CENTER FOR CYBERSIKKERHED

Trusselsvurdering

# Cybertruslen mod finanssektoren

1. udgave december 2020
Seneste opdatering juni 2022

**Indhold**


Cybertruslen mod finanssektoren ..... 3

Hovedvurdering ..... 3

Indledning ..... 4

Cyberkriminalitet ..... 5

De fleste angreb starter med phishing, der ikke er målrettet ..... 5
Phishing af kunder giver institutterne indirekte tab ..... 6
En infektion via spam-mails kan ende i et målrettet angreb ..... 7
Truslen fra målrettede ransomware-angreb er steget ..... 8
Truslen fra digitale bankrøverier består ..... 10
DDoS-angreb kan forstyrre sektorens online services ..... 11
Cyberkriminelle kan udnytte kapitalmarkedet ..... 12

Cyberspionage ..... 13

Fremmede stater har betydelige kapaciteter ..... 13
Cyberspionage kan både være politisk og økonomisk motiveret ..... 14

Leverandørtruslen ..... 15

Ransomware kan også ramme via forsyningskæden ..... 16

Cyberaktivisme ..... 18

Destruktive cyberangreb ..... 20

Cyberterror ..... 21

Trusselsniveauer ..... 22


CENTER FOR CYBERSIKKERHED


Kastellet 30 2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk


2. Udgave juni 2022

# Cybertruslen mod finanssektoren

Formålet med trusselsvurderingen er at opdatere finanssektoren om cybertruslen, så den bedre kan beskytte sig. Trusselsvurderingen henvender sig til beslutningstagere og risikoejere i myndigheder og institutter i sektoren. Trusselsvurderingen erstatter den tidligere trusselsvurdering fra august 2018 for den finansielle sektor.

Trusselsvurderingen er blevet opdateret juni 2022 med et tilpasset kapitel om truslen fra cyberaktivisme som følge af en ændring af trusselsniveauet beskrevet i CFCS' vurdering "CFCS hæver trusselsniveauet for cyberaktivisme mod Danmark fra LAV til MIDDEL" udgivet d. 18. maj 2022. Trusselsniveauet for cyberaktivisme er hævet fra **LAV** til **MIDDEL**. Den øvrige tekst er uændret.

# Hovedvurdering

- Truslen fra cyberkriminalitet mod den danske finanssektor er **MEGET HØJ**. Der er en vedvarende trussel fra cyberkriminelle, og nogle af deres angreb kan være avancerede og omfattende. Cyberkriminalitet kan potentielt forstyrre tilgængeligheden af den danske finanssektors ydelser. Det gælder f.eks. ransomware-angreb.

- Truslen fra cyberspionage er **HØJ**. Det er sandsynligt, at fremmede stater både har politiske og økonomiske interesser i at udføre cyberspionage mod virksomheder og myndigheder i den danske finanssektor.

- Truslen fra cyberaktivisme er hævet fra **LAV** til **MIDDEL**. CFCS har hævet trusselsniveauet på baggrund af aktivistiske cyberangreb udført mod europæiske NATO-lande i forbindelse med krigen i Ukraine. Det er muligt, at særligt pro-russiske hackere vil gå efter mål i Danmark, herunder finanssektoren.

- Truslen fra destruktive cyberangreb er **LAV**. Det er mindre sandsynligt, at fremmede stater vil rette destruktive cyberangreb mod dansk samfundsvigtig infrastruktur, herunder finanssektoren. Det er dog muligt, at den danske finanssektor kan blive påvirket af destruktive cyberangreb mod mål udenfor Danmark.

- Truslen fra cyberterror er **INGEN**. Alvorlige cyberangreb, hvor hensigten er at skabe samme effekt som mere konventionel terror, forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten er samtidigt begrænset.

# Indledning

Trusselsvurderingen beskriver den generelle cybertrussel mod den danske finanssektor. Det er anden gang, at Center for Cybersikkerhed (CFCS) udgiver en generel trusselsvurdering for finanssektoren.

Cyberangreb udgør fortsat en væsentlig og vedvarende trussel mod institutter i finanssektoren, deres kunder og samarbejdspartnere. Siden den generelle trusselsvurdering fra 2018 er truslerne fra aktivisme og terror sænket til henholdsvis **LAV** og **INGEN**. Derudover fastsætter CFCS nu et trusselsniveau for destruktive cyberangreb. Truslen fra destruktive cyberangreb er **LAV**.

Den mest udbredte måde, et cyberangreb starter, er fortsat via phishing. Samarbejdet mellem kriminelle grupper fortsætter i større økosystemer, og nogle aktører specialiserer sig i udpræget grad i at skabe adgang til ofre og sælge denne adgang videre til andre kriminelle. En ny tendens er, at målrettede ransomware-angreb er begyndt at ramme danske virksomheder. Den type angreb udgør nu en trussel mod mange sektorer, inklusive finanssektoren. Truslen fra digitale bankrøverier består, selvom der de seneste par år kun er set få offentligt kendte angreb. Stater og kriminelle benytter sig fortsat af mange af de samme værktøjer, og de benytter sig også i høj grad af at misbruge legitime programmer i cyberangreb.

Finanssektoren har en samfundsvigtig rolle i Danmark. 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 derved Danmarks nationaløkonomi. Det er vigtigt, at virksomhederne, infrastrukturen og ydelserne er tilgængelige, troværdige og stabile, så borgere og virksomheder benytter sektorens ydelser med fuld tillid til systemernes integritet.

Finanssektoren består af forskellige virksomheder, der varetager mange forskellige funktioner. Sektoren inkluderer i denne vurdering virksomheder, som er underlagt finansiel regulering samt relevante myndigheder for det finansielle område.

# Cyberkriminalitet

CFCS vurderer, at truslen fra cyberkriminalitet er **MEGET HØJ**. Det betyder, at det er meget sandsynligt, at institutter i den danske finanssektor vil blive udsat for forsøg på cyberkriminalitet inden for de næste to år.

Cyberkriminelle angriber på mange forskellige måder. Fælles for alle angrebsmetoderne er, at hackerne i sidste ende forsøger at få adgang til følsomme oplysninger eller systemer, som hackerne kan udnytte til at berige sig med økonomisk.

