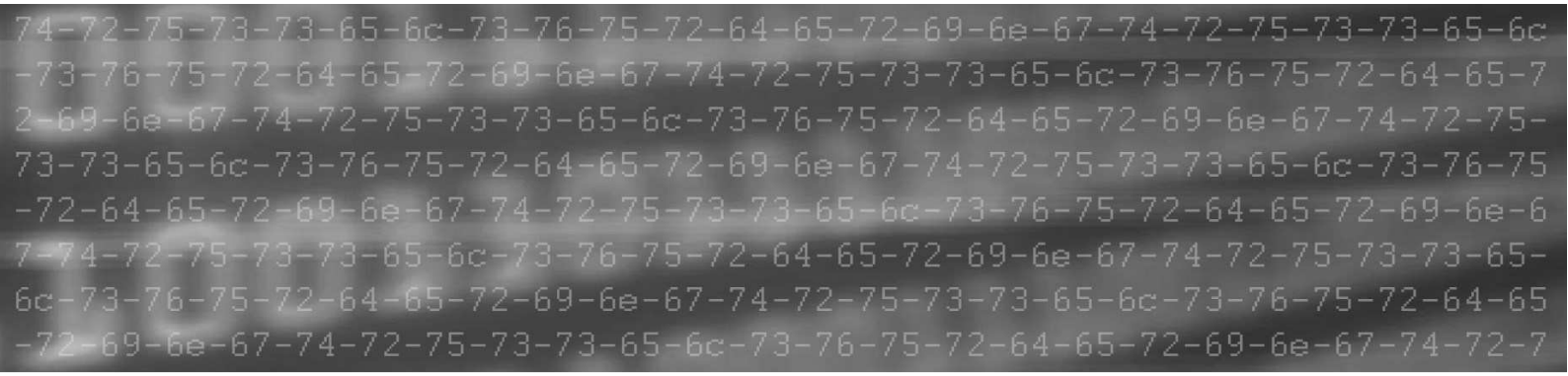
CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod finanssektoren



Trusselsvurderingsenheden ved Center for Cybersikkerhed

August 2018

CENTER FOR CYBERSIKKERHED

Trusselsvurdering: Cybertruslen mod finanssektoren

Trusselsvurderingen redegør for de cybertrusler, der er rettet imod den danske finanssektor. Finanssektoren i Danmark er vigtig for samfundets funktion, stabilitet og økonomi. Hensigten er at orientere finanssektoren om truslerne, så den bedre kan beskytte sig. Trusselsvurderingen kan eksempelvis indgå i risikovurderingen for sektoren i forbindelse med den nationale strategi for cyber- og informationssikkerhed.

Hovedvurdering

- Truslen fra cyberkriminalitet mod den danske finanssektor er **MEGET HØJ**. Truslen fra cyberkriminalitet bliver fortsat mere avanceret og kompleks, og cyberkriminelle angreb kan forstyrre tilgængeligheden af den danske finanssektors ydelser.
- Truslen fra cyberspionage er **HØJ**. Det er sandsynligt, at fremmede stater har både politiske og økonomiske interesser i at udføre cyberspionage mod den danske finanssektor.
- Truslen fra cyberaktivisme mod den danske finanssektor er **MIDDEL**. For danske finansielle virksomheder kan truslen mod den enkelte virksomhed ændre sig pludseligt, hvis den kommer i aktivisters søgelys af politiske eller ideologiske årsager.
- Truslen fra cyberterrror er **LAV.** Militante ekstremister har i få tilfælde ytret intentioner om at udføre cyberterror, men de har ikke kapacitet til dette på nuværende tidspunkt.
- 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 ramt utilsigtet eller kan blive påvirket af destruktive cyberangreb mod mål udenfor Danmark.

Indledning

Trusselsvurderingen beskriver den generelle cybertrussel mod den danske finanssektor. Vurderingen tager primært udgangspunkt i nordiske og internationale eksempler på cyberangreb mod finanssektoren, som sammenholdes med danske forhold samt viden om trusselsaktørernes kapacitet og intention.

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 derfor vigtigt, at virksomhederne, infrastrukturen og ydelserne er tilgængelige, troværdige og stabile, så borgere og virksomheder med fuld tillid til systemernes integritet f.eks. kan foretage ind- og udbetalinger, optage lån eller handle værdipapirer.

At cyberangreb potentielt kan have alvorlige konsekvenser for Danmark ses i Finanstilsynets undersøgelse af systemisk risiko for første halvår 2018. Det fremgår, at danske finansielle virksomheder anser cyberforhold som den største risikokilde i forhold til hvilke risici, som har størst betydning for den finansielle stabilitet i Danmark i de kommende tre år. Af samme rapport fremgår også, at cyberforhold er den risiko, som er mest udfordrende for virksomhederne at håndtere.

Finanssektoren består af forskellige virksomheder, der varetager mange forskellige funktioner. Finanssektoren inkluderer i denne vurdering virksomheder, som er underlagt finansiel regulering. Det drejer sig om banker, realkreditinstitutter og forsikringsselskaber, men også virksomheder som beskæftiger sig med finansiel infrastruktur såsom datacentraler, børser m.fl. Myndigheder og offentlige finansielle institutioner som eksempelvis Finanstilsynet og Nationalbanken indgår også i finanssektoren. Da markedet for kryptovalutaer på nuværende tidspunkt i udgangspunktet ikke er omfattet af finansiel regulering, indgår det ikke i trusselsvurderingen. Trusselsvurderingen giver et overblik over cybertruslerne mod finanssektoren i Danmark som helhed, og der skelnes kun mellem enkeltdele af sektoren i begrænset omfang.

