DANMARKS NATIONALBANK

28. AUGUST 2020 — NR. 14

Hvordan prioriteres fælles tiltag til at håndtere cyberrisici?

- Nogle systemiske risici kan bedst adresseres i fællesskab. Den danske finansielle sektor har udviklet en metode til at prioritere det fælles arbejde med cyberrisici.
- Sektoren samarbejder om at identificere og adressere systemiske risici på et struktureret grundlag. Metoden øger cybersikkerheden både for den enkelte institution og for samfundet.
- Metoden kan også anvendes i andre sektorer end den finansielle.

I den finansielle sektor i Danmark er der stor fokus på at modvirke den stigende risiko for cyberangreb. Både i de enkelte institutioner, på sektorniveau og på nationalt plan arbejdes der på at håndtere cyberrisici, se boks 1.

Den enkelte institution har ansvaret for at sikre stabil drift og operationel robusthed i egne systemer. Men de tekniske og finansielle sammenhænge medfører, at cyberangreb kan sprede sig på tværs af institutioner

Centrale aktører i cyberarbejdet Boks 1

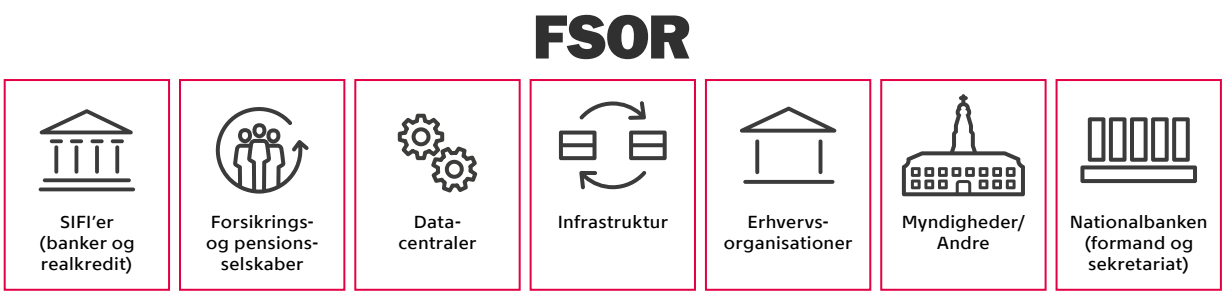
De enkelte institutioner arbejder med cyberrisiko og anvender betydelige og nødvendige ressourcer for at øge cybersikkerheden. Derudover fører Finanstilsynet tilsyn med finansielle institutioner og datacentraler, og Nationalbanken overvåger betalingsinfrastrukturen.

Finansielt Sektorforum for Operationel Robusthed, FSOR, er også en central aktør i cyberarbejdet i den finansielle sektor. Se boks 2 for en beskrivelse af FSOR.

På nationalt plan udgav den daværende regering i 2018 en national strategi for cyber- og informationssikkerhed (*link*), som bl.a. definerer seks samfundskritiske sektorer, heriblandt den finansielle sektor. Strategien indeholder tværgående initiativer, der har til formål at øge cyberrobustheden. Center for Cybersikkerhed, CFCS, varetager en koordinerende rolle for disse tværgående initiativer. Den Nationale Operative Stab, NOST, koordinerer i tilfælde af en national krise.

FSOR samler private og offentlige aktører i den finansielle sektor Boks 2

Den danske finansielle sektor er gået 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: 1) de største og systemisk vigtige finansielle institutioner, SIFI'er, og forsikrings- og pensionsselskaber, 2) datacentraler, som drifter kritiske systemer og opbevarer og håndterer dele af sektorens data, 3) de virksomheder, som ejer infrastrukturen – herunder platforme til finansielle transaktioner, 4) finansielle erhvervsorganisationer, 5) centrale myndigheder. Danmarks Nationalbank er formand for FSOR og varetager sekretariatsfunktionen.



og systemer. Derfor giver det mening både for den enkelte institution og for samfundet, at flere af de operationelle risici, herunder cyberrisici, adresseres i fællesskab.

