DANMARKS NATIONALBANK

1. SEPTEMBER 2021 — NR. 20

Hvor cyber-robust er den finansielle sektor i Danmark?

- Nationalbankens undersøgelser viser en højere cyberrobusthed i dag end i 2018. De centrale aktører i den finansielle sektor har et stærkt ydre forsvar og har fået flere værktøjer til at opdage og reagere på cyberangreb.
- Risikoen for, at avancerede hackergrupper bryder igennem det ydre forsvar, kan ikke elimineres.
- Det er vigtigt, at sikkerheden på indersiden af virksomhederne styrkes, at kritiske data beskyttes yderligere, og at evnen til sikkert og effektivt at genoprette centrale systemer efter et cyberangreb fortsat forbedres.

I alvorlige tilfælde kan et cyberangreb blive systemisk og skabe finansiel ustabilitet. Som følge af den systemiske risiko undersøger Nationalbanken den finansielle sektors robusthed på cyberområdet. Det sker bl.a. gennem en spørgeskemaundersøgelse, der på baggrund af respondenternes selvevalueringer skaber et overblik over cyberrobustheden i den finansielle sektor. Spørgeskemaet giver input til initiativer, der iværksættes for at adressere de væsentligste cyberrisci i sektoren. Samtidig kan deltagerne anvende resultaterne til at benchmarke sig mod hele respondentgruppen.

Nationalbanken gennemførte i sommeren 2020 den tredje spørgeskemaundersøgelse

I spørgeskemaundersøgelsen i 2020 selvevaluerede de samfundskritiske banker, realkreditinstitutter, datacentraler og infrastrukturselskaber deres aktuelle cyberrobusthedsniveau. Tilsvarende undersøgelser blev gennemført i 2016 og 2018. Dog er barren i undersøgelserne løftet i takt med den løbende udvikling i risici. Således tilpasses spørgsmål og svarmuligheder de konkrete udfordringer, som respondenterne står over for. Undersøgelsernes form og indhold er beskrevet nærmere i boks 1, og undersøgelsens overordnede resultater præsenteres i de følgende afsnit.

Fremskridt i arbejdet med organisation, strategi og ledelsesansvar

Sammenlignet med de tidligere undersøgelser indikerer besvarelserne fra 2020 et løft i respondenternes tilrettelæggelse, organisation og udmøntning af ledelsesansvar på cyberområdet (governance). Langt de fleste respondenter angiver, at den overordnede strategi og ramme for risikostyringen fastlægges af virksomhedernes topledelser, dvs. direktion og bestyrelse. Da truslen fra cyberangreb potentielt udgør

en risiko for de finansielle virksomheders forretning, hører fastlæggelsen af det strategiske fokus og prioritering af arbejdet med cyberrobusthed naturligt til på øverste ledelsesniveau.

Højt niveau i beskyttelsen mod cyberangreb

Perimetersikkerhed, dvs. evnen til at beskytte systemer og netværk mod udefrakommende cyberangreb (protect), er et område, som den finansielle sektor historisk set har haft stort fokus på. Det skyldes bl.a., at finansielle virksomheder siden halvfemserne, hvor digitaliseringen for alvor begyndte at tage fart, har været et oplagt mål for cyberkriminelle. På den baggrund er der opbygget en langvarig erfaring med beskyttelse mod udefrakommende angrebsforsøg.

Resultaterne fra den nyeste undersøgelse indikerer yderligere fremskridt. For eksempel er det positivt, at alle respondenter angiver, at der er implementeret flere lag af sikkerhed for at sikre, at virksomhedernes netværk er effektivt segregeret[1] og beskyttet. Ligeledes har alle nu formaliserede programmer for træning og uddannelse af medarbejdere, der har til formål at øge opmærksomheden på god praksis, så risikoen for kompromittering kan begrænses.

Mere og bedre overvågning

Da de teknikker og taktikker, som cyberkriminelle benytter sig af, løbende bliver mere sofistikerede, kan den ydre beskyttelse af systemer ikke stå alene. Erfaringer fra cyberangreb i både Danmark og udlandet viser, at de mest avancerede trusselsaktører har de fornødne ressourcer, teknikker, tid og tålmodighed til at kunne bryde igennem de ydre forsvar af selv velbeskyttede virksomheder. Et eksempel er kompromitteringen af SolarWind Orion-platformen, der ramte flere store virksomheder verden over, og som er nærmere beskrevet i boks 2. Det er derfor positivt, at besvarelserne af de spørgsmål, der omhandler arbejdet med overvågning af systemer og netværk for at opdage afvigelser fra normal aktivitet (detect), indikerer klare forbedringer sammenlignet med tidligere.