Danske finansielle institutioner er i høj grad forbundet gennem en samlet digital infrastruktur. Finanssektorens robusthed overfor cyberangreb afhænger i nogen grad af alle organisationerne, da de med svag cybersikkerhed kan blive udnyttet af hackere med det formål at ramme bedre beskyttede organisationer. Den danske finanssektor kan også blive påvirket af cyberangreb, der rammer udenlandske eller internationale samarbejdspartnere eller modparter.

Interbankmarkedet
Interbankmarkedet er markedet for indbyrdes transaktioner mellem pengeinstitutter og omfatter alle finansielle produkter, herunder låneaftaler, rentederivater og handel med valuta.

SWIFT
SWIFT står for Society for Worldwide Interbank Financial Telecommunication. Det er et internationalt finansielt datanetværk, der gør det muligt for finansielle institutioner at sende og modtage betalingsdata.

Det skyldes, at danske finansielle institutioner også er forbundet med udenlandske finansielle institutioner f.eks. gennem interbankmarkedet, som flere gange er blevet udnyttet i cyberangreb. Cyberangreb mod centrale leverandører af f.eks. software til finanssektoren udgør også en trussel, da hackerne kan bruge leverandørerne som et springbræt til deres egentlige mål.

Hvad er cybertrusler
Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) definerer cybertrusler som trusler fra cyberangreb, hvor en aktør ved hjælp af it forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester. Anden brug af internettet, der kan have negative konsekvenser for samfundet, såsom facilitering af hvidvaskning af penge, indgår ikke i denne definition af cybertrusler.

Trusselsbilledet kan beskrives ud fra flere vinkler. I denne vurdering er der fokus på, hvilket formål anvendelsen af cyberangreb har for de aktører, der udfører dem. CFCS beskriver og vurderer her aktiviteter, der har til formål at udføre cyberspionage, cyberkriminalitet, cyberaktivisme eller cyberterror. Desuden vurderer CFCS den potentielle trussel fra destruktive cyberangreb.

Trusselsniveauerne er baseret på en analyse af aktørernes intention og cyberkapaciteter. CFCS vurderer en aktørs cyberkapacitet ud fra de menneskelige og materielle ressourcer, aktøren har til rådighed. Det kan være teknisk dygtige hackere og udviklere af malware eller viden om mål, der kan bruges til eksempelvis social engineering. Det kan også være it-infrastruktur, tid, penge og adgang til information. Hvor stor en cyberkapacitet, en aktør har, vil derfor afhænge af flere forskellige forhold og aktørens evne til at udnytte dem.

Vurderingen tager udgangspunkt i det aktuelle trusselsbillede og har en varslingshorisont på op til to år. Da cybertruslen er dynamisk, kan trusselsbilledet på nogle områder ændre sig pludseligt, både generelt og for den enkelte myndighed eller virksomhed. Vurderingen anvender Forsvarets Efterretningstjenestes trusselsniveauer og sandsynlighedsgrader, der er forklaret i slutningen af vurderingen.

Der er mørketal, når det gælder viden om cyberangreb mod myndigheder og virksomheder i bl.a. finanssektoren. Mørketallene skyldes bl.a., at nogle cyberangreb ikke bliver anmeldt til relevante myndigheder, enten fordi organisationen ønsker mindst mulig opmærksomhed omkring et angrebsforsøg, eller fordi de ikke er klar over, at de har været udsat for angreb. Der er ved lov, i maj 2018, indført nye indberetningsordninger, der forventeligt vil give bedre indsigt i cyberangreb mod samfundsvigtige virksomheder.

Cyberkriminalitet

Truslen fra cyberkriminalitet mod finanssektoren er **MEGET HØJ**. Cyberkriminalitet dækker i denne vurdering handlinger, hvor gerningsmanden bruger cyberangreb til at begå kriminalitet, som er motiveret af ønsket om økonomisk vinding.

Truslen fra cyberkriminalitet mod finanssektoren er rettet både mod virksomhederne og deres kunder. Truslen mod virksomhederne i finanssektoren er størst fra avancerede, målrettede cyberangreb, som finder sted med relativt lav frekvens. Cyberkriminelle forsøger bl.a. at stjæle likvider og data fra finansielle virksomheder.

De cyberkriminelle angreb mod finanssektorens kunder er mindre sofistikerede og med mindre afkast, men til gengæld angriber hackerne mange personer på én gang, og de angriber ofte igen og igen. Grundlaget for de cyberkriminelle er stort, bl.a. fordi stort set alle danskere og danske virksomheder anvender netbank eller mobilbank.

Hvor cyberkriminalitet mod virksomhederne i finanssektoren kan have konsekvenser for sektorens samfundsvigtige funktioner og i værste fald true den finansielle stabilitet, så kan cyberkriminalitet mod virksomhedernes kunder særligt skade tilliden til sektoren.

Truslen fra cyberkriminalitet bliver stadigt mere kompleks
Cyberkriminelle aktører, som angriber finanssektoren, kan være alt fra enkeltpersoner, der retter usofistikerede angreb mod mange mål, til avancerede aktører med væsentlige cyberkapaciteter, der målrettet går efter enkelte virksomheder eller myndigheder. Nogle af de avancerede cyberkriminelle grupper er velorganiserede og opererer som virksomheder med ledelsesstrukturer og f.eks. enheder til udvikling og test af malware og til hvidvaskning af penge. Trusselsbilledet, som finanssektoren står overfor, kompliceres yderligere af, at statsstøttede hackere sandsynligvis også retter cyberangreb mod finanssektoren med det formål at opnå økonomisk vinding. Angrebstyper og aktører, som finanssektoren skal forsvare sig mod, er dermed blevet mere avancerede.