### De fleste angreb starter med phishing, der ikke er målrettet

Phishing er fortsat en effektiv metode til at angribe myndigheder, virksomheder og borgere på. Mange både større og mindre cyberangreb starter med, at en medarbejder bliver narret af en phishing-mail. Det sker på trods af, at størstedelen af den phishing, der rammer finanssektoren, er opportunistisk og til tider dårligt udført. Hackerne kan uden de store omkostninger sende et meget stort antal phishing-mails. Det øger risikoen for, at en medarbejder ved en fejl eller i uopmærksomhed kommer til at klikke på et link eller en vedhæftning i en phishing-mail.

**Phishing anvendes til mange formål, men oftest til**:
- Tyveri af brugernavn og kodeord til internettjenester, som mail, sociale medier, webbutikker etc.
- BEC-svindel, hvor ofret narres til at overføre penge til kriminelle.
- Installation af malware på ofrets computer.
- Få fodfæste i et it-netværk for yderligere kompromittering.
- Tyveri af anden sensitiv eller beskyttelsesværdig information.
- Tyveri af betalingskortoplysninger.
- Tyveri af NemID-oplysninger.

Hackere bruger bl.a. phishing- og spear phishing-mails til at skabe den første adgang til offerets systemer, hvorfra de kan bevæge sig videre til resten af organisationen. For at opnå det sender hackere eksempelvis spear phishing-mails til it-medarbejdere. Hackerne forsøger dermed at få adgang til it-medarbejdernes administratorrettigheder eller netværksværktøjer, som kan udnyttes til at trænge længere ind i organisationens systemer.

En anden tendens er, at hackere angriber HR-afdelinger med phishing-mails, der ligner jobansøgninger, men som har vedhæftninger, der indeholder malware. Hackere benytter sandsynligvis denne metode, fordi de forventer, at HR-afdelinger er nødt til at åbne sådanne mails. Hackerne kan dermed tro, at HR-afdelingerne udgør en nemmere vej ind i en organisations systemer. Det var eksempelvis ved hjælp af en falsk jobansøgning, at hackere kompromitterede Bangladeshs centralbank, som de efterfølgende stjal 81 mio. USD fra i 2016.

Hackere bruger også phishing-mails til BEC-svindel, hvor de narrer virksomheder eller myndigheder til at overføre penge til konti, som hackeren kontrollerer. De kriminelle forsøger ofte at få modtagerne af mailen til at tro, at anmodningen om

pengeoverførslen kommer fra ledelsen. I nogle tilfælde misbruger de kriminelle kompromitterede mailkonti, der faktisk tilhører ledende medarbejdere i organisationen. CFCS er ikke bekendt med, at der har været succesfuld BEC-svindel mod organisationer i den danske finanssektor. Der er dog løbende forsøg.

**Norfund taber cirka 10 mio. USD i et BEC-svindel**
Den norske statsejede investeringsfond, Norfund, blev i marts måned 2020 offer for, hvad der sandsynligvis var BEC-svindel. Det lykkedes aktøren at forfalske betalingsoplysninger til udbetaling af et mikrofinansieringslån til et cambodiansk institut, så ti mio. USD i stedet blev sendt til konti i Mexico.

**High frequency trader var offer for BEC-svindel**
Det amerikanske selskab, Virtu Financial, blev i maj 2020 offer for BEC-svindel for 6,9 mio. USD. En ledende medarbejders mail blev ifølge hacket og misbrugt til at sende instruktioner til regnskabsafdelingen om to pengeoverførsler til to forskellige banker i Kina.

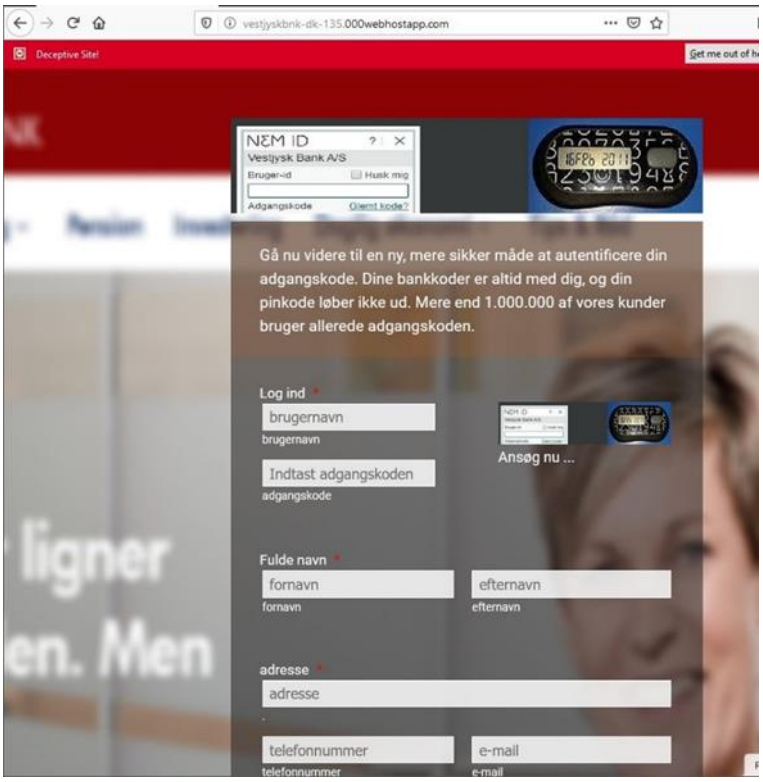
Phishing-mails kan også komme fra legitime samarbejdspartnere, som bliver misbrugt af cyberkriminelle. CFCS har kendskab til flere tilfælde, hvor danske virksomheder har modtaget mails fra betroede samarbejdspartnere, hvis mailkonti var blevet hacket. Ofte kom mailen som led i en samtale, der allerede er i gang mellem modtageren og afsenderen. Det er svært for modtageren at gennemskue, at det er en phishing-mail, da mailen ser ud til at komme fra en person eller virksomhed, modtageren kender og har tillid til. Hackerne kan via denne metode sprede sig fra én organisation til en anden.

