CENTER FOR CYBERSIKKERHED

Trusselsvurdering 2020:

Cybertruslen mod Danmark

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave juni 2020.

Cybertruslen mod Danmark

Denne vurdering informerer beslutningstagere i myndigheder og virksomheder samt offentligheden om cybertruslen mod Danmark. Viden om truslen kan bl.a. bruges til at prioritere tiltag for at forbedre cybersikkerheden og beredskabet hos den enkelte myndighed og virksomhed såvel som for Danmark som helhed.

Hovedvurdering

- Cybertruslen er en alvorlig trussel mod Danmark. Cyberangreb har især økonomiske og politiske konsekvenser.

- Hackere har forsøgt at udnytte COVID-19-pandemien til deres fordel. Det udgør et nyt element i det samlede trusselsbillede.

- Truslen fra cyberkriminalitet er **MEGET HØJ**. Truslen er rettet mod alle. Der er en stigende trussel fra målrettede ransomware-angreb mod danske myndigheder og virksomheder.

- Truslen fra cyberspionage er **MEGET HØJ**. Truslen er især rettet mod myndigheder, som arbejder med udenrigs- og sikkerhedspolitik, samt virksomheder, der besidder en viden, som andre stater har interesse i.

- Truslen fra destruktive cyberangreb er **LAV**. Det er mindre sandsynligt, at fremmede stater vil udføre destruktive cyberangreb mod Danmark. Virksomheder og myndigheder, som har aktiviteter i regioner præget af konflikter, er mere udsatte for truslen

- Truslen fra cyberaktivisme er **LAV**. På globalt plan er antallet af aktivistiske cyberangreb faldet de seneste år, og cyberaktivister retter sjældent deres fokus mod danske myndigheder og virksomheder.

- 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.

- Den teknologiske udvikling, herunder udviklingen af kunstig intelligens og kvanteteknologi, skaber både nye muligheder og udfordringer for cybersikkerheden.

Analyse

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) udgiver for femte gang den årlige vurdering af cybertruslen mod Danmark. Cyberangreb bruges af forskellige aktører og skal derfor opfylde forskellige formål.

Vurderingen af cybertruslen er som i tidligere år opdelt i trusler fra cyberangreb, der understøtter kriminalitet, spionage, aktivisme og terrorisme samt destruktive cyberangreb. Truslen fra destruktive cyberangreb har i år for første gang fået et trusselsniveau i erkendelsen af, at destruktive cyberangreb ikke kun er en angrebsmetode, men også kan være et selvstændigt formål.

Truslen fra cyberspionage og cyberkriminalitet er fortsat **MEGET HØJ**. Cybertruslen er derfor fortsat en alvorlig trussel mod Danmark, og det vil den blive ved med at være i fremtiden i takt med den fortsatte digitalisering og afhængighed af digitale tjenester.

CFCS har siden sidst ændret to af trusselsniveauerne. Cyberaktivisme er sat ned til **LAV** fra **MIDDEL**, og cyberterror er sat ned til **INGEN** fra **LAV**. Det sker som konsekvens af en faldende trussel fra begge typer cyberangreb, som beskrevet senere i vurderingen.

I 2020'erne kan nye teknologier såsom kvanteteknologi og kunstig intelligens skubbe udviklingen af cybertruslen og cybersikkerhed i nye retninger på både godt og ondt. Begge teknologier er fokus for dette års tendensanalyse sidst i vurderingen.

Cybertruslen under COVID-19-pandemien
Digitaliseringen har været med til at modvirke konsekvenserne af den sundhedsfaglige krise i forbindelse med COVID-19-pandemien. Behovet for at holde fysisk afstand er bl.a. blevet understøttet af større brug af hjemmearbejde, online møder, hjemmeskoling, sociale medier og ibrugtagningen af nye teknologier og platforme.

Ændringerne har samtidigt vist vores afhængighed af disse digitale løsninger, herunder af deres integritet, fortrolighed og tilgængelighed. Det har medført et øget fokus på cybersikkerheden hos mange myndigheder og virksomheder.

Der er altid hackere, der forsøger at udnytte aktuelle begivenheder, udviklinger eller vilkår til deres fordel. Det er også tilfældet med COVID-19-pandemien, som både fremmede stater og cyberkriminelle har udnyttet ved bl.a. at sende phishing-mails med COVID-19 som tema.

Udnyttelsen af COVID-19 udgør et nyt element i det samlede trusselsbillede, men udnyttelsen af pandemien har i sig selv ikke ændret den generelle trussel væsentligt. Udnyttelsen af COVID-19 har således primært påvirket trusselsbilledet ift. hvilke angrebsmetoder, hackerne vælger. Hovedparten af denne vurdering har derfor fokus på mange andre forhold af betydning for cybertruslen end COVID-19.

Myndigheder og virksomheder kan være mere sårbare under kriser som den igangværende COVID-19-pandemi. It-sikkerheden i mange myndigheders og

virksomheders netværk er under pres fra det ændrede brugsmønster i form af nye hjemmearbejdspladser, og fordi tilgængeligheden af systemerne prioriteres højt.