CFCS vurderer, at en delmængde af den cyberkriminalitet, der rammer sektoren, fortsat bliver mere kompleks, og at de avancerede cyberkriminelle grupper fortsat bliver mere målrettede i deres angreb. Hackerne bliver bl.a. mere målrettede i forhold til, hvilke regioner, lande, virksomheder og kundesegmenter de angriber.

De cyberkriminelle er opfindsomme og hurtige til at udnytte nye teknikker, sårbarheder og angrebsmetoder. Eksempelvis har nogle hackere kapacitet til på kort tid at udvikle nye varianter af malware, så de kan omgå antivirusløsninger. Til tider går der kun få dage fra, at et første angreb bliver afværget, til at hackerne angriber igen med en lettere modificeret version af malwaren. Visse aktører har i løbet af 2017 reduceret antallet af dage mellem nye malware-versioner helt ned til én dag. Sektoren står derfor overfor en trussel, der hele tiden udvikler og tilpasser sig.

Cyberkriminelle sælger også deres ydelser og værktøjer, hvilket gør, at kriminelle uden de store itkompetencer kan udgøre en mere alvorlig trussel. Hackere sælger og deler også mere avancerede værktøjer og sårbarheder på internettet. Det betyder, at værktøjer og sårbarheder, der tidligere primært blev udnyttet af stater, i nogen grad også bruges af cyberkriminelle hackere, der ikke har tilknytning til stater.

Cyberkriminelle har på globalt plan rettet mange forskellige typer cyberangreb mod finansielle virksomheder og myndigheder. En række af disse beskrives på de følgende sider. Selvom visse af disse angrebstyper endnu ikke er blevet rettet mod den danske finanssektor, så vurderer CFCS, at de er en del af sektorens samlede trusselsbillede.

Hackere stjæler penge i avancerede digitale bankrøverier
De seneste år har der været en række avancerede cyberangreb mod banker i udlandet, hvor det er lykkedes at stjæle betragtelige beløb. Angrebene har desuden også i få tilfælde forstyrret tilgængeligheden af de berørte bankers ydelser. I flere af de digitale bankrøverier har hackerne udnyttet interbankmarkedets infrastruktur. Eksempelvis blev en indisk bank, City Union Bank, i februar 2018 udsat for et angreb, hvor hackerne forsøgte at stjæle to millioner US dollars ved at kompromittere bankens systemer og derigennem foretage uautoriserede overførsler via SWIFT-netværket. Angrebet lykkedes dog kun delvist, da nogle af de uautoriserede overførsler blev opdaget og stoppet. Samarbejde mellem banker har i flere tilfælde forhindret de cyberkriminelle i at gennemføre de uautoriserede pengeoverførsler, således at angrebene er blevet helt eller delvist afværget. I 2016 og 2017 lykkedes det dog samlet set hackere at stjæle beløb svarende til over 500 millioner danske kroner ved at udnytte netop

SWIFT-netværket, efter at de havde kompromitteret lokale banker. Bankerne var i flere tilfælde tilsyneladende blevet kompromitteret ved hjælp af spear phishing-mails sendt til medarbejdere. Flere sikkerhedsfirmaer har tilskrevet en del af disse digitale bankrøverier til hackergrupper, som CFCS vurderer har tilknytning til Nordkorea.

Der er andre finansielle datanetværk end SWIFT, der gør det muligt for finansielle institutioner at sende og modtage betalingsdata. Disse datanetværk kan også blive udnyttet i digitale bankrøverier. Det mexicanske finansielle datanetværk SPEI blev i foråret 2018 udnyttet til at stjæle penge fra banker i Mexico. Den mexicanske centralbank offentliggjorde i maj 2018, at fem unavngivne banker var blevet hacket, og at hackerne stjal, hvad der svarer til tæt på 100 millioner danske kroner.

Det er meget sandsynligt, at hackerne forud for de avancerede digitale bankrøverier har udført rekognoscering bl.a. ved at hacke sig til informationer om bankens systemer og processer. Banker, der har været udsat for cyberangreb, hvor hackerne har fået adgang til beskyttelsesværdige informationer eller centrale systemer, er derfor mere sårbare overfor digitale bankrøverier.

I begyndelsen af 2017 blev det polske finanstilsyns hjemmeside udnyttet i et vandhulsangreb til at sprede malware. Angrebet var muligvis en indledende rekognoscering forud for senere cyberangreb. CFCS har ikke kendskab til, om angrebet indtil nu har givet anledning til økonomiske tab blandt ofrene. Vandhulsangrebet muliggjorde, at en række bestemte organisationer, der besøgte tilsynets hjemmeside, blev inficerede med malware. Der var, blandt andre, tre danske finansielle virksomheder, som angrebet var målrettet. Vandhulsangrebet var omfattende, og spredte sig til mere end 100 finansielle virksomheder i mere end 30 lande. Sikkerhedsfirmaer vurderer, at det er samme statslige aktør, der står bag det polske vandhulsangreb, som udførte det digitale bankrøveri mod centralbanken i Bangladesh i 2016.

Vandhulsangreb
Et vandhulsangreb er, når en ellers legitim hjemmeside inficeres med malware med det formål at kompromittere dem, der besøger hjemmesiden. Hackerne kan forsøge at kompromittere alle eller udvalgte besøgende.

Denne aktør er også blevet udpeget af it-sikkerhedsfirmaer som ansvarlig for cyberangreb mod tyrkiske finansielle institutioner i 2018, hvor formålet muligvis var at indsamle informationer til brug for senere angreb. I angrebene i Tyrkiet anvendte aktøren spear phishing-mails, der indeholdt vedhæftede filer med en malware kaldet Bankshot.

