FINANSTILSYNET

Strategi for den finansielle sektors cyber- og informationssikkerhed 2019 - 2021

FINANSTILSYNET

Indholdsfortegnelse

1. Oversigt over strategiens initiativer

Decentral enhed for cyber- og informationssikkerhed (DCIS) oprettes
DCIS'en forankrer ansvaret og søger gennem samarbejde at samle den eksisterende kapacitet og opbyggede kapabilitet i Finansielt Sektorforum for Operationel Robusthed (FSOR) og Nordic Financial Computer Emergency Response Team (NFCERT).

Sektorberedskabet i FSOR fastholdes og udvikles
FSORs sektorberedskabsplan er en nøglefaktor ved en krise og derfor fastholdes og udvikles planen yderligere og kommunikationsberedskabet styrkes. Sektorberedskabsplanen testes fortsat for hændelser, som kan true finansiel stabilitet, og finanssektoren indgår i nationale og internationale beredskabsøvelser. Tilsvarende styrkes beredskabsplaner for hændelser i forsikrings- og pensionsselskaber også i regi af FSOR.

Sårbarheder og risici skal afdækkes systematisk og løbende
En afgørende forudsætning for at prioritere indsatsen for sektorens cyber- og informationssikkerhed er et løbende opdateret overblik over, hvilken infrastruktur og hvilke tjenester i sektoren som er samfundskritiske, og hvilke sårbarheder og risici der er forbundet hermed. Derfor gennemføres løbende risiko- og sårbarhedsvurdering for hele sektoren. Dermed understøttes også, at væsentlige aktører kortlægger sårbarheder og risici i deres egen cyberrobusthed.

Lovgivningen skal modsvare trusselsniveauet
Lovgivning kan være et væsentligt middel til at sikre, at kravene til IT-sikkerhed er tilstrækkelige i forhold til at imødegå trusselsniveauet. Der foretages derfor en gennemgang og analyse af lovgivningen for at sikre, at denne er tidssvarende i forhold til cyber- og informationssikkerhed. Overvejelserne vil blandt andet tage udgangspunkt i en analyse af kontrollen med væsentlige IT-leverandører.

Viden skal udnyttes til at bekæmpe IT-sikkerhedstrusler effektivt
Indsatsen i forhold til at styrke cyber- og informationssikkerheden skal bygge på et oplyst grundlag. Derfor styrkes indberetningen af hændelser for at forbedre videngrundlaget, og der anvendes spørgeundersøgelser til at få viden om sektorens cybermodenhed. Tilsvarende distribueres viden om trusler, sårbarheder og angreb hurtigt og effektivt i sektoren.

Ansatte og kunder skal rustes til forsvar mod IT-sikkerhedstrusler
Den menneskelige faktor er væsentlig indenfor cyber- og informationssikkerhed. Derfor analyseres, om der er behov for en fælles oplysningsindsats over for finanssektorens kunder. Tilsvarende analyseres, om der er behov for indsats for at sikre relevante kompetencer i sektoren, og om der bør indføres krav om træning af ansatte.

Samarbejde på tværs af sektorer skal styrke cyber- og informationssikkerheden
Cybertrusler er grænseoverskridende, såvel mellem sektorer som lande. Derfor styrkes videndeling blandt andet via aftale mellem Center for Cybersikkerhed (CFCS) og DCIS'en, og eventuelt fortsat indstationering af medarbejdere ved CFCS. Desuden søges samarbejdet med de øvrige samfundskritiske sektorer styrket og gensidige afhængigheder og samarbejdsmuligheder afdækkes.

Strategien evalueres
Strategien evalueres ved udløbet af strategiperioden, således at resultaterne herfra kan indgå i udarbejdelsen af en forventet ny strategi.

2. Indledning

Cyberangreb er dybt skadelige for samfundet. Forebyggelse og bekæmpelse af cyberangreb er derfor et højt prioriteret område for regeringen.

Indsatsen for at forebygge og bekæmpe cyberangreb har derfor gennem de seneste år været et væsentligt fokusområde. Senest offentliggjorde regeringen den 15. maj 2018 *National strategi for cyber- og informationssikkerhed*. Strategien indeholder en række initiativer, der skal øge robustheden i den digitale infrastruktur og styrke den nationale koordinering og samarbejde på området. I tilknytning hertil skal hver enkelt sektor udarbejde sektorspecifikke strategier, der tager udgangspunkt i de særlige forhold, der gør sig gældende i sektorerne.

Derudover vedtog et bredt flertal af Folketinget i maj 2018 lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester. Med loven er der blevet indført krav til operatører af væsentlige tjenester inden for dele af den digitale infrastruktur, operatører på det finansielle område og udbydere af visse digitale tjenester, der tager højde for samfundets afhængighed af sådanne tjenester og afspejler det aktuelle trusselsbillede

Indsatsen for cyber- og informationssikkerhed er en vigtig samfundsopgave for såvel myndigheder som private aktører, og det er et område, som kræver en vedvarende og intensiv indsats. Det skyldes bl.a., at den teknologiske udvikling gør, at truslen er i konstant forandring.

