DANMARKS NATIONALBANK

1. MARTS 2017 — NR. 3

# Cyberrobusthed i den finansielle sektor

Alvorlige cyberangreb kan i værste fald være en trussel mod selve stabiliteten i den finansielle sektor. Nationalbanken og Finanstilsynet har derfor ved en spørgeskemaundersøgelse undersøgt cyberrobustheden hos kerneaktører i den finansielle sektor i Danmark i 2016. Undersøgelsen omfatter store banker og realkreditinstitutter samt infrastrukturselskaber, som leverer kritiske services til disse.

Undersøgelsen af cyberrobusthed hos kerneaktører i den finansielle sektor i Danmark viser:

- Kerneaktørerne i den finansielle sektor i Danmark har et betydeligt fokus på cybersikkerhed, men der er plads til forbedring.
- Når cybersikkerhed forankres i topledelsen, er niveauet af cyberrobusthed højere.
- Uddannelse og træning af alle medarbejdere i cybersikkerhed er centralt.

## Fokus

**Betydeligt fokus på cybersikkerhed men plads til forbedring**

Læs mere

## Ledelse

**Forankring af cybersikkerhed i topledelsen**

Læs mere

## Uddannelse

**Uddannelse af medarbejdere i cybersikkerhed**

Læs mere

KONTAKT

**Karsten Biltoft**
Vicedirektør og chef for Finansiel Stabilitet

*kbi@nationalbanken.dk*
*+45 3363 6101*

FINANSIEL STABILITET

## Undersøgelsens resultater

**Betydeligt fokus på cybersikkerhed, men plads til forbedring**
Kerneaktørerne i den finansielle sektor i Danmark har et betydeligt fokus på cybersikkerhed, viser en undersøgelse, som Nationalbanken og Finanstilsynet har gennemført.

Kerneaktørerne omfatter systemisk vigtige banker og realkreditinstitutter samt infrastrukturselskaber. Infrastrukturselskaberne omfatter både betalings- og afviklingssystemer, som er kritiske, for at banker og realkreditinstitutter kan afvikle betalinger og værdipapirhandler, samt fælles datacentraler, som håndterer den operationelle drift for mange banker, realkreditinstitutter og betalings- og afviklingssystemer.

Der er stor variation i niveauet blandt undersøgelsens 15 respondenter og plads til forbedring hos de fleste. Det generelle billede af cyberrobustheden er baseret på en spørgeskemaundersøgelse, hvor deltagerne selv har angivet deres niveau på et overordnet plan. Detaljer om spørgeskemaet findes i boks 2.

**Større cyberrobusthed, hvor topledelsen er involveret**
Cybersikkerhed er ikke et teknisk emne, der berører en snæver kreds af medarbejdere, fx i it-afdelingen, da cyberangreb kan have alvorlige konsekvenser for hele forretningen. Det berører derfor alle i organisationen fra bestyrelse til medarbejdere.

### Betalingsinfrastrukturen

**Kerneaktører i den finansielle infrastruktur har deltaget i undersøgelsen**


**Cyberangreb**

Boks 1

Cyberrisiko er risikoen for udefrakommende elektroniske angreb rettet mod it-aktiviteter, herunder computere, servere, systemer, netværk, tjenester mv. Et cyberangreb vil typisk forsøge at finde og udnytte en svaghed i enten it-systemer, interne processer eller hos medarbejderne.

Den direkte effekt af et cyberangreb kan påvirke it-systemerne i institutter og hos betalings- og afviklingssystemer på følgende områder:

- *Tilgængelighed:* Hjemmesider, netbanker og kritiske forretningssystemer til afvikling af transaktioner sættes ud af drift, og tidskritiske betalinger kan blive forsinket.
- *Fortrolighed*: Fortrolige data kan blive delt med uvedkommende, og eventuelt offentliggjort.
- *Integritet*: Data kan blive kompromitteret.

