor står over for. Det omfatter bl.a. en analytisk afdækning af systemiske afhængigheder og centrale forretningsprocesser, tidligere hændelser, trusselsvurderinger og flere spørgeskemaer.

Nationalbanken har i 2020 offentliggjort risikoanalysens metode på hjemmesiden *(link)*, så andre kan drage fordel af den. Metoden er generisk og kan også anvendes af andre sektorer end den finansielle.

Risikoanalysen opdateres halvårligt. Ved opdateringerne i 2020 er der identificeret syv nye risici, og vurdering af de eksisterende risici er genbesøgt i forhold til sandsynlighed og konsekvens. Samlet set har FSOR ultimo 2020 identificeret 39 operationelle risici, som potentielt kan true finansiel stabilitet.

I løbet af 2020 har forsikrings- og pensionsbranchen også udarbejdet en risikoanalyse ud fra den samme metodiske ramme som resten af finanssektoren. Således er den samlede finansielle sektors operationelle risici nu afdækket via en risikoanalyse.

FSOR har identificeret 39 risici, som potentielt kan true finansiel stabilitet og arbejder i fællesskab på at mitigere de centrale risici.

VP Securities, Finans Danmark, e-nettet og Nationalbanken indgår i et tæt samarbejde om at identificere og håndtere risici og hændelser som følge af gensidige afhængigheder mellem systemerne VP-afviklingerne, detailbetalingssystemerne og Kronos2.

Baseline bliver et stærkt redskab til at forbedre cyberrobustheden

På baggrund af risikoanalysens konklusioner påbegyndte FSOR i 2020 at udarbejde en fælles baseline for arbejdet med cyberrobusthed på tværs af sektorens kritiske aktører og leverandører.

Baseline skal – med udgangspunkt i gældende lov og allerede kendte internationale standarder – formulere konkrete og målbare anbefalinger til cyberrobusthed på forskellige områder, fx databeskyttelse eller governance. Målet er at udvikle 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.

I 2020 begyndte arbejdet med *baseline*. Det er besluttet, hvilke områder *baseline* skal dække, og den fremadrettede arbejdsproces er blevet fastlagt. Endvidere er der ansat en ekstern konsulent til at facilitere processen og bidrage til opsætning af platformen, ligesom en fordelingsnøgle til finansiering af omkostningerne er blevet godkendt af FSOR. Det er forventningen, at de første dele af *baseline* er klar omkring sommeren 2021.

Undersøgelse af cyberrobustheden viser fremgang siden 2018, men der er stadig arbejde forude

Nationalbanken gennemførte i sommeren 2020 den tredje spørgeskemaundersøgelse af cyberrobustheden hos de operationelle deltagere i FSOR. Tilsvarende undersøgelse blev gennemført i 2016 og 2018. Dog løftes barren i undersøgelserne i takt med den løbende udvikling i risici. Som noget nyt deltog også en gruppe af forsikrings- og pensionsselskaber og flere centrale leverandører.

Undersøgelsen skaber på baggrund af organisationernes selvevaluering et samlet overblik over cybermodenheden i den finansielle sektor. Undersøgelsen for 2020 indikerer væsentlig fremgang i forhold til undersøgelserne i 2016 og 2018, men peger samtidig også på konkrete områder, hvor niveauet stadig kan løftes både individuelt og i fælleskab. De overordnede resultater er drøftet på FSOR-mødet

i november med henblik på at identificere, hvad der skal arbejdes med i fællesskab. Nationalbanken har endvidere givet individuelle tilbagemeldinger til brug for de enkelte FSOR-medlemmers arbejde med at øge cyberrobustheden i egen organisation.

TIBER-DK tester sektorens forsvarsværn for at opnå læring og styrke cyberrobustheden

TIBER-DK blev formelt etableret i december 2018 som et af de allerførste TIBER-programmer i Europa og har i 2020 fulgt den fastlagte testplan.

I en TIBER-test simuleres de avancerede angreb fra organiserede kriminelle cybergrupper eller statssponsorerede grupper i live produktionsmiljøer. Nationalbanken understøtter disse test og faciliterer vidensdeling blandt deltagerne i TIBER-DK.

TIBER-test har til formål at gøre sektoren bedre til at identificere og stoppe angreb. Testen tager udgangspunkt i de taktikker, teknikker og procedurer, som anses for de mest realistiske på baggrund af efterretningsbaseret trusselsinformation.

Der udarbejdes efter hver test en testrapport og en plan for udbedring af de fundne svagheder og sårbarheder hos de enkelte deltagere. Der afholdes også workshops for at forankre den værdifulde læring og resultaterne fra testen.

Erfaringen er, at TIBER gør en forskel og giver værdi, fordi testen skaber opmærksomhed på alle niveauer i den testede organisation, også på højt ledelsesniveau. Desuden igangsætter de resultater og den læring, der kommer fra testene, konkrete forbedringer, der øger cyberrobustheden, fx når sikkerheden i systemerne styrkes, eller processer forbedres.