Hackere viser villighed til at slette eller kryptere data i digitale bankrøverier

I få tilfælde har hackere de seneste år vist vilje til at slette eller kryptere finansielle virksomheders data i forbindelse med digitale bankrøverier, sandsynligvis i et forsøg på at slette deres spor eller forhindre virksomhederne i at reagere på tyveriet. CFCS vurderer, at dette også vil kunne ske i forbindelse med et digitalt bankrøveri mod en dansk finansiel virksomhed.

Sletning eller kryptering af data i digitale bankrøverier er foreløbigt et relativt sjældent fænomen, men det kan have potentielt store konsekvenser for den berørte finansielle institution. Hvis hackere lykkes

med at kryptere eller slette kritiske data, kan den berørte institutions ydelser blive forstyrret eller gjort utilgængelige. Eksempelvis slettede hackere ifølge åbne kilder i maj 2018 indhold på computernes harddiske i den chilenske bank Banco De Chile, hvilket forstyrrede nogle af bankens services. Angrebets egentlige formål var umiddelbart at stjæle likvider, og hackerne slettede sandsynligvis data for at besværliggøre efterfølgende efterforskning.

Hackere stjæler informationer fra finansielle virksomheder
CFCS vurderer, at cyberkriminelle også har intention om og kapacitet til at stjæle informationer fra danske finansielle virksomheder.

Finansielle virksomheder er meget dataafhængige i drift og forretning. En stor del af de data, de besidder, kan være værdifulde for hackere, og tyveri af data kan være særdeles kritisk for en finansiel virksomhed i forhold til drift og omdømme. Beskyttelsesværdige oplysninger kan dække over alt fra simple data om kunders kreditkortoplysninger og konti til mere komplekse data om f.eks. kundeforhold, kreditværdighed og andre finansielle forhold, forretningsplaner, børsplaner og lignende. Hertil kommer data om de finansielle virksomheders egne forhold, såsom regnskaber, forretningsplaner, opkøb, software, afvikling- og genopretningsplaner.

De cyberkriminelle kan f.eks. forsøge at stjæle informationer fra finanssektoren for at videresælge dem. I udlandet har en gruppe, som ofte kaldes Carbanak, kompromitteret finansielle virksomheder for bl.a. at stjæle følsomme informationer. De har efter kompromittering bl.a. søgt i virksomhedernes netværk efter konkrete programmer og processer, som vedrørte kreditkortoplysninger. Gruppen har monitoreret ansattes skærmbilleder for at lære at anvende virksomhedens systemer. Efter gruppen har identificeret data og en metode til at tilgå disse, har de eksfiltreret data.

Hackere kan også stjæle data fra finansielle virksomheder for at afpresse dem. CFCS har ikke kendskab til tilfælde i den danske finanssektor, hvor hackere har afpresset offeret med truslen om at lække eller videresælge stjålne informationer. Finansielle virksomheder i andre lande og virksomheder i andre sektorer i Danmark har dog været udsat for dette. I maj 2018 lykkedes det eksempelvis hackere at stjæle cirka 40 GB data fra en brasiliansk bank, hvor der efterfølgende blev krævet en løsesum i bitcoins. Der er en risiko for, at cyberkriminelle forsøger at udnytte den nye persondataforordning til at afpresse myndigheder og virksomheder. De kriminelle kan true med at hacke organisationen, medmindre den betaler. I tilfælde af at de allerede har hacket virksomheden, kan de forlange betaling for ikke at lække eventuelle stjålne data og offentliggøre, at virksomheden er kompromitteret.

Cyberkriminelle kan også forsøge at hacke sig til informationer, som de kan udnytte til insider trading. I marts 2018 forsøgte hackere eksempelvis at få adgang til forsikringsselskabet Trygs systemer, muligvis for at stjæle oplysninger, der kunne bruges til f.eks. insider trading ift. Trygs aktier. Hackerne sendte spear phishing-mails med vedhæftede filer, der indeholdt malware, til fire nøglemedarbejdere. Angrebet blev opdaget i tide, og der skete ingen skade.

DDoS-angreb forstyrrer sektorens online services
DDoS-angreb har været en trussel for tilgængeligheden i finanssektoren igennem de senere år. Internationalt er der mange eksempler på DDoS-angreb mod finanssektoren. I 2017 var Lloyds Bank i Stor-

britannien offer for et kraftigt DDoS-angreb, som forstyrrede bankens online services i to dage. Aktøren krævede en betaling på 75.000 britiske pund i bitcoins for at stoppe angrebet. Det lykkedes myndighederne i Storbritannien at finde frem til aktøren bag angrebet og retsforfølge den ansvarlige person. Et af de mest kendte eksempler på DDoS-angrebs potentielt forstyrrende effekter er helt tilbage fra 2007, da Estland var mål for et omfattende DDoS-angreb, som lammede mange af de samfundsvigtige sektorer, herunder finanssektoren. Det gjorde i perioder to af de største bankers online tjenester utilgængelige.

En årsag til den høje forekomst af DDoS-angreb er også, at simple angreb er lette at udføre ved hjælp af værktøjer, som er tilgængelige via internettet. En hollandsk onlinebank blev i september 2017 gjort utilgængelig af DDoS-angreb udført af en teenager, som ifølge åbne kilder havde købt sig til et DDoS-værktøj på internettet. Teenageren blev anholdt kort efter, at flere hollandske bankers online services blev forstyrret af DDoS-angreb i slutningen af januar 2018, men det er uvist, om teenageren også stod bag disse angreb.

DDoS-angrebstyper

Volumen-angreb overbelaster kapaciteten (båndbredden) på internetforbindelsen.