Hackere har også brugt denne metode mod finanssektoren i Danmark. I et eksempel forsøgte hackere at sprede malwaren Ursnif. Hackerne kompromitterede en mailkonto og gennemgik de igangværende korrespondancer. De sendte derefter inficerede mails som svar, så de inficerede mails kom i naturlig forlængelse af samtalerne.

**Ursnif**
Ursnif er en malware, som bl.a. kan stjæle bankoplysninger, passwords og andre følsomme oplysninger fra offeret. Ursnif leveres typisk til offeret i Word eller Excel-dokumenter i spamkampagner. Cyberangreb med Ursnif er ofte rettet mod virksomheder.

### Phishing af kunder giver institutterne indirekte tab

Cyberkriminelle forsøger løbende at phishe oplysninger fra institutternes kunder, f.eks. ved hjælp af falske hjemmesider. I foråret 2020, da COVID-19-pandemien påvirkede Danmark særligt meget, oprettede cyberkriminelle mange falske hjemmesider. Hackerne forsøgte bl.a. at misbruge hjemmesiderne til at franarre følsomme oplysninger fra danskere, herunder oplysninger om NemID eller betalingskort. Nogle falske sider er næsten tro kopier af den originale hjemmeside. Det er ikke kun de største danske banker, som cyberkriminelle efterligner i deres phishing-forsøg.




*I august 2020 advarede Vestjysk Bank sine kunder om en falsk hjemmeside, som forsøgte af franarre NEMID fra bankens kunder.*

**En infektion via spam-mails kan ende i et målrettet angreb**

Hvis man som organisation bliver ramt at opportunistisk phishing, kan det bane vejen for større og mere målrettede cyberangreb, som kan have alvorlige konsekvenser for en finansiel organisation.

Der er cyberkriminelle grupper, der har specialiseret sig i at skabe adgang til så mange mål som muligt. De sælger eller giver adgangen videre til andre hackere, der så udfører mere målrettede cyberangreb mod de ramte organisationer.

"Målrettet" betyder ikke, at hackerne nødvendigvis på forhånd udvælger konkrete organisationer og aktivt går efter dem. Det betyder derimod, at hackerne ser på, hvilke organisationer, de har adgang til, og så målretter deres tid og indsats mod de ofre, de vil gå videre med. Det kan f.eks. være virksomheder, som hackerne forventer vil betale en meget stor løsesum i ransomware-angreb.

Malwaren Emotet er et eksempel på en malware, der ofte fordeles i spam, men som kan føre til cyberangreb med alvorlige konsekvenser. Emotet har i en årrække været målrettet den finansielle sektor og stjålet bankinformationer. Den bliver nu i stedet hovedsageligt brugt som indtjeningskilde for kriminelle, der videresælger og faciliterer adgange til mere målrettede angreb. Emotet er generelt en meget udbredt malware. Den har ramt et meget stort antal ofre verden over, også i Danmark.

Ligesom mange andre cyberkriminelle udvikler operatørerne af Emotet løbende deres malware og udskifter deres samarbejdspartnere. I 2020 et det f.eks. set, at Emotet i højere grad er begyndt at installere malwaren Qakbot, fremfor Trickbot. Qakbot kan f.eks. blive brugt til at installere ransomwaren ProLock på ofrets system. Aktøren bag

ProLock har krævet løsesumme på op mod 660.000 USD, og de har ødelagt ofres data, da deres dekrypteringsløsning ikke virkede ordentligt. Det understreger, hvor alvorlig en infektion med Emotet kan ende med at blive.

### Truslen fra målrettede ransomware-angreb er steget

CFCS har det seneste år set en stigende trussel fra målrettede ransomware-angreb. Den øgede trussel fra ransomware gælder også for den finansielle sektor. På globalt plan ses det nu næsten dagligt, at større internationale virksomheder er ofre for omfattende ransomware-angreb. I målrettede cyberangreb, bruger hackerne tid på at bevæge sig videre i kompromitterede organisationers systemer. De arbejder i høj grad manuelt fremfor at bruge automatiserede værktøjer til hacking. Hackernes mål er at kryptere store eller centrale dele af en organisations systemer, så de kan afpresse store pengebeløb fra dem.

CFCS har ikke kendskab til, at danske finansielle organisationer har været udsat for vellykkede målrettede ransomware-angreb. Der har dog været forsøg. Mindst en organisation har været kompromitteret af malware, der primært bliver brugt forud for målrettede ransomware-angreb. Angrebet blev dog hurtigt stoppet af it-sikkerhedsorganisationen.

I udlandet er der i 2020 set flere ransomware-angreb, der har ramt organisationer i den finansielle sektor. Der har i 2020 også været succesfulde ransomware-angreb mod udenlandske leverandører, som danske finansielle institutter benytter. Angrebene berørte ikke de danske institutters systemer eller information. Leverandørtruslen beskrives nærmere senere i vurderingen.

Den seneste udvikling i målrettede ransomware-angreb er, at hackerne også stjæler data fra deres ofre for at afpresse dem yderligere. Flere kriminelle grupper truer således med at offentliggøre følsomme data, hvis ofrene ikke betaler løsesummen. Andre forsøger at sælge information til interesserede købere. Blandet andet er aktørerne kendt som Sodinokibi eller REvil begyndt at afholde online auktioner, hvor de sælger ofres data til højstbydende.