De ændrede arbejdsvilkår kan give hackere lettere adgang til organisationernes systemer og gøre det sværere at opdage hackerne. Selvom trusselbilledet grundlæggende er uændret, kan myndigheder og virksomheder derfor stå overfor et ændret risikobillede.

Hackere misbruger COVID-19 som tema
CFCS har viden om, at der under COVID-19-pandemien bliver sendt flere phishing-mails til danske myndigheder og virksomheder end normalt. Flere sikkerhedsfirmaer rapporterer også om en stigning i phishing i andre lande siden marts.

Mange af disse phishing-mails misbruger COVID-19 som tema for at øge sandsynligheden for, at modtageren læser mailen og klikker på links eller vedhæftede filer. Hackerne forsøger dermed at udnytte danskernes efterspørgsel på viden om COVID-19 og den nuværende sundhedskrise.

CFCS vurderer, at kriminelle fremadrettet også vil forsøge at udnytte statslige kompensationsordninger som tema i deres phishing-mails.

Under COVID-19-pandemien er der blevet oprettet en relativt stor mængde falske hjemmesider, som bl.a. udnyttes af hackere til at forsøge at franarre danske borgere deres NEMID-oplysninger og andre loginoplysninger. En del af hjemmesidernes domæner lægger sig tæt op ad legitime sundhedsmyndigheders hjemmesider og navne. CFCS samarbejder med andre partnere på at få nedtaget erkendte falske domæner.

Der er desuden set falske applikationer og malware rettet mod mobile enheder, som udnytter COVID-19 som tema. De falske apps kan eksempelvis stjæle informationer fra den mobile enhed.

CFCS vurderer, at hackere under COVID-19-pandemien forsøger at udnytte, at der er et øget behov for fjernadgange, VPN-løsninger samt samarbejds- og kommunikationsplatforme.

Cybertruslen ved overgangen til et nyt årti
Cybertruslen er ikke kun påvirket af aktuelle forhold som COVID-19 men er et resultat af den langsigtede udvikling af hvordan cyberangreb anvendes af såvel stater som ikke-statslige aktører. Med overgangen til et nyt årti er det oplagt at gøre status på udviklingen i cybertruslen i løbet af de seneste år.

Cyberangreb har fortsat hovedsaligt økonomiske og politiske konsekvenser. Der er endnu ikke tale om en generel trussel mod liv og helbred i modsætning til truslen fra eksempelvis krig og terrorisme. Enkeltstående eksempler på cyberangreb med fysisk skadevirkning og konsekvenser ved bl.a. ransomware-angreb mod hospitaler viser

dog, at cyberangreb også udgør en potentiel trussel mod liv og helbred. Med den fortsatte digitalisering af samfundsvigtige funktioner vil cyberangreb i stigende grad kunne få alvorlige konsekvenser i den fysiske verden.

Nogle stater, især Rusland og Kina, bruger cyberspionage meget aktivt og der er ingen tegn på, at truslen fra disse stater vil aftage. Der har i de seneste år været en stigning i antallet af lande, især i Asien, der bruger cyberspionage. Destruktive cyberangreb er med enkelte undtagelser forblevet et regionalt fænomen med særlig tilknytning til konflikten i Ukraine og rivaliseringen mellem Iran og Saudi Arabien. Angrebene kan imidlertid sprede sig og ramme Danmark, som det var tilfældet under NotPetya-angrebet i 2017.

Stigningen i brug af sociale medier og udfordringer forbundet med at vurdere, om information er sand eller falsk, har givet stater nye muligheder for at påvirke befolkninger. Hack og læk i forbindelse med det amerikanske præsidentvalg i 2016 var en ny og alvorlig anvendelse af cyberangreb til at understøtte en påvirkningsoperation, hvor cyberangreb bruges i forsøg på at påvirke den folkelige meningsdannelse i andre lande.

Kriminelle har fortsat digitaliseringen af den traditionelle berigelseskriminalitet. Teknologier som kryptovaluta og værktøjer til anonymisering har givet profitable rammer for et mere udviklet kriminelt miljø med bedre muligheder for samarbejde. Der er eksempler på, at cyberkriminelle indbyrdes bruger franchiseordninger og kundeservice.

Cyberaktivisme har i de seneste år været på retræte med undtagelse af steder præget af sociale og politiske uroligheder. Militante ekstremistiske grupper har været under massivt pres fra den internationale kontraterrorindsats, og det er ikke lykkedes militante ekstremister at udføre alvorlige cyberangreb med et terrorsigte.

Kendte cyberangreb i 2010'erne
Her er eksempler på kendte cyberangreb fra 2010'erne.

Stuxnet (2010) Iranske centrifuger til berigelse af uran blev i 2010 udsat for et destruktivt cyberangreb med malwaren Stuxnet, der medførte fysisk ødelæggelse af centrifugerne.

Saudi Aramco (2012) Det saudiske nationale olie- og gasselskab, Saudi Aramco, blev i 2012 udsat for et cyberangreb, der ødelagde en stor mængde data tilhørende selskabet.