Besvarelserne peger bl.a. på fremgang i arbejdet med at udvikle og vedligeholde en baseline for netværks- og systemaktivitet, hvilket er en forudsætning for at understøtte en effektiv overvågning, der identificerer unormal adfærd. Samtidig angiver de fleste, at de har implementeret alarmer i deres overvågningssystemer, der er knyttet direkte til hændelseshåndteringen, så responsplanerne aktiveres automatisk, hvis alarmerne går.

Samlet set er arbejdet med system- og netværksovervågning blandt de områder i undersøgelsen, hvor aktørerne i den finansielle sektor har flyttet sig mest sammenlignet med 2018. Det er vigtigt, at tendensen fastholdes, så der fortsat sker fremgang. Der er stadig forbedringspotentialer, fx i forhold til omfanget af systemer og netværk, der overvåges, og i forhold til frekvensen for hvor ofte de genkendelsesmønstre, som opsporingen baserer sig på, opdateres.

Forbedringspotentiale i styringen af cyberrisiko og informationsaktiver

Undersøgelsen fra 2020 peger også på andre områder, hvor niveauet kan løftes. Et område, der samlet set kan forberedes, er arbejdet med identifikation og vurdering af cyberrisici og styringen af informationsaktiver, dvs. hardware, software, systemer, data mv. (identify).

Det er vigtigt, at de systemer, processer og data, der understøtter samfundskritiske forretningsaktiviteter, er identificeret, risikovurderet og klassificeret efter kritikalitet. Alle institutioner bør som minimum have et samlet overblik over deres informationsaktiver, fx i form af en samlet database.[2] Besvarelserne viser, at flere respondenter med fordel kan indføre mere systematik i styringen af informationsaktiver, herunder også i den måde udløbsdatoerne på alt kritisk hard- og software overvåges. De aktiver, der er udløbet og derfor ikke længere supporteres, kan udgøre potentielle sårbarheder. Alle respondenter har etableret formaliserede processer for opfølgningen på sårbarheder i hardware/software, men for nogle respondenter kan frekvensen og systematikken i opfølgningen med fordel forøges.

Behov for øget fokus på arbejdet med databeskyttelse og recovery

Der er gennem de seneste år sket en udvikling i kompleksiteten på cyberområdet, hvilket bl.a. har givet

1 Netværkssegregering indebærer udvikling og håndhævelse af et regelsæt til at styre den trafik, der løber mellem virksomhedens kritiske netværk og andre mindre følsomme netværk, som fx internettet.

2 En mulighed er at etablere af et CMDB-system (Configuration Management Database), hvor oplysninger om hardware- og softwareaktiver løbende kan opdateres og gemmes.