**Europæisk bank fik lækket data i ransomware-angreb**

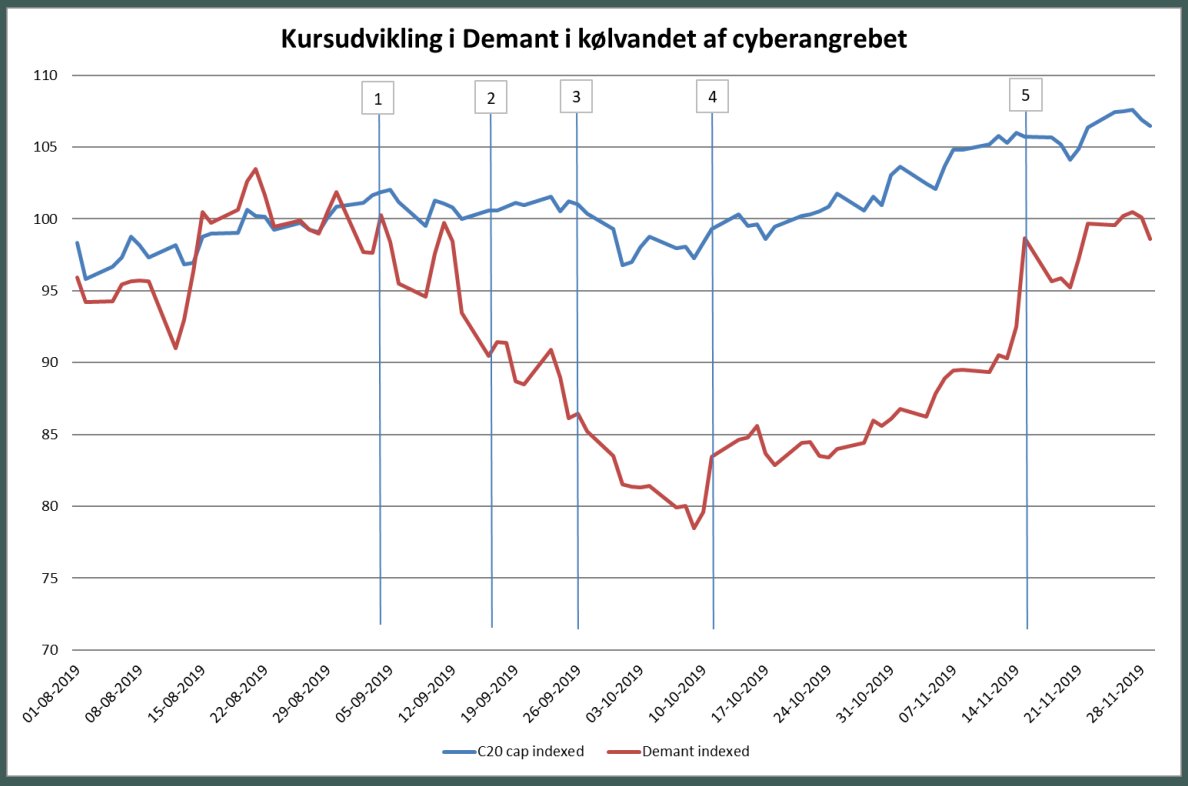
Ifølge åbne kilder blev den Kosovobaserede bank, Banka Ekonomike, i starten af 2020 ramt af ransomwaren DoppelPaymer. Hackerne lækkede efterfølgende mere end 70 GB data, som bl.a. indeholdt information om kunders finansielle transaktioner, såsom kundenavne, kreditkortnummer, oplysninger om indkomst og information om kunders lån. Lækket indeholdt også følsomme data om bankens medarbejdere.

Det er meget sandsynligt, at cyberkriminelle er opmærksomme på værdien af særlig følsomme data, som sektoren kan have adgang til. Det skyldes bl.a., at læk af data om finansielle virksomheder og deres kunder, såsom de såkaldte FinCen files, har fået stor mediebevågenhed. Det er sandsynligt, at cyberkriminelle vil forsøge at få fat i sådan information for at kunne lægge et stort pres på deres ofre.

De økonomiske konsekvenser for nogle af de danske og internationale virksomheder i andre sektorer, som er blevet ramt, har været ganske omfattende. Det gælder i forhold til nedetid, indtjening, genopretning og usikkerheden, der følger i perioden

efter. Angrebene og håndteringen af dem har også påvirket kursudviklingen for børsnoterede virksomheder.

**Cyberangreb og håndteringen af dem kan påvirke aktiekurser**
Høreapperatkoncernen Demant blev ramt af ransomware i september 2019. Nedenfor er kursudviklingen for Demant-aktien (rød) i perioden før og efter angrebet. For at vise hvordan aktien klarede sig i forhold til resten af markedet (blå), er den illustreret i sammenhæng med det generelle aktieindeks C20.




Datakilde: Nasdaq

1: Demant offentliggør, at der er sket en IT-hændelse, som er relateret til cyberkriminalitet
2: Demant offentliggør, at selskabets systemer har været hårdt ramt, men at Demant nu har reaktiveret nøgle-it-infrastruktur
3: Demant offentliggør et forventet tab som følge af hændelse på op til DKK 650 mio., og at selskabet har fuldført genopretning af størstedelen af systemerne
4: Demant offentliggør, at de har fuldført genopretning af alle systemer
5: Demant offentliggør et positivt regnskab, hvor tabet fra cyberangrebet fastholdes i størrelsesordenen, som Demant tidligere havde udmeldt.

I kølvandet på angrebet var der en periode, hvor aktien faldt væsentligt i værdi ift. det generelle indeks. Det kan have været markedets udtryk for den usikkerhed, der var, indtil Demant fik genoprettet systemer og fik overblik over omfanget af skaden. Demant opgjorde det samlede tab til DKK 550-650 mio., men aktien tabte samlet cirka 10 mia. i markedsværdi i perioden fra angrebet blev offentliggjort til Demant igen var fuldt genoprettet. Herefter genvandt aktien stødt noget af det tabte. Efter en positiv regnskabsmeddelelse i november kom kursen tilbage på samme niveau som før cyberangrebet.

## Truslen fra digitale bankrøverier består

Der er en potentiel trussel fra målrettede cyberangreb i form af såkaldte digitale bankrøverier mod organisationer i den danske finanssektor. CFCS vurderer, at nogle hackerne bag denne type angreb er statsstøttede.

CFCS er bekendt med, at hackere, som muligvis har kapacitet til at udføre digitale bankrøverier, har angrebet institutioner i den danske finanssektor i 2019. I et af disse angreb har hackerne haft held med at få et indledende fodfæste inden angrebet blev opdaget.

En af aktørerne, der er kædet sammen med digitale bankrøverier, udgav sig i 2019 for at være fra det danske finanstilsyn i phishing-mails. Hackerne havde oprettet domæner, der til forveksling lignede Finanstilsynets og de misbrugte også navne på faktiske medarbejdere fra Finanstilsynet.

