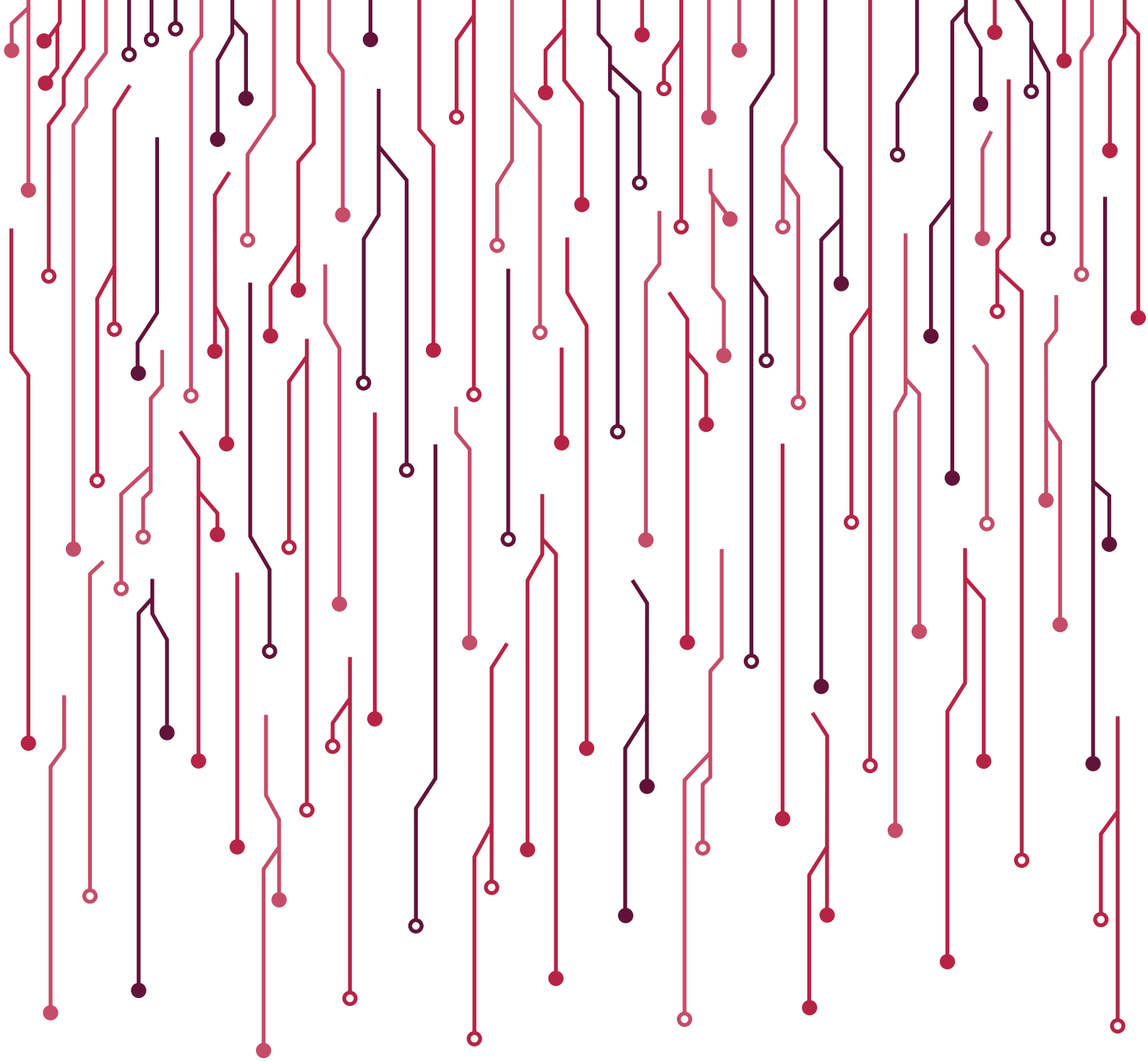

FINANSTILSYNET

Strategi for den finansielle sektors

cyber- og informationssikkerhed
2022 - 2025

Sammen om at sikre forbindelsen

Indholdsfortegnelse

Indledning

Cyberangreb mod den danske finansielle sektor kan have alvorlige konsekvenser for Danmark. Længerevarende IT-nedbrud i sektorens samfundsvigtige funktioner kan true den finansielle stabilitet og tilliden til den finansielle sektor. For at opretholde robustheden i den finansielle sektor skal den samfundskritiske IT-infrastruktur være tilgængelig, troværdig og stabil, så virksomheder og borgere kan have berettiget tillid til det finansielle system.

IT-relaterede risici har gennem flere år toppet listen over risici, som de finansielle virksomheder er mest bekymrede for[1]. Danske finansielle virksomheder anser dermed trusler mod cybersikkerheden for at udgøre den største risiko for den finansielle stabilitet i Danmark. Det understøttes af, at Danmark er et af de mest digitaliserede lande på betalingsområdet, hvor langt de fleste betalinger foregår digitalt[2]. Samtidig er trusler mod cybersikkerheden den risiko, som virksomhederne finder mest udfordrende at håndtere[3].