Et cyberangreb, der rammer et stort finansielt institut, kan medføre faldende tillid, der kan lede til investor- og indskyderflugt. Hvis et kritisk betalings- eller afviklingssystem rammes, kan det sætte hele eller væsentlige dele af sektoren ud af drift i en periode. Et cyberangreb kan derfor potentielt true den finansielle stabilitet. Se mere om cyberrisiko i Danmarks Nationalbank, *Finansiel stabilitet*, 1. halvår 2016, kapitel 5 (link).

Undersøgelsen viser, at der er størst fokus på cybersikkerhed blandt de finansielle aktører, der har en bestyrelsesgodkendt strategi for cybersikkerhed, som er kendt bredt i organisationen – dvs. at både topledelsen, andre ledelsesniveauer og medarbejderne er involveret. Disse aktører har generelt også et højere niveau for cybersikkerhed på andre områder, hvilket peger på, at cybersikkerhedsstrategierne er bredt implementeret i disse aktørers organisationer. Undersøgelsen viser, at aktører med en bestyrelsesgodkendt cybersikkerhedsstrategi bl.a. også er bedre til at træne deres medarbejdere i cybersikkerhed og langt oftere tester deres beredskabsplaner specifikt mod cyberhændelser.

Ledelsen kan fremme arbejde med cybersikkerhed gennem krav og forventninger for virksomhedens arbejde med cybersikkerhed. Krav og forventninger har til formål at specificere, hvordan virksomheden identificerer, styrer og håndterer risici relateret til cyber. Strategien skal imidlertid også bundfælde sig i hele organisationen blandt medarbejdere på alle niveauer. Derudover kan niveauet af cybersikkerhed styrkes og holdes ved lige ved, at de udførende niveauer har fokus på at benytte målinger og kontroller som udgangspunkt for at rapportere til ledelsen, så ledelsen kan benytte læring fra den modtagne feedback til at justere de mål og krav, de har udstukket.

Involvering af hele organisationen kan være en stor forandring, som kræver en indsats for at lykkes, og at topledelsen går forrest og viser vejen.[1] For at støtte implementeringen af en cybersikkerhedsstrategi er det vigtigt at anvende effektive virkemidler. Det kan fx være at præsentere behovet for ændringen på en måde, som appellerer til forskellige typer af medarbejdere, at opstille gode rollemodeller, at give lederne feedback på, hvordan de fremstår som rollemodeller, at opbygge medarbejdernes kompetencer til at udføre forandringerne og at sørge for, at medarbejderne har tid til at indarbejde forandringerne i praksis.[2]

**Der skal arbejdes struktureret med kortlægning af cyberrisici**

Risikostyring er en løbende proces til identificering, vurdering og håndtering af risici. Som led i god it-sikkerhed og som grundlag for at kunne lægge en effektiv strategi for styring af cyberrisiko, er det nødvendigt at arbejde struktureret med kortlægning af kritiske forretningsområder og de systemer og processer, som understøtter disse.

Endvidere skal konkrete risici identificeres på et tilstrækkeligt detaljeret niveau til, at der kan tages beslutning om, hvordan hver enkelt risiko skal håndteres. Når risici er formelt identificeret, øges sandsynligheden betydeligt for, at risici håndteres på en passende måde. Passende håndtering indebærer, at organisationen beskytter sig mod risici, ruster sig til at opdage om risici materialiserer sig, samt udarbejder og tester planer for genopretning af driften, hvis risici har resulteret i en hændelse. I besvarelserne på spørgeskemaet kan der ses en tydelig overensstemmelse mellem de respondenter, som specifikt har identificeret cyberrisici i deres risikovurdering og de respondenter, som fx får testet deres beredskabsplaner mod cyberhændelser.

Endelig bør resultater fra det daglige arbejde med cyberrisici – kontroller, hændelser mv. – løbende indarbejdes i organisationens styring af cyberrisiko for at opnå de bedste resultater.