Nationalbankens spørgeskemaundersøgelser om cyberrobusthed

Boks 1

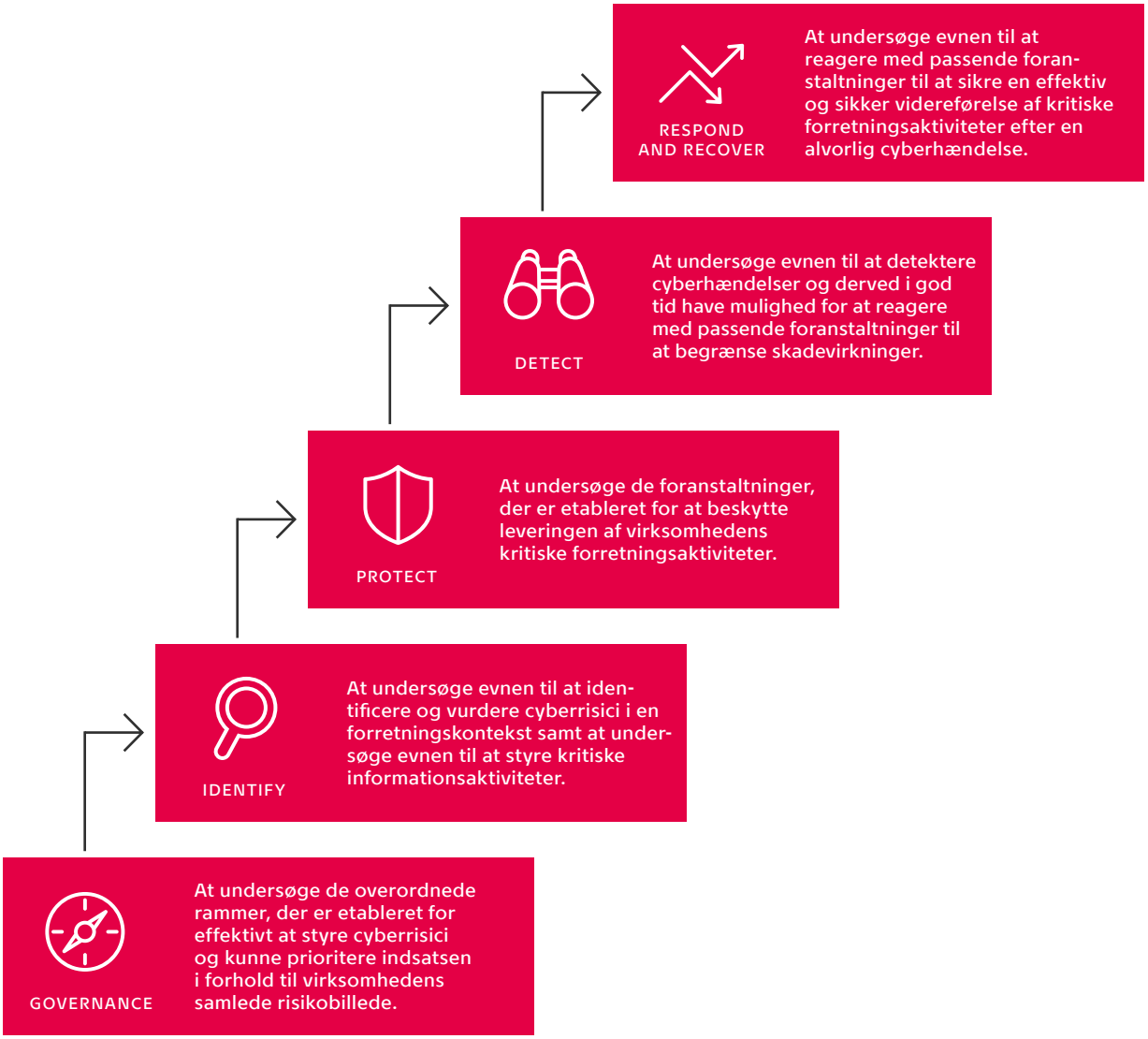
Formål og metode
Formålet med spørgeskemaundersøgelsen er at give et overblik over det aktuelle cyberrobusthedsniveau blandt de væsentligste aktører i den finansielle sektor. Resultaterne baserer sig på respondenternes selvevalueringer, og der foretages ingen efterprøvning af svarene.

Spørgeskemaet
Nationalbankens spørgeskemaundersøgelser er baseret på en tilpasset udgave af et spørgeskema, der er udviklet af Bank of England (*link*). Skemaet indeholder spørgsmål til 5 overordnede områder om cyberrobusthed, der er nærmere beskrevet i figuren herunder.

Hvert spørgsmål har 4 konkrete svarmuligheder, der afhænger af, hvor formaliseret, konsistent og risikobaseret en tilgang hver organisation har til det emne, der spørges til. En tilsvarende graduering af robusthedsniveauet kan findes i fx NIST Cybersecurity Framework Tiers[1], som definerer 4 niveauer af cybersikkerhed med en stigende grad af forfinelse og kompleksitet i organisationens styring af cyberrisiko.

Fortsættes

Spørgeskemaets områder og deres formål



1. NIST Cybersecurity Framework er et amerikansk rammeværk, der på baggrund af erfaringer fra en lang række virksomheder i forskellige sektorer sætter standarder og giver anbefalinger til en organisations arbejde med cybersikkerhed.

Nationalbankens spørgeskemaundersøgelser om cyberrobusthed Boks 1
fortsat

Udover at undersøge niveauet på de enkelte områder giver besvarelserne også en indikation af, hvilken måde de enkelte respondenter arbejder med cyberrobusthed på. Det er fx vigtigt, at hver respondent som noget af det første har udarbejdet en overordnet og ledelsesgodkendt strategi, der sikrer, at prioriteringen og retningen i arbejdet med cyberrobusthed er tilpasset virksomhedens samlede risikobillede.