Sony-hacket (2014) Hackere angreb i 2014 filmselskabet Sony Pictures Entertainment, hvor de ødelagde data og systemer og lækkede bl.a. e-mails og kopier af film, der endnu ikke var udkommet.

Strømafbrydelser i Ukraine (2015) I 2015 blev flere elselskaber i det vestlige Ukraine ramt af cyberangreb. Hackerne fik adgang til elselskabernes kontrolsystemer og lukkede for strømmen i op til 6 timer.

Demokraternes Nationale Komité (2016) Demokraternes Nationale Komité i USA blev i 2016 udsat for hack og læk af informationer, bl.a. e-mails, forud for det amerikanske præsidentvalg samme år.

Mirai (2016) Malwaren Mirai blev i 2016 brugt til at lave nogle af de største overbelastningsangreb (DDoS-angreb), der hidtil var set. Et angreb gjorde en række store internettjenester utilgængelige.

WannaCry (2017) WannaCry-ransomwaren begyndte at sprede sig automatisk til computere verden over i maj 2017. WannaCry var i stand til at kryptere filer på ofrets computer, slette originalerne og opkræve en løsesum for at dekryptere filerne igen. WannaCry ramte bl.a. hospitaler i Storbritannien.

NotPetya (2017) NotPetya-malwaren ramte i juni 2017 mange computere på verdensplan. NotPetya udgav sig for at være ransomware, men havde reelt en destruktiv karakter. NotPetya ramte bl.a. A.P. Møller-Mærsk, der har opgjort tabet til mellem 1,6 og 1,9 mia. kr.

OPCW (2018) Russiske efterretningsagenter blev i 2018 taget på fersk gerning af hollandske myndigheder i et forsøg på at skaffe sig adgang til organisationen for forbud mod kemiske våben OPCW's wifi-netværk.

Demant (2019) Den danske producent af bl.a. høreapparater, Demant, blev i 2019 udsat for et ransomware-angreb, der medførte, at virksomheden lukkede ned for it-systemer på tværs af virksomheden. Angrebet medførte et tab på op mod 650 mio. kr.

Georgien (2019) Den 28. oktober 2019 blev Georgien ramt at et omfattende cyberangreb, hvor tre TV-stationer fik afbrudt transmissionen og over 2.000 hjemmesider blev lukket ned af hackerne.

Cybersikkerhed er ved at blive institutionaliseret

Cybersikkerheden har også udviklet sig i det seneste årti. Cybersikkerhed er med den øgede opmærksomhed og regulering samt store cyberhændelser som NotPetya- og WannaCry-angrebene i 2017 flyttet fra it-afdelingerne til direktionsgangene i danske virksomheder og myndigheder. COVID-19-pandemien har som nævnt også øget fokus på cybersikkerheden i kølvandet på de pludseligt ændrede brugsmønstre af digitale tjenester og systemer.

I Danmark blev CFCS oprettet i 2012, og andre lande, herunder Storbritannien, Australien og Canada, har efterfølgende også oprettet nationale cybercentre med udgangspunkt i deres efterretningstjenester. Samfundsvigtige sektorer og virksomheder har opbygget funktioner, som kan højne cybersikkerheden, såsom decentrale cyber- og informationssikkerhedenheder (DCIS), computer emergency response teams (CERT) og operationscentre for cybersikkerhed (SOC).

Mellemstatslig normdannelse og forsøg på at fordømme og afskrække cyberangreb gennem bl.a. offentlige tilskrivninger af cyberangreb og stævninger af udenlandske hackere viser en villighed fra flere lande til at modvirke truslen. Det sker ikke kun ved

at opbygge et stærkt cyberforsvar, men også ved at lægge et pres på de lande, der udgør en cybertrussel.

Nogle lande er villige til at gå endnu længere for at modvirke truslen. Israels bombning af en bygning i 2019, der ifølge Israel husede hackere fra Hamas, er foreløbigt det mest vidtgående eksempel på det.

På trods af denne udvikling er viden om cybertruslen stadig ikke tilstrækkeligt udbredt. Det betyder bl.a., at hackerne fortsat kan misbruge gammelkendte sårbarheder, og at selv simple cyberangreb kan have alvorlige konsekvenser. Det betyder også, at mange cyberhændelser fortsat ikke bliver opdaget eller rapporteret til relevante myndigheder.

Mørketal og underrapportering er dermed fortsat en udfordring for vurderingen af cybertruslen mod Danmark.

CFCS anbefaler, at myndigheder og virksomheder løbende orienterer sig i vejledninger til, hvordan man kan øge cybersikkerheden. Vejledninger, trusselsvurderinger og undersøgelsesrapporter kan findes på CFCS' hjemmeside.

Cybersikkerhed kan føles fjernt, indtil ulykken indtræffer

"We do quite basic and simple things. We help accountants. We saw ourselves as quite distant from cybersecurity issues."