Men hvordan kan man på tværs af institutioner identificere, hvad der er mest centralt, og prioritere, hvad der skal gøres i fællesskab? Det giver finanssektorens arbejde med en fælles risikoanalyse et bud på!

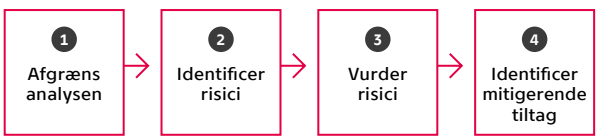
Nedenfor præsenteres den metode til en struktureret risikoanalyse, som finanssektoren har udarbejdet og anvender. Metoden er generisk og kan også anvendes i andre sektorer end den finansielle. Resultaterne af analysen er sensitive og fortrolige. De fremgår derfor kun som overordnede eksempler. Fokus i det følgende er på selve metoden.[1]

Sådan udformes en risikoanalyse på sektorniveau – trin for trin

Den finansielle sektor i Danmark er gået sammen i et privat-offentligt samarbejde (Finansielt Sektorforum for Operationel Robusthed, FSOR) om at øge sektorens robusthed over for bl.a. cyberangreb, se boks 2. Centralt for samarbejdet er udformning af en risikoanalyse. Risikoanalysen bidrager dels til at afdække de operationelle risici, som potentielt kan true stabiliteten i det finansielle system, dels til at give et struktureret grundlag for at prioritere tiltag til at reducere disse risici.

Metoden til at udarbejde en risikoanalyse på sektorniveau indeholder overordnet set fire trin:

1. Analysen afgrænses
2. Risici identificeres
3. Risici vurderes i forhold til sandsynlighed og konsekvens
4. Mitigerende tiltag for de væsentligste risici identificeres.



1 For yderligere detaljer om metoden, se *Metodehåndbog for FSOR's risikoanalyse*, august 2020 (*link*).

FSOR har nedsat en arbejdsgruppe, som står for den praktiske udarbejdelse af risikoanalysen. Et bredt udvalg af aktører i den finansielle sektor er repræsenteret i arbejdsgruppen. På baggrund af analysen beslutter FSOR, hvilke tiltag der skal implementeres, hvornår og hvordan.

1. Analysen afgrænses
Første skridt i risikoanalysen er at identificere sektorens kronjuveler. Her udarbejdes en bruttoliste over forretningsaktiviteter for sektoren som helhed. Ud fra bruttolisten identificeres de mest kritiske forretningsaktiviteter, dvs. aktiviteter, hvor nedbrud, brud på fortrolighed eller tab af integritet potentielt kan have systemiske konsekvenser og true den finansielle stabilitet.

Blandt kronjuvelerne har FSOR's risikoanalyse i første omgang fokus på de forretningsaktiviteter, hvor nedbrud og lignende hurtigst bliver kritisk, se figur 1. Fokus er p.t. afgrænset til de aktiviteter, der vurderes kritiske inden for en tidsramme på op til en uge. Det er centralt på forhånd at have en dyb forståelse af netop disse aktiviteter, fordi de skal kunne håndteres akut.

Når de mest kritiske forretningsaktiviteter identificeres, indsnævres fokus dermed på at adressere de mest centrale risici. Ved denne prioritering accepteres også, at alt ikke er lige vigtigt, og at alle funktioner i den finansielle sektor ikke kan beskyttes på samme høje niveau. Ofte vil det dog være sådan, at et højt forsvarsværn for de kritiske funktioner også vil reducere risikoen for en række af de mindre kritiske funktioner.

2. Risici identificeres
Risici opstår, hvor en trussel kan udnytte en sårbarhed. Indsamling af trusler og sårbarheder har til formål at give en bred afdækning af de risici, som potentielt kan true de kritiske forretningsaktiviteter og dermed den finansielle stabilitet.

De kritiske forretningsaktiviteter, som analysen er afgrænset til, kortlægges. Der skabes et overblik over systemer, netværk, leverandører og sammenhængene mellem disse. Kortlægningen giver input til, hvor der kan være sårbarheder, fx i forhold til gensidige afhængigheder og koncentration i anvendelsen af leverandører af kritiske systemer og netværk.

