CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod finanssektoren

November 2024

Indhold

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

November 2024, opdateret 22. november 2024
Forsidefoto: Danmarks Nationalbank

Cybertruslen mod finanssektoren

Formålet med denne trusselsvurdering er at beskrive cybertruslen rettet mod den danske finanssektor. Vurderingen kan styrke risikoejeres forståelse af cybertruslen og bl.a. indgå som en del af grundlaget for risikovurderingsarbejdet i sektoren. Vurderingen erstatter "Cybertruslen mod finanssektoren", der blev udgivet i 2020 og løbende er blevet opdateret.

Hovedvurdering

- Truslen fra cyberkriminalitet mod den danske finanssektor er **MEGET HØJ**. Cyberkriminelle, der udfører ransomware-angreb og andre afpresningsangreb, udgør en særligt alvorlig trussel.

- Truslen fra cyberaktivisme mod finanssektoren er **HØJ**. Truslen består primært af DDoS-angreb mod hjemmesider. Cyberaktivister kan dog også forsøge at lave andre typer cyberangreb, herunder hack og læk-angreb.

- Truslen fra cyberspionage mod den danske finanssektor er **MIDDEL.** Niveauet er sænket fra **HØJ** til **MIDDEL**, da Center for Cybersikkerhed (CFCS) vurderer, at sektoren på nuværende tidspunkt ikke er et højt prioriteret mål for denne type angreb. CFCS vurderer, at fremmede stater vil angribe sektoren, hvis der opstår muligheder for opportunistiske angreb, som kræver relativt få ressourcer.

- Truslen fra destruktive cyberangreb mod den danske finanssektor er **MIDDEL**. Rusland er blevet mere risikovillig i forhold til at bruge hybride virkemidler med destruktive effekter i europæiske NATO-lande. CFCS vurderer, at den øgede risikovillighed også omfatter destruktive cyberangreb. Finanssektoren kan i lighed med andre samfundsvigtige sektorer udgøre et attraktivt mål for destruktive cyberangreb.

- Truslen fra cyberterror mod den danske finanssektor er **INGEN**. Cyberterror forudsætter kapaciteter, som militante ekstremister aktuelt ikke har. Samtidig er hensigten yderst begrænset.

Indledning

Finanssektoren har i årtier draget nytte af digitaliseringen og den teknologiske udviklings mange muligheder til stor fordel for det danske samfund. Det har dog også bidraget til, at finanssektoren og samfundet bredere set i høj grad er afhængig af sektorens digitale systemers stabile drift og integritet.

Viden om truslerne mod disse systemer, herunder cybertruslen, er derfor central for at kunne sikre og understøtte sektorens mange funktioner. Trusselsbilledet stiller store krav til myndigheder og virksomheder. Det gælder også finanssektoren, der har en kritisk funktion i Danmark. Vedvarende eller avancerede cyberangreb mod sektorens virksomheder eller infrastruktur kan true den finansielle stabilitet og dansk økonomi.

Mange forskellige trusselsaktører forsøger at udnytte cyberangreb til at nå deres mål. Berigelseskriminalitet, den løbende konkurrence mellem stater og også aktivisme er over de seneste par årtier i stigende grad rykket ind i cyberdomænet.

CFCS opdeler cybertruslen i fem forskellige kategorier: cyberkriminalitet, cyber-aktivisme, cyberspionage, destruktive cyberangreb og cyberterror. Hver kategori tager udgangspunkt i formålet med en given angrebstype. Det er ikke gjort for at simplificere truslen, men for at understrege, at cybertruslen er en sammensat størrelse, som ikke lader sig beskrive ud fra én vinkel. CFCS anvender Forsvarets Efterretningstjenestes trusselsniveauer og sandsynlighedsgrader. Definitionen af disse fremgår sidst i trusselsvurderingen.

Den danske finanssektor

Danmarks finanssektor består af virksomheder, der varetager mange forskellige funktioner i sektoren og i den finansielle værdikæde. Når finanssektoren omtales i denne vurdering, omfatter det hovedsageligt banker, realkreditinstitutter, forsikrings- og pensionsselskaber, datacentraler, betalingsinfrastruktur, betalingsinstitutter mv. Dertil kommer relevante myndigheder og institutioner på det finansielle område.

Virksomheder i sektoren adskiller sig væsentligt fra hinanden, for så vidt angår virksomhedstypen, tjenesteydelser, kundesegment med mere. Virksomhederne har derfor også forskellige tilgange til og standarder for cybersikkerhed. Nuancerne i sektoren behandles ikke yderligere i trusselsvurderingen, men bør indgå i den enkelte organisations risikovurdering.

Denne vurdering berører ikke trusler forbundet med diverse kryptoaktiver.

Cyberkriminalitet

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

De cyberkriminelle forsøger at berige sig økonomisk på forskellig vis. Typisk forsøger de kriminelle at afpresse offeret, sælge offerets data eller systemadgange, eller at svindle offeret til at overføre penge til hackeren. Der er derudover en potentiel trussel fra såkaldte digitale bankrøverier, der dog finder sted meget sjældent.