Protokol-angreb overbelaster kapaciteten på en firewall, router eller anden netværkskomponent.

Applikations-angreb udnytter svagheder i programmerne på en netværkskomponent, f.eks. en webserver.

Færre, men mere målrettede ransomware-angreb fremover

Ransomware har indtil videre været en meget udbredt angrebsform, som fortsat udgør en trussel mod finanssektoren. Ransomware gør offerets data eller systemer utilgængelige, og bagmændene kræver en løsesum for at gøre disse tilgængelige igen. Efter et par år, hvor antallet af ransomware-angreb steg betragteligt, beretter it-sikkerhedsfirmaer om, at antallet af angreb er faldende. Det er dog muligt, at ransomware-angreb vil blive mere målrettede og avancerede, så de fremover f.eks. vil udgøre en trussel mod virksomheders infrastruktur eller produktionslinjer.

Ransomware kan også bruges i sammenhæng med andre typer angreb mod finanssektoren. I åbne kilder er det blevet beskrevet, at hackere, der stjal penge fra Far Eastern International Bank i Taiwan i 2017, også rettede et ransomware-angreb mod bankens systemer for at aflede opmærksomheden eller skjule deres spor.

Business Email Compromise (BEC) scams er en udfordring

Såkaldte BEC-scams er fortsat en udfordring i alle sektorer, herunder finanssektoren. BEC-scams har til formål at franarre virksomheder og myndigheder penge via e-mails, der indeholder instrukser om at gennemføre pengeoverførsler til aktøren. For at udnytte medarbejdernes loyalitet udgiver de kriminelle sig typisk for at være en ledende medarbejder i organisationen. Bedrageri af denne type kaldes derfor også ofte for CEO-fraud eller direktørsvindel. Finanssektoren behandler dagligt tusinder af transaktioner, hvor tid ofte er en afgørende faktor. Det kan gøre sektoren sårbar overfor BEC-scams, da det kan være vanskeligt for medarbejdere at verificere, om anmodningerne er legitime på grund af tidspres.

De bedrageriske e-mails sendes ofte fra fremmede mailkonti, som er manipuleret til at ligne velkendte adresser, men aktøren kan også misbruge kompromitterede mailkonti, der tilhører medarbejdere i virksomheden. Hvis en aktør er lykkedes med at kompromittere medarbejderes konti, øger det risikoen for et succesfuldt bedrageriforsøg, bl.a. fordi hackerne dermed ofte også har adgang til informationer, der ikke er offentlige tilgængelige.

Malware, der udvinder kryptovaluta, kan gøre systemer langsommere

Der er en stigende tendens til, at cyberkriminelle benytter malware, som misbruger ofrets computerkapacitet til at genere kryptovaluta såsom bitcoins. Denne type angreb er sandsynligvis ansporet af, at kryptovalutaers værdi er steget betydeligt. Det er muligt, at større kursfald for kryptovalutaer kan medføre, at denne type angreb bliver mindre hyppige. It-sikkerhedsfirmaer rapporterer også om, at der kan være en sammenhæng mellem fald i ransomware og en stigning i malware, der udvinder kryptovaluta. Et fald i kryptovalutaers kurs kan derfor potentielt også medføre en stigning i brugen af ransomware igen.

Det kræver typisk anselige ressourcer af det inficerede system at genere kryptovaluta, hvilket kan påvirke servere og skabe driftsforstyrrelser, længere svartider og i værste tilfælde nedbrud. Finansielle systemer og software, som inficeres med malware, der misbruger processorkraft, kan derfor have konsekvenser for tilgængeligheden i finanssektoren. Malware, der udvinder kryptovaluta, kan derudover være problematisk i forbindelse med de dele af finanssektorens arbejde, der er tidskritisk, såsom refinansieringsauktioner, emissioner eller almindelig værdipapirhandel. Værdipapirhandel er udelukkende elektronisk, og det stiller store krav til børsernes handelsservere og den hastighed, som handler kan gennemføres med. Hvis en handelsservers processorkraft misbruges, kan det nedsætte hastigheden, hvormed markedsdeltagere på børserne kan handle og udveksle information om værdipapirer med hinanden. Sænkes den drastisk, fordi serverens kapacitet er overbelastet, kan det i yderste konsekvens betyde, at markedsdeltagere ikke kan gennemføre handler på værdipapirmarkederne, eller at informationen bliver meget forsinket.

Selv hvis det ikke medfører driftsforstyrrelser, er det problematisk, hvis systemerne i finansielle virksomheder eller myndigheder bliver inficeret med malware, der udvinder kryptovaluta. De cyberkriminelle kan senere benytte adgangen til systemet til andre formål eller forvolde utilsigtet skade. Malwaren kan også have et ressourceforbrug, der gør, at it-afdelingen starter en større undersøgelse af, hvad der forårsager forbruget. Det kan lægge beslag på it-afdelingens tid og ressourcer at fjerne malwaren, og systemerne kan være utilgængelige, mens arbejdet står på.

Cyberangreb mod hæveautomater sker primært i udlandet

En anden teknik, som anvendes af cyberkriminelle grupper, er malware rettet mod hæveautomater, som har givet anledning til større tyverier af kontanter. CFCS er ikke bekendt med, at denne angrebsform er udbredt i Danmark, men det er sket i 2017. It-sikkerhedsfirmaer rapporterer generelt om en stigning i brugen af malware rettet mod hæveautomater udenfor Europa. Angreb mod hæveautomater foregår eksempelvis ved, at en person forklædt som tekniker skaber sig fysisk adgang til en hæveautomat f.eks. med en telefon eller PC, som installerer malware. Aktøren kan så få hæveautomaten til at udbetale kontanter på bestemte tidspunkter, hvor pengene efterfølgende hentes af andre medlemmer

af den kriminelle gruppe kaldet ”money mules”. I nogle angreb på hæveautomater i udlandet har malwaren også stjålet kortoplysninger fra kunder, der har anvendt hæveautomaten. CFCS er bekendt med, at gruppen kaldet Cobalt Gang er aktive i Norden, og at gruppen har forsøgt at få adgang til nordiske bankers systemer. Gruppen har foretaget cyberangreb i udlandet bl.a. mod hæveautomater ved at kompromittere bankers IT-systemer.