Finanssektoren har en samfundsvigtig rolle i Danmark, jf. boks 1. Vedvarende eller avancerede cyberangreb mod kritiske dele af den danske finanssektors infrastruktur kan give anledning til tab af tillid og i værste fald true den finansielle stabilitet og dermed Danmarks nationaløkonomi. Det er derfor vigtigt, at virksomhederne, infrastrukturen og ydelserne er tilgængelige, troværdige og stabile, så borgere og virksomheder kan bevare den fulde tillid til systemernes integritet.

Boks 1. Den finansielle sektors funktioner

Den finansielle sektor varetager en række samfundskritiske funktioner. Vores formue opbevares i den finansielle sektor. Den finansielle sektor sikrer bl.a., at vi kan betale for varer og tjenesteydelser, at både borgere og virksomheder kan optage lån til at finansiere investeringer, som man ikke har midler til at betale på én gang, og at der kan handles med værdipapirer.

Samfundet kan ikke fungere normalt uden de tjenester, som den finansielle sektor leverer. Det gælder fx, hvis vi ikke kan få udbetalt løn, eller vi ikke kan betale med elektroniske betalingsmidler. Det vil også være kritisk for samfundet og for den enkelte borger, hvis oplysninger om, hvem der ejer indeståender på bankkonti, værdipapirer eller fast ejendom mv. bliver kompromitteret. På sigt kan også tilliden til den finansielle sektor blive påvirket negativt, hvis sektoren ikke kan levere sine tjenester.

Finanssektoren trues i stigende grad af cyberangreb, som skal imødegås. Center for Cybersikkerhed (herefter CFCS) vurderede i 2018, at truslen fra cyberangreb mod finanssektoren er meget høj, og at angrebene bliver stadig mere avancerede og målrettede. Samtidig vurderede de risikoansvarlige i Danmarks største finansielle virksomheder i 2018, at cyberangreb udgør den største risiko i forhold til den finansielle stabilitet.

Den finansielle sektor yder en stor indsats for IT-sikkerhed
Aktørerne i den finansielle sektor yder allerede i dag en stor indsats for at beskytte deres IT-systemer mod cyberangreb mv., og modenheden i sektoren er generelt høj.

I 2016 tog Nationalbanken sammen med den finansielle sektor initiativ til at oprette Finansielt Sektorforum for Operationel Robusthed (FSOR). FSOR har til opgave at:

- Sikre et fælles overblik over operationelle risici, der potentielt kan ramme på tværs af sektoren og potentielt kan true den finansielle stabilitet.
- Beslutte og sikre gennemførelsen af fælles tiltag til at sikre den finansielle sektors robusthed over for store operationelle hændelser, herunder cyberangreb.
- Skabe rammer for samarbejde og videndeling.

FSOR har ydet en meget væsentlig indsats i forhold til at styrke cyberrobustheden i sektoren.

Hertil kommer, at finanssektoren har etableret Nordic Financial CERT (NFCERT), som har en operativ kapacitet i forhold til bl.a. løbende informationsdeling om trusler og bistand til håndtering af hændelser, jf. boks 2.

Boks 2. CERT
CERT står for Computer Emergency Response Team. En CERT rykker ud i tilfælde af IT-sikkerhedsbrud. Derudover har en CERT typisk også til opgave at forebygge IT-sikkerhedsbrud ved at dele oplysninger om trusler, anbefale sikringstiltag mv.

Endelig har brancheorganisationen Forsikring & Pension taget initiativ til at oprette en Arbejdsgruppe for Cyber- og Informationssikkerhed på baggrund af forsikrings- og pensionssektorens behov herfor.

Det er alle sammen vigtige initiativer, som nærværende strategi vil bygge videre på. Et højt niveau af robusthed over for cyberrisici i den finansielle sektor forudsætter, at alle aktører har kendskab til og forståelse for de risici, som de er udsat for, med henblik på at de kan styrke deres individuelle indsats for cyber- og informationssikkerhed i videst muligt omfang, jf. boks 3.

Boks 3. Aktørerne bevarer ansvaret for egen cyber- og informationssikkerhed
Denne strategi handler om sektorindsatsen. Den baserer sig på det grundlæggende princip, at hver enkelt aktør har ansvaret for sin egen cyber- og informationssikkerhed, herunder både forebyggende sikkerhed, og for videreførelse af funktioner og genoprettelse efter et eventuelt angreb. De enkelte aktører har også ansvaret for at holde sig orienteret om cyber- og informationssikkerhed.

Sektorindsatsen handler altså ikke om at overtage opgaver eller ansvar fra de enkelte aktører, men om at fremme finansiel stabilitet og tillid til den finansielle sektor ved at understøtte de enkelte aktørers indsats og tværgående indsatser.

For at målrette og intensivere den samlede indsats fremlægges hermed en samlet strategi for at styrke indsatsen for cyber- og informationssikkerhed i den finansielle sektor. Strategien skal være med til at sikre, at bekæmpelse af cyberangreb sker på en så effektiv og transparent måde som muligt.