Truslen fra ransomware-angreb er fortsat aktuel
Ransomware-angreb udgør en betydelig trussel, også for den danske finanssektor. Der finder et højt antal angreb sted verden over, herunder i Danmark, og truslen understøttes af et omfattende miljø af cyberkriminelle. Visse dele af det cyberkriminelle miljø råder over avancerede kapaciteter, og formår derfor også at kompromittere ellers godt beskyttede virksomheder.

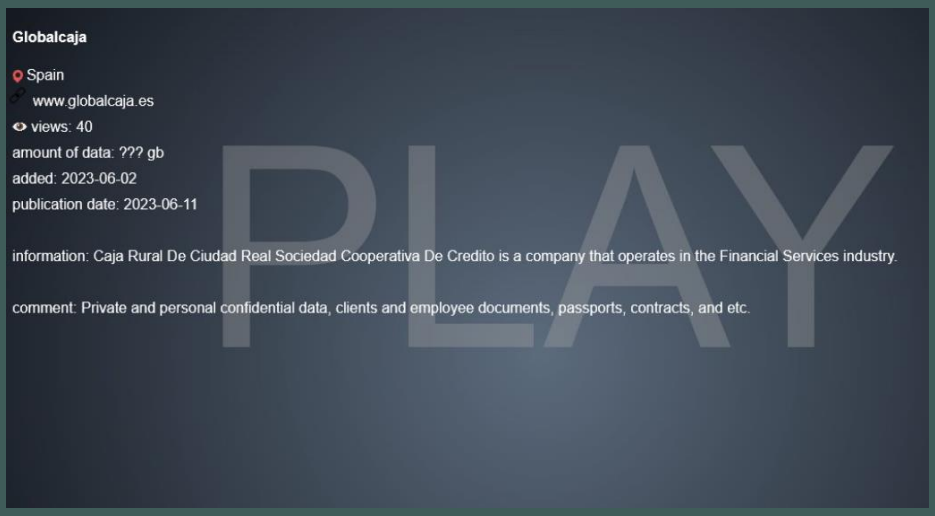
Internationalt har der de seneste år været flere eksempler på vellykkede ransomware-angreb mod den finansielle sektor. CFCS har ikke kendskab til, at organisationer i den danske finanssektor har været ofre for succesfulde ransomware-angreb siden CFCS' seneste trusselsvurdering for sektoren, men der er observeret forsøg på ransomware-angreb. Derudover har der været ransomware-angreb mod leverandører, som virksomheder i den danske finanssektor benytter sig af.

Ransomware-angreb kan have alvorlige konsekvenser for finanssektoren og for samfundet bredere set. Ransomware-angreb kan potentielt medføre driftsforstyrrelser eller afbrydelser af de samfundsvigtige services, som finanssektoren leverer. Derudover kan de påvirke tilliden til de ramte organisationer eller det finansielle system, især fordi mange ransomware-aktører offentliggør detaljer om deres angreb.

Forsikringsgigant betalte USD $40 millioner til kriminelle
Ifølge åbne kilder betalte den amerikanske forsikringsvirksomhed, CNA Financial, i marts 2021 USD $40 millioner i løsepenge efter at være blevet ramt af ransomware-angreb. Hackerne fik fodfæste på koncernens netværk gennem en falsk browseropdatering på en legitim hjemmeside. Herfra kunne hackerne bevæge sig videre, udtrække data, destruere backups og deployere ransomware.

Det er i den seneste række år blevet mere udbredt, at ransomware-aktører stjæler informationer fra ofrene og afpresser dem yderligere med trusler om at lække eller sælge informationerne. Visse aktører, der ellers er kendt for at udføre ransomware-angreb, vælger nogle gange at stjæle følsomme informationer uden at kryptere data. Banker i udlandet har i nogle tilfælde været ofre for sådanne angreb.
Finanssektoren behandler store mængder sensitive data, hvilket kan gøre sektoren særlig attraktiv for denne type afpresning.

Selvom afpresning uden kryptering ikke medfører direkte forstyrrelser af driften, kan det stadig være nødvendigt at foretage en selvvalgt nedlukning af systemer, mens angrebet håndteres. Driftsforstyrrelser eller ej, kan både ransomware-angreb og afpresning uden kryptering få store konsekvenser for offeret, bl.a. i form af tab af tillid, udgifter til håndtering af hændelsen, eventuelle GDPR-bøder og tab af markedsværdi.



Skærmbillede fra hackernes Dedicated Leak Site (DLS), hvor angrebet på Globalcaja blev offentliggjort

Spansk bank afspresset med trusler om læk

Den spanske bank, Globalcaja, blev i juni 2023 offer for et ransomware-angreb. Globalcaja har i omegnen af 500.000 kunder. Hackerne truede bl.a. med at lække fortrolige oplysninger om kunder og ansatte samt dokumenter og kontrakter.