Det er en stor styrke i TIBER, at læring ligger i forsvaret mod ”rigtige” trusler og de angrebsmetoder, som er mest realistiske i forhold til egen forretning og samfundskritiske funktioner. Hvert år udarbejdes en trusselslandskabsrapport til brug for TIBER-testene. I år er rapporten udarbejdet af NFCERT med involvering af relevante parter.

Kriseberedskabet overvåger corona-situationen og sikrer koordinering på tværs af sektoren i tilfælde af en krise

Til trods for de gode forebyggende tiltag, så kan operationelle hændelser forekomme. Derfor er det centralt at have udarbejdet en detaljeret plan til at sikre en koordineret indsats på tværs af den finansielle sektor i tilfælde af en systemisk krise.

FSOR har i forbindelse med oprettelsen i 2016 etableret et kriseberedskab på sektorniveau, som supplerer medlemmernes egne kriseplaner og det nationale kriseberedskab, NOST.

Kriseberedskabet testes to gange om året for at sikre, at kriseplanen fungerer i praksis i tilfælde af en alvorlig hændelse i sektoren. Den 26. august blev der afholdt en kriseøvelse. Under øvelsen lykkedes det at håndtere flere krisescenarier på én gang, skifte fra partiel til fuld aktivering samt håndtere udskiftning i kriseledelsen. Den 19. november blev koordineringen på tværs af de seks samfundskritiske sektorer testet i forbindelse med et fiktivt phishing-angreb. Center for cybersikkerhed orkestrerede øvelsen, og det var første gang, at en test på tværs af de kritiske sektorer blev afholdt. Øvelserne bekræfter, at den finansielle sektors kriseplan er et velfungerende redskab til at strukturere og håndtere en krisesituation, og der blev skabt vigtig viden i forhold til at forbedre den operationelle koordinering på tværs af de seks kritiske sektorer. Ved årets øvelser blev anvendt virtuel krisestyring, og anvendelsen af den virtuelle platform som kommunikationsredskab er i løbet af året blevet væsentligt modnet.

Koordinering i forbindelse med en hændelse på tværs af de seks kritiske sektorer blev i 2020 testet for første gang.

I 2020 har bl.a. corona-situationen bidraget til læringspunkter, der har givet anledning til opdateringer til FSOR-kriseberedskabsplanen, som nu foreligger i version 3.6. Der er endvidere afholdt en workshop i Vejle den 5. marts og et webinar den 27. oktober med det formål at vedligeholde FSOR-medlemmernes viden om kriseberedskabet.

Sekretariatet har udarbejdet en opdateret plan for FSOR-kriseberedskabet 2021-2023, der fokuserer på modning og tværsektorielt samarbejde.

FSOR samarbejder med andre kritiske sektorer i danmark

Som en del af den nationale cyberstrategi er der udpeget seks kritiske sektorer i Danmark. For hver af disse sektorer er der etableret

en decentral enhed for cyber- og informationssikkerhed, DCIS. Finanstilsynet varetager funktionen som DCIS for finanssektoren.

Nationalbanken, som varetager formandskab og sekretariat for FSOR, deltager sammen med Finanstilsynet i DCIS-forum. Det er et netværk med deltagelse af de seks kritiske sektorer, og som faciliteres af Center for Cybersikkerhed. DCIS-forum har til formål at øge videndelingen, styrke koordinationen på tværs af de samfundskritiske sektorer samt igangsætte og gennemføre fælles indsatser. Den fælles kriseøvelse i november udspringer bl.a. herfra. Endvidere er fokus bl.a. på videndeling om varsler, hændelseshåndtering og beredskab. DCIS-forum har nedsat en arbejdsgruppe, som arbejder for effektivt at dele viden om trusler på tværs af sektorer. I dette arbejde deltager NFCERT fra finanssektoren.

CIISI-EU har etableret fælles platform til vidensdeling

ECB besluttede i 2017 at etablere et offentlig-privat samarbejde mellem de vigtigste europæiske finansielle aktører kaldet Euro Cyber Resilience Board, ECRB. ECRB vedtog i begyndelsen af 2020 et såkaldt "Cyber Information and Intelligence Sharing Initiative", CIISI-EU, hvor der er etableret en fælles platform for videndeling på både strategisk, taktisk og operationelt niveau mellem deltagerne i EU. Nationalbanken er formelt medlem af CIISI-EU og vil se på, hvordan trusselsinformation kan udveksles til gavn for flere.

Tak til FSOR-kredsen

Stor tak til FSOR-kredsen for et godt samarbejde og for at bidrage til at forbedre cyberrobustheden på tværs af sektoren. Også tak til deltagerne i arbejdsgrupperne for deres store indsats med at frembringe de konkrete resultater til gavn for den samlede finansielle sektor.

Karsten Biltoft
Formand for FSOR, chef for Finansiel Stabilitet
19. januar 2021