Misbrug af finansielle myndigheder i phishing-angreb er sandsynligvis motiveret af, at finansielle institutter ofte skal reagere meget hurtigt på forespørgsler fra myndigheder. Det kan øge sandsynligheden for, at modtageren reagerer på phishing-mailen. Den Europæiske Centralbank (ECB) bliver eksempelvis ofte misbrugt i kampagner af cyberkriminelle aktører.

**Hackere spoofede Finanstilsynets hjemmeside til indberetning af data**

I maj måned 2020 varslede Finanstilsynet om en side, som forsøgte at spoofe Finanstilsynets engelske indberetningsportal for finansielle virksomheder. Det er sandsynligt, at linket har været brugt i en phishing-kampagne.

Nogle forsøg på digitale bankrøverier er sandsynligvis også startet ved, at hackere har sendt falske jobopslag eller -ansøgninger til medarbejdere i udvalgte banker. Hackergruppen Lazarus benytter sig f.eks. ofte af falske jobopslag og til tider endda falske jobsamtaler.

**Lazarus har i årevis profiteret på at hacke**

Hackergruppen Lazarus har været aktiv i mange år blandt andet mod den finansielle sektor. Gruppen har stor kapacitet til at udføre cyberangreb og har udført velplanlagte og avancerede cyberangreb. Senest er den f.eks. begyndt at bruge filløse angrebstekniker.

Udover digitale bankrøverier har gruppen rettet cyberangreb mod kryptovalutabørser og såkaldte krypto-wallets. En årsag til gruppens fokus på kryptovaluta kan være, at det er lettere for gruppen at hvidvaske kryptovaluta end almindelig valuta. I åbne kilder har der også været rapporteringer om, at Lazarus er begyndt at bruge andre taktikker til at tjene penge, såsom målrettet ransomware-angreb, web-skimmere og BEC-svindel.

*Lazarus stod sandsynligvis bag hacket af Bangladeshs centralbank, hvor de stjal 81 millioner USD i 2016. Banken fik efterfølgende femten millioner tilbage fra et kasino i Filippinerne, som hackerne havde brugt til at hvidvaske en del af de stjålne penge. FOTO: Jason Arlan Raval/AP/Ritzau Scanpix*

**DDoS-angreb kan forstyrre sektorens online services**

Der er fortsat en trussel mod finanssektoren fra DDoS-angreb, også kaldet overbelastningsangreb. Organisationer i finanssektoren oplever jævnligt mindre kraftige DDoS-angreb, og mange af organisationerne har beskyttelse mod disse angreb.

DDoS-angreb har mange formål, herunder alt fra afbrydelse af tjeneste og services på nettet til spænding, chikane, sløring af cyberangreb eller f.eks. afpresning.

Flere europæiske finansielle institutter er i andet halvår af 2020 blevet udsat for afpresningsforsøg, hvor aktørerne bag krævede betaling for ikke at udføre DDoS-angreb. Betalingen skulle ske i Bitcoin og varierede i størrelse fra offer til offer. DDoS-angrebene mod europæiske organisationer var i de fleste tilfælde korte og kunne afværges af organisationernes normale værn for DDoS-beskyttelse.

I New Zealand, derimod, blev børsen The New Zealand Stock Exchange (NZX) i slutningen af august 2020 ramt af DDoS-angreb, der påvirkede børsens services. Handel på børsen blev afbrudt gentagne gange over flere dage.

## Cyberkriminelle kan udnytte kapitalmarkedet

Cyberkriminelle kan også forsøge at hacke sig til information fra danske børsnoterede institutter for at misbruge dem til insiderhandel. Et sådant angreb fandt sted i USA i 2016. Ifølge amerikanske myndigheder hackede to ukrainske mænd U.S. Securities and Exchange Commission (SEC) og stjal intern viden om amerikanske børsnoterede selskaber. Hackerne tjente både penge ved at sælge informationerne, og ved at videregive dem til børsmæglere og virksomheder, som de samarbejdede med, så de kunne profitere af insiderhandel. SEC er det amerikanske børstilsyn, som derfor har intern viden om børsnoterede selskaber. I Danmark varetages denne funktion af Finanstilsynet.

På mellemlangt sigt er det muligt, at cyberkriminelle vil forsøge at kompromittere og udnytte infrastrukturen på finans- og kapitalmarkeder, hvor der også findes en potentiel højere profit for cyberkriminelle. Sikkerhedsfirmaer påpeger blandt andet, at den komplekse og omfattende infrastruktur af kapitalmarkeder kan være et attraktivt mål, som hackere kan udnytte.

Kapitalmarkeder kan potentielt udnyttes på mange måder, f.eks. ved at forfalske handelsordrer eller ved at kompromittere infrastruktur omkring ejerskabsforhold af værdipapirer og manipulere med data for ejerskab. CFCS har ikke viden om, at denne type angreb endnu er sket. CFCS vurderer, at det vil kræve mange ressourcer og indgående viden om finans- og kapitalmarkeder at kunne misbruge kapitalmarkeders infrastruktur i cyberangreb.

# Cyberspionage

CFCS vurderer, at truslen fra cyberspionage mod den finansielle sektor er **HØJ**. Det betyder, at organisationer i den danske finanssektor sandsynligvis vil blive udsat for forsøg på cyberspionage indenfor de næste to år.

Udenlandske finansielle institutter er løbende udsat for forsøg på cyberspionage. CFCS vurderer, at det er sandsynligt, at det samme sker i Danmark. Spionage er mindre synligt end f.eks. cyberkriminalitet, som ofte medfører umiddelbare og synlige tab af værdier eller nedetid for offeret. Det gør, at der er et stort mørketal, når det kommer til cyberspionage.

### Fremmede stater har betydelige kapaciteter

Oftest udføres cyberspionage af fremmede stater eller statsstøttede hackergrupper. Hackere, der arbejder på vegne af fremmede stater har adgang til omfattende ressourcer. Ressourcerne består bl.a. af specialudviklet, avanceret malware og viden om sårbarheder, der endnu ikke er offentligt kendte, også kaldet nul-dags-sårbarheder.