Adgang til sektorens systemer og data er i høj kurs

CFCS vurderer, at informationer stjålet fra finanssektoren samt adgange til sektorens systemer og netværk er eftertragtede på de cyberkriminelle markedspladser. Det er meget sandsynligt, at cyberkriminelle er opmærksomme på værdien af de følsomme data, finanssektoren har adgang til.

De cyberkriminelle kan berige sig ved at sælge følsomme informationer om finans-sektoren og dens kunder, som de har hacket sig til. Kriminelle aktører påstår med jævne mellemrum at have data fra organisationer i finanssektorer i udlandet. Eksempelvis satte en aktør i marts 2023 60GB data, angiveligt stjålet fra Deutsche Bank, til salg på et cyberkriminelt forum. Det kan som tidligere nævnt være skadeligt for tilliden til organisationer i sektoren samtidig med, at det kan forårsage andre økonomiske tab for organisationen og dens kunder.

Derudover kan kriminelle hackere berige sig ved at skabe den indledende adgang til finanssektorens systemer for derefter at sælge adgangen videre.

Hackere, der specialiserer sig i at skabe og videresælge adgange til systemer, kaldes Initial Access Brokers (IAB). IAB spiller en væsentlig rolle i det samlede trusselsbillede mod finanssektoren. Deres salg af adgange indgår i et lukrativt økosystem på diverse undergrundsfora.

På disse fora køber og sælger cyberkriminelle adgange, malware og services af hinanden via en art platformsøkonomi, hvilket bidrager til at øge både omfanget og udbyttet af cyberkriminelle angreb. Hackernes mulighed for at købe sig til specialiserede ydelser sænker adgangsbarrieren for at udføre et vellykket cyberangreb. Derudover understøtter samarbejdet og handlen de cyberkriminelles kapaciteter, da hackere kan specialisere og dygtiggøre sig i enkelte led af angrebs-kæden.

Det er meget sandsynligt, at enkelte fremmede stater udnytter det cyberkriminelle miljø ved eksempelvis at anskaffe sig malware fra cyberkriminelle. Det kan f.eks. ske via online fora, hvor hackere sælger og udveksler værktøjer og services. De kriminelle ved derfor ikke nødvendigvis, at de samarbejder med eller sælger til en statslig aktør. Det betyder derudover, at en indledningsvis kompromittering kan ende i mange forskellige typer angreb.

Agent Tesla

Agent Tesla er en blandt mange typer malware, som de cyberkriminelle bruger for at understøtte deres cyberangreb, bl.a. mod finanssektoren. Agent Tesla kan bl.a. indsamle keystrokes, tage skærmbilleder og stjæle login-oplysninger gemt i eksempelvis webbrowsere.

Kriminelle svindler organisationer via mail

Organisationer i både den danske og udenlandske finanssektor er løbende udsat for forsøg på BEC-svindel (Business E-mail Compromise). BEC-svindel er globalt set blandt de mest lukrative former for angreb for de kriminelle. Ved BEC-svindel forsøger de kriminelle at franarre organisationer penge gennem falske anmodninger om overførsler af penge. I nogle tilfælde kompromitterer hackerne f.eks. en legitim mailkonto hos en virksomhed eller hos en virksomheds samarbejdspartnere for derefter at manipulere medarbejdere til at overføre penge til de kriminelles konti.

BEC-svindel fra en kompromitteret mailkonto kan være svært at opdage, da mailens afsender er legitim. Ofte behøver de cyberkriminelle dog ikke at kompromittere en mailkonto for at deres angreb lykkes. I stedet får de blot deres mails til at se legitime ud på overfladen. De kriminelle kan eksempelvis oprette en mailadresse, der ligner en legitim mailadresse fra modtagerens arbejdsplads.

De kriminelle kan også bruge viden om virksomheden eller myndigheden og dens medarbejdere til at få deres mails til at virke overbevisende. I udlandet er det set, at hackere bl.a. bruger LinkedIn til at identificere virksomheders nye ansatte, da de ofte endnu ikke kender virksomhedens procedurer og arbejdsgange, og derfor kan være nemmere at narre.

Cyberkriminalitet mod bankkunder er fortsat et problem
Kriminelle retter fortsat cyberangreb mod bankernes kunder i forsøg på at få adgang til kundernes netbank, betalingskortoplysninger eller i forsøg på at manipulere kunderne til at overføre penge til hackerne. Cyberkriminelle bruger eksempelvis malware til at opsnappe loginoplysninger, men mange forsøg på netbankssvindel udføres dog også uden brug af cyberangreb. Netbanksvindel med og uden brug af cyberangreb medfører hvert år betydelige økonomiske tab.

Manipulerede overførsler via cyberangreb

Kriminelle hackere har i en årrække udsat den italienske finanssektor for cyberangreb med webinject-værktøjet, drIBAN.