**Alle medarbejdere skal trænes i cybersikkerhed**

Cyberkriminelle benytter i stigende grad bl.a. spear-phishing, som er målrettet enkeltpersoner i en organisation.[3] Spear-phishing er målrettede forsøg på at franarre følsomme oplysninger fra folk med henblik på misbrug, fx via e-mail eller en hjemmeside. En organisations medarbejdere kan derfor være en indgang for cyberkriminalitet, uanset hvor sikre organisationens it-systemer ellers er, og det er derfor nødvendigt, at alle medarbejdere løbende uddannes og trænes i god adfærd i cyberspace, fx håndtering af e-mails og usb-stik.

1 Undersøgelser viser, at kun 3 ud af 10 forandringsprojekter lykkes med at blive forankret i den organisation, som indfører forandringen.

2 Der eksisterer en omfattende litteratur om forandringsledelse. Se fx Scott Keller and Carolyn Aiken, *The Inconvenient Truth About Change Management. Why it isn't working and what to do about it*, McKinsey & Company, 2008.

3 Jf. bl.a. Forsvarets Efterretningstjeneste og Center for cybersikkerheds *Efterretningsmæssig Risikovurdering 2015* (link) og *Sikkerhedsvejledning: Spear-phishing – et voksende problem* (link).

## Cyberrobusthed i den finansielle sektor

Boks 2

Spørgeskemaundersøgelsen om cyberrobusthed hos kerneaktører i den finansielle sektor blev gennemført i 2016 i regi af det finansielle sektorforum for operationel robusthed, FSOR[1], der er et samarbejdsforum mellem myndigheder og vigtige aktører i den finansielle sektor i Danmark. Der blev benyttet en modificeret udgave af et spørgeskema udviklet af Bank of England (link). Spørgeskemaet giver et overordnet billede af følgende områder:

- Governance og ledelse
- Identifikation af risici
- Beskyttelse mod cyberrisici
- Opdagelse af cyberhændelser
- Reaktion på cyberhændelser og genoprettelse af driften.

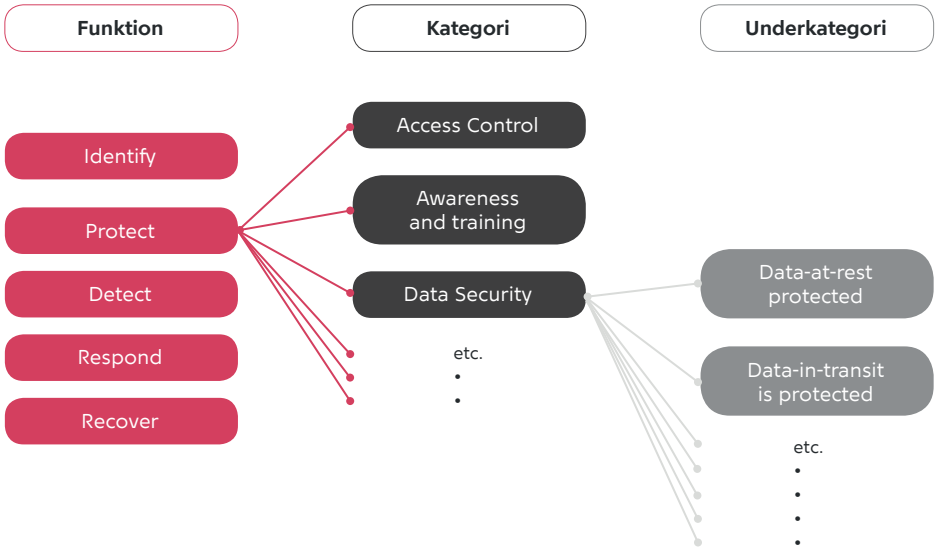
Spørgeskemaet stiller primært lukkede spørgsmål med svarmuligheder, der repræsenterer et spektrum fra en uformaliseret, ad hoc tilgang til cybersikkerhed til en formaliseret, konsistent og risikobaseret tilgang, hvor organisationen løbende tilpasser sig. En lignende graduering af cybersikkerhedsniveau kan findes fx i NIST Cybersecurity Framework Tiers, som definerer fire niveauer af cybersikkerhed med en stigende grad af forfinelse og kompleksitet i organisationens styring af cyberrisiko på hvert niveau.