På trods af at de har adgang til disse ressourcer, angriber statsstøttede hackergrupper ofte med de samme metoder, som de har brugt i årevis. Det skyldes, at de samme relativt simple angrebsmetoder stadig er effektive, da mange myndigheder og virksomheder fortsat er sårbare overfor dem. De anvender eksempelvis brute force-angreb eller udnytter kendte sårbarheder.

**Scanninger mod finanssektoren**
Der sker løbende scanninger mod organisationer i den danske finanssektor. Det er sandsynligt, at både cyberkriminelle og stater har udført rekognoscering ved hjælp af scanninger mod mål i den danske finanssektor. Selvom scanninger i sig selv er uskadelige, kan de være tegn på forberedelser til et cyberangreb.

Nogle statsstøttede hackere anvender også værktøjer til at hacke med, der i princippet er tilgængelige for alle. Det kan gøre det vanskeligere at adskille og identificere aktører og deres formål. En del af værktøjerne er oprindeligt udviklet til brug for white-hat hackere til at udføre it-sikkerhedstest af organisationer. Disse værktøjer er bl.a. Cobalt Strike, Empire Powershell og Mimikatz. De anvendes også i stor udstrækning af cyberkriminelle og i visse cyberaktivistiske miljøer.

Typisk kan en organisation reducere risikoen for at blive kompromitteret ved at gøre det svært for hackere at benytte simple angrebsmetoder mod dem. Jo vanskeligere det er for hackere at kompromittere deres mål med simple angrebsmetoder, desto flere ressourcer skal de bruge. Specialudviklet malware og viden om nul-dags-sårbarheder er sædvanligvis meget værdifuld og bliver derfor kun brugt relativt sjældent.

Fremmede stater bruger ofte en angrebsteknik, hvor de misbruger ofrenes egne programmer til at udføre cyberangreb. Teknikken er effektiv og kan bruges til at opnå samme mål, som hvis hackere havde angrebet med malware. Angrebsteknikken kaldes "living off the land". Den er svær at opdage, fordi hackerne udnytter legitime programmer på ofrets systemer. Der har været mange eksempler i udlandet på denne type angreb de seneste år. Der har også været eksempler i Danmark.

### Cyberspionage kan både være politisk og økonomisk motiveret

Meget af den viden, som findes hos myndighederne og institutterne i sektoren, er værdifuld for fremmede stater. Dels kan den type viden bruges til at informere om politiske eller strategiske beslutninger. Dels kan den udnyttes til at fremme staters økonomi og styrke deres nationale virksomheder.

Den politiske interesse i at spionere mod sektoren kan både være rettet mod følsomme informationer om bankernes kunder og mod oplysninger af relevans for staters økonomiske politik. Fremmede stater kan også forsøge at få kendskab til den finansielle sektors organisering, struktur, robusthed eller institutters individuelle forhold. Derudover kan personfølsomme oplysninger (PII) have værdi for en fremmed stat. Stater kan f.eks. være interesserede i at indhente på bestemte målpersoner. PII om en enkelt person kan også bidrage til at målrette fremtidige cyberangreb mod personen.

Viden relateret til fremmede staters økonomiske interesser kan bl.a. omhandle handelsaftaler og investeringer. Fremmede stater kan også styrke deres økonomi ved at kopiere systemer, teknologier eller ved at indsamle intern viden om danske selskaber fra myndigheder og institutter i finanssektoren. Denne viden kan stater udnytte i forhandlinger eller videregive til deres nationale virksomheder, der konkurrerer med de danske.

Cyberspionage kan gå forud for andre trusler, såsom destruktive cyberangreb og hack og læk angreb. Disse trusler beskrives nærmere senere.

**EU sanktionerer for første gang hackere**

I forlængelse af en række cyberangreb mod europæiske virksomheder og myndigheder indførte EU ved Rådets gennemførelsesforordning (EU) 2020/1125 af 30.juli 2020 for første gang sanktioner for hacking. Sanktionerne kom som følge af anklager om, at grupper og personer fra Rusland, Kina og Nordkorea havde udført cyberspionage. Nogle af de sanktionerede grupper har angrebet finanssektoren i andre lande.

# Leverandørtruslen

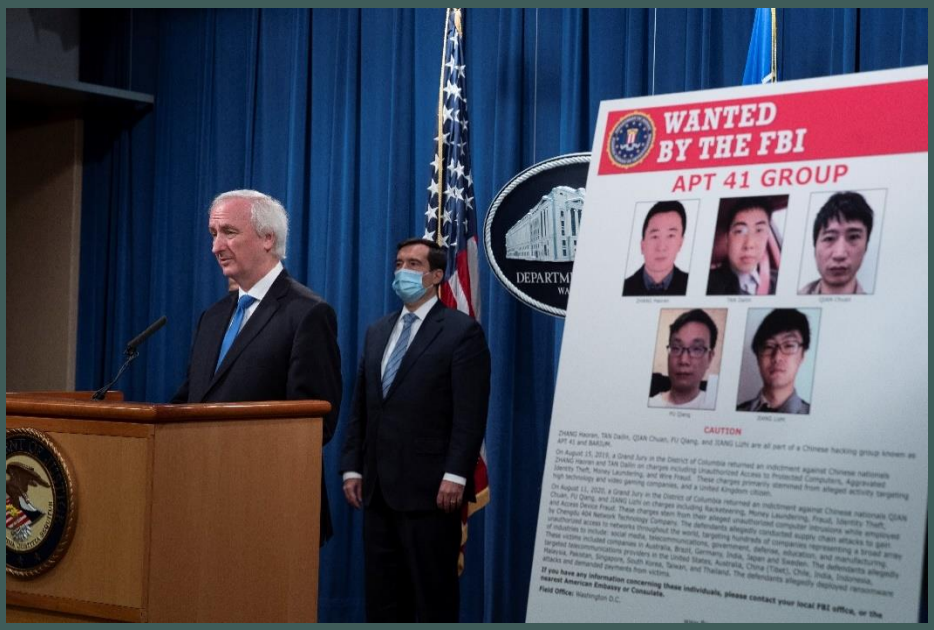
Internationalt har der de seneste år været mange cyberangreb mod virksomheder og myndigheder gennem leverandører og samarbejdspartnere. CFCS vurderer, at cyberangreb mod leverandører og samarbejdspartnere vil fortsætte.