Formålet med kampagnen var at inficere systemer i bankernes produktionsmiljø. Det gav hackerne mulighed for at ændre modtageroplysningerne ved legitime bankoverførsler. Modtagerkonti tilhørte enten hackerne selv eller affilierede, som hjalp med at hvidvaske de stjålne midler.

Cyberangrebene startede med en spoofet phishing-mail. Mailen indeholdt en ondartet fil, der, når eksekveret, fungerede som downloader for rekognosceringsmalware. Dernæst kunne hackerne installere en bank trojan-malware, der banede vejen for drIBAN.

Digitale bankrøverier og andre angreb
Cyberkriminelle er kreative. Selvom de typiske cyberkriminelle angreb enten er ransomware, salg af informationer eller BEC-svindel, er der en potentiel trussel for, at finanssektoren kan blive ramt af andre typer cyberkriminalitet.

Informationer stjålet fra sektoren kan eksempelvis potentielt bruges til finansiel kriminalitet, såsom insiderhandel eller forsikringssvindel.

Tidligere er organisationer i udenlandske finanssektorer blevet udsat for såkaldte digitale bankrøverier. Mange af disse angreb er af it-sikkerhedsselskaber og andre landes myndigheder blevet tilskrevet Nordkorea.

Nordkorea er underlagt et omfattende regime af sanktioner, og statens hackere udfører sandsynligvis cyberkriminalitet for at skaffe penge til staten. De seneste år er Nordkorea bl.a. blevet kædet sammen med tyveri af kryptovaluta. Kryptovalutaer er dog relativt volatile, og det er derfor muligt, at Nordkorea også vil målrette cyberangreb mod traditionelle finansielle virksomheder.

En kædereaktion af supply chain-angreb

Ifølge åbne kilder blev software-virksomheden, 3CX, angrebet af nordkoreanske hackere i begyndelsen af 2023. 3CX har mere end 12 millioner daglige brugere af selskabets Voice over Internet Protocol-løsninger (VoIP). En ansat ved 3CX installerede en inficeret version af X Trader-applikationen. Applikationen plantede en bagdør på medarbejderens enhed. Derefter kunne hackerne bevæge sig gennem 3CX's netværk og inficere hovedapplikationen til lyd- og videoopkald. Den kompromitterede applikation blev dernæst installeret af 3CX's intetanende kunder. Ofrene tæller også virksomheder inden for det finansielle område.

I oktober 2023 varslede amerikanske FBI, at Nordkorea har sendt tusindvis af it-medarbejdere til udlandet med det formål at generere penge til staten. Ifølge FBI har nogle af it-medarbejderne misbrugt deres medarbejderadgange til at infiltrere deres arbejdsplads' netværk og stjæle informationer. Denne adgang og information kan ifølge de amerikanske myndigheder udnyttes til bl.a. afpresning. Tiltalen understreger Nordkoreas kreative tilgang til cyberkriminalitet.

Hyppige angrebsmetoder

I det følgende afsnit gennemgår vi nogle af hackernes forskellige angrebsmetoder. Listen er langt fra udtømmende, men indbefatter nogle af de gængse angrebsvektorer. Metoderne bruges af både cyberkriminelle og statslige aktører. Mange af metoderne har været anvendt mod finanssektorer i udlandet og i nogle tilfælde også mod sektoren i Danmark.

Phishing

CFCS vurderer, at phishing-mails fortsat er blandt hackeres foretrukne værktøjer. Hackere phisher i forsøget på at kompromittere både virksomheder og myndigheder i den danske finanssektor. Phishing er en forholdsvis billig og skalerbar angrebsmodus. Trænger en phishing-mail først igennem anti phishing-filteret, kan det være op til den enkelte medarbejder at agere firewall. Phishing-mails udnytter det menneskelige element og dermed risikoen for, at en medarbejder klikker på et ondartet link eller en vedhæftet fil.

Phishing-mails bruges bl.a. til at franarre modtageren sine login-oplysninger eller til at distribuere malware. Udbredelsen af generativ AI kan gøre phishing-mails endnu sværere at opdage, da hackere kan misbruge teknologien til at lave detaljerede, fejlfrie mails – også på sprog, hackerne ikke selv behersker.

Angreb via leverandører

Leverandører, særligt softwareleverandører eller cloududbydere, er eftertragtede mål for både statslige hackere og cyberkriminelle. Angreb på leverandører, der har adgang til kunders it-systemer eller data, er attraktive, fordi de potentielt kan give hackere adgang til mange mål på én gang.

Hackerne kan også gå efter leverandører i mere målrettede angreb, hvor de udnytter leverandører til at få adgang til ellers vel-beskyttede organisationer, der er svære at kompromittere direkte.

Udnyttelse af sårbarheder i software og systemer

Sårbarheder i software, som ikke er opdateret, er fortsat en populær angrebsmetode for både kriminelle og stater. CFCS vurderer, at begge typer aktører generelt er hurtige til at udnytte deres viden om sårbarheder.