De ovennævnte fem områder i spørgeskemaet indgår i diverse standarder for cybersikkerhed, jf. fx NIST Cybersecurity Framework (link), CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (link) og G7 Fundamental elements of cybersecurity for the financial sector (link).

Især CPMI-IOSCO's Guidance fremhæver vigtigheden af, at øverste ledelse er involveret i at opretholde en passende cybersikkerhed og er ansvarlige for, at arbejdet med cybersikkerhed forankres i hele organisationen samt hos serviceleverandører.

NIST Cybersecurity Framework giver vejledning i, hvordan kritisk infrastruktur kan styre cyberrisici og opbygge deres cybersikkerhed. Kernen er et sæt af funktioner (aktiviteter): "Identify", "Protect", "Detect", "Respond" og "Recover". Funktionerne opdeles yderligere i kategorier og underkategorier, for at nå frem til et detaljeret, operationelt niveau. Et eksempel på opdelingen i underkategorier ses i figur B.1.

### NIST Cybersecurity Framework Core




Kilde: NIST Cybersecurity Framework (link).

1. For yderligere information om FSOR, se www.nationalbanken.dk (link).

Medarbejdergrupper med kritiske funktioner og adgange til organisationens følsomme data har særlig høj risiko for at blive udsat for et cyberangreb. Disse medarbejdere er særligt attraktive mål for hackere, som fx forsøger at lægge malware på it-udstyr eller opsnappe passwords mv. Derfor skal disse medarbejdere være særligt opmærksomme på cyberangreb, og organisationen kan med fordel give dem ekstra træning i cybersikkerhed.

Undersøgelsen viser, at halvdelen af spørgeskemaets respondenter ikke konsekvent uddanner alle medarbejdere i cybersikkerhed. En tredjedel gennemfører særlig træning af højrisikomedarbejdere.

**Test beredskabsplaner mod cyberhændelser**

Cyberangreb kan have nogle særlige karakteristika i forhold til andre operationelle hændelser, og det er derfor vigtigt, at en organisations beredskabsplaner testes specifikt mod cyberhændelser. De særlige karakteristika omfatter, at nye typer af angreb udvikles løbende, de kan være sværere at opdage, varigheden kan potentielt være betydeligt længere end ved andre typer operationelle hændelser, og de kan ramme driftscentre, som ellers er teknisk uafhængige, samtidigt.

Test af beredskabsplaner er generelt et nyttigt værktøj til at udvikle og forbedre planerne. Det er centralt, at fundne resultater fra test såvel som fra andre kilder løbende rapporteres og indgår i arbejdet med cybersikkerhed.

Særlig lærerigt kan det være at udføre omfattende test af alle beredskabsplaner samlet, så man får kontrolleret, at alle dele af planerne spiller sammen og ikke kun fungerer enkeltvist. En faktisk cyberhændelse vil kunne påvirke flere områder samtidig. Spørgeskemaundersøgelsen viser, at omkring halvdelen af respondenterne ikke har testet deres beredskabsplaner mod en cyberhændelse. Af de resterende har halvdelen testet planerne samlet, mens den anden halvdel nøjes med at teste delplaner hver for sig. For at få fuldt udbytte af at teste beredskabsplaner mod cyberhændelser skal organisationen have et robust fundament bestående af en forankring af cybersikkerhedstiltag hos både ledelse og medarbejdere, et formaliseret risikostyringsprogram samt værktøjer til at opdage cyberangreb.

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

**Søren Truels Nielsen**
*stn@nationalbanken.dk*

**Katrine Skjærbæk Rasmussen**
*ks@nationalbanken.dk*

FINANSIEL STABILITET

DANMARKS NATIONALBANK