Citatet er fra Olesya Linnyk, som ledte virksomheden Linkos Group, der blev hacket og udnyttet til at starte det mest omfattende destruktive cyberangreb indtil nu, nemlig NotPetya-angrebet i 2017. Hackere misbrugte Linkos Groups software M.E.doc til at levere NotPetya-malwaren til Linkos Groups kunder, herunder A.P. Møller-Mærsk. Citatet fremgår i bogen 'Sandworm' af Andy Greenberg.

Cyberkriminalitet

Truslen fra cyberkriminalitet er **MEGET HØJ.** Det betyder, at det er meget sandsynligt, at danske virksomheder og myndigheder vil blive udsat for forsøg på cyberkriminalitet inden for de næste to år.

Cyberkriminalitet er i denne vurdering en fællesbetegnelse for handlinger, hvor hackere bruger cyberangreb til at begå kriminalitet, som er motiveret af ønsket om økonomisk berigelse.

Cyberkriminalitet udgør en vedvarende og aktiv trussel mod alle danske myndigheder, virksomheder og borgere.

Cyberkriminelle udfører oftest relativt simple angreb mod mange potentielle ofre på en gang, bl.a. gennem phishing-angreb. Der findes dog også netværk med kapacitet til at udføre mere komplekse og tidskrævende cyberangreb, herunder målrettede ransomware-angreb.

Cyberangreb fra kriminelle grupper starter typisk, uden at aktøren på forhånd har udset sig et specifikt offer. De fleste cyberangreb starter som opportunistiske angreb, hvor eksempelvis phishing-mails bliver spredt til tusinder af ofre, eller hvor kriminelle misbruger it-systemer og enheder med kendte sårbarheder.

Cyberkriminelle udnytter også løbende nye sårbarheder. Der går ofte ikke mere end et par uger fra en teknisk sårbarhed bliver offentligt kendt, til den bliver brugt til at forsøge at hacke danske mål med.

Det høje angrebstempo stiller store krav til, at it-afdelingerne i danske myndigheder og virksomheder opdaterer systemer og programmer i tide eller får opsat kompenserende foranstaltninger i de tilfælde, hvor det ikke er muligt at lukke en sårbarhed.

Citrix sårbarhed efterlod mere end tusind danske enheder potentielt sårbare
Et eksempel på hvor hurtigt og let hackere kan tilegne sig adgang til tusindvis af servere udspillede sig i slutningen af 2019 og i starten af 2020, efter en sårbarhed i Citrix-udstyr blev offentliggjort.

De berørte Citrix-enheder anvendes bl.a. til at styre datatrafikken mellem internettet og hjemmearbejdspladser samt kommunikationen mellem webservere og interne it-systemer. Da sårbarheden blev offentliggjort, fandtes der ingen sikkerhedsopdatering, som kunne udbedre sårbarheden. Citrix anviste dog, hvordan indledende modforanstaltninger kunne implementeres.

To uger efter at sårbarheden blev offentlig kendt, blev de første beskrivelser af, hvordan sårbarheden kunne udnyttes, delt på internettet. Herefter var det let for hackere at bruge beskrivelserne som en opskrift på cyberangreb. Dagen efter at vejledningen blev

offentliggjort, registrerede et it-sikkerhedsfirma 290.000 angrebsforsøg og scanninger fra IP-adresser i 42 lande mod bare et enkelt Citrix-system.

I de følgende dage var der meldinger om, at forskellige hackere kæmpede om adgangen til de sårbare systemer. Nogle hackere smed endda de først ankomne hackere ud og lukkede ned for angrebsmuligheden. De ville have systemet for sig selv.

Det er sandsynligt, at hackerne brugte offentlige søgemaskiner såsom Shodan til at finde sårbare Citrix-enheder i verden, som de kunne forsøge at kompromittere. En søgning i Shodans database ved offentliggørelsen af sårbarheden viste over tusind potentielt sårbare enheder i Danmark.

CFCS er bekendt med flere danske organisationer, der i perioden er forsøgt kompromitteret. CFCS har udsendt varsler til identificerede sårbare myndigheder og virksomheder og løbende vejledt om modforanstaltninger. Antallet af sårbare enheder er i Danmark i dag under hundrede.

Truslen fra målrettede ransomware-angreb er stigende
Der er en stigende trussel fra målrettede ransomware-angreb mod danske myndigheder og virksomheder.

I målrettede ransomware-angreb forsøger kriminelle at afpresse myndigheder og virksomheder for store pengebeløb ved at kryptere centrale dele af offerets it-systemer ved hjælp af ransomware.

Siden slutningen af 2019 truer hackere, der har stået bag målrettede ransomware-angreb, nu også af og til med at lække følsomme data indsamlet fra det ramte system, hvis offeret ikke betaler løsesummen.

Målrettede ransomware-angreb har ramt danske virksomheder, og angreb sker nu relativt hyppigt. I efteråret 2019 har to danske virksomheder, Demant og GlobalConnect, eksempelvis været udsat for separate ransomware-angreb. Angrebet på Demant medførte iflg. virksomheden et tab på op mod 650 mio. kr. I februar 2020 blev den internationale servicevirksomhed ISS ramt af et ransomware-angreb, der også påvirkede den danske del af virksomheden. I april 2020 blev landbrugsvirksomheden Danish Agro og pumpeproducenten Desmi også ramt. I maj 2020 blev GlobalConnect igen kompromitteret. Angrebet ramte systemer tilhørende en række af GlobalConnects kunder, herunder medicin-indkøberen Amgros.