Ifølge trusselsvurderingen fra Center for Cybersikkerhed (CFCS) står den danske finanssektor overfor et meget højt trusselsniveau fra cyberkriminalitet, der kan forstyrre tilgængeligheden af sektorens ydelser. Samtidig er truslen fra cyberspionage udført af statsstøttede hackere med både politiske og økonomiske motiver høj. Viden fra den danske finansielle sektor er værdifuld for fremmede stater, der kan udnytte denne viden til at træffe politiske og strategiske beslutninger, fremme staters økonomi eller styrke deres nationale virksomheder.

I lyset af trusselsniveauet og den finansielle sektors samfundsvigtige rolle sætter strategien fokus på fælles indsatser, der kan bidrage til at øge robustheden af sektorens samfundsvigtige funktioner.

Regeringen har lanceret en ny national strategi for cyber- og informationssikkerhed for perioden 2022-2024. Den nationale strategi sætter bl.a. fokus på sikkerheden for kritisk IT-infrastruktur, der understøtter samfundsvigtige funktioner og derved er afgørende for at opretholde samfundets generelle funktionsdygtighed. Det er et mål, at de samfundsvigtige funktioner er robust beskyttede. Det betyder, at disse funktioner skal kunne opretholdes i en krisesituation, hvor kritisk IT-infrastruktur sættes ud af kraft i kortere eller længere tid. Det er derfor vigtigt, at Danmark har et højt sikkerhedsniveau for kritisk IT-infrastruktur og en evne til med kort varsel at agere i tilfælde af alvorlige cyberhændelser.

Strategiens overordnede mål

Den finansielle sektor har en robust beskyttelse af den kritiske IT-infrastruktur, der understøtter sektorens samfundsvigtige funktioner, samt evnen til at opretholde drift i krisesituationer og sikre effektiv genopretning.

1 Finanstilsynet "Systemisk risiko - spørgeskemaundersøgelse" 2022
2 Danmarks Nationalbank "Danmark er blandt de mest digitaliserede lande på betalingsområdet" 2022
3 Finanstilsynet "Systemisk risiko - spørgeskemaundersøgelse" 2018

Den finansielle sektor er udpeget som en samfundskritisk sektor og er dermed omfattet af målsætningen i "National strategi for cyber- og informationssikkerhed 2022-2024". Det indebærer, at sektoren skal have en strategi for cyber- og informationssikkerhed, som kan være med til at understøtte den fælles indsats for at øge robustheden af de samfundsvigtige funktioner.

Denne strategi bygger desuden videre på det eksisterende samarbejde i sektoren og på den første strategi for den finansielle sektors cyber- og informationssikkerhed (2019-2021). Med den første strategi blev den Decentrale enhed for Cyber- og Informationssikkerhed i den finansielle sektor (DCIS Finans) etableret i Finanstilsynet. For at understøtte strategiens initiativer blev der etableret et samarbejde mellem DCIS Finans og eksisterende kapaciteter i sektoren, herunder Nationalbanken, Finansielt Sektorforum for Operationel Robusthed (FSOR) og Nordic Financiel CERT (NFCERT). Den første strategi indeholdt bl.a. initiativer om udarbejdelse af risikovurderinger på sektorniveau samt initiativ om udvikling og vedligehold af sektorens kriseberedskab i regi af Nationalbanken og FSOR, som i forvejen havde etableret sådanne indsatser. Derudover indeholdt strategien et initiativ om løbende indsamling og videndeling af operationelle hændelser. Dette initiativ fik NFCERT til opgave at varetage, da NFCERT i forvejen indsamler og deler viden om operationelle hændelser blandt dets medlemmer i den finansielle sektor. Med delstrategien er der blevet taget et væsentligt skridt i retningen af at styrke indsatsen med at forebygge og bekæmpe cyberrisici.

Hvor den første strategi satte rammerne for strategiarbejdet, er nærværende strategi fokuseret på at fortsætte og videreudvikle initiativerne og samarbejdet fra den første strategi.

Samarbejdet omkring strategien

"Strategi for den finansielle sektors cyber- og informationssikkerhed" er en strategi for at fremme robustheden i den finansielle sektors samfundsvigtige funktioner ved at understøtte de tværgående indsatser og knytte dem til indsatser i relation til andre sektorers cyber- og informationssikkerhed og indsatsen på nationalt plan. Den bygger på det grundlæggende princip, at hver enkelt aktør har ansvaret for sin egen cyber- og informationssikkerhed. Det gælder forebyggende sikkerhed såvel som videreførelse af funktioner og genoprettelse efter et eventuelt angreb. De enkelte aktører har også ansvar for at holde sig orienteret om relevant cyber- og informationssikkerhed.

Aktørerne i den finansielle sektor er tæt forbundet via en fælles infrastruktur. Fælles sektorforankrede indsatser kan bidrage til at styrke den samlede sektors beskyttelse af samfundsvigtige funktioner. Strategien skal bidrage til at binde indsatserne sammen og understøtte samarbejdet internt i sektoren såvel som på tværs af samfundsvigtige sektorer på nationalt niveau.

Strategien bygger videre på initiativer og organisering, der er skabt før og under seneste strategiperiode. DCIS Finans har ansvaret for at rapportere strategiens fremdrift til Erhvervsministeriet. Det sker ved løbende at vurdere indsatserne i forhold til målsætningerne.