Betalingskortoplysninger bliver også stjålet i cyberangreb mod mål udenfor sektoren
Cyberkriminelle er i årevis gået efter kunders betalingskortoplysninger for at misbruge eller videresælge dem. Ofte stjæler hackere betalingskortoplysninger ved at kompromittere virksomheder eller systemer, der ikke er en del af finanssektoren. Det kan f.eks. være en webbutik, som har en sårbarhed i sit betalingssystem, de cyberkriminelle udnytter. Selvom de hackede virksomheder ikke er en del af finanssektoren, så berører det alligevel sektoren, der bruger ressourcer på at håndtere misbruget af kundernes betalingskort.

Der er mange eksempler på, at cyberkriminelle har kompromitteret udenlandske virksomheder og fået adgang til betalingskortoplysninger, som i nogle tilfælde har involveret kort udstedt i Danmark. I 2016 anbefalede Nets de danske banker at udskifte 100.000 betalingskort præventivt, fordi der var risiko for, at kortinformationerne var blevet kompromitterede. Nets, der udbyder betalingskort i Danmark, meddelte, at kilden til udnyttelsen var en udenlandsk webbutik. Det var en af de største potentielle kompromitteringer af danske betalingskort. Et nyere eksempel på kompromittering af betalingsoplysninger er fra 2018. I slutningen af juni 2018 informerede Ticketmaster UK om, at de havde fundet ondsindet software på et kundesupportprodukt hostet af en ekstern leverandør, og at kunders betalingsoplysninger muligvis var blevet kompromitterede. Danske kunder, der havde handlet hos Ticketmaster i en bestemt periode, blev som en sikkerhedsforanstaltning opfordret til at overvåge deres kontoudskrifter for muligt bedrageri. Seneste misbrugstal fra Nets viser dog et fald i anmeldelser af misbrug af betalingskort i webbutikker. Det skyldes sandsynligvis gradvis indførelse af 2-faktor autentifikation på Dankort, som begyndte i maj 2017.

Malware stjæler loginoplysninger til kunders netbank
Malware udgør fortsat en væsentlig trussel mod finanssektorens kunder med tab af likvider som følge. Malware leveres ofte til ofrene ved hjælp af phishing-mails fra hackere. Aktører anvender bl.a. malware til at stjæle kundernes loginoplysninger til deres netbank. Malwaren TrickBot viderestiller f.eks. kunden til en falsk netbank-side, som ligner brugerens egen netbank. Efter at kunden har indtastet sine loginoplysninger til netbanken, sørger malwaren for, at kunden bliver logget ind på den legitime netbank, men at loginoplysningerne samtidig bliver sendt til hackerne.Trickbot har tidligere været rettet mod danske banker, og det er meget sandsynligt, at malware med lignende funktioner igen vil blive målrettet kunder i den danske finanssektor.

Malware rettes også mod bankers apps til mobiltelefoner. Malwaren danner et falsk skærmbillede henover den legitime app på enheden. Her bliver brugeren bedt om at indtaste eksempelvist kreditkortoplysninger, som malwaren opsamler. Det er vanskeligt for brugerne at opdage, da appen ser ud til at virke som normalt. Sikkerhedsfirmaer rapporterer om, at den seneste udvikling viser, at aktørerne er begyndt at målrette malware mere specifikt mod kundesegmenter, f.eks. mod henholdvis private kunder og institutionelle kunder for at gøre malwaren mere effektiv.

CFCS vurderer, at truslen fra malware rettet mod danske apps til mobilbank er stigende, idet kompleksiteten og omfanget af malwaren er steget markant. Stadig flere kunder anvender apps i relation til finansielle tjenesteydelser, som har gjort grundlaget for aktørernes profit væsentligt større. Aktører har udviklet malware rettet specifikt mod apps, som er udviklet af den danske finanssektor. Eksempelvis er malwaren Red Alert ifølge sikkerhedsfirmaer udviklet til mobilbank-apps for bl.a. de fem største danske banker.

It-sikkerhedsfirmaer har senest set malware til bankers apps udviklet i udgaver med key-logger funktioner, som kan opfange og lagre alle brugerens øvrige indtastninger på mobiltelefonen. Hackere har også udbygget malware til bankers apps, så hackerne kan vælge at bruge malwaren til at kryptere offerets mobil eller til at udvinde kryptovaluta.

Cyberspionage

Truslen fra cyberspionage mod danske finansielle virksomheder er **HØJ**. CFCS vurderer, at truslen især kommer fra fremmede stater. Det er sandsynligt, at fremmede stater har både politiske og økonomiske interesser i at udføre cyberspionage mod den danske finanssektor. Det generelle niveau for cyberspionage mod Danmark er MEGET HØJ, da fremmede stater vedholdende forsøger at stjæle informationer fra staten og visse sektorer. CFCS har ikke kendskab til et ligeså højt aktivitetsniveau mod finanssektoren, men vurderer, at fremmede stater både har intention og kapacitet til at udføre cyberspionage mod sektoren. Truslen fra cyberspionage kan være højere for enkelte institutioner i finanssektoren.