Stater har i længere tid haft ressourcer til at udvikle og købe sig til viden om zero days, også kaldet nul-dags-sårbarheder. Kina har siden 2021 vedtaget ved lov, at individer og virksomheder skal indberette viden om zero days til myndighederne inden for to dage fra, at de bliver opdaget. En zero day er en sårbarhed, hvor leverandøren af softwaren eller systemet endnu ikke kender til sårbarheden, og der derfor endnu ikke findes en opdatering, der kan lukke sårbarheden. Angreb udført via zero days kan derfor være svære at imødegå. CFCS vurderer, at flere kriminelle hackere nu også investerer tid og ressourcer i at opdage eller købe sig til zero days. Et eksempel på dette var, da den cyberkriminelle gruppe Cl0p i maj 2023 udnyttede en zero day i MOVEit-applikationen til at angribe og afpresse et højt antal ofre verden over. Angrebet berørte flere banker og finansielle virksomheder i Vesten, inklusive i Norden.

Udnyttelse af svage eller genbrugte passwords

Simple angrebsmetoder såsom brute force-angreb er fortsat effektive. Brute force-angreb dækker over forskellige variationer af angreb, hvor hackere forsøger at gætte kombinationer af brugernavne og passwords. Dette kan eksempelvis ske gennem udnyttelse af passwords fra tidligere datalæk eller via systematisk gæt af kombinationer fordelt på mange forskellige brugerkonti. Brute force-angreb rettes mod mange forskellige former for systemer, herunder alt fra mailkonti til organisationers fjern-adgangssystemer, såsom Remote Desktop Protocol (RDP).

Insider-angreb

Truslen kommer fra medarbejdere med adgang til it-systemer, kundedata eller viden, der ubevidst eller bevidst faciliterer eller udfører cyberangreb. Der har i udlandet været eksempler på bevidste insidere i finansielle virksomheder, og der har også været eksempler på cyberkriminelle, der forsøger at rekruttere virksomheders ansatte til angreb.

Malvertising og vandhulsangreb

Malvertising dækker over, når hackere bruger online reklamer til at sprede malware. Hackerne indsætter ofte de malwareinficerede reklamer på ellers legitime hjemmesider. En af de mere gængse variationer er tilbud om downloads af applikationer, såsom anti virus-programmer.

En anden angrebsteknik, der udnytter hjemmesider, er vandhulsangreb. Her kompromitterer hackere legitime hjemmesider med malware. Brugere, der normalt benytter hjemmesiden uden problemer, risikerer at blive inficeret med malwaren. Ved et vandhuls-angreb er hjemmesiden typisk udvalgt for at ramme en specifik målgruppe eller fordi hjemmesiden har mange besøgende. Hackere kan dog også overtage tilfældige hjemmesider, hvis de er nemme at kompromittere.

Cyberaktivisme

Truslen fra cyberaktivisme mod den danske finanssektor er **HØJ**. Det er meget sandsynligt, at danske virksomheder og myndigheder i sektoren bliver udsat for forsøg på cyberaktivisme inden for de næste to år.

Cyberaktivisme udføres i udgangspunktet af individer og grupper, der bruger cyber-angreb for at få mest mulig opmærksomhed til deres dagsorden. Cyberaktivister angriber også organisationer, de anser som modstandere af deres sag. De pro-russiske grupper er et godt eksempel på, hvordan cyberaktivister kan understøtte staters interesser. Det er dog ikke ensbetydende med, at de arbejder direkte for staten. CFCS vurderer dog, at nogle pro-russiske cyberaktivistiske grupper har forbindelse til den russiske stat.

Aktivister udfører forskellige typer angreb. Nogle udfører simple defacement- og over-belastningsangreb, mens andre har kapacitet til mere krævende hack og læk-angreb.

DDoS er aktivisternes foretrukne metode
Pro-russiske hackere retter løbende DDoS-angreb mod hjemmesider tilhørende vestlige myndigheder og virksomheder. Finanssektoren, sammen med bl.a. transportsektoren, har både i Danmark og i udlandet været et prioriteret mål for aktivisternes DDoS-angreb. CFCS vurderer, at cyberaktivisterne ser sektoren som et symbolsk mål, men at de også motiveres af sektorens samfundskritiske rolle samt befolkningens daglige interaktion med sektorens tjenester. Nedetid på finansielle institutioners hjemmesider har stor synlighed, da finanssektorens eksponering mod befolkningen er stor.

Pro-russiske aktivistiske hackeres DDoS-angreb mod danske banker har i nogle tilfælde betydet, at bankkunder kortvarigt ikke har kunnet tilgå deres netbank.

"De fortsætter med at forsyne Ukraine med våben. Så må vi bare give de to 😈 ovenstående lande en lærestreg"

DDoS-angreb begrundes med Danmarks støtte til Ukraine
Citatet er en oversættelse af en pro-russisk aktivistisk gruppes begrundelse for deres DDoS-angreb mod bl.a. en dansk banks hjemmeside i slutningen af februar 2024. I løbet af 2023 udpegede gruppen flere gange danske bankers hjemmesider som mål for gruppens DDoS-angreb.