Der har i flere lande været sager, hvor målrettede ransomware-angreb medførte, at myndigheder og virksomheder i perioder ikke kunne udføre dele af deres arbejde. Lokale myndigheder, skoler, produktionsvirksomheder, hospitaler, it-firmaer, havne og rederier har bl.a. været ramt.

Målrettede cyberangreb som disse kan få alvorlige konsekvenser for samfundsvigtige funktioner. Det har f.eks. været tilfældet i forbindelse med ransomware-angreb mod

sundhedssektoren i bl.a. USA og Storbritannien, hvor nedetid i administrative systemer medførte, at patientaftaler måtte aflyses.

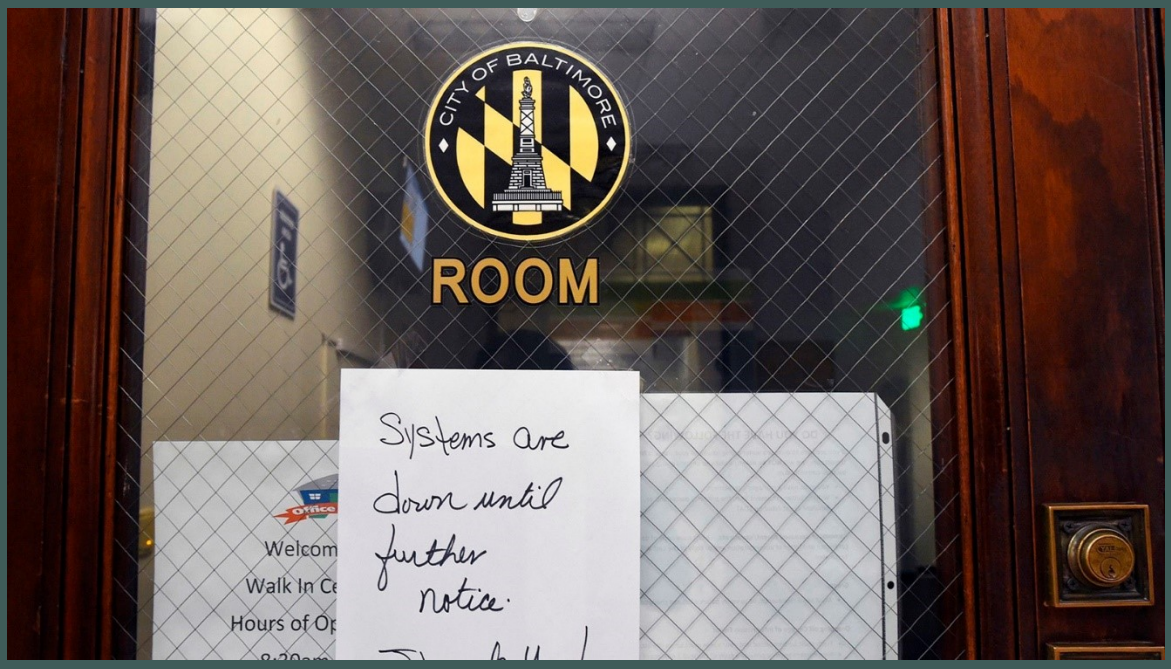
Et vellykket målrettet ransomware-angreb på leverandører af samfundsvigtige ydelser under en krise, som f.eks. mod sundhedssektoren i Danmark under COVID-19 krisen, vil kunne øge det pres, som sektoren allerede oplever pga. krisen.

Angrebet mod Amgros, der er leverandør til danske sygehusapoteker, er et eksempel på et ransomwareangreb mod sundhedssektoren i Danmark under krisen. Angrebet betød bl.a. at Amgros i nogle dage ikke kunne købe og sælge lægemidler via deres forretningssystem Naviline. Angrebet førte dog ikke til mangel på lægemidler på de offentlige hospitaler.

Lokale myndigheder i udlandet er blevet ramt flere gange
Lokale myndigheder i særligt USA har været hyppige mål for målrettede ransomware-angreb i de seneste år. Skoler og skoledistrikter har også været hyppige mål. I august 2019 har der eksempelvis været et målrettet angreb mod en it-leverandør, der lammede it-systemer hos 22 lokale myndigheder i Texas.

Nogle af myndighederne har også været udsat for afpresning med trusler om læk af dokumenter stjålet fra de ramte systemer i forbindelse med ransomware-angrebene. Det skete bl.a. for byen Pensacola, hvor afpresserne endte med at lække data på internettet i november 2019.

Angreb mod lokale myndigheder har ikke været afgrænset til USA.
I efteråret 2019 var der også en bølge af angreb på lokale myndigheder i Spanien.



Byen Baltimore i USA blev ramt af ransomware i 2019.
FOTO: Kenneth K. Lam/SIPA/Ritzau Scanpix

Digitale bankrøverier er rykket tættere på Danmark
Målrettede cyberangreb rettet mod finansielle virksomheder, såkaldte digitale bankrøverier, er i 2019 rykket indenfor Europas grænser. Der er en øget sandsynlighed for, at danske finansielle virksomheder kan blive udsat for denne type angreb.

I februar 2019 blev den maltesiske bank, Bank of Valletta, udsat for et digitalt bankrøveri. Hackerne forsøgte at stjæle 13 mio. Euro fra banken, hvilket svarede til omtrent 100 mio. kroner. Det lykkedes dog efterfølgende for banken at tilbageføre størstedelen af beløbet. Andre europæiske banker blev i samme periode sandsynligvis også udset som mål for digitale bankrøverier.

CFCS er bekendt med, at hackere, som sandsynligvis har kapacitet til at udføre digitale bankrøverier, er gået målrettet efter institutioner i den danske finanssektor i 2019, dog uden succes. Hackere har desuden udgivet sig for at være fra det danske finanstilsyn i phishing-mails, som blev sendt til banker i udlandet. Hackerne brugte navne på faktiske medarbejdere i Finanstilsynet.

Misbrug af finansielle myndigheders navne i phishing-angreb er sandsynligvis motiveret af, at det er almindeligt for finansielle institutioner at modtage forespørgsler fra myndigheder, som der skal reageres meget hurtigt på. Det kan øge sandsynligheden for, at modtageren reagerer på phishing-mailen ved eksempelvis at klikke på links eller åbne filer sendt af hackerne, under dække af en legitim henvendelse.

Simple angreb er en trussel mod alle
Cyberkriminelle udfører oftest relativt simple angreb mod mange potentielle ofre på en gang i håbet om at få et afkast fra så mange som muligt. Disse angreb udgør en vedvarende trussel for virksomheder, myndigheder og borgere i Danmark.

Disse angreb sker ofte gennem phising-angreb rettet mod tusinder af modtagere. Der findes dog også mange andre metoder. Cyberkriminelle kan f.eks. inficere hjemmesider og derfra sprede malware til besøgende på hjemmesiderne eller stjæle information, som ofret indtaster, når de besøger hjemmesiderne.

Den spredte malware kan have forskellige formål, der understøtter cyberkriminalitet. Trojanere bruges eksempelvis til tyveri af personlige og finansielle oplysninger. Kryptominere misbruger inficerede computeres maskinkraft og strømforbrug til at genere kryptovaluta. Ransomware holder data og systemer på offerets computer som gidsel, da de krypteres og derved bliver utilgængelige for offeret.

Spredningen af malware gennem phishing udføres af kriminelle grupper og netværk, der samarbejder og udveksler tjenester og kapaciteter såsom malware og infrastruktur.

Kriminelle sælger adgange, der bliver brugt i målrettede angreb
Der er et samarbejde mellem de kriminelle, der udfører mere målrettede angreb, og de kriminelle, der rammer tusindvis af ofre gennem bl.a. phishing. Målrettede ransomware-angreb sker eksempelvis ofte opportunistisk efter en indledende

kompromittering af offeret med malware spredt gennem phishing. Videregivelse og salg af disse indledende kompromitteringer kaldes for access-as-a-service.

Massekompromitteringer gennem phishing udgør derfor ikke kun en trussel i sig selv, men understøtter også den stigende trussel fra målrettede cyberangreb udført af kriminelle.

Med stigende indtjeningsmuligheder ved bl.a. målrettede ransomwareangreb stiger indtjeningsmulighederne også for de kriminelle, der videresælger og faciliterer adgange til de målrettede angreb.

Disse indtjeningsmuligheder er muligvis årsagen til, at en af de mest udbredte malware på globalt plan, Emotet, siden 2017 ikke længere bruges som direkte indtjeningskilde for de kriminelle gennem tyveri af finansielle oplysninger. Emotet bliver nu hovedsageligt brugt som et værktøj, som andre kriminelle kan købe sig adgang til.

Statslige aktører kan også udnytte kriminelles adgange og tjenester i eksempelvis cyberspionage. Det kan både ske via køb af adgange eller via afpresning af hjemlige kriminelle netværk. Amerikanske myndigheder har i 2019 eksempelvis officielt beskyldt russiske myndigheder for at samarbejde med cyberkriminelle.

Flere statslige aktører benytter desuden malware og teknikker brugt af kriminelle. Det kan vanskeliggøre identifikationen af cyberspionage iblandt de mere hyppige kriminelle cyberangreb.

Amerikanske sanktioner mod netværk i Rusland
I december 2019 indførte amerikanske myndigheder i koordination med britiske myndigheder økonomiske sanktioner mod flere navngivne personer og virksomheder i Rusland, der menes at stå i ledtog med et cyberkriminelt netværk kaldet Evil Corp.

De amerikanske myndigheder beskylder samtidigt den russiske føderale sikkerhedstjeneste, FSB, for at samarbejde med netværket i spionageøjemed.

Netværket har ifølge sanktionerne stået bag spredningen af malwaren Dridex. Dridex, der i tidligere varianter blev kaldt Bugat og Cridex, er siden 2012 blevet spredt gennem massive spam-kampagner med et udbytte svarende til mere end en halv milliard danske kroner. Dridex har også været brugt til spredningen af ransomware.

Russiske myndigheder har officielt afvist anklagerne som propaganda. Amerikanske retsdokumenter viser dog, at russiske myndigheder har hjulpet med at identificere lederen af netværket, Maksim Yakubets.

Anklagerne blev gennemgået på en pressekonference i det amerikanske justitsministerium. FOTO: Samuel Corum/AFP/Ritzau Scanpix

Cyberspionage

Truslen fra cyberspionage er **MEGET HØJ**. Det betyder, at det er meget sandsynligt, at danske myndigheder og virksomheder vil blive udsat for forsøg på cyberspionage inden for de næste to år.

Danmark er udsat for både politisk og kommercielt motiveret cyberspionage fra fremmede stater.

Det er en vedvarende trussel, der især er rettet mod danske myndigheder, som arbejder med udenrigs- og sikkerhedspolitik, samt virksomheder, der besidder en viden, som andre stater har interesse i.

Leverandører og samarbejdspartnere til disse myndigheder og virksomheder kan også blive udsat for forsøg på cyberspionage med det formål at misbruge dem som trædesten i forsøg på at opnå adgang til myndighederne og virksomhederne.

Cyberspionage kan føre til pres på danske beslutningstagere
Truslen fra cyberspionage mod myndigheder er generelt et udtryk for aktuelle udenrigs- og sikkerhedspolitiske forhold.

Som FE beskriver i Efterretningsmæssig Risikovurdering fra 2019 er den verdensorden, der har dannet den overordnede ramme for håndteringen af Danmarks og Europas geopolitiske og sikkerhedsmæssige interesser de sidste mange årtier, under pres. Det ses eksempelvis ved, at USA's dominerende position i international politik bliver udfordret.

Cyberspionage bruges aktivt af flere lande, herunder Rusland og Kina, til at fremme nationale handlemuligheder og undgå strategiske overraskelser i et foranderligt udenrigspolitisk miljø. Flere offentligt kendte cyberangreb på europæiske udenrigsministerier de seneste år understreger, at truslen er højaktuel, og at viden om udenrigspolitiske beslutninger og dispositioner er en prioritet for flere landes cyberspioner.

CFCS ser kontinuerligt forsøg på cyberspionage mod danske myndigheder. Truslen er især rettet mod myndigheder og personer, der arbejder med sikkerheds- og udenrigspolitik, herunder Udenrigsministeriet og Forsvaret.

Danmark deltager i internationale fora, som fremmede stater har udvist en vedvarende interesse i at udføre cyberspionage imod. Der findes bl.a. eksempler på cyberspionage mod NATO, EU og OSCE.

Det er sandsynligt, at fremmede stater forsøger at bruge cyberspionage som et middel til at opnå viden om danske interesser, overvejelser og beslutninger i forbindelse med større internationale sager eller udenrigspolitiske forhandlinger. Denne viden kan staterne bl.a. udnytte til at modarbejde danske interesser eller sætte danske forhandlere og beslutningstagere under pres.

Særligt Rusland og Kina råder over meget væsentlige cyberkapaciteter og begge lande bruger deres kapaciteter aktivt på globalt plan. Det er sandsynligt, at bl.a. Iran også udfører cyberspionage og andre typer cyberangreb mod mål i og uden for deres nærområde.

Andre stater, der også har en cyberkapacitet, anvender hovedsageligt deres cyberkapaciteter i deres nærområder. Disse stater udgør en potentiel cybertrussel mod Danmark. De kan eksempelvis forsøge at udføre cyberspionage mod danske repræsentationer, dels for at få adgang til viden om dansk sikkerheds- og udenrigspolitik i regionen, og dels for at få adgang til viden om det land eller den region, repræsentationen ligger i.

Flere udenrigsministerier i Europa er blevet angrebet
Kort efter nytår offentliggjorde østrigske myndigheder, at landets udenrigsministerium var blevet udsat for et alvorligt cyberangreb. De østrigske myndigheder udelukker ikke, at en statslig aktør stod bag angrebet.

Et par måneder tidligere havde Tjekkiets efterretningstjeneste, BIS, beskyldt Ruslands føderale sikkerhedstjeneste, FSB, for at stå bag gentagne kompromitteringsforsøg mod det tjekkiske udenrigsministerium og det tjekkiske forsvarsministerium i 2018. Tjekkiske myndigheder har også udtalt offentligt, at Kina sandsynligvis også har stået bag et omfattende angreb på en "strategisk vigtig regeringsinstitution" i Tjekkiet i 2018.

Disse eksempler skriver sig ind i en lang række af cyberangreb mod europæiske udenrigsministerier. Over de seneste år har bl.a. Italien, Kroatien, Belgien og Tyskland offentliggjort, at deres udenrigsministerier har været udsat for cyberangreb.