CFCS vurderer, at det er muligt, at både cyberkriminelle og fremmede stater vil forsøge at kompromittere organisationer i den danske finanssektor gennem forsyningskæden.

Der findes flere eksempler fra udlandet, hvor finansielle institutter er blevet angrebet eller forsøgt angrebet via forsyningskæden. Et eksempel på dette er kampagnen kendt som GoldenSpy. I juni 2020 offentliggjorde IT-sikkerhedsfirmaet Trustwave en rapport om en bagdør kaldet GoldenSpy. Ifølge Trustwaves rapport giver GoldenSpy fuld adgang til ofrets systemer, hvilket bl.a. giver mulighed for at installere yderligere malware eller køre ondsindede programmer. GoldenSpy er blevet gemt og installeret sammen med en legitim og obligatorisk software, der bliver brugt til at opkræve lokal skat i Kina fra virksomheder, som opererer i landet.

Selvom det til tider kan være tilfældigt, at en leverandør bliver angrebet, så går nogle hackere målrettet efter leverandører for at få adgang til deres kunders netværk eller systemer. Dermed kan hackerne udnytte en organisation til at få adgang til information eller systemer, der tilhører hackernes egentlige mål.

**Kinesere anklaget for at hacke leverandør og dens kunder**
Amerikanske myndigheder anklagede i midten af september 2020 medlemmer af hackergruppen APT 41 for at have hacket over 100 forskellige ofre verden over. Hackerne angreb nogle af virksomhederne gennem en leverandør. Tre af de kinesiske mænd er anklaget for både at have hacket organisationer på vegne af den kinesiske stat og for deres egen vindings skyld.




*I alt fem kinesiske statsborgere er anklaget af de amerikanske myndigheder for at være medlemmer af APT 41.*
*FOTO: Tasos Katopodis/EPA/Ritzau Scanpix*

Angrebsmetoden er effektiv, fordi hackerne ved at kompromittere en leverandør eller samarbejdspartner på én gang kan få adgang til mange mål, til indhentning af kundedata eller adgang til væsentlige dele af en sektors infrastruktur.

Hvis der er tale om en leverandør med en betroet adgang, søger hackerne typisk efter de fjernadministrationsløsninger og konti, som leverandøren bruger til at tilgå deres kunder. Med de adgange kan hackerne tilgå netværket hos leverandørens kunder med samme privilegier, som leverandøren normalt har. Som tidligere nævnt kan hackerne også sende spear phishing-mails fra leverandøren til dens kunder.

### Ransomware kan også ramme via forsyningskæden

I 2020 har der været flere succesfulde ransomware-angreb mod større internationale finansielle leverandører. Der har i 2020 også været flere succesfulde ransomware-angreb mod leverandører, som danske virksomheder i finanssektoren benytter. Angrebene spredte sig ifølge CFCS' oplysninger ikke til de danske virksomheders systemer.

Ransomware-angreb mod leverandører kan i værste fald sprede sig til organisationer i den danske finanssektor. Selv hvis angrebene ikke spreder sig, kan de have alvorlige konsekvenser. Dels kan det medføre driftsforstyrrelser og forsinkelser i services fra leverandøren. Dels kan de føre til læk af følsomme informationer, som leverandøren opbevarer eller behandler.

**Cognizant ramt af Maze-ransomware**
I april 2020 offentliggjorde Cognizant, at de var blevet offer for ransomwaren Maze. Cognizant advarede i samme omgang sine kunder om, at de skulle afbryde forbindelse til Cognizant for at undgå at blive inficerede. Udover at være ramt af nedetid og driftsforstyrrelser, har Cognizant senere offentliggjort, at der i ransomware-angrebet muligvis blev stjålet følsomme kundedata samt data om medarbejderes kreditkort. Cognizant er et globalt selskab, som blandt andet leverer it-tjenester til den finansielle sektor. De har produkter både til bankdrift og kapitalmarkedet. Cognizant er også til stede i Danmark.

**Finastra (tidligere Mysis) ramt af Ryuk-ransomware**
Finanstra blev i marts sandsynligvis offer for et målrettet ransomware-angreb med Ryuk ransomware. Hundredvis af udenlandske banker meddelte, at de var påvirket af angrebet.  Ifølge åbne kilder lykkedes det Finastra at genoprette systemerne uden at betale løsesum. Finastra er leverandør af tjenesteydelser til flere tusinde banker på globalt plan og drifter mange vitale dele til finansielle tjenester i alt fra websites til back-office systemer.

# Cyberaktivisme

Truslen fra cyberaktivisme mod den danske finanssektor er **MIDDEL**. Det betyder, at det er muligt, at danske virksomheder og myndigheder i sektoren vil blive udsat for forsøg på cyberaktivisme inden for de næste to år.

CFCS har hævet trusselsniveauet på baggrund af aktivistiske cyberangreb udført mod europæiske NATO-lande i forbindelse med krigen i Ukraine. På globalt plan er antallet af aktivistiske cyberangreb faldet de seneste år, men Ruslands invasion af Ukraine har skabt stor opmærksomhed i dele af det aktivistiske miljø. Hvor cyberaktivistiske angreb indledningsvist fandt sted i direkte forlængelse af krigen og var fokuseret mod Rusland, Ukraine og Belarus, har cyberaktivistiske angreb sidenhen også ramt europæiske NATO-lande.

De aktivistiske cyberangreb har også ramt mål i finanssektoren i udlandet. Pro-russiske cyberaktivister hævder bl.a. at have udført DDoS-angreb mod banker i Tyskland, Rumænien, Letland og Ukraine.

Formålet med cyberaktivisme er at skabe størst mulig opmærksomhed om en sag. Cyberaktivister er i stand til at udføre forskellige typer cyberangreb, fra simple overbelastningsangreb og defacement-angreb til mere ressourcekrævende hack og læk-operationer.