Centrale operationelle opgaver i henhold til målsætninger og initiativer beskrevet i strategien varetages fortsat

af Nationalbanken, FSOR og NFCERT. Opgaverne løftes under hensyn til både det samfundsmæssige ansvar og de mulige gevinster for de enkelte virksomheder og for den finansielle sektor som helhed. Den samlede strategi knyttes sammen af DCIS Finans, der desuden fungerer som bindeled til de andre samfundsvigtige sektorer og de nationale indsatser sammen med Nationalbanken.

Centrale aktører

Erhvervsministeriet er i henhold til "National strategi for cyber- og informationssikkerhed 2022-2024" ansvarlig for, at der etableres en DCIS og udarbejdes en strategi for den finansielle sektor.

Decentral enhed for Cyber- og Informationssikkerhed i den finansielle sektor (DCIS Finans) er forankret i Finanstilsynet og har bl.a. ansvar for at udforme en strategi og rapportere strategiens fremdrift til Erhvervsministeriet ved løbende at vurdere indsatserne i forhold til målsætningerne. DCIS Finans varetager desuden opgaven med at skabe og formidle overblik over strategiarbejdet.

Finansielt Sektorforum for Operationel Robusthed (FSOR) er et privat-offentligt samarbejdsforum, hvor Nationalbanken varetager sekretariatet og formandspost. Medlemmer af FSOR inkluderer systemisk vigtige finansielle institutter (SIFI'er), forsikring- og pensionsselskaber, fælles datacentraler, Financial Markets Infrastructures (FMI'er[4]), brancheorganisationer, myndigheder og Nationalbanken. I forhold til strategien varetager Nationalbanken og FSOR opgaver på sektorniveau i forbindelse med f.eks. kortlægning, risikovurdering, kriseberedskab og videndeling.

Nordic Financial CERT (NFCERT) er en medlemsorganisation etableret af virksomheder i den finansielle sektor med det formål at gøre virksomhederne i stand til i fællesskab at opdage og reagere på cybertrusler og angreb. NFCERT varetager tilsvarende opgaver i regi af strategien og har desuden en rolle i forhold til situationsbilledet og kriseberedskabet.

Center for Cybersikkerhed (CFCS) er national IT-sikkerhedsmyndighed og nationalt kompetencecenter på cybersikkerhedsområdet og skal bl.a. understøtte arbejdet i de samfundsvigtige sektorer. I forbindelse med strategien spiller CFCS en central rolle, bl.a. i forhold til det nationale samarbejde, trusselsvurderinger samt videndeling og rådgivning.

Finans Danmark og Forsikring & Pension er som brancheorganisationer centrale aktører i forhold til bredt at sikre strategiens forbindelse til den finansielle sektors virksomheder. Brancheorganisationerne indgår i den løbende dialog med DCIS og er en del af forskellige initiativer i strategien.

Finanstilsynet er sektoransvarlig myndighed, der fører tilsyn med de finansielle virksomheder, herunder at lovgivningens krav til IT-sikkerhed er overholdt.

4 FMI'er er de organisationer, der er ansvarlige for de centrale betalings- og afviklingssystemer i infrastrukturen. Betalingsinfrastrukturen er et netværk af forskellige systemer, der muliggør, at borgere, virksomheder og finansielle aktører kan udveksle betalinger og værdipapirhandler med hinanden.

Strategiens opbygning

Strategien er bygget op om syv indsatsområder med hver deres målsætninger, der sætter rammen for arbejdet i den kommende strategiperiode. Indsatsområderne er inddelt i kategorierne *Forstå*, *Forsvar* og *Forbind*:

- *Forstå* handler om at sikre, at finanssektoren har et vidensgrundlag, der kan understøtte prioritering af fælles initiativer, som kan bidrage til en robust beskyttelse af den kritiske IT-infrastruktur.
- *Forsvar* bygger videre på sektorens vidensgrundlag og handler om evnen til at forsvare og opretholde drift i krisesituationer og sikre effektiv genopretning af de samfundsvigtige funktioner.
- *Forbind* er rammesættende for arbejdet med de øvrige indsatsområder, da det interne og eksterne samarbejde er grundlaget for strategien.

En robust beskyttelse af den kritiske IT-infrastruktur indebærer løbende forbedringer, så beskyttelsen modsvarer det aktuelle trusselsniveau. Prioritering af initiativer under hvert indsatsområde i strategien, der skal følge udviklingen i sektoren og i trusselsniveauet, finder dermed kontinuerligt sted.

Målsætning for indsatsområder

FORSTÅ

Kortlægning

Der findes et fælles overblik over sektorens samfundsvigtige funktioner og understøttende IT-infrastruktur samt viden om konsekvenserne ved kompromittering eller nedbrud.

Måling af robusthed

Det undersøges løbende, hvor robust den finansielle sektor er i forhold til at kunne beskytte samfundsvigtige funktioner mod cyberangreb og opretholde driften i en krisesituation.

Risikovurdering

Der udarbejdes løbende fælles vurderinger af de systemiske operationelle risici i den finansielle sektor.

FORSVAR

Trusler og sårbarheder

Der tilvejebringes relevant og opdateret viden om trusler og sårbarheder, som distribueres hurtigt og effektivt til virksomheder i den finansielle sektor.

Situationsbillede

Der kan hurtigt og effektivt etableres et overblik over, hvordan den finansielle sektor er påvirket af udbredte sårbarheder og trusler, hændelser eller andre aktuelle situationer.