Organisationer i den danske finanssektor kan også blive indirekte ofre for DDoS-angreb, når angrebene rammer sektorens leverandører. Eksempelvis blev Microsofts cloudservice, Azure, og mailklient, Outlook, i juni 2023 udsat for et layer 7-overbelastningsangreb. Layer 7 er også kendt som applikationslaget og huser de protokoller og tjenester, som en applikation bruger for at fungere. Laget udgør dermed fundamentet for den software-applikation, som brugeren interagerer med. Angrebet påvirkede tilgængeligheden i Microsofts services.

DDoS-angreb er dog ofte teknisk usofistikerede og har ikke i sig selv varige eller destruktive effekter. Angrebene kan dog påvirke systemernes tilgængelighed og tilliden til den ramte organisation.

Cyberaktivisme er også andet end DDoS
Selvom DDoS-angreb har fyldt meget i mediebilledet, kan finanssektoren også blive mål for andre typer cyberaktivistiske angreb. Hack-og-læk er et eksempel på en sådan type angreb. Der har i udlandet været flere eksempler på, at hackere har lækket store datasæt på bankers privatkunder. Dataene har været frit tilgængelige på hackerfora og har bl.a. omfattet kunders kreditkortoplysninger og personoplysninger.

CFCS vurderer, at visse cyberaktivistiske grupper har intention om at udføre cyberangreb med destruktiv effekt, men at deres kapacitet er begrænset.

Hvis cyberaktivister forsøger at udføre destruktive cyberangreb, er det særligt svage sikkerhedsforanstaltninger, der kan gøre det muligt for dem at komme ind i systemer, de efterfølgende kan angribe. Svage sikkerhedsforanstaltninger betyder, at selv cyberaktivister med begrænset kapacitet kan kompromittere systemerne.

Nogle cyberaktivistiske grupper har påstået at have udført destruktive cyberangreb i forbindelse med konflikter, f.eks. konflikten mellem Israel og Hamas og Ruslands invasion af Ukraine i 2022. Det er dog de færreste af angrebene, hvor der er blevet bekræftet en reel effekt.

Cyberaktivisternes kommunikation kan give misvisende trusselsbillede
Cyberaktivisters primære mål er typisk at skabe opmærksomhed omkring deres sag. Derfor spiller omtalen af deres angreb en næsten lige så stor rolle som angrebene i sig selv. Ofte er aktivisternes omtale af deres angreb dog misvisende og overdreven. Den misvisende kommunikation er et redskab, som cyberaktivisterne bruger til at forstærke deres politiske fortælling og den psykologiske effekt af deres cyberangreb.

Cyberaktivisterne bruger bl.a. deres platforme på sociale medier til at overdrive effekten af deres angreb. Her beskriver de f.eks. simple overbelastningsangreb mod brugervendte hjemmesider som hændelser, der giver driftsforstyrrelser i kritisk infra-struktur, selvom dette ikke er tilfældet i praksis.

Cyberspionage

Truslen fra cyberspionage mod finanssektoren er **MIDDEL**. Det er muligt, at finanssektoren i Danmark bliver udsat for forsøg på cyberspionage inden for de næste to år.

Trusselsniveauet er sænket fra **HØJ** til **MIDDEL** i forhold til CFCS' tidligere trusselsvurdering. Trusselsniveauet ændres på baggrund af en fornyet analyse af truslen fra cyberspionage mod finanssektoren. CFCS vurderer, at selvom fremmede stater har kapacitet og intention om at udøve cyberspionage mod finanssektoren, er det mindre sandsynligt, at den danske finanssektor er et højt prioriteret angrebsmål på kort sigt, hvilket vil sige op til to år. Det betyder, at det er mindre sandsynligt, at fremmede stater på kort sigt vil prioritere at afsætte de nødvendige ressourcer til at gå målrettet efter den danske finanssektor.

Spionage sker i mørket

Cyberspionage er typisk mindre synligt end andre former for cyber-angreb. Hackere, der ofte råder over betydelige ressourcer, forsøger at bevæge sig uset rundt i ofrets IT-systemer for at få adgang til værdifuld viden. Det gør, at der sandsynligvis er et mørketal forbundet med truslen.

Sektoren kan blive ramt af opportunistisk cyberspionage
CFCS vurderer, at fremmede stater vil forsøge at udføre cyberspionage mod sektoren, hvis der opstår muligheder for opportunistiske angreb, som kræver relativt få ressourcer. Det kan eksempelvis være, hvis der opstår en udbredt sårbarhed, der nemt kan udnyttes. Eller i forbindelse med et bredt supply chain-angreb, der giver adgang til mange ofre på én gang.

Finanssektoren vil derfor sandsynligvis også blive udsat for rekognoscering fra fremmede stater, bl.a. i form af sårbarhedsscanninger.

Sektoren råder over attraktive data, der ofte også kan findes i andre sektorer
Erkendte eksempler på cyberspionage i udlandet indikerer, at finanssektoren kan være et attraktivt mål. Formålet med cyberspionage mod andre landes finanssektorer kan have været at høste datasæt, herunder følsomme personoplysninger, samt opnå viden om finansieringsplaner, investeringer og forretningskritiske anliggender.

Generelt har finanssektorer adgang til store mængder data. I Danmark har finanssektoren omfattende data på både privat- og erhvervskunder. Selvejende institutioner, kommuner og myndigheder er også kontoførende ved institutioner i sektoren. Dataene består bl.a. af personhenførbare oplysninger, kunders strategiske investeringer og finansielle dispositioner samt statens og det offentliges låntagning.

CFCS vurderer, at meget af denne data nemmere kan indhentes i andre sektorer. I udlandet har der eksempelvis været flere cyberspionageangreb mod advokater, revisorer og konsulenthuse.

Advokater, revisorer og konsulenthuse varetager også sensitive data og viden om fusioner og opkøb, finansielle dispositioner, patenter, forretningshemmeligheder etc. Endelig kan en stats hackere også vælge at gå direkte efter en specifik kunde og på den måde ligeledes omgå finanssektoren.

Hackere plukker gerne de lavthængende frugter. Hvis tilsvarende data er tilgængelig i andre sektorer, som hackerne nemmere kan kompromittere, er det sandsynligt, at hackere vil prioritere at målrette deres angreb mod disse.

Truslen vil sandsynligvis stige i en konflikt
CFCS vurderer, at truslen fra cyberspionage mod den danske finanssektor vil stige, hvis Danmark indgår i en skærpet konflikt, herunder hvis den sikkerhedspolitiske situation eskalerer i retning af en militær konfrontation mellem Rusland og NATO.

I en skærpet konflikt vil finanssektoren sandsynligvis blive et højere prioriteret mål for cyberspionage.

Stater bruger bl.a. cyberspionage til at forberede destruktive cyberangreb. Destruktive cyberangreb mod finanssektoren vil potentielt kunne få stor indvirkning på befolkningen og samfundsøkonomien. Derfor kan finanssektoren udgøre et attraktivt mål for destruktive cyberangreb i en konflikt. Truslen fra destruktive cyberangreb er uddybet senere i trusselsvurderingen.

At finanssektorer sandsynligvis udgør et højere prioriteret mål i konflikter, illustreres også af offentligt kendte cyberspionagesager mod finanssektorer i Ukraine, Taiwan og Israel. Disse lande indgår alle i henholdsvis højspændte politiske eller væbnede konflikter med Rusland, Kina eller Iran.

Taiwans finanssektor udsat for langvarig cyberspionage

Spændingerne i Taiwanstrædet er de seneste år taget til i styrke. Flere sektorer i Taiwan udsættes for cyberangreb, og landets finanssektor går heller ikke fri af truslen. Ifølge åbne kilder begik kinesiske hackere eksempelvis cyberspionage mod Taiwans finanssektor fra 2021 til 2022. Hackerne udnyttede en sårbarhed i en software-løsning. Softwaren var bredt anvendt blandt virksomheder i landets finanssektor. Kompromitteringen betød, at hackerne havde fodfæste i enkelte netværk i flere måneder.

Cyberdomænet er en arena for staters konkurrence
Fremmede stater, herunder særligt Rusland og Kina, har betydelige kapaciteter til at udføre cyberspionage. CFCS vurderer, at særligt Rusland og Kina arbejder strategisk med cyberspionage, og at det udgør et prioriteret aktiv i deres udenrigs- og sikkerhedspolitiske værktøjskasse.

Stater bruger spionage til en række formål. Spionage kan bl.a. bruges til at informere politiske beslutninger, til at opnå komparative fordele inden for forskning og udvikling af avanceret teknologi og til at forme slagmarken i tilfælde af fremtidige konflikter. Hvis fremmede stater stjæler viden fra finanssektoren, kan det bl.a. skade danske interesser, tilliden til sektoren samt de enkelte ofres konkurrenceevne og markeds-andele.

Destruktive cyberangreb

CFCS vurderer, at truslen fra destruktive cyberangreb mod finanssektoren er **MIDDEL**. Truslen fra destruktive cyberangreb blev i juni 2024 hævet fra **LAV** til **MIDDEL** for Danmark generelt, og CFCS vurderer, at niveauet også er gældende for finanssektoren. Trusselsniveauet er **MIDDEL**, fordi Rusland er villig til at bruge hybride virkemidler med destruktive effekter mod europæiske NATO-lande. CFCS vurderer, at dette også indbefatter destruktive cyberangreb.

Hvad er destruktive cyberangreb?

CFCS definerer destruktive cyberangreb som cyberangreb, hvor den forventede effekt er:

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

Formålet med angreb er sandsynligvis at påvirke befolkningen

CFCS vurderer, at mange typer af organisationer i samfundsvigtige sektorer, herunder i finanssektoren vil kunne blive udvalgt som mål for destruktive cyberangreb. Finanssektoren har en stor synlighed og berøringsflade med borgerne og spiller en kritisk rolle i forhold til at understøtte samfundets evne til at udveksle varer og tjenesteydelser. Derfor kan finanssektoren udgøre et attraktivt mål for destruktive cyberangreb. Udvælgelsen af mål vil dog sandsynligvis også været påvirket af, hvor hackerne har adgang eller nemt kan få det.

Russiske hackergrupper har før stået bag flere destruktive cyberangreb mod Ukraine, herunder landets finanssektor. Mange af disse angreb er blevet tilskrevet Rusland af it-sikkerhedsselskaber og flere landes myndigheder.

CFCS vurderer, at et destruktivt cyberangreb sandsynligvis vil have til formål at påvirke befolkningen og beslutningstagere. Fordi det primære formål sandsynligvis er påvirkning, er det i den nuværende situation sandsynligt, at den konkrete fysiske effekt af eventuelle destruktive cyberangreb mod Danmark vil være sekundær for hackerne, der udfører det. I stedet vil det primære mål være, at angrebene skaber bred opmærksomhed.

Wiper-angreb

Den klart mest udbredte type destruktive cyberangreb er såkaldte wiper-angreb. I et wiper-angreb slettes, overskrives eller krypteres data, så den er utilgængelig eller er umulig at genskabe. Et sådan angreb kan være en alvorlig trussel mod den ramte organisation og, afhængigt af målet, potentielt også det omkringliggende samfund. Ved at destruere kritisk information og systemer kan angriberne besværliggøre eller stoppe en organisations arbejde og derved potentielt afbryde samfundsvigtige funktioner.

Destruktive cyberangreb kan få betydelige konsekvenser
Det er mindre sandsynligt, at Rusland i den nuværende situation vil gennemføre destruktive cyberangreb mod Danmark, hvor hensigten er at skabe alvorlige og omfattende konsekvenser for samfundsvigtige funktioner, herunder i den finansielle sektor. Selvom disse angreb er mindre sandsynlige, vurderer CFCS, at hackergrupper knyttet til Rusland løbende forbereder sig på at kunne udføre den form for destruktive cyberangreb mod Danmark. Sandsynligheden for, at disse angreb finder sted, kan derfor stige med kort eller uden varsel – særligt hvis konflikten mellem Rusland og Vesten eskalerer eller ændrer karakter.

Mindre omfattende cyberangreb kan dog stadig få betydelige konsekvenser for offeret og for samfundet. Det kan f.eks. være angreb, der påvirker samfundsvigtige funktioner i begrænset omfang. Selv hvis destruktive cyberangreb ingen konsekvenser har for samfundsvigtige funktioner, kan de skabe utryghed og dermed påvirke samfundet.

Ruslands øgede risikovillighed vil også kunne komme til udtryk som omfattende DDoS-angreb mod centrale systemer i eksempelvis finanssektoren. DDoS-angreb er ikke destruktive, men omfattende DDoS-angreb mod centrale systemer vil potentielt kunne afbryde eller forstyrre samfundsvigtige funktioner i kortere eller længere tid og derved påvirke befolkningen og beslutningstagere på samme måde som destruktive cyberangreb.

Cyberterror

Truslen fra cyberterror mod finanssektoren i Danmark er **INGEN**. Det er usandsynligt, at finanssektoren vil blive udsat for forsøg på cyberterror inden for de næste to år.

CFCS definerer cyberterror som cyberangreb, hvor hensigten er at skabe samme effekt som konventionel terror. Det kan f.eks. være cyberangreb, der forårsager fysisk skade på mennesker eller omfattende forstyrrelser af kritisk infrastruktur.

Så alvorlige cyberangreb forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten er samtidigt yderst begrænset.

CFCS har fulgt truslen fra cyberterror siden 2016 med fokus på militante ekstremister. Center for Terroranalyse ved PET vurderer for nuværende, at truslen fra konventionel terror mod Danmark er alvorlig. Derfor følger CFCS udviklingen, uagtet at truslen fra cyberterror har været vurderet til **INGEN** i flere år.

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen tegn på en trussel. Der er ingen aktør, der både har kapacitet til og intention om angreb/skadelig aktivitet.
LAV	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men enten er kapaciteten eller intentionen eller begge dele begrænset.
MIDDEL	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men der er ikke indikationer på specifik planlægning af angreb/skadelig aktivitet.
HØJ	En eller flere aktører har kapacitet til og foretager specifik planlægning af angreb/skadelig aktivitet, eller har allerede gennemført eller forsøgt angreb/skadelig aktivitet.
MEGET HØJ	Der er enten oplysninger om, at en eller flere aktører iværksætter angreb/skadelig aktivitet, herunder oplysninger om tid og mål, *eller* en eller flere aktører iværksætter kontinuerligt angreb/skadelig aktivitet.

Et givent trusselsniveau er udtryk for FE's vurdering af aktørers intention, kapacitet og aktivitet på baggrund af de tilgængelige oplysninger.