Når trusselsniveauet for cyberaktivisme er hævet på grund af konkrete aktiviteter udført af pro-russiske cyberaktivister i forbindelse med krigen i Ukraine, betyder det ligeledes, at niveauet kan ændre sig igen med kort varsel afhængigt af krigens udvikling.

Cyberaktivisme udføres af individer og hackergrupper, der udfører cyberangreb for at få mest mulig opmærksomhed på deres dagsorden eller for at straffe organisationer. Cyberaktivisme er typisk drevet af forskellige ideologiske eller politiske motiver der strækker sig fra politiske enkeltsager til modstand mod magthavere. Cyberaktivister angriber både ofre de ser som symbolske mål og modstandere af deres sag. Finansielle virksomheder bør derfor være særligt opmærksomme på cyberaktivisme i situationer, hvor negative enkeltsager, som vedrører virksomheden eller sektoren, er genstand for offentlig debat i medierne, eller i tilfælde hvor cyberaktivister varsler angreb.

Der findes aktivistiske kampagner, som gentages år efter år. Det er mindre sandsynligt, at danske finansielle virksomheder bliver mål i sådanne kampagner. Et eksempel er den anti-kapitalistiske kampagne #OpIcarus. I kampagner fra tidligere år optrådte der et dansk mål på en målliste, som også inkluderer mange andre udenlandske mål.

**Cyberaktivist hackede bank og udlovede dusør**
Et eksempel på en cyberaktivist, der sandsynligvis har væsentlige ressourcer, er gruppen eller individet bag aliaset Phineas Fisher. Phineas Fisher blev kendt i 2014 og 2015 for at hacke virksomhederne Gamma Group og Hacking Team, som bl.a. solgte overvågningssoftware til stater. Phineas Fisher lækkede 400 GB data fra Hacking Team, herunder værktøjer til hacking.

I slutningen af 2019 hævdede Phineas Fisher at have hacket Cayman National Bank og stjålet både penge og data fra banken. Banken bekræftede, at de havde fået stjålet data i et cyberangreb. Phineas Fisher lækkede bankens data, beskrev hvordan data var stjålet og opfordrede andre til lignende hack og læk angreb. Phineas Fisher udlovede endda en dusør på 100.000 amerikanske dollars i kryptovaluta til personer, der hacker banker for at lække information af interesse for offentligheden.


*Phineas Fisher har flere gange offentliggjort beskrivelser af, hvordan ofrene er blevet hacket.*
*FOTO: Raphael Satter/AP/Ritzau Scanpix*

# Destruktive cyberangreb

CFCS vurderer, at truslen fra destruktive cyberangreb mod danske myndigheder og virksomheder er **LAV**. På kort sigt er det mindre sandsynligt, at fremmede stater har intention om at rette destruktive cyberangreb mod Danmark, herunder mod finanssektoren.

Det er dog muligt, at finanssektoren kan blive ramt som følge af destruktive cyberangreb mod mål udenfor Danmark, hvor malwaren spreder sig. Det gælder især danske virksomheder med aktiviteter i Ukraine og Saudi Arabien. I enkelte tilfælde er det muligt, at danske virksomheder med aktiviteter i Ukraine og Saudi Arabien også kan blive udset som direkte mål for destruktive cyberangreb.

Danske virksomheder kan også blive påvirket af angreb mod væsentlige internationale samarbejdspartnere, som sektoren er direkte eller indirekte afhængige af. Et sådant scenarie kan betyde, at institutternes væsentlige services påvirkes på grund af nedbrud hos en leverandør.

**Hvad er destruktive cyberangreb?**
CFCS definerer et destruktivt cyberangreb som et cyberangreb, hvor den forventede effekt er:

- Død eller personskade
- Betydelig skade på fysiske objekter
- Ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning

Destruktive cyberangreb er et værktøj, som primært bliver brugt i politiske og militære konflikter. Flere stater har cyberkapaciteter, der kan bruges destruktivt. Langt de fleste af de destruktive cyberangreb, der har fundet sted indtil nu, har ødelagt data ved at slette eller kryptere dem uden mulighed for at genskabe dem.

Der findes flere eksempler på, at udenlandske finansielle virksomheder er blevet ramt af destruktive cyberangreb. Eksempelvis blev Ukraines finansministerium og Centralbank angrebet i 2016. Angrebet medførte bl.a., at 150.000 elektroniske overførsler blev stoppet. I oktober 2020 anklagede amerikanske myndigheder navngivne russiske statsborgere for at stå bag angrebet. Ifølge de amerikanske myndigheder arbejdede hackerne for en russisk efterretningstjeneste.

# Cyberterror

Der er **INGEN** trussel fra cyberterror mod finanssektoren.

CFCS vurderer, at militante ekstremister har begrænsede evner og ressourcer til at udføre alvorlige cyberangreb. Samtidigt findes der kun få eksempler på, at militante ekstremister har opfordret til cyberterror.

Der er derfor ingen trussel mod finanssektoren i Danmark fra cyberangreb, hvor hensigten er at skabe samme effekt som mere konventionel terror. Det kunne f.eks. være cyberangreb, der forårsager fysisk skade på mennesker eller materiel eller skaber omfattende forstyrrelser af finanssektorens infrastruktur.

# Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

| | |
|---|---|
| **INGEN** | Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt.<br>Angreb/skadevoldende aktivitet er usandsynlig. |
| **LAV** | Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt.<br>Angreb/skadevoldende aktivitet er mindre sandsynlig. |
| **MIDDEL** | Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning.<br>Angreb/skadevoldende aktivitet er mulig. |
| **HØJ** | Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning.<br>Angreb/skadevoldende aktivitet er sandsynlig. |
| **MEGET HØJ** | Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse.<br>Angreb/skadevoldende aktivitet er meget sandsynlig. |

FE bruger denne skala for sandsynligheder i analyser

**Usandsynligt** | **Mindre sandsynligt** | **Muligt** | **Sandsynligt** | **Meget sandsynligt**

*"FE vurderer" svarer til "Sandsynligt", medmindre en anden sandsynlighed er angivet.*