I 2020 besluttede Nationalbanken at udvide spørgeskemaet med en række detaljerede spørgsmål om respondenternes arbejde med datasikkerhed og evne til at sikre en effektiv og sikker genopretning efter et cyberangreb. Baggrunden var, at de tidligere undersøgelser viste, at respondenterne samlet set er nået langt med etableringen af overordnede rammer og med beskyttelsen af systemerne og netværk. Det betyder, at der i mere detaljeret grad var plads til at fokusere på særlige aspekter udvalgt ud fra en risikobaseret tilgang.

Deltagere
De systemisk vigtige banker, realkreditinstitutter, datacentraler og infrastrukturselskaber har deltaget i undersøgelserne i hhv. 2016, 2018 og 2020. Som noget nyt deltog også en gruppe af forsikrings- og pensionsselskaber og flere centrale leverandører i den seneste undersøgelse. Med udvidelsen af deltagerkredsen giver undersøgelsen bredere indsigt i det aktuelle niveau af cyberrobusthed på tværs af forskellige aktører i den finansielle sektor. I denne analyse fokuseres dog alene på besvarelserne fra de deltagere, der også har deltaget i de foregående to undersøgelser.

sig udslag i flere alvorlige cyberangreb med kritiske følger, heraf flere i Danmark. Som følge af udviklingen i risikobilledet besluttede Nationalbanken at udvide spørgeskemaundersøgelsen i 2020 med en række detaljerede spørgsmål om respondenternes arbejde med datasikkerhed og evnen til at sikre en effektiv og sikker genopretning efter et cyberangreb (recovery).

Databeskyttelse og recovery er tæt beslægtede områder: Hvis kritiske data ikke er tilgængelige, vil det i væsentlig grad påvirke systemernes evne til at genoprette driften.

Brugen af kryptering og backup er centrale elementer i en effektiv databeskyttelse. Det er vigtigt, at de løsninger, der anvendes, er nøje tilpasset de systemer og den infrastruktur, som den enkelte virksomhed benytter sig af. Det bør ske i tæt samarbejde med eksterne leverandører, hvis lagringen og dermed også beskyttelsen af data varetages af en ekstern cloud- eller it-driftsleverandør. Samtidig medfører brugen af kryptering og backup også afledte risici, som bør vurderes og adresseres. Formålet er forhindre, at de løsninger, som anvendes, ikke i sig selv medfører sårbarheder, der vil kunne udnyttes at ondsindede hackere.

På recovery-området er det vigtigt, at alle centrale aktører har udarbejdet og vedligeholder en specifik cyberberedskabsplan, der målrettet adresserer genopretning af it-systemer og videreførelse af kritiske forretningsområder efter en cyberhændelse. Planen bør løbende testes ud fra en risikobaseret tilgang, der tager udgangspunkt i de ekstreme, men plausible scenarier, som et cyberangreb kan forårsage.

Der er stor variation i respondenternes svar til spørgeskemaundersøgelsens spørgsmål om databeskyttelse og recovery, og undersøgelsen viser, at der generelt er behov for øget fokus på disse områder. Det er vigtigt, at alle centrale aktører i den finansielle sektor løbende arbejder på at sikre, at deres aktuelle foranstaltninger matcher udviklingen i risikobilledet.

Bredere samarbejde om operationel robusthed

Deltagerne i spørgeskemaundersøgelserne får detaljerede tilbagemeldinger på egne resultater. Disse tilbagemeldinger anvendes i de enkelte organisationer til at forbedre cybersikkerheden. Endvidere inviteres deltagerne til workshops, hvor viden om best practice deles blandt deltagere.

Alle aktører i det finansielle økosystem er individuelt ansvarlige for at sikre, at de har et tilstrækkeligt højt cyberrobusthedsniveau, og at de lever op til kravene i gældende standarder og i lovgivningen. Det inkluderer også styring af de risici, som den enkelte aktør påfører andre dele af systemet.

De tekniske og finansielle sammenhænge betyder, at cyberangreb kan sprede sig på tværs af institutioner og systemer i den finansielle sektor. Endvidere er nogle initiativer så ressourcetunge, at de kun kan løftes i fællesskab. Derfor giver det mening både for den enkelte institution og for samfundet, at sektoren i tillæg til det individuelle arbejde også samarbejder om at adressere cyberrisici.

På denne baggrund tog Nationalbanken i 2016 initiativ til at etablere Finansielt Sektorforum for Operationel Robusthed, FSOR[3], med deltagelse af de mest centrale aktører og myndigheder i den finansielle sektor. Der afholdes to årlige møder i FSOR, hvor der deles viden, rapporteres om fremdrift på FSOR's arbejdsspor, og nye initiativer besluttes. Mellem møderne arbejdes der med de aftalte initiativer i en række arbejdsgrupper. Aktuelle arbejdsspor omhandler bl.a. løbende analyse af systemiske risici, fælles kriseberedskab og fælles initiativer til at løfte niveauet for sektorens beskyttelse af kritisk data og til at styrke evnen til recovery efter et angreb.

Et andet centralt element i arbejdet med cyberrobusthed i den finansielle sektor er Nationalbankens testprogram TIBER-DK. TIBER står for Threat Intelligence Based Ethical Red-teaming og er et red-team-testforløb, hvor deltagerne testes gennem simulerede cyberangreb mod systemer i drift.

Hvor spørgeskemaundersøgelsen giver et bredt overblik over finanssektorens cyberrobusthed, tryksprøver TIBER-DK-testene den enkelte organisation i praksis. Man kan ikke bestå eller dumpe en TIBER-DK-test. Succeskriteriet er, at hver testdeltager får et stort læringsudbytte.

Der foregår således et betydeligt arbejde, både i de enkelte institutioner og i fællesskab i sektoren. Spørgeskemaundersøgelserne giver en indsigt i, hvordan dette arbejde har forbedret sektorens modenhed på cyberområdet.

Flere eksempler på alvorlige cyberangreb gennem de senere år

Boks 2

Markante eksempler i Danmark omfatter malware[1]-angrebet mod Maersk i juni 2017 og ransomware[2]-angrebene mod Demant i september 2019 og ISS i februar 2020, der i alle tilfældene medførte, at virksomhederne helt eller delvist mistede tilgængeligheden til kritiske it-systemer og data i en periode på en uge eller længere. Angrebene havde store forretningsmæssige konsekvenser og medførte tab som følge af tabt omsætning og udgifter til ekstern hjælp til genopretning. De tre angreb anslås tilsammen at have kostet virksomhederne mere end 3 mia. kr.

Der har også været en række eksempler på cyberangreb i udlandet, herunder også angreb mod den finansielle sektor. Fx blev den største bank på Malta i februar 2019 ramt af et cyberangreb mod bankens betalingssystemer. Cyberangrebet mod Bank de Valletta førte bl.a. til, at banken lukkede ned for alle interne og kundevendte systemer i en hel dag, herunder nedlukning af alle filialer og pengeautomater.

I december 2020 blev det afdækket, at en fjendtlig aktør havde foretaget ondsindede ændringer i opdateringer af SolarWinds Orion, som er en platform til netværksovervågning, der anvendes af mange store private virksomheder og offentlige organisationer over hele verden. Angrebet ramte en central leverandør i den danske finansielle sektor, men uden det havde reelle konsekvenser. De relevante systemer blev inddæmmet og analyseret, så snart kompromitteringen blev kendt. Angrebet var ikke målrettet mod systemer i den danske finansielle sektor, hvilket kan have været medvirkende til, at det kunne håndteres uden egentlige skadevirkninger.

Risikoen fra leverandørkædeangreb blev for nylig yderligere aktualiseret, da den svenske supermarkedskæde Coop i juni 2021 måtte lukke stort set alle sine 800 butikker i Sverige efter et hackerangreb mod den amerikanske software-leverandør Kaseya. Coop benyttede ikke selv det kompromitterede software, men blev ramt gennem den it-leverandør, der drifter kædens kassesystemer. Nedlukningen af butikker varede flere dage, før problemerne med kassesystemerne var løst.

1. Malware er en type ondsindet software, der er specielt designet til at forstyrre, beskadige eller få uautoriseret adgang til et computersystem.
2. Ransomware er en speciel type malware, der er designet til at blokere adgangen til et computersystem, indtil der er betalt en løsesum.

3 Læs mere om FSOR på Nationalbankens hjemmeside (*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
LANGELINIE ALLÉ 47
2100 KØBENHAVN Ø
WWW.NATIONALBANKEN.DK

Redaktionen er afsluttet
25. august 2021

Gustav Kaas-Jacobsen
Infrastructure Advisor
joj@nationalbanken.dk
FINANSIEL STABILITET

DANMARKS NATIONALBANK

KONTAKT

Teis Hald Jensen
Kommunikations- og presserådgiver
tehj@nationalbanken.dk
+45 3363 6066
SEKRETARIAT OG KOMMUNIKATION