Fremmede stater kan f.eks. foretage cyberspionage mod finanssektoren for at få indsigt i investeringer eller potentielle virksomhedsopkøb. Staterne kan også have interesse i at spionere mod danske virksomheder for at videregive informationer til deres hjemlige virksomheder for at give dem konkurrencemæssige fordele. Fremmede stater kan derfor have en særlig interesse i danske finansielle virksomheder, som driver forretning i udlandet, eksempelvis gennem filialer eller datterselskaber.

Det kan have store konsekvenser for Danmark, hvis fremmede stater får uønsket adgang til værdifulde oplysninger om f.eks. den finansielle infrastruktur eller følsom data fra en større finansiel virksomhed. Udover at have samfundsøkonomiske konsekvenser kan det skade den danske finanssektors ry og påvirke borgeres, kunders og samarbejdspartneres tillid til sektoren.

Cyberspionage kan derudover understøtte andre typer cyberangreb og trusler. En allerede kompromitteret virksomhed eller myndighed er derfor mere sårbar over for destruktive cyberangreb og hack og læk angreb.

Cyberspionage kan bl.a. afdække sårbarheder i finanssektoren i tilfælde af en fremtidig skærpet konflikt. Den viden kan anvendes forud for destruktive cyberangreb.

Cyberspionage kan også give en modstander adgang til følsomme oplysninger, der senere kan lækkes til offentligheden med henblik på at påvirke meningsdannelsen. Lækager af stjålne informationer kan finde sted som del af bredere påvirkningskampagner. Eksempelvis kan følsomme informationer fra

banker om f.eks. politikeres økonomi eller investeringer lækkes for at sætte politikerne i et dårligt lys. Informationer om f.eks. større finansielle virksomheders solvens eller forventninger til fald i markedspriser, eksempelvis på værdipapirmarkederne, kan også lækkes i et forsøg på at påvirke den enkelte finansielle virksomheds økonomi og værdi og derigennem Danmarks nationaløkonomi. CFCS har dog ikke kendskab til eksempler på hack og læk angreb mod den danske finanssektor.

Cyberaktivisme

Truslen fra cyberaktivisme mod den danske finanssektor er **MIDDEL**.

Cyberaktivisme er typisk drevet af ideologiske eller politiske motiver, og cyberaktivister fokuserer ofte på personer eller organisationer, de opfatter som modstandere af deres sag. Nogle hackergrupper og individer i cyberaktivistiske netværk har væsentlige evner og ressourcer til at udføre cyberangreb. Truslen kan derfor pludselig stige, hvis danske finansielle virksomheder kommer i cyberaktivisters søgelys. Finansielle virksomheder bør dermed 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.

Hackere, der hævder at tilhøre hackerkollektivet Anonymous, har eksempelvis i årevis opfordret til og varslet cyberangreb mod større finansielle institutioner i verden. I 2010 rettede Anonymous aktivister DDoS-angreb mod bl.a. Visa, Mastercard og PayPal, efter at disse virksomheder havde blokeret for deres kunders mulighed for at donere til WikiLeaks. I en efterfølgende retssag mod nogle hackere, der havde medvirket i angrebet, angav PayPal, at angrebet havde kostet virksomheden 3,5 millioner britiske pund.

Cyberaktivister anvender også andre angrebsformer end DDoS-angreb til at skabe opmærksomhed om deres sag. Cyberaktivister hacker og lækker blandt andet følsomme data eller udfører såkaldte defacement-angreb, hvor de indsætter budskaber på hackede hjemmesider. I maj 2018 hackede en italiensk gruppe, der kaldte sig AnonPlus og brugte Anonymous' grafiske og sproglige udtryk, en mindre dansk banks hjemmeside. Hackerne udskiftede bankens normale hjemmeside med AnonPlus' politiske manifest, hvori de bl.a erklærede sig som modstandere af finansielle institutioner. Hackerne havde ikke adgang til kundernes oplysninger, men angrebet medførte, at services som f.eks. netbank ikke var tilgængelige, mens angrebet stod på.

Finansielle myndigheder eller virksomheder i Danmark kan blive mål for cyberaktivisme, selvom de ikke har en egentlig forbindelse til den sag, der har fanget hackernes opmærksomhed. Det kan skyldes, at hackerne betragter myndigheden eller virksomheden som et symbolsk mål. Myndigheder eller virksomheder, som er meget eksponerede i offentligheden, kan også blive mål, idet det potentielt giver aktørernes budskab større opmærksomhed. Hvem, der bliver angrebet, kan i visse tilfælde også være styret af opportunistisme og afhænge af, hvor aktørerne kan skaffe sig adgang eller udnytte sårbarheder.

Det er sandsynligt, at tyrkiske cyberaktivister i september 2017 så Nationalbanken som et symbol på staten Danmark, da de rettede DDoS-angreb mod Nationalbankens hjemmeside. Angrebet var sand-

synligvis en reaktion på en debat om Muhammed-tegningerne kort forinden, som Nationalbanken ikke var en del af.

Cyberterror

Truslen fra cyberterror mod finanssektoren er **LAV**.

CFCS vurderer, at militante ekstremister har begrænsede evner og ressourcer til at udføre alvorlige cyberangreb. Selvom militante ekstremister i få tilfælde har ytret interesse for at udføre cyberterror, har de aktuelt ikke kapacitet til dette.