Samarbejdet mellem myndighederne og de private aktører spiller en helt central rolle for en effektiv indsats for cyber- og informationssikkerheden. Med strategien understreges det, at bekæmpelse af cyberangreb er en samfundsopgave, der kræver en fokuseret og fælles indsats fra såvel myndigheder som private aktører.

Det overordnede formål med strategien er at fremme finansiel stabilitet og tillid til den finansielle sektor ved at styrke den samlede fælles indsats for cyber- og informationssikkerhed.

I det følgende beskrives de enkelte fokusområder i strategien for den finansielle sektor samt de initiativer, der er knyttet til fokusområderne.

3. Decentral enhed for cyber- og informationssikkerhed (DCIS) oprettes

Der oprettes i 2019 en decentral enhed for cyber- og informationssikkerhed for finanssektoren (herefter DCIS).

DCIS'en har det overordnede ansvar for den tværgående indsats i forhold til cyber- og informationssikkerhed på det finansielle område for derigennem at fremme den finansielle stabilitet og tilliden til den finansielle sektor. Det skal ske ved at understøtte, at den fælles samlede indsats for cyber- og informationssikkerhed styrkes via initiativer, som fordeler sig på 3 hovedspor:

- Trussels-, sårbarheds- og risikovurdering
- Sektorberedskab
- Videndeling

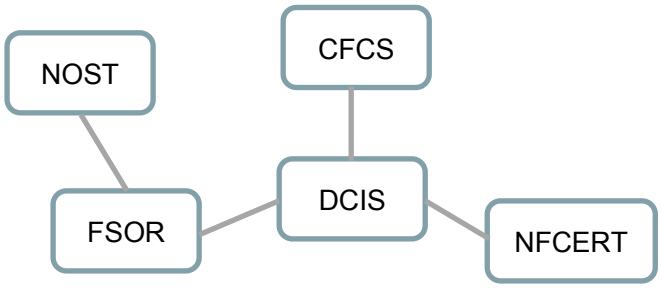
Ansvaret for DCIS'en forankres hos Finanstilsynet, som er den sektoransvarlige tilsynsmyndighed.

DCIS'ens organisering

De eksisterende enheder, FSOR og NFCERT, vil indgå i og bidrage til DCIS'ens opgaveløsning, hvorfor DCIS'en indgår samarbejdsaftaler med både FSOR og NFCERT. Målet hermed er at sikre, at DCIS'ens arbejde er forankret i sektoren, og at der undgås ressourcespild som følge af overlappende funktioner.

Udførelsen af strategien forudsætter, at aktørerne i sektoren bidrager aktivt hertil, og at der er et effektivt samarbejde mellem myndigheder og private aktører. Der oprettes derfor i FSOR en følgegruppe med repræsentanter for aktører fra sektoren. Formålet med følgegruppen er at sikre forankring af strategiens initiativer i sektoren og at sikre initiativernes relevans for sektorens arbejde med cyber- og informationssikkerhed.

Oversigt over aktører



DCIS'ens opgaver
DCIS'en har i det daglige primært til opgave at følge op på, at strategiens initiativer føres ud i livet. DCIS'en vil også sikre, at strategien evalueres.

De løbende sårbarheds- og risikovurderinger, som skal dække hele sektoren, forankres hos DCIS'en for at sikre de bedst mulige forudsætninger for at kunne følge op på strategiens initiativer og vurdere, om de er tilstrækkelige. Sårbarheds- og risikovurderingerne baserer sig på arbejdet hermed i FSOR og NFCERT, samt CFCS' trusselsvurderinger og hændelsesrapportering direkte fra virksomheder under tilsyn.

Ved kriser og større hændelser skal DCIS'en varetage kommunikationen til erhvervsministeren, som er ansvarlig for beredskabsplanlægningen i medfør af § 24 i beredskabsloven.

DCIS'en er aftalepart med CFCS, i forhold til udmøntningen af den nationale strategi for cyber- og informationssikkerhed. Desuden vil DCIS'en for finanssektoren samarbejde med DCIS'erne for de øvrige samfundsvigtige sektorer. I forhold til videndeling er DCIS'en også kontaktpunkt til CFCS.

FSOR er kontaktpunkt til Den nationale operative stab (NOST). NOST varetager koordinationsopgaver i forbindelse med større hændelser, hvor flere myndigheder medvirker ved konkrete beredskabsindsatser.

4. Sektorberedskabet i FSOR fastholdes og udvikles

Et væsentligt element i et cyberforsvar er at have et beredskab klar, som kan bruges, når der opstår en hændelse eller en krise. I lyset af trusselsvurderingen for finanssektoren vurderes det som meget sandsynligt, at et angreb, som har potentialet til at påvirke den finansielle stabilitet, vil forekomme på et tidspunkt.

De enkelte aktører har ansvaret for deres eget beredskab. Derudover skal der være et sektorberedskab. Sektorberedskabet er relevant i forhold til større hændelser, som har potentiale til at påvirke den finansielle stabilitet, jf. boks 4.