Sektorberedskab

Den finansielle sektor har et fælles beredskab, der kan koordinere indsatsen mellem relevante aktører internt og eksternt i tilfælde af en større hændelse.

FORBIND

Samarbejde og synergi

Den finansielle sektor har et aktivt internt og eksternt samarbejde om sikkerhedsopbygning, som sikrer, at relevante risici adresseres, og mulige synergier udnyttes.

FORSTÅ

Kortlægning

Der findes et fælles overblik over sektorens samfundsvigtige funktioner og understøttende IT-infrastruktur samt viden om konsekvenserne ved kompromittering eller nedbrud.

Måling af robusthed

Det undersøges løbende, hvor robust den finansielle sektor er i forhold til at kunne beskytte samfundsvigtige funktioner mod cyberangreb og opretholde driften i en krisesituation.

Risikovurdering

Der udarbejdes løbende fælles vurderinger af de systemiske operationelle risici i den finansielle sektor.

Forstå

Kortlægning

Der findes et fælles overblik over sektorens samfundsvigtige funktioner og understøttende IT-infrastruktur samt viden om konsekvenserne ved kompromittering eller nedbrud.

Med strategiens overordnede målsætning om en robust beskyttelse af den finansielle sektors samfundsvigtige funktioner er det nødvendigt med en kortlægning af disse og af den IT-infrastruktur, der understøtter dem. Det er samtidig vigtigt at kende konsekvenserne, hvis kritisk IT-infrastruktur kompromitteres, så der kan udarbejdes beredskabsplaner for håndteringen af disse. Kortlægningen udgør et fælles fundament og en fælles reference, når samarbejdet om at øge cyberrobustheden finder sted. Det kræver, at det grundlæggende overblik er etableret og vedligeholdt, og at det er bredt anerkendt og benyttet.

Overblikket danner udgangspunkt for flere af strategiens øvrige indsatsområder, som f.eks. risikovurderingen og sektorberedskabet, og kan hjælpe med at prioritere indsatserne. På samme måde er overblikket afgørende for samarbejdet med de øvrige samfundsvigtige sektorer og for de nationale og internationale indsatser, hvor fælles definitioner og tilgange på tværs af sektorerne er nødvendige.

Etablering og vedligeholdelse af et fælles overblik varetages i dag af Nationalbanken og FSOR. Den eksisterende risikovurdering for den finansielle sektor kortlægger sektorens forretningsaktiviteter. For de forretningsaktiviteter, hvor nedbrud kan true den finansielle stabilitet på under en uge, kortlægges desuden de underliggende processer og systemer og deres indbyrdes afhængigheder. Som en del af FSOR's årshjul indgår genbesøg af kortlægningen. Denne bruges desuden i FSOR's kriseberedskab. Nationalbanken, FSOR og Risikoforum for Gensidige Afhængigheder (RGA) mellem Financial Market Infrastructures (FMI'erne) har også igangsat yderligere kortlægningsaktiviteter[5].

Finanstilsynet lancerer medio 2022 et nyt program om styrket operationel robusthed, som ved hjælp af cyberstresstest skal analysere konsekvenserne af et omfattende IT-nedbrud. Formålet med programmet er at kortlægge, hvad der vil ske i tilfælde af et større IT-nedbrud i den finansielle sektor. Det gælder både i den enkelte virksomhed og på sektorniveau. Med udgangspunkt i resultaterne vil Finanstilsynet understøtte, at de enkelte virksomheder iværksætter passende initiativer til at forebygge og reducere konsekvenserne af et nedbrud. Eventuelle opfølgende initiativer på sektorniveau koordineres med Nationalbanken og det øvrige arbejde i FSOR.

I den kommende strategiperiode vil fokus være på at vedligeholde og yderligere udbygge den eksisterende kortlægning som fundament for sektorens fælles indsats på området for cybersikkerhed og for samarbejdet med eksterne interessenter.

5 I RGA deltager Nationalbanken (interbankbetalinger), Euronext Securities Copenhagen (værdipapirhandler), Finans Danmark (detailbetalinger) og e-nettet (kommunikationsnetværk).

På baggrund af ovenstående beskrivelse tager arbejdet udgangspunkt i følgende aktiviteter:

- **Den eksisterende kortlægning af sektorens forretningsaktiviteter og underliggende processer og systemer genbesøges årligt i forbindelse med udarbejdelse af risikovurdering på sektorniveau.**
- **Der arbejdes med kortlægning af den finansielle sektors kritiske data med henblik på yderligere beskyttelse heraf.**
- **Den finansielle sektors kortlægning sammenholdes med nationale målsætninger og kortlægningsaktiviteter.**
- **Finanstilsynet lancerer et program om styrket operationel robusthed, som ved hjælp af cyberstresstest skal analysere konsekvenserne af et omfattende IT-nedbrud.**
- **Kortlægningen af samfundsvigtige funktioner og understøttende infrastruktur samt gensidige afhængigheder opdateres på baggrund af ovenstående aktiviteter.**

Forstå

Måling af robusthed

Det undersøges løbende, hvor robust den finansielle sektor er i forhold til at kunne beskytte samfundsvigtige funktioner mod cyberangreb og opretholde driften i en krisesituation.