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

Destruktive cyberangreb

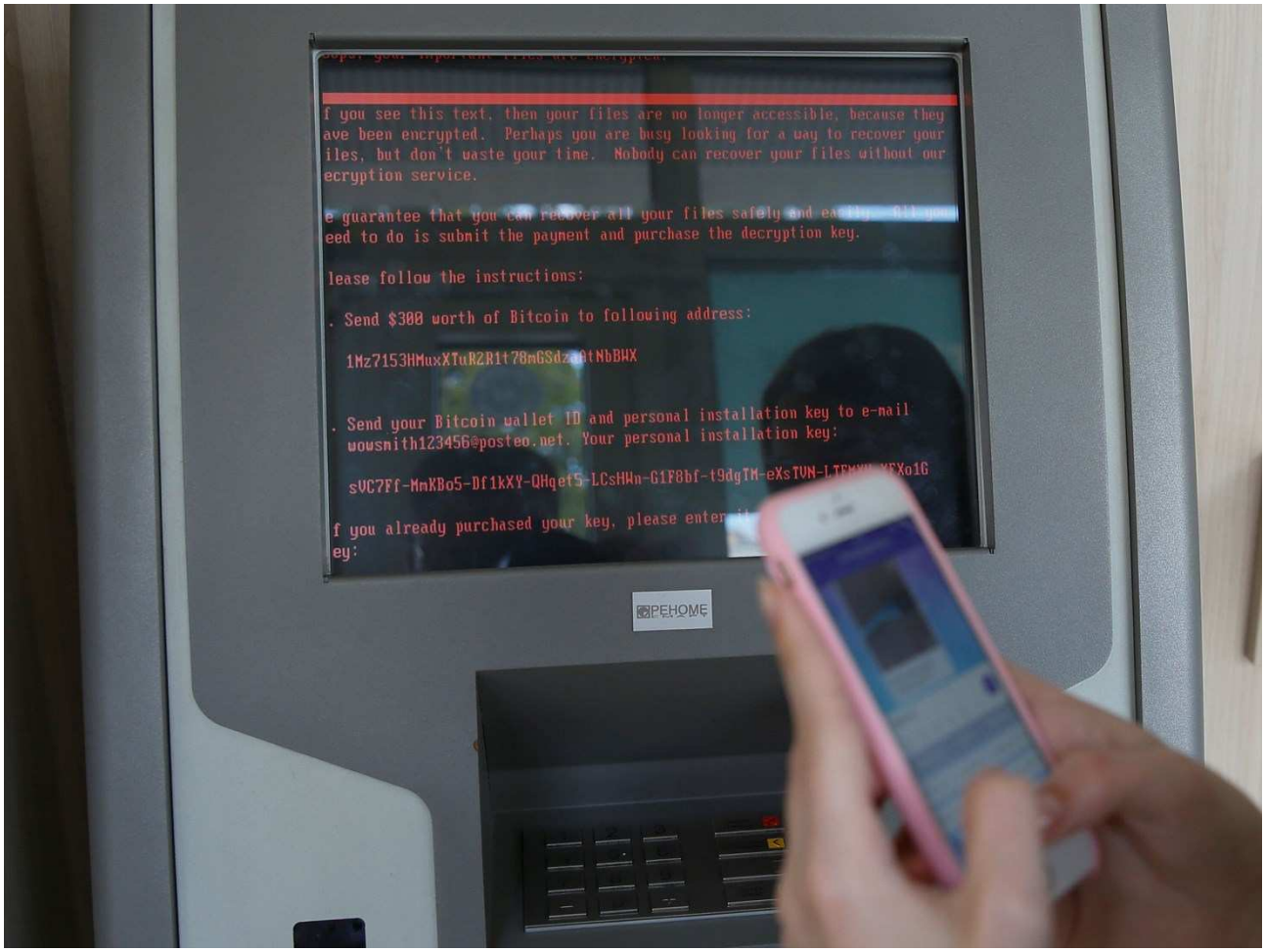
En række lande har cyberkapaciteter, der potentielt kan bruges destruktivt mod samfundsvigtig infrastruktur såsom finanssektoren.

CFCS vurderer, at det er mindre sandsynligt, at fremmede stater har til hensigt at ramme dansk samfundsvigtig infrastruktur, herunder finanssektoren, med destruktive cyberangreb. Truslen kan stige i forbindelse med en skærpet politisk eller militær konflikt, hvor Danmark deltager.

Destruktive cyberangreb
CFCS definerer et destruktivt cyberangreb som et cyberangreb, hvor den forventede effekt er død, personskade, betydelig skade på fysiske objekter eller ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning.

På nuværende tidspunkt er det dog muligt, at danske myndigheder og virksomheder kan blive ramt som følgevirkning af destruktive cyberangreb mod mål uden for Danmark. Det gælder især danske virksomheder fra bl.a. finanssektoren, der er til stede i konfliktområder, hvor fremmede stater eller organiserede hackergrupper med kapacitet til at udføre destruktive cyberangreb har interesser, såsom i dele af Østeuropa, Mellemøsten og Sydøstasien.

Udenlandske finansielle virksomheder i Ukraine og Sydkorea er blevet ramt af destruktive cyberangreb, som har haft betydning for tilgængeligheden af finansielle ydelser. I slutningen af 2016 blev Ukraines finansministerium og andre finansielle myndigheder inficeret med en malware, der slettede data. Bankoverførsler blev forsinkede eller helt stoppet, hvilket også havde konsekvenser for borgere. I 2017 blev ukrainske banker også ramt af NotPetya-angrebet, som sandsynligvis var et destruktivt cyberangreb forklædt som et ransomware-angreb. Den ukrainske bank Oschadbank blev hårdt ramt, og effekten var meget synlig, da kravet om løsepenge stod på bankens hæveautomaters skærme i Kiev.



Hæveautomat i Kiev sat ud af funktion af NotPetya-angrebet

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

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

FE bruger denne skala for sandsynlighed i analyser: