DANMARKS NATIONALBANK

6. SEPTEMBER 2018 — NR. 12

Cyberrobustheden i den finansielle sektor

Løft i cyberrobusthedsniveauet

De fleste kerneaktører i den finansielle sektor har i en spørgeskemaundersøgelse vurderet, at de har løftet deres cyberrobusthedsniveau siden 2016. Få har ikke forbedret deres niveau, og de bør opprioritere cyberindsatsen.

Læs mere

Plads til forbedring

Alle aktører har fortsat områder, der kan forbedres. Det gælder fx i forhold til kortlægning af kritiske forretningsområder, hvor flere aktører med fordel kan inddrage de bagvedliggende informationsaktiver, systemer og data mere regelmæssigt i kortlægningen.

Læs mere

Højt cybertrusselsniveau

Trusselsniveauet forventes fortsat at være højt i de kommende år. Det er derfor vigtigt, at arbejdet med cyberrobusthed i den finansielle sektor også fremover matcher udviklingen i risikobilledet. Nationalbanken vil følge udviklingen tæt og gennemføre lignende undersøgelser af kerneaktørernes cyberrobusthedsniveau.

Læs mere

Undersøgelse af cyberrobustheden i den finansielle sektor Boks 1

Alvorlige cyberangreb kan i værste fald true stabiliteten i den finansielle sektor. Et af Nationalbankens overordnede formål er at bidrage til at sikre stabiliteten i det finansielle system. Derfor har Nationalbanken i samarbejde med Finanstilsynet undersøgt cyberrobustheden hos kerneaktører ved en spørgeskemaundersøgelse i den finansielle sektor i Danmark i 2018. Undersøgelsen er en opfølgning på en lignende undersøgelse fra 2016 og omfatter store banker og realkreditinstitutter samt centrale infrastrukturselskaber.

Løft i cyberrobusthedsniveauet

Kerneaktørerne i den finansielle sektor vurderer, at de samlet set er blevet mere cyberrobuste sammenlignet med niveauet i 2016[1]. Det er et af hovedresultaterne af en ny spørgeskemaundersøgelse, som er gennemført i foråret 2018. Fremgangsmåden for undersøgelsen er beskrevet i boks 2. Ligesom i 2016 er det de systemisk vigtige banker og realkreditinstitutter samt centrale infrastrukturselskaber, der har deltaget i undersøgelsen. Infrastrukturselskaberne inkluderer dels betalings- og afviklingssystemer, som er kritiske for, at banker og realkreditinstitutter kan gennemføre betalinger og værdipapirhandler, og dels fælles datacentraler, som håndterer den operationelle drift for mange banker, realkreditinstitutter og betalings- og afviklingssystemer.

Generelt viser undersøgelsen en betydelig fremgang i robusthedsniveauet sammenlignet med resultaterne fra 2016. For nogle af respondenterne er der tale om markant fremgang inden for alle kategorier. De fleste vurderer, at de har løftet sig på nogle parametre, og de bør derfor opprioritere cyberindsatsen på udvalgte områder. Få har ikke forbedret deres niveau, og de bør opprioritere cyberindsatsen og forbedre robusthedsniveauet.

I 2016 anbefalede Nationalbanken flere af respondenterne en række tiltag: at der skulle udarbejdes en bestyrelsesgodkendt cyberstrategi; at alle medarbejdere blev trænet i cybersikkerhed; at beredskabsplaner blev testet mod cyberhændelser; og endelig at der blev arbejdet struktureret med kortlægning af cyberrisici. Undersøgelsen indikerer, at der er sket positive fremskridt inden for alle anbefalingerne, om end i forskelligt omfang.

Højere robusthedsniveau, hvor topledelsen er involveret

Undersøgelsen viser, at de fleste respondenter angiver, at de nu har en bestyrelsesgodkendt cyberstrategi. Det er en positiv udvikling, og resultaterne viser også en klar tendens til, at aktører med en bestyrelsesgodkendt strategi har et højere niveau af cyberrobusthed på andre områder. Ledelsen kan således via strategien fremme arbejdet med cybersikkerhed, da strategien indeholder krav og forventninger til, hvordan virksomheden identificerer, styrer og håndterer cyberrisici.

Svarene viser også, at de fleste respondenter gennemfører effektivitetsmålinger for at vurdere, om de fastsatte målsætninger for cyberrobusthed indfries. Målingerne er vigtige redskaber for ledelsen til at vurdere tilstrækkeligheden og effektiviteten i arbejdet med cybersikkerhed.

Flere udbyder træning og uddannelse af medarbejdere i cybersikkerhed

Størstedelen af respondenterne angiver, at alle medarbejdere gennemgår regelmæssig awareness- og cybersikkerhedstræning. En organisations medarbejdere kan være indgang for cyberkriminalitet, uanset hvor sikre organisationens it-systemer ellers er. Cyberkriminelle benytter ofte angreb, der er målret-

1 Hovedkonklusionerne fra undersøgelsen i 2016 findes i Danmarks Nationalbank, Cyberrobusthed i den finansielle sektor, *Danmarks Nationalbank Analyse*, nr. 3, marts 2017 (*link*).

Spørgeskemaundersøgelse om cyberrobusthed i den finansielle sektor Boks 2

Danmarks Nationalbank og Finanstilsynet gennemførte i foråret 2018 spørgeskemaundersøgelsen om cyberrobusthed hos kerneaktører i den finansielle sektor. Undersøgelsen er den anden af sin slags i Danmark; den første blev gennemført i august 2016. Ligesom i 2016 blev der benyttet en modificeret udgave af et spørgeskema udviklet af Bank of England (*link*). Spørgeskemaet er baseret på forskellige standarder for cybersikkerhed, 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*). Spørgeskemaet indeholder spørgsmål til følgende fem kategorier:

1. Governance
2. Identifikation af risici
3. Beskyttelse mod cyberrisici
4. Opdagelse af cyberhændelser
5. Reaktion på cyberhændelser og genoprettelse af driften.

Resultaterne giver en indikation af det overordnede modenhedsniveau i sektoren
Spørgeskemaet stiller lukkede spørgsmål med svarmuligheder (A, B eller C), der repræsenterer et spektrum fra en uformaliseret ad hoc-tilgang til cybersikkerhed til en formaliseret, konsistent og risikobaseret tilgang, hvor organisationen løbende tilpasser sig. Respondenterne vurderer selv, hvilket niveau de ligger på inden for spørgeskemaets fem kategorier, og resultaterne giver på den baggrund en indikation af modenhedsniveauet. Denne analyse fokuserer på status, udvikling og spredning i respondenternes modenhedsniveau.

tet enkeltpersoner i en organisation. Angrebene sker typisk via phishingmails eller via inficering af hjemmesider, som offeret besøger. Derfor bør der fremadrettet også være mere fokus på særlig træning af højrisikomedarbejdere og opfølgning på effekten af træningen.

Markant flere respondenter øver sig på at håndtere cyberhændelser
Undersøgelsen fra 2018 viser, at markant flere end i 2016 gennemfører test af beredskabsplaner mod cyberhændelser. Et cyberangreb hos en systemisk vigtig bank, et realkreditinstitut eller et centralt infrastrukturselskab, der i alvorlig grad påvirker tilgængeligheden til systemer eller integriteten af data, vil hurtigt kunne få konsekvenser for hele det finansielle system i Danmark. Cyberangreb kan have særlige karakteristika i forhold til andre operationelle hændelser. Fx kan et cyberangreb vare betydeligt længere end andre operationelle hændelser, og cyberangreb kan på samme tid ramme driftscentre, som ellers er teknisk uafhængige. Derfor er det vigtigt, at kerneaktørerne tester evnen til at genoprette driften hurtigt, effektivt og sikkert.

Finansielt Sektorforum for Operationel Robusthed, FSOR, (*link*) etablerede i 2016 den finansielle sektors kriseberedskab, som skal håndtere alvorlige operationelle hændelser, herunder cyberangreb. Formålet med beredskabet er at sikre en koordineret indsats på tværs af sektoren, så en krises omfang og konsekvenser minimeres mest muligt. Beredskabet blev senest testet i efteråret 2017.

Struktureret arbejde med kortlægning af cyberrisici
Undersøgelsen viser, at respondenter med en struktureret tilgang til kortlægning af cyberrisici samlet set også har et højere niveau inden for de områder, der handler om at beskytte sig mod, opdage og reagere på cyberhændelser. Struktureret kortlægning af cyberrisici er et vigtigt element i at kunne lægge en effektiv strategi for styring af cyberrisici. Det kræver en formaliseret og konsistent tilgang, hvor organisationen løbende tilpasser sig udviklingen i risikobilledet. En ikke-formaliseret og inkonsistent tilgang kan betyde, at konkrete risici ikke identificeres rettidigt og på et tilstrækkeligt niveau til, at der kan tages beslutning om, hvordan arbejdet med hver enkelt risiko skal prioriteres og håndteres.

Fortsat plads til forbedring

Et højt cyberrobusthedsniveau kræver en kontinuerlig indsats, og der vil sandsynligvis altid være indsatsområder, der kan forbedres. Dertil kommer, at kapaciteten hos cyberkriminelle og statslige aktører er steget siden 2016, hvilket understreger, at niveauet og indsatsen for at bevare og højne niveauet også hele tiden skal forbedres. Med dette udgangspunkt i mente viser undersøgelsen, at de fleste respondenter vurderer, at deres cyberrobusthedsniveau generelt er steget, men også at der er plads til forbedring. De få, der endnu ikke har fået fulgt op på anbefalingerne fra 2016, opfordres til hurtigst muligt at følge op på disse anbefalinger. Undersøgelsen viser, at der er en række indsatsområder, der bør prioriteres fremadrettet, og som kan føre til et endnu højere cyberrobusthedsniveau. Eksempler på disse områder er angivet nedenfor.

Kortlægning af kritiske forretningsområder
En grundlæggende forudsætning for at kunne identificere risici er, at der regelmæssigt udarbejdes en detaljeret kortlægning af kritiske forretningsområder og de processer, som understøtter områderne. En anden vigtig forudsætning er, at aktørerne udarbejder og løbende vedligeholder et vejledende udgangspunkt for, hvordan den normale netværksaktivitet og datatrafik ser ud.

Undersøgelsen viser, at de fleste kerneaktører har etableret en rutinemæssig proces for kortlægning af kritiske forretningsområder. Samtidig viser undersøgelsen dog også, at bagvedliggende informationsaktiver, systemsammenhænge og data i flere tilfælde ikke indgår regelmæssigt i processen. Det kan i værste fald betyde, at væsentlige sårbarheder overses og dermed ikke inddrages i risikostyringen. Der opfordres derfor til, at de nødvendige informationsaktiver mv. fremadrettet indgår struktureret i kortlægningsprocessen.

Nye værktøjer til opdagelse af hackerangreb
Stigningen i avancerede cyberangreb understreger vigtigheden af at anvende sporingsværktøjer, der så tidligt som muligt kan opdage cyberhændelser, som allerede har materialiseret sig. Derfor opfordres til øget anvendelse af automatiserede sporingsværktøjer. Automatiserede sporingsværktøjer kan fx ved hjælp af analyser baseret på kunstig intelligens opdage uregelmæssigheder i den normale netværksaktivitet og i dataflow.

I tilknytning til ovenstående skal der fortsat gennemføres løbende sårbarhedsscanninger og også penetrationstest, dvs. en teknisk test, hvor man forsøger at trænge ind i et kritisk system. Det er essentielle redskaber i arbejdet med at opdage og afdække mulige huller i forsvarsværket.

Penetrationstest kan med fordel suppleres af andre testværktøjer, der i højere grad tester evnen til at opdage og reagere på angreb, der allerede har materialiseret sig. En mulighed er fx en såkaldt red team-test, der simulerer de teknikker, taktikker og procedurer, der aktuelt anvendes af avancerede hackergrupper. Nationalbanken og kerneaktørerne i den finansielle sektor er i foråret 2018 blevet enige om at etablere et dansk red team-testprogram. Etableringen blev annonceret i en pressemeddelelse fra Nationalbanken 8. februar 2018 (*link*). Det er vigtigt at anvende et bredt udvalg af redskaber for at kunne opdage avancerede hackerangreb som fx Advanced Persistent Threat, der kan være længe undervejs i systemerne og være svære at opdage.

Fortsat højt cybertrusselsniveau

Truslen fra cyberkriminalitet og cyberspionage mod den danske finanssektor er høj. Det vurderer Center for Cybersikkerhed i sin publikation "Cybertruslen mod finanssektoren" fra 2018 (*link*). Et flertal af aktørerne i den finansielle sektor peger også på, at cyberrisikoen er den risiko, der kan få størst betydning for den finansielle stabilitet i Danmark i de næste tre år, jf. boks 3. Det er dog ifølge Center for Cybersikkerhed mindre sandsynligt, at fremmede stater vil rette destruktive cyberangreb mod finanssektoren.

Samlet set er der behov for, at der i sektoren fortsat er fokus på at udvikle og forbedre cyberrobusthedsniveauet, så niveauet kontinuerligt modsvarer risikobilledet. Det er også baggrunden for, at Nationalbanken fortsat vil følge udviklingen på cyberområdet tæt i de kommende år og gennemføre nye undersøgelser af cyberrobusthedsniveauet.

Cyberrisiko og den finansielle sektor

Boks 3

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:* Kritiske forretningssystemer sættes ud af drift.
- *Fortrolighed:* Data kan blive delt med uvedkommende og eventuelt offentliggjort.
- *Integritet:* Data kan blive kompromitteret.

De seneste år har der i udlandet været angreb, hvor bankers systemer er blevet kompromitteret, og det derigennem er lykkedes at foretage uautoriserede betalinger via datanetværk til interbankbetalinger, fx SWIFT-netværket. Derudover har der været eksempler på angreb, hvor det er lykkedes at sprede malware til mere end 100 forskellige finansielle virksomheder i mere end 30 lande, jf. Center for Cybersikkerheds trusselsvurdering for finanssektoren fra 2018 *(link)*.

En undersøgelse fra Finanstilsynet fra maj 2018 viser, at forhold omkring cybersikkerhed er den risiko, som flest finansielle virksomheder tror, kan få betydning for den finansielle stabilitet i Danmark i de næste tre år.[1] I undersøgelsen nævner flere specifikt risikoen for angreb på større finansielle institutioner og den finansielle infrastrukturs betalings- og afviklingssystemer. Enkelte nævner begrænsede ressourcer og fokus på cybersikkerhed som risikofaktorer. Ud over direkte tab og skader forbundet med cyberangreb udtrykker respondenterne bekymring for et medfølgende tab af tillid til det finansielle system.

1. Se Finanstilsynet, Systemisk risiko – spørgeskemaundersøgelse, 31. maj 2018 (*link*).

OM ANALYSE

Som en konsekvens af Nationalbankens rolle i samfundet udarbejdes analyser af økonomiske og finansielle forhold.

Analyserne udkommer løbende og omfatter bl.a. vurderinger af den aktuelle konjunktursituation og den finansielle stabilitet.

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

Redaktionen er afsluttet
5. september 2018

Johan Gustav Kaas-Jacobsen
Principal Infrastructure Expert

FINANSIEL STABILITET

DANMARKS NATIONALBANK