Boks 4: Sektorberedskab
Formålet med et sektorberedskab er at koordinere indsatsen mellem relevante aktører i tilfælde af en større hændelse, som har potentiale til at påvirke den finansielle stabilitet på kort eller længere sigt, dvs. at der er tale om en tværgående indsats. Beredskabet koordinerer også til eventuelle andre implicerede sektorer og/eller det nationale beredskab. Sektorberedskabet skal desuden sikre kommunikationen til relevante parter og til offentligheden.

Den enkelte virksomheds ansvar for eget beredskab fastholdes uændret, også under en alvorlig hændelse eller krise.

Sektorberedskabet i forhold til alvorlige hændelser, som kan påvirke den finansielle stabilitet, har forskellige behov for koordination, men organiseres fremadrettet samlet i FSOR.

4.1 FSORs sektorberedskabsplan udvikles yderligere

FSOR har udviklet og testet en sektorberedskabsplan 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.

Fremadrettet udvikles sektorberedskabsplanen yderligere i overensstemmelse med FSORs målsætning om at være "best in class" i Europa. Det skal bl.a. sikres, at planen i løbet af strategiperioden lever op til en international standard for kriseberedskab – tilpasset det forhold, at der er tale om et sektorberedskab med en koordinerende rolle og ikke en enkelt aktørs beredskab. Som led heri analyseres planens modenhed. FSOR varetager denne opgave.

4.1.1 Kommunikationsberedskabet styrkes
Et væsentligt aspekt af sektorberedskabet er tværgående koordinering og kommunikation, idet selve håndteringen af krisen varetages af de berørte aktører. Kommunikationen handler både om kommunikation mellem de relevante aktører i forhold til at koordinere indsatsen og kommunikation rettet mod offentligheden.

Kommunikationslinjerne fastlægges mellem de deltagende aktører i FSOR, de aktører, som måtte være berørt af en alvorlig hændelse eller krise, og eventuelt relevante aktører uden

for sektoren i tilfælde af en alvorlig hændelse eller krise, som rækker ud over sektoren. Kommunikationen til erhvervsministeren fastlægges også. Endelig fastlægges, hvordan kommunikationen til offentligheden skal foregå. FSOR varetager denne opgave.

4.2 Sektorberedskabsplanen for hændelser, som kan true finansiel stabilitet, testes

4.2.1 Sektorberedskabsplanen testes

Et kriseberedskab, der ikke er testet og afprøvet, vil være i risiko for ikke at være tilstrækkeligt, når en krise indtræffer. Det er derfor afgørende for effektiviteten, at planen for kriseberedskabet testes. Desuden bør en test afspejle det modenhedsniveau, en beredskabsplan er på for at sikre størst muligt udbytte af testen.

Der udarbejdes en testplan, som tager højde for sektorberedskabets modenhed. Desuden vurderes, hvorvidt og i givet fald i hvilket omfang beredskaberne hos de enkelte aktører skal indgå i testene. Testplanen udføres. FSOR varetager denne opgave.

Resultaterne af beredskabstests vil indgå systematisk i styrkelsen af sektorberedskabsplanerne.

4.2.2 Finanssektoren indgår i nationale og internationale beredskabsøvelser

En krise i finanssektoren kan stamme fra en anden sektor eller potentielt sprede sig til andre sektorer. Det gælder både Danmark og udlandet. Det er derfor vigtigt, at finanssektoren indgår i tværsektorielle tests, herunder eventuelt internationale tests.

FSOR står for sammen med DCIS'en at koordinere finanssektorens deltagelse i sådanne tværsektorielle øvelser.

Resultaterne af beredskabstests indgår systematisk i styrkelsen af beredskabsplanerne, det gælder både sektorberedskabsplanen og de enkelte deltagende aktørers planer i relevant omfang.

4.3. Samarbejdet styrkes med kritiske leverandører om beredskabsplan og tests

De samfundskritiske aktører benytter sig af private leverandører af IT-systemer, og der er i høj grad tale om de samme, få leverandører. Det medfører øgede risici på en række parametre, herunder i forhold til rækkevidden af et eventuelt succesfuldt cyberangreb og kompleksiteten i genopretningen.

Der er derfor behov for at analysere dette yderligere og at arbejde for at styrke samarbejdet med de kritiske leverandører, bl.a. i forhold til sektorberedskabet. FSOR varetager denne opgave.

Dette initiativ handler om problemstillinger i forhold til koordinering og analyser, mens forholdet mellem de enkelte virksomheder og deres leverandører i forhold til beredskab ikke indgår heri.

4.4 Beredskabsplaner styrkes i forsikrings- og pensionsselskaber i regi af FSOR

Det vurderes umiddelbart, at eventuelle alvorlige hændelser eller kriser i forhold til cyber- og informationssikkerhed i et forsikrings- eller pensionsselskab ikke på kort sigt vil påvirke den finansielle stabilitet, selvom det kan være meget alvorligt for den enkelte, ramte virksomhed. Sårbarheden i denne del af sektoren skal dog analyseres nærmere.

FSOR vil styrke forsikrings- og pensionsselskabers kriseberedskab, bl.a. ved at dele "playbooks" for beredskabstests. Desuden vil FSOR i samarbejde med DCIS'en klarlægge kommunikationslinjerne mellem de berørte aktører i tilfælde af alvorlige hændelser eller kriser. De enkelte aktører på forsikrings- og pensionsområdet, som indgår i beredskabet, bevarer fortsat ansvaret for egne systemer og data.

5. Sårbarheder og risici skal afdækkes systematisk og løbende

En afgørende forudsætning for at prioritere indsatsen for sektorens cyber- og informationssikkerhed er et løbende opdateret overblik over, hvilken infrastruktur og hvilke tjenester i sektoren som er samfundskritiske, og hvilke sårbarheder og risici der er forbundet hermed.

Der findes allerede væsentlige kortlægninger af sektoren. FSOR har kortlagt de mest kritiske forretningsaktiviteter i forhold til at sikre finansiel stabilitet på kort sigt, de underliggende systemer og processer og afhængighederne imellem dem. Finanstilsynet har desuden udpeget en række tjenester, som er væsentlige for at opretholde finansiel stabilitet, fx likviditetsstyring, afvikling af værdipapirhandler og detailbetalinger, håndtering lån mv. Det er sket i regi af implementeringen af EU's direktiv om sikkerhed i net- og informationssystemer i samfundskritiske sektorer – NIS-direktivet, jf. boks 5.

Boks 5: EU's direktiv om sikkerhed i net- og informationssystemer i samfundskritiske sektorer (NIS-direktivet)
Danske myndigheder har implementeret et EU-direktiv om sikkerhed i net- og informationssystemer, det såkaldte NIS-direktiv. Direktivet stiller blandt andet krav om, at operatører af væsentlige tjenester, som er af betydning for opretholdelsen af samfundskritiske funktioner og tjenester, træffer foranstaltninger til at håndtere sikkerheden i de net- og informationssystemer, som de anvender ved levering af deres tjenester.

5.1 Overblik over kritisk infrastruktur, tjenester og afhængigheder udbygges

Som grundlag for indsatsen for cyber- og informationssikkerhed bør der være et løbende opdateret overblik over hele sektorens samfundskritiske infrastruktur og tjenester samt afhængighederne både imellem disse og til andre sektorers kritiske infrastruktur.

DCIS'en vil samle de eksisterende kortlægninger til én samlet oversigt og sikre, at oversigten er dækkende i forhold til, hvad der er væsentligt for at sikre finansiel stabilitet. Oversigten skal opdateres løbende.

Oversigten for den finansielle sektor skal indgå i en samlet national oversigt over myndigheder og virksomheder med digital infrastruktur, der er væsentlige for samfundskritiske funktioner. Den samlede oversigt vil kunne anvendes af finanssektoren i forhold til arbejdet med afhængigheder mellem finanssektoren og øvrige sektorer.

5.2 Sårbarheds- og risikovurdering for hele sektoren gennemføres løbende

Det er afgørende at have en dækkende og opdateret sårbarheds- og risikovurdering for at kunne prioritere de rigtige initiativer i strategien og de løbende justeringer heraf.

Der findes allerede forskellige sårbarheds- og risikovurderinger af finanssektoren. FSOR har udarbejdet en fælles risikoanalyse i 2018 med henblik på at prioritere det fremtidige

arbejde. Finanstilsynet udarbejder halvårlige risikovurderinger af den finansielle sektor, også med fokus på cyber- og informationssikkerhed.

Fremadrettet vil DCIS'en udarbejde en sårbarheds- og risikovurdering med udgangspunkt i en international standard herfor og med input fra FSOR og NFCERT. Desuden vil virksomhedernes hændelsesrapportering og forskellige undersøgelser af sektoren indgå i grundlaget for vurderingerne. Arbejdet vil bygge videre på de eksisterende analyser og vurderinger og vil blive opdateret løbende. I forhold til trusler vil vurderingen tage udgangspunkt i den sektorspecifikke trusselsvurdering, som CFCS udarbejder. DCIS'en vil være i dialog med CFCS om trusselsvurderingen.

Det eksisterende overblik over sårbarheder og risici for forsikrings- og pensionssektoren er ikke så udbygget som for betalings-, kredit og afviklingssektoren. FSOR vil samarbejde med forsikrings- og pensionsselskaber om at udarbejde en grundlæggende sårbarheds- og risikovurdering, som vil indgå i den samlede vurdering for sektoren.

5.3 Det understøttes, at væsentlige aktører kortlægger sårbarheder og risici i deres cyberrobusthed

Det er vigtigt, at de enkelte virksomheder med samfundskritisk infrastruktur og tjenester konkret kender deres sårbarheder og risici og dermed deres reelle cyberrobusthed.

Der er adskillige metoder til at opnå et sådant overblik. Den eksisterende lovgivning stiller generelt krav både om, at virksomhederne gennemfører risikovurderinger og udfører tests og anden kvalitetssikring, herunder er der konkret krav om, at beredskabsplaner testes.

FSOR har taget initiativ til at gennemføre et program, hvor de enkelte virksomheder med samfundskritisk infrastruktur og tjenester kan teste deres cyberrobusthed i praksis via såkaldte red team-tests, jf. boks 6.

Boks 6: Red team-test
En red team-test er en live-test, hvor eksterne konsulenter efter aftale forsøger at få adgang til en virksomheds systemer og data, uden at virksomhedens medarbejdere – ud over dem som har bestilt test, er informeret. Dermed simuleres et reelt angreb så vidt muligt. Erfaringerne fra testene bruges efterfølgende til at forbedre virksomhedens cyberrobusthed.

Den europæiske centralbank har udviklet et rammeværktøj til red team-test målrettet den finansielle sektor, hvilket FSOR har tilpasset til den danske finansielle sektor. I alt 14 institutioner har givet Nationalbanken tilsagn om, at de vil gennemføre programmet

Det er afgørende for at sikre et godt udbytte af sådanne tests, at deltagernes modenhedsniveau i forhold til alle aspekter af cyberrobusthed er tilstrækkeligt. Det gælder beskyttelsesniveauet, evnen til at opdage et angreb og evnen til at bekæmpe det og reetablere de ramte systemer og data.

6. Lovgivningen skal modsvare trusselsniveauet

Lovgivning er et væsentligt middel til at sikre, at kravene til IT-sikkerhed er tilstrækkelige i forhold til at imødegå trusselsniveauet.

6.1 Lovgivningen om IT-sikkerhed analyseres med henblik på at sikre tydelige og dækkende krav

Den finansielle lovgivnings krav til en finansiel virksomheds IT-sikkerhed er primært defineret i lov om finansiel virksomhed. En finansiel virksomhed skal have etableret effektiv virksomhedsstyring, herunder betryggende kontrol- og sikringsforanstaltninger på IT-området, jf. § 71. Kravene er nærmere udmøntet i bilagene om IT-sikkerhed i ledelsesbekendtgørelserne for henholdsvis forsikringsselskaber mv. og pengeinstitutter m.fl. Der er desuden fastsat krav til outsourcing af IT i outsourcingbekendtgørelsen og til IT-revisionen af datacentraler i systemrevisionsbekendtgørelsen for fælles datacentraler. Derudover er der en række krav fra EU, som er fastsat i forordninger, direktiver og guidelines fra bl.a. Den Europæiske Banktilsynsmyndighed (EBA) og Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger (EIOPA). Endelig findes forskellige krav til indberetning af hændelser mv.

Det vurderes, at der kan være grundlag for at opdatere lovgivningen om kravene til IT-sikkerhed på grundlag af den store udvikling på området. Derudover vil DCIS'en analysere lovgivningens krav i forhold til de trussels-, sårbarheds- og risikovurderinger for sektoren, som gennemføres.

6.2 Kontrolmulighederne i forhold til væsentlige IT-leverandører analyseres

Brugen af leverandører til samfundskritisk infrastruktur og tjenester udgør en risiko, bl.a. fordi de finansielle virksomheders infrastruktur og systemer er koncentreret hos få leverandører, hvilket øger sårbarheden.

Det er outsourcingvirksomhedens ansvar at sikre, at leverandørerne udfører de outsourcede opgaver på en tilfredsstillende måde, og oursourcingvirksomheden skal føre løbende kontrol med leverandørerne.

DCIS'en vil gennemføre en analyse af kontrollen med væsentlige IT-leverandører.

På den baggrund vil Finanstilsynet vurdere, om der er behov for at opdatere lovgivningen og i givet fald komme med anbefalinger hertil.

7. Viden skal udnyttes til at bekæmpe IT-sikkerhedstrusler effektivt

Indsatsen i forhold til styrke cyber- og informationssikkerheden skal bygge på et oplyst grundlag. Det gælder både den fælles indsats, de enkelte virksomheders indsats og Finanstilsynets indsats som tilsynsmyndighed.

7.1 Indberetningen af hændelser styrkes for at forbedre vidensgrundlaget

Viden om faktiske hændelser og situationer, som kunne have udviklet sig hertil, udgør et væsentligt grundlag for at vurdere sektorens sårbarheder og risici og på den baggrund iværksætte relevante tiltag.

Finanstilsynet stiller i dag forskellige krav til de finansielle virksomheder om at indrapportere hændelser. Det gælder generelt i forhold til væsentlige hændelser og derudover specifikt for udbydere af betalingstjenester og for udbydere af væsentlige tjenester.

DCIS'en vil analysere og vurdere behovet for at opdatere kravene til virksomhedernes indberetninger til Finanstilsynet, og om der er behov for at ændre kravene. Indberetningerne forventes at indgå i DCIS'ens sårbarheds- og risikovurderinger af sektoren, og dermed som input til kriseberedskabet i FSOR. Desuden vil DCIS'en undersøge muligheden for at offentliggøre data om hændelserne, som sektoren vil kunne anvende i sit arbejde med cyber- og informationssikkerhed.

7.2 Viden om trusler, sårbarheder og angreb distribueres hurtigt og effektivt i sektoren

Sårbarheder findes i mange tilfælde på tværs af flere aktører. Samtidig vil cyberangreb ofte ske mod flere aktører inden for kort tid. Hurtig deling af viden om sårbarheder, trusler og angreb kan derfor være afgørende for at undgå eller begrænse skaderne mest muligt.

NFCERT blev etableret for at øge medlemmernes cyberrobusthed. NFCERT er en privat forening ejet af sine medlemmer og har hele Norden som sit optageområde. NFCERT's primære rolle er videndeling i forhold til trusler mv., og koordinering af medlemmernes repons på angreb. NFCERT kan optage alle virksomheder under tilsyn som medlemmer.

DCIS'en vil arbejde for, at NFCERT fortsat varetager den operative opgave med videndeling.

En afgørende forudsætning for, at NFCERT kan opfylde sit formål, er tillid fra medlemmerne i forhold til, at følsomme og forretningskritiske oplysninger behandles fortroligt. Håndtering af videndeling indgår som et centralt element i medlemsaftalen mellem NFCERT og hvert af dets medlemmer. I forhold til DCIS'en, som varetages af Finanstilsynet, er udgangspunktet, at de enkelte virksomheder under tilsyn rapporterer om hændelser mv. di-

rekte til Finanstilsynet. NFCERT orienterer kun DCIS'en direkte i de tilfælde, hvor der er umiddelbar risiko for, at den finansielle stabilitet kan blive påvirket.

Det vil indgå i det videre arbejde at overveje, hvordan det sikres, at flere aktører optages som medlemmer i NFCERT, herunder datacentraler, med henblik på at sikre, at sektoren er dækket af CERT'en i tilstrækkelig grad.

7.3 Der afholdes informationsmøder mv. for sektoren om relevante emner

I arbejdet med cyber- og informationssikkerhed kan aktørerne med fordel lære af hinandens erfaringer og drøfte løsninger mv. Det gælder både i sektoren og på tværs af andre sektorer.

DCIS'en vil enten i samarbejde med, eller opfordre til, at FSOR og NFCERT arrangerer informationsmøder, workshops, konferencer mv. om relevante emner. Det kan fx være om leverandørstyring, sikkerhedsaspekter ved ny teknologi, konkrete sikkerhedsløsninger, overholdelse af sikkerhedskrav mv. Brancheorganisationerne vil også blive inddraget i forhold til at sikre relevansen af de emner, der tages op. Desuden vil DCIS'en samarbejde med CFCS og de øvrige sektorers DCIS'er om dette.

8. Ansatte og kunder skal rustes til forsvar mod IT-sikkerhedstrusler

Menneskelige fejl er skyld i en stor andel af de sikkerhedskompromitteringer, der sker. Der er derfor et stort potentiale i at styrke ansattes og kunders viden om cyber- og informationssikkerhed i forhold til at forebygge, at cyberangreb lykkes, eller at informationssikkerheden bliver kompromitteret på anden vis.

Den nationale strategi for cyber- og informationssikkerhed indeholder en række tiltag i forhold til at styrke både borgeres og medarbejderes IT-sikkerhedskompetencer, herunder en informationsportal målrettet borgere og virksomheder, Sikkerdigital.dk, og et erhvervspartnerskab for øget IT-sikkerhed i dansk erhvervsliv. Derudover har brancheorganisationerne for de samfundskritiske sektorer indgået en cyberalliance, som har som mål at styrke cyber- og informationssikkerheden i de samfundskritiske sektorer. Alliancen vil arbejde for at styrke samarbejdet om fremtidens behov for uddannelse, efteruddannelse og kurser på cyber- og informationssikkerhedsarbejdet. Endelig udføres en række konkrete kampagner. Bl.a. har Europols cybercrimecenter, EC3, og de europæiske bankers brancheorganisation, EBF, udarbejdet en oplysningskampagne om cyberkriminalitet under navnet #CyberScams.

Strategiens målsætning på dette område er at sikre, at oplysnings- og uddannelsesindsatsen i forhold til finanssektoren er tilstrækkelig. Det kan både ske ved selvstændige initiativer og ved at samarbejde med eksisterende initiativer i andre sektorer, på nationalt plan eller internationalt.

8.1 Det analyseres, om der er behov for fælles oplysningsindsats over for finanssektorens kunder

DCIS'en analyserer i samarbejde med brancheorganisationerne FinansDanmark og Forsikring & Pension, om der er behov for en særskilt oplysningsindsats over for finanssektorens kunder i forhold til cyber- og informationssikkerhed i regi af strategien. Såfremt det er tilfældet, så iværksættes en sådan særskilt oplysningsindsats.

Desuden vil DCIS'en sammen med brancheorganisationerne FinansDanmark og Forsikring & Pension samarbejde med Digitaliseringsstyrelsen og Erhvervsstyrelsen, som står bag den nationale informationsportal sikkerdigital.dk, med henblik på at understøtte, at informationen i forhold til finanssektorens kunder er dækkende.

8.2 Det analyseres, om der er behov for indsats for at sikre relevante kompetencer

DCIS'en analyserer i samarbejde med brancheorganisationerne FinansDanmark og Forsikring & Pension, om der er behov for en særskilt indsats for at sikre relevante cyber- og informationssikkerhedskompetencer målrettet finanssektoren, og i bekræftende fald hvordan behovet kan imødekommes. Analysen vil tage højde for de øvrige iværksatte indsatser på dette område.

8.3 Det analyseres, om der bør indføres krav om træning af ansatte

DCIS'en vil som led i analysen og vurderingen af den nuværende lovgivning om IT-sikkerhed for finansielle virksomheder undersøge, om der er behov for at stille specifikt krav om, at ansatte i finanssektoren skal trænes i cyber- og informationssikkerhed.

9. Samarbejde på tværs af sektorer skal styrke cyber- og informationssikkerheden

Trusler om cyberangreb mv. er grænseoverskridende, såvel mellem sektorer som lande. Desuden er der væsentlige afhængigheder mellem de samfundsvigtige sektorer, fx er finanssektoren grundlæggende afhængig af energi- og telesektoren, mens alle øvrige sektorer er afhængige af finanssektoren. Desuden udveksles fortrolige data på tværs af sektorgrænser, fx mellem sundhedssektoren og finanssektorens forsikrings- og pensionsselskaber. Derfor er et effektivt samarbejde med andre sektorer, med CFCS og dets cybersituationscenter (CSIRT) og med udlandet afgørende for at øge cyber- og informationssikkerheden i finanssektoren.

9.1 Videndeling styrkes via aftale mellem CFCS og DCIS'en

CFCS spiller en vigtig rolle i forhold til arbejdet med cybersikkerhed i finanssektoren. Bl.a. udarbejder CFCS trusselsvurderinger rettet specifikt mod finanssektoren, de udsender sikkerhedsvarsler og øvrig relevant information, og de er kontaktpunkt med henblik på håndtering og videndeling ved sikkerhedshændelser, der har grænseoverskridende konsekvenser for EU-medlemslandene.

Desuden vil DCIS'en arbejde for, at CFCS udbygger den tværsektorielle tekniske overvågning via sensornetværket og deler oplysningerne effektivt med de samfundsvigtige sektorers aktører.

9.1.1 Sektorens indstationering af medarbejdere ved CFCS

Finanssektoren har i 2018 indstationeret en medarbejder ved CFCS med henblik på at øge sektorkendskabet i CFCS. Det analyseres, hvorvidt der er grundlag for at udvide denne ordning.

9.2 Samarbejdet med de øvrige samfundskritiske sektorer styrkes

9.2.1 Gensidige afhængigheder og samarbejdsmuligheder afdækkes

De samfundskritiske sektorer er gensidigt afhængige, jf. ovenfor, og har også på væsentlige områder samme behov i forhold til at øge cyber- og informationssikkerheden.

De ansvarlige for delstrategierne for hver af de samfundsvigtige sektorer har som led i udarbejdelsen af strategierne været i dialog herom. DCIS'en vil i løbet af strategiperioden bidrage til, at følgende forhold analyseres:

- gensidige afhængigheder mellem de samfundsvigtige sektorer
- hvordan man bedst muligt kan samarbejde om at øge cyber- og informationssikkerheden på tværs af sektorerne – både i forhold til forebyggelse og under en eventuel krise

9.2.2 DCIS'en vil kortlægge relevante cyber- og informationssikkerhedsfora

Der findes en række forskellige organisationer, initiativer mv., som beskæftiger sig med cyber- og informationssikkerhed både generelt og specifikt for den finansielle sektor.

DCIS'en vil kortlægge de forskellige fora med henblik på at sikre, at der samarbejdes og koordineres med alle relevante parter, så der opnås synergier, samtidig med at dobbelt-funktioner undgås.

10. Strategien evalueres

Denne strategi og dens initiativer bør være fleksible. Indsatserne for cyber- og informationssikkerhed i den finansielle sektor har været i gang i en årrække. Samtidig udvikler cyber- og informationssikkerhedstruslerne sig hurtigt. På den baggrund er det vigtigt løbende at lære af erfaringer og justere strategiinitiativerne på baggrund heraf.

Strategien evalueres første gang i efteråret 2019 med henblik på at sikre et fortsat fokus på og en styrkelse af finanssektorens arbejde med cyber- og informationssikkerhed.

Ved strategiperiodens udløb i 2021 slutevalueres strategien, herunder DCIS'en.

Det forventes, at der vil blive udarbejdet en ny strategi som opfølgning på denne. Slutevalueringen skal derfor være afsluttet tids nok til, at dens resultater kan indgå som input til udformningen af en forventet ny strategi.