Endvidere indsamles information om trusler og sårbarheder fra en række andre kilder. Det gælder bl.a.:

Afgrænsning af risikoanalysen Figur 1

	≤ ½ dag	≤ 1 dag	2 dage	> 1 uge
Forretningsaktivitet 1	(X)	X		
Forretningsaktivitet 2			(X)	X
Forretningsaktivitet 3			X	
Forretningsaktivitet 4			X	
Forretningsaktivitet 5		(X)	X	
Forretningsaktivitet 6				X
Forretningsaktivitet 7				X
Forretningsaktivitet 8				X

Anm.: (X) = for særlig kritiske dage. Den røde linje skiller de forretningsaktiviteter, som bliver kritiske inden for en tidshorisont på henholdsvis under og over en uge.

- historiske hændelser
- trusselsvurderinger
- sårbarheder identificeret i FSOR's cyberstocktake, som er en spørgeskemaundersøgelse af cyberrobustheden hos FSOR's medlemmer
- input fra viden om kommende systemændringer mv.

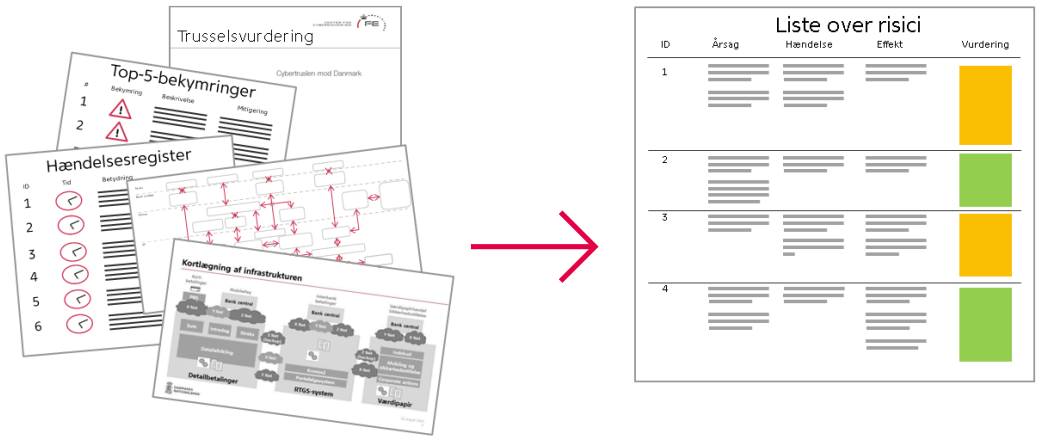
FSOR gennemfører regelmæssigt en rundspørge hos medlemmerne for at afdække deres top-5-bekymringer i relation til stabil drift af de kritiske forretningsaktiviteter. Tilbagemeldingerne giver input til, hvilke sårbarheder og trusler mod operationel robusthed der bekymrer sektoren.

Derudover er arbejdsgruppens medlemmer en central kilde til at identificere og indrapportere nye sårbarheder, trusler og risici. På den måde sikres, at de risici, som fylder mest i de enkelte institutioner, også inddrages i risikoanalysen.

Ud fra ovenstående kilder udarbejdes en liste over systemiske risici, og hver risiko beskrives med årsag, hændelse og effekt, se figur 2. Risikobeskrivelserne danner grundlag for at vurdere risikoens sandsynlighed og konsekvens.

FSOR har pr. juli 2020 identificeret 36 operationelle risici, der potentielt kan true den finansielle stabilitet. Et overordnet eksempel på en risiko er et cyberangreb, der ødelægger kritisk data hos en central aktør i den finansielle sektor. Et andet eksempel er, at risikostyring

Risici identificeres Figur 2



Anm.: Systemiske risici indsamles fra forskellige kilder og konsolideres i en liste med en beskrivelse af risikoårsag, risikohændelse og risikoeffekt.

i centrale dele af den finansielle infrastruktur er så siloopdelt, at det komplicerer håndteringen af en hændelse.

3. Risici vurderes i forhold til sandsynlighed og konsekvens

De identificerede risici vurderes hver især i forhold til sandsynlighed og konsekvens ud fra en række kriterier, se figur 3.

Sandsynlighed vurderes typisk efter, hvor ofte en hændelse forventes at indtræffe, men andre faktorer kan også påvirke scoringen, fx manglende indsigt i problemstillingen. Konsekvens vurderes efter, i hvilken grad finansiel stabilitet potentielt er truet.

FSOR anvender en skala fra 1-5 til at vurdere sandsynlighed og konsekvens. Risici indplaceres i risikomatricen, se figur 4, som er inddelt i fire farver. Farvefordelingen i matricen er ikke symmetrisk, da hændelser med høj konsekvens, men lille sandsynlighed (såkaldte black swans) også har fokus i forhold til finansiel stabilitet.

4. Mitigerende tiltag for de væsentligste risici identificeres

For de væsentligste risici udarbejder en arbejdsgruppe forslag til mitigerende tiltag, som drøftes i FSOR. De tiltag, som besluttes, skal derefter implementeres. Dette arbejde sker i separate arbejdsspor, og der følges løbende op på fremdriften. Andre risici accepteres – og adresseres således ikke.

Et af de mitigerende tiltag, der udspringer af risikoanalysen, er TIBER-DK[2], som Nationalbanken er myndighed for. I den forbindelse gennemfører de

Kriterier for vurdering af sandsynlighed og konsekvens Figur 3

SANDSYNLIGHED

- Frekvens
- Trusselsbillede efter mitigerende tiltag
- Vidensdeling og samarbejde
- Deling af information om trusler
- Sporbarhed
- Leverandørkompleksitet
- Modenhed og kontrolmiljø
- Manglende indsigt i risiko
- Kompleksitet af forretningsaktivitet og it-arkitektur

KONSEKVENS

- Påvirkning af kritiske forretningsaktiviteter
- Offentlig fokus og påvirkning
- Tab af tillid til det finansielle system
- Integritet af kritisk data og fortrolighed

2 Threat Intelligence Based Ethical Red-teaming in Denmark, TIBER-DK.

største aktører i den finansielle sektor trusselsbaserede red team-tests, hvor rigtige hackergruppers procedurer, teknikker og taktikker efterlignes af etiske hackere, der forsøger at få adgang til de samfundskritiske systemer (kronjuveler). Formålet er at styrke cyberrobustheden og dermed den finansielle stabilitet gennem læring fra testene.[3]

Andre eksempler på mitigerende tiltag er bl.a. samarbejde om sikring af sektorens vigtige data, samarbejde om styrkelse af kravstillelse til og øget dialog med leverandører, tættere samarbejde om risici mellem ejere af sektorens centrale infrastruktur og et fælles kriseberedskab i tilfælde af systemiske hændelser.

Nogle mitigerende tiltag kan sektoren ikke selv implementere. De kan bedre håndteres på nationalt plan. FSOR melder derfor forslag til mitigerende handlinger ind til fx den nationale cyberstrategi eller går i dialog med relevante myndigheder. Et eksempel er behovet for sikring af tilstrækkelig præcis tidsstyring, der er relevant for flere sektorer.

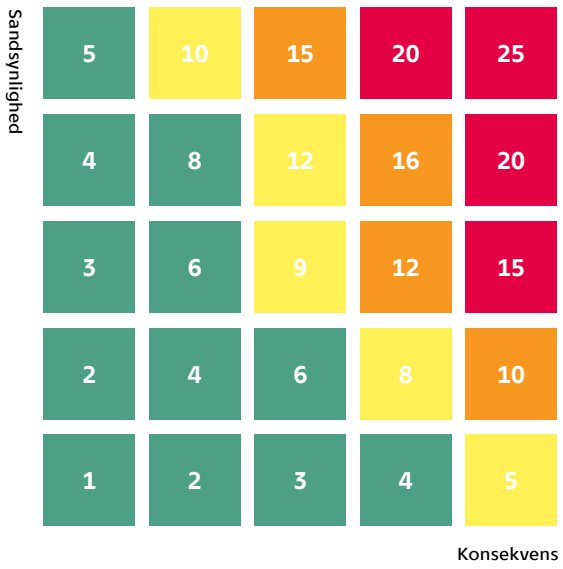
Risikoanalysen opdateres efter et årshjul, som sikrer, at man løbende forholder sig til de identificerede risici. Opdateringen sikrer også opmærksomhed på, om selve afgrænsningen af analysen skal justeres.

Erfaringer og videre refleksioner

Risikoanalyse på sektorniveau er nyttigt både for de individuelle institutioner, for sektoren og for samfundet som helhed, idet den peger på centrale risici og sikrer koordination, videndeling og hensigtsmæssig arbejdsdeling i forhold til at adressere risici. Risikoanalysen sikrer endvidere, at den danske finansielle sektor arbejder struktureret, i dybden og på et prioriteret grundlag for derved at få maksimal afkast af det udførte arbejde og de anvendte ressourcer.

For at en risikoanalyse på tværs af sektoren skal give værdi, er det vigtigt,

Risikomatrice Figur 4



- at analysen forankres i en troværdig institution, der har analytisk kapacitet, viden og leveringskompetence til at få analysen i mål
- at et sekretariat faciliterer et tillidsfuldt, fortroligt og tæt samarbejde mellem parterne, så der er villighed til at dele indsigt og erfaringer – både gode og dårlige
- at der sikres bredde i arbejdsgruppens kompetencer, så både den tekniske og forretningsmæssige del af institutionerne er repræsenteret
- at sektoren er repræsenteret på tilstrækkelig højt niveau til at sikre beslutningskraft – også når det involverer ressourcer.

Der anvendes betydelige og nødvendige ressourcer for at øge de enkelte institutioners robusthed. Omkostningerne til arbejdet på tværs af sektoren er i sammenligning hermed begrænsede – men afkastet er betydeligt. Risici, som er identificeret og adresseret i fællesskab, vil i de fleste tilfælde ikke kunne løftes af den enkelte virksomhed eller institution. Derfor giver det mening som sektor i fællesskab at arbejde med at identificere og adressere systemiske risici.

3 Se Danmarks Nationalbank, *TIBER-DK General Implementation Guide*, 18. april 2020 (*link*).

NYT

Nyt giver et hurtigt og tilgængeligt indblik i en Analyse, et Economic Memo, et Working Paper eller en Rapport fra Nationalbanken. Nyt udkommer løbende.

ANALYSE

Nationalbankens Analyseserie har fokus på økonomiske og finansielle forhold. Nogle af analyserne udkommer med fast frekvens, fx *Udsigter for dansk økonomi* og *Finansiel stabilitet*, der begge udkommer halvårligt. Andre analyser udkommer løbende.

RAPPORT

Nationalbankens Rapportserie er tilbagevendende rapporter og beretninger om Nationalbankens virke. Det er fx *Årsrapport* og *Statens låntagning og gæld*.

ECONOMIC MEMO

Economic Memo er en mellemting mellem en Analyse og et Working Paper og viser ofte forfatternes igangværende analysearbejde. Serien henvender sig primært til fagpersoner. Economic Memo udkommer løbende.

WORKING PAPER

Working Paper præsenterer forskningsarbejde udført af ansatte i Nationalbanken og samarbejdspartnere. Serien henvender sig primært til fagpersoner og folk med interesse for den akademiske tilgang. Working Paper udkommer løbende.

Analysen består af en dansk og engelsk version.
I tilfælde af tvivl om oversættelsens korrekthed gælder den danske version.

DANMARKS NATIONALBANK
HAVNEGADE 5
1093 KØBENHAVN K
WWW.NATIONALBANKEN.DK

Redaktionen er afsluttet
24. august 2020

Mette K. Petry
Senior Advisor,
FSOR Secretariat
mpk@nationalbanken.dk

Lone Natorp
Head of Oversight
ln@nationalbanken.dk

Katrine Skjærbæk Rasmussen
Infrastructure Advisor
ks@nationalbanken.dk
FINANSIEL STABILITET

DANMARKS NATIONALBANK

KONTAKT

Mette K. Petry
Senior Advisor,
FSOR Secretariat

mpk@nationalbanken.dk
+45 3363 6170

FINANSIEL STABILITET