Viden om den aktuelle grad af robusthed skal danne udgangspunkt for at styrke den finansielle sektors cybersikkerhed. På baggrund af denne viden kan man identificere områder med behov for forbedring, og hvor sektoren i fællesskab bør sætte ind for at øge robustheden af de samfundsvigtige funktioner.

Allerede i dag gennemføres en række forskellige undersøgelser af robustheden, som med hver deres formål og metode bl.a. kan bidrage til den fælles risikovurdering for sektoren og danne grundlag for nye initiativer.

Finanstilsynet fører tilsyn med, at de finansielle virksomheder overholder lovgivningens krav til IT-sikkerhed. Det sker både gennem IT-undersøgelser og ved løbende overvågning. De generelle observationer fra undersøgelserne indgår i forskellige sammenhænge, bl.a. i Finanstilsynets samlede risikobillede for sektoren. Tilsvarende overvåger Nationalbanken, at de centrale systemer og løsninger i den danske betalingsinfrastruktur efterlever internationale standarder. Nationalbanken udgiver vurderingsrapporter og årlige overvågningsrapporter.

Siden begyndelsen af 2019 har Nationalbanken koordineret test af cybersikkerheden i den finansielle sektor under et program kaldet TIBER-DK (Threat Intelligence Based Ethical Red-teaming)[6]. En særlig enhed i Nationalbanken understøtter disse test og faciliterer videndeling blandt deltagere i programmet. TIBER-testene simulerer 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 og at øge cyberrobustheden ved at adressere svaghederne.

Nationalbanken har desuden tre gange siden 2016 ved hjælp af en spørgeskemaundersøgelse undersøgt cybersikkerheden hos store banker og realkreditinstitutter, infrastrukturselskaber, som leverer kritiske services til disse, og fællesejede datacentraler. Undersøgelsen, der er baseret på virksomhedernes selvevaluering, kan hjælpe til at identificere områder, hvor niveauet i sektoren kan hæves via fælles indsatser. Der er planlagt en ny spørgeskemaundersøgelse i strategiperioden.

I 2022 har FSOR lanceret et baselineværktøj, der er en IT-platform, hvor de finansielle virksomheder og leverandører har mulighed for at undersøge og evaluere deres eget sikkerhedsniveau i forhold til gældende lov og kendte internationale standarder. Derigennem kan virksomhederne få konkrete tiltag, som de kan iværksætte for at opnå et ønsket sikkerhedsniveau. Baselineværktøjet bidrager desuden til at udvikle et fælles sprog om IT-sikkerhed i sektoren.

Der skal i den kommende strategiperiode arbejdes videre med at måle den finansielle sektors robusthed i forhold til at kunne beskytte samfundsvigtige funktioner mod cyberangreb og opretholde driften i en krisesituation.

6 Danmarks Nationalbank "Kort om TIBER-DK" 2021

På baggrund af ovenstående beskrivelse tager arbejdet udgangspunkt i følgende aktiviteter:

- **Der ses på muligheden for og arbejdes for, at resultaterne af IT-tilsyn og overvågning systematisk inddrages i sektorens risikovurdering.**
- **Det etablerede TIBER-DK-program fortsættes, og de overordnede erfaringer inddrages bl.a. i sektorens risikovurdering.**
- **Der gennemføres en ny spørgeskemaundersøgelse om cybersikkerhed i strategiperioden.**
- **Brugen af baselineværktøjet drøftes, og der tages stilling til evt. behov for yderligere udvikling.**

Forstå

Risikovurdering

Der udarbejdes løbende fælles vurderinger af de systemiske operationelle risici i den finansielle sektor.

Det er afgørende at kende de risici, der kan påvirke driften, for at kunne øge robustheden af sektorens samfundsvigtige funktioner. På baggrund af en række solide og bredt dækkende kilder skal landskabet af risici kortlægges og vurderes i forhold til sandsynlighed og konsekvens. Det skal danne grundlag for, at sektoren i fællesskab prioriterer mulige sektorinitiativer indenfor cyber- og informationssikkerhed og igangsætter tiltag, der kan nedbringe de alvorligste risici.

Enhver finansiel institution er ansvarlig for risikostyring i forhold til deres egen operationelle robusthed og IT-sikkerhed. Sektorens fælles risikovurdering erstatter ikke de enkelte aktørers egen risikostyring, men skal ses som et supplement og input til denne.

Nationalbanken og FSOR udarbejder i dag en risikoanalyse for at give et fælles overblik over operationelle risici, der kan ramme på tværs af sektoren og potentielt true den finansielle stabilitet. Rammerne for arbejdet er beskrevet i den publicerede metodehåndbog[7]. Kilderne til risikovurderingen inkluderer bl.a. aktiviteter beskrevet under de øvrige indsatsområder, eksempelvis kortlægning af systemer og data, måling af robusthed samt overblik over trusler og sårbarheder. En arbejdsgruppe under FSOR opdaterer vurderingen to gange årligt. På baggrund af analysen udvælger FSOR-kredsen tiltag med fokus på, hvor den finansielle sektor med fordel kan koordinere og samarbejde for at øge den operationelle robusthed. I de seneste år har FSOR bl.a. arbejdet med udvikling indenfor databeskyttelse og recovery.

I 2020 havde brancheorganisationen Forsikring & Pension ansvar for at udarbejde en tilsvarende risikovurdering med fokus på forsikrings- og pensionsbranchen.

Der skal i den kommende strategiperiode arbejdes med at videreføre og videreudvikle sektorens fælles risikovurderinger. Disse kan danne baggrund for igangsættelse af fælles initiativer til at reducere alvorlige risici.

På baggrund af ovenstående beskrivelse tager arbejdet udgangspunkt i følgende aktiviteter:

- **FSOR's risikovurdering opdateres halvårligt, og der tages stilling til igangsættelse af fælles tiltag til at øge cyberrobustheden.**
- **Risikovurderingen for forsikrings- og pensionsområdet genbesøges, og der tages stilling til behovet for yderligere tiltag.**

7 FSOR "Metodehåndbog for FSOR's risikoanalyse" 2020

FORSVAR

Trusler og sårbarheder

Der tilvejebringes relevant og opdateret viden om trusler og sårbarheder, som distribueres hurtigt og effektivt til virksomheder i den finansielle sektor.

Situationsbillede

Der kan hurtigt og effektivt etableres et overblik over, hvordan den finansielle sektor er påvirket af udbredte sårbarheder og trusler, hændelser eller andre aktuelle situationer.

Sektorberedskab

Den finansielle sektor har et fælles beredskab, der kan koordinere indsatsen mellem relevante aktører internt og eksternt i tilfælde af en større hændelse.

Forsvar

Trusler og sårbarheder

Der tilvejebringes relevant og opdateret viden om trusler og sårbarheder, som distribueres hurtigt og effektivt til virksomheder i den finansielle sektor.

Sårbarheder i IT-systemer findes i mange tilfælde på tværs af flere aktører. Samtidig kan cyberkriminelle rette den samme type angreb mod flere aktører indenfor kort tid. Hurtig og effektiv deling af viden om sårbarheder, trusler og angreb kan derfor være afgørende for at undgå eller begrænse effekten af cyberangreb mest muligt.

Med henblik på at styrke robustheden af den finansielle sektors cybersikkerhed skal relevant og opdateret viden om trusler og sårbarheder kunne distribueres hurtigt og effektivt i sektoren. Sektorens aktører skal kunne bruge denne viden i det operationelle og strategiske arbejde med IT-sikkerhed.

Distributionsformen skal tage højde for forskelle i virksomhedernes behov, modenhed og kapacitet til at modtage og bruge viden om trusler og sårbarheder. Den finansielle sektors landskab har stor variation i virksomhedernes størrelse og tilknytning til fælles IT-leverandører, hvilket indebærer et differentieret informationsbehov.

NFCERT varetager i dag en væsentlig rolle i den operationelle videndeling i den finansielle sektor. De faciliterer et aktivt lukket delingsfællesskab mellem sektorens virksomheder og samarbejder med en række myndigheder og internationale organisationer. NFCERT udarbejder også situations- og trusselsvurderinger og skaffer detaljeret trusselsefterretning, som medlemmerne kan bruge til at opdage og standse cyberangreb. På samme måde deler CFCS løbende varsler om sårbarheder og trusler og udarbejder både sektorspecifikke og nationale trusselvurderinger. Varslerne distribueres til den finansielle sektor via NFCERT.

I sidste strategiperiode valgte de seks samfundskritiske sektorer at oprette en tværsektoriel informationsplatform, MISP (Malware Information Sharing Platform), med henblik på at arbejde for mere effektiv og operationel deling af viden om trusler og sårbarheder på tværs af forskellige sektorer. NFCERT deltager i MISP-samarbejdet på vegne af finanssektoren og deler deres viden herfra med de øvrige samfundskritiske sektorer. Relevant viden til finanssektoren videredistribueres gennem NFCERT's egne platforme.

Der skal i den kommende strategiperiode arbejdes for, at sektoren hurtigt og effektivt modtager opdateret viden om relevante trusler og sårbarheder, samtidig med at samarbejdet med de andre samfundskritiske sektorer styrkes.

På baggrund af ovenstående beskrivelse tager arbejdet udgangspunkt i følgende aktiviteter:

- **Den finansielle sektors virksomheder deltager aktivt i fællesskaber, hvor de deler relevant viden om trusler og sårbarheder.**
- **Tilgængelig viden om trusler og sårbarheder distribueres fortsat til sektorens virksomheder.**
- **Der udarbejdes løbende samlede trusselsvurderinger for den finansielle sektor.**
- **Den finansielle sektor deltager fortsat i den operationelle videndeling med de andre samfundsvigtige sektorer.**

Forsvar

Situationsbillede

Der kan hurtigt og effektivt etableres et overblik over, hvordan den finansielle sektor er påvirket af udbredte sårbarheder og trusler, hændelser eller andre aktuelle situationer.

For at Danmarks samfundsvigtige funktioner bedst muligt skal kunne forsvares mod aktuelle trusler, kan det være nødvendigt med et hurtigt og effektivt overblik over, hvordan de samfundsvigtige sektorer – herunder den finansielle sektor – er påvirket af en given hændelse eller trussel. Billedet af den aktuelle situation skal gøre det muligt at handle hurtigt og effektivt på trusler, både hvad angår de enkelte aktører og på sektor- og/eller nationalt niveau.

På baggrund af et situationsbillede skal den finansielle sektor kunne skabe overblik over og fokusere på en konkret trussel og risikoen for, at den materialiserer sig i sektoren. Der er dermed tale om noget andet end det løbende trusselsbillede, idet situationsbilledet undersøger påvirkningen af den finansielle sektor i forbindelse med en specifik trussel. I løbet af den seneste strategiperiode har det eksempelvis været nødvendigt at etablere et hurtigt overblik over, hvordan den finansielle sektor var påvirket af SolarWinds-angrebet[8]. Det kan også være nødvendigt at følge udviklingen af situationsbilledet over en periode. Det var bl.a. relevant i forbindelse med nedlukningen af Danmark under COVID-19-krisen og gør sig nu gældende i forbindelse med Ruslands invasion af Ukraine.

Finanssektoren har flere aktører, der hurtigt og effektiv har mulighed for at skabe overblik i situationer med øget trusselsniveau. NFCERT overvåger løbende situationsbilledet med input fra både medlemmer og samarbejdspartnere og kan dermed samle og dele information om en aktuel situation. På samme måde kan FSOR-kriseberedskab igangsætte løbende overvågning, hvor beredskabsmedlemmer melder ind om udviklingen i deres virksomheder.

CFCS er i gang med at implementere et omfattende sensornetværk, hvorfra der kan trækkes opdateret information om, hvad der rammer de tilkoblede virksomheder. Flere virksomheder i den finansielle sektor er enten i dialog med CFCS om opkobling til sensornetværket eller er allerede koblet på. Sensornetværket dækker på tværs af statslige myndigheder og virksomheder i de samfundskritiske sektorer og kan dermed bidrage til et nationalt situationsbillede.

Der skal i den kommende strategiperiode arbejdes for mere systematisk og effektivt at kunne etablere et dækkende overblik over, hvordan den finansielle sektor er påvirket af udbredte sårbarheder, trusler og hændelser i aktuelle situationer.

8 Center for Cybersikkerhed "SolarWinds: Statsstøttet globalt software supply chain-angreb" 2021

På baggrund af ovenstående beskrivelse tager arbejdet udgangspunkt i følgende aktiviteter:

- **Behovet for og kravene til et situationsbillede afdækkes.**
- **Det undersøges, hvilke kilder og nuværende aktiviteter der er relevante for etableringen af et situationsbillede.**
- **Der arbejdes for, at det rette grundlag for etableringen af et situationsbillede er til stede, og at der er klarhed over roller og ansvar i forbindelse med etablering og kommunikation.**

Forsvar

Sektorberedskab

Den finansielle sektor har et fælles beredskab, der kan koordinere indsatsen mellem relevante aktører internt og eksternt i tilfælde af en større hændelse.

I tilfælde af en større hændelse, som kan forstyrre driften af kritisk IT-infrastruktur og dermed påvirke leverancen af samfundsvigtige funktioner, er det afgørende at begrænse konsekvenserne og sikre hurtig genopretning. Da aktørerne i flere af de samfundsvigtige sektorer, herunder den finansielle sektor, er tæt forbundet af fælles infrastruktur, er det vigtigt at koordinere indsatsen, dels for at undgå at hændelsen og dens konsekvenser breder sig, dels for at støtte hinanden med at løse udfordringerne. Der skal derfor være et tværgående sektorberedskab, som i tilfælde af en krise kan koordinere indsatsen mellem relevante aktører.

Den tværgående indsats afhænger af de enkelte aktørers aktive deltagelse. Det er derfor afgørende, at det lokale beredskab hos hver enkelt aktør spiller sammen med sektorberedskabet, og at aktørerne sikrer det rette niveau af involvering i sektorberedskabet. De berørte aktører skal varetage selve håndteringen af krisen, og den enkelte virksomhed har fortsat ansvar for eget beredskab – også under en alvorlig hændelse eller krise.

Sektorberedskabet skal både koordinere indsatsen internt i den berørte sektor og med andre relevante aktører udenfor sektoren. Ved aktivering af sektorberedskabet oprettes kontakt til CFCS. I tilfælde af tværsektorielle hændelser skal beredskabet kunne indgå i dialog med andre implicerede sektorer og Den Nationale Operative Stab (NOST).

Nationalbanken og FSOR varetager i dag den finansielle sektors fælles kriseberedskab og har udviklet og testet FSOR-kriseberedskabsplanen for de dele af sektoren, som har ansvaret for samfundskritiske systemer og infrastruktur, hvor manglende tilgængelighed eller brud på integriteten på kort sigt kan påvirke den finansielle stabilitet. De enkelte aktører, som indgår i dette beredskab, bevarer fortsat ansvaret for egne systemer og data. Sektorberedskabet skal løbende tilpasses det aktuelle trusselsbillede. FSOR gennemfører to årlige test af sektorberedskabet, en partiel test i første halvdel af året og en fuld test i anden halvdel. Sektorberedskabet skal desuden fortsat indgå i tværsektorielle og nationale beredskabsaktiviteter, der skal forbedre den tværgående koordinering på nationalt niveau. De forskellige test bidrager til at sikre, at sektorberedskabet løbende forbedres.

Der skal i den kommende strategiperiode fortsat arbejdes med at opdatere og forbedre FSOR-kriseberedskabsplanen og med at sikre, at den understøttes af de enkelte aktørers lokale beredskabsplaner. Endeligt skal FSOR-kriseberedskabsplanen integreres med den nationale indsats.

På baggrund af ovenstående beskrivelse tager arbejdet udgangspunkt i følgende aktiviteter:

- **FSOR-kriseberedskabsplanen testes to gange årligt og planen opdateres og forbedres på baggrund af de opsamlede erfaringer.**
- **Der arbejdes for, at de enkelte aktørers beredskaber understøtter sektorens fælles kriseberedskab.**
- **FSOR-kriseberedskab deltager i nationale og europæiske beredskabsaktiviteter.**

FORBIND

Samarbejde og synergi

Den finansielle sektor har et aktivt internt og eksternt samarbejde om sikkerhedsopbygning, som sikrer, at relevante risici adresseres, og mulige synergier udnyttes.

Forbind

Samarbejde og synergi

Den finansielle sektor har et aktivt internt og eksternt samarbejde om sikkerhedsopbygning, som sikrer, at relevante risici adresseres, og mulige synergier udnyttes.

Et aktivt samarbejde mellem sektorens aktører såvel som eksternt med aktører i de andre samfundsvigtige sektorer er en forudsætning for at nå målet om robust beskyttelse af den finansielle sektors samfundsvigtige funktioner. Samarbejdet i sektoren skal fokusere på de fælles udfordringer og de løsninger, som aktørerne sammen kan løfte. Samarbejdet bliver dermed rammesættende for flere af strategiens øvrige indsatsområder. Forudsætningen for et velfungerende samarbejde er, at sektoren etablerer netværk og samarbejdsstrukturer og har fælles viden om aktiviteter og muligheder.

Den finansielle sektor har gennem en længere periode arbejdet tæt sammen om cyber- og informationssikkerhed, bl.a. i FSOR. Det er et eksempel på, hvordan sektorens aktører i fællesskab bidrager til at løfte robustheden gennem bl.a. fælles initiativer, der er prioriteret på baggrund af fælles kortlægning og risikovurdering. På samme måde danner NFCERT rammen om et videndelingsfællesskab for den finansielle sektor. Samarbejdet i NFCERT omfatter de nordiske lande og bidrager til videndeling både internationalt og på tværs af sektorer. Yderligere samarbejdsflader og videndelingsfællesskaber er til stede på andre områder af den finansielle sektor. Brancheorganisationerne Forsikring & Pension og Finans Danmark har oprettet hver deres gruppe med fokus på samarbejde om cyber- og informationssikkerhed, og den finansielle sektor er repræsenteret i Cybersikkerhedsrådet og Cyberalliancen.

Med oprettelsen af DCIS'er i de samfundsvigtige sektorer i 2019 opstod formaliserede netværk til at samarbejde og dele viden på tværs af sektorerne. Samarbejdet har som udgangspunkt været faciliteret af CFCS og har engageret flere aktører fra den finansielle sektorer, herunder FSOR og NFCERT.

I den kommende strategiperiode skal både det interne og det eksterne samarbejde fortsættes og styrkes, der hvor det giver værdi for sektorens samlede cyber- og informationssikkerhed at løfte initiativer i et bredere fællesskab. DCIS Finans vil bidrage til at skabe overblik over samarbejdsrelationer, aktiviteter og muligheder i den finansielle sektor, i de andre samfundsvigtige sektorer samt på nationalt og internationalt plan. DCIS Finans skal kommunikere dette overblik, så det kan bidrage til at understøtte synergier i arbejdet med cyber- og informationssikkerhed. Desuden skal fokus være på, hvordan nuværende og kommende lovgivning rammesætter og understøtter IT-sikkerhedsarbejdet. I de kommende år forventes bl.a. EU-lovgivningsinitiativerne DORA og NIS at påvirke dette arbejde.

Den finansielle sektor skal desuden bidrage til og drage nytte af initiativerne fra den nye nationale strategi for cyber- og informationssikkerhed. Det gælder f.eks. initiativer indenfor awareness og uddannelse, hvor aktører på tværs af samfundsvigtige sektorer og offentlige myndigheder med fordel kan samarbejde.

Der skal i den kommende strategiperiode arbejdes med at understøtte internt og eksternt samarbejde om cyber- og informationssikkerhed og med at udnytte synergier ved at understøtte og udvikle relevante samarbejdsflader.

På baggrund af ovenstående beskrivelse tager arbejdet udgangspunkt i følgende aktiviteter:

- FSOR skaber rammer for samarbejde mellem den finansielle sektors aktører med henblik på at styrke sektorens operationelle robusthed.
- NFCERT danner rammen for et videndelingsfællesskab i sektoren.
- Der skabes overblik over og kommunikeres omkring relevante indsatser med henblik på at fremme synergi og samarbejde.
- Den finansielle sektor indgår i operationelt og strategisk samarbejde med de andre samfundsvigtige sektorer.
- Der er løbende fokus på nationale og internationale indsatser, som den finansielle sektor kan bidrage til eller drage nytte af.
- Behovet for sikkerhedsgodkendelser af relevante aktører og sikre kommunikationskanaler til klassificeret information vurderes årligt.
- Der er løbende fokus på, hvordan nuværende og kommende lovgivning rammesætter og understøtter IT-sikkerhedsarbejdet.