CFCS har i to undersøgelsesrapporter beskrevet hvordan Udenrigsministeriet blev forsøgt kompromitteret i 2014 og 2015. Rapporterne er på CFCS's hjemmeside.

Cyberspionage kan skade dansk konkurrenceevne og økonomi
Stater bruger også cyberspionage med det formål at styrke den nationale udvikling og konkurrenceevne. Den form for cyberspionage retter sig især mod virksomheder og institutioner, der har en viden, som fremmede stater har interesse i.

Staterne kan bruge den stjålne information til at understøtte udviklingen af deres nationale sektorer, der kan springe flere led af deres innovations- og udviklingsproces over. Det er f.eks. sandsynligt, at udviklingen af motoren i det kinesiske passagerfly C919 bl.a. er sket på baggrund af målrettet statsstøttet cyberspionage mod flyproducenter og underleverandører i udlandet.

Forskning relateret til COVID-19 er også et eksempel på viden, der kan have værdi for fremmede stater. CFCS vurderer, uafhængigt af COVID-19-pandemien, at fremmede stater særligt har interesse i de dele af sundhedssektoren, der har adgang til forskningsdata eller intellektuel ejendom. Det er f.eks. virksomheder, universiteter og hospitaler, der beskæftiger sig med udvikling af bl.a. biokemi, biotek og lægemidler.

Det kan skade Danmarks konkurrenceevne og derved dansk økonomi, hvis danske virksomheder udsættes for cyberspionage, især inden for områder hvor danske virksomheder besidder en konkurrencestærk viden.

Grænsen mellem denne kommercielt motiverede og den sikkerhedspolitisk motiverede cyberspionage kan være overlappende. Der er flere eksempler på cyberspionage mod teknologier, som både kan bruges civilt og militært, eksempelvis inden for luftfart og rumfart. NASA offentliggjorde eksempelvis i 2019, at de havde været kompromitteret i ti måneder fra 2017 til 2018. Ifølge NASA lykkedes det bl.a. aktøren at stjæle information underlagt amerikansk våbeneksportkontrol.

Leverandører og samarbejdspartnere bruges som springbræt
Der er også en trussel mod leverandører og samarbejdspartnere til de ovennævnte typer myndigheder og virksomheder, som fremmede stater er interesserede i. I forsøget på at få adgang til disse myndigheder og virksomheder kan fremmede stater forsøge at bruge myndighedernes og virksomhedernes leverandører og samarbejdspartnere som et mellemliggende mål.

Her er der tale om en angrebsmetode, hvor hackere angriber en organisation for at bruge den som springbræt til at kompromittere de af organisationens kunder og samarbejdspartnere, der er interessante for den fremmede stat.

Målet med cyberspionage er derfor ikke nødvendigvis altid at skaffe konkret viden, men kan også være at skaffe en specifik adgang. Visse underleverandører eller samarbejdspartnere har måske ikke en viden, der er interessant for fremmede lande, men de kan til gengæld have en adgang eller troværdighed, hackerne kan udnytte til at kompromittere deres egentlige mål.

It-leverandører, eksempelvis hosting-udbydere og it-servicevirksomheder, kan have adgang til kundernes data eller it-systemer. Hackerne kan forsøge at kompromittere disse leverandører med det formål at tilgå disse data eller it-systemer via leverandøren. Kompromitterede software- og udstyrsleverandører kan også misbruges til at sprede malware, der kan bruges i cyberspionage, til deres kunder gennem eksempelvis inficerede systemopdateringer.

Fremmede stater kompromitterer også sårbare it-systemer i virksomheder og myndigheder på tværs af samfundet for at opbygge en it-infrastruktur, der kan misbruges i cyberangreb mod andre mål. Danske myndigheder og virksomheder kan derfor blive udsat for cyberangreb udført af fremmede lande uden at være i besiddelse af specifik viden eller adgang, som landene er interesserede i.

I 2015-2016 blev en række danske virksomheder og myndigheder eksempelvis systematisk angrebet som del af en angrebsbølge rettet mod sårbare JBoss-systemer, der bruges i en række it-løsninger. Angrebene ramte et bredt udsnit af mål, der ikke synes at have andet tilfælles end brugen af JBoss.

Cyberangreb mod norske Visma
Den norske softwareleverandør Visma offentliggjorde i februar 2019, at den var blevet kompromitteret. Ifølge åbne kilder var formålet at få adgang til Vismas kunders data.

Visma er en stor international leverandør, som blandt andet leverer cloud-software til virksomheders regnskab og forretning.

Selskabet har også afdelinger i Danmark og har blandt andet været leverandør til den danske Søfartsstyrelse. CFCS har ikke kendskab til, at Søfartsstyrelsen har været påvirket af angrebet, men angrebet viser den potentielle trussel fra angreb via leverandører.

Destruktive cyberangreb

CFCS vurderer, at truslen fra destruktive cyberangreb mod danske myndigheder og virksomheder er **LAV**. Det betyder, at det er mindre sandsynligt, at danske virksomheder og myndigheder vil blive udsat for forsøg på destruktive cyberangreb inden for de næste to år.

Det skyldes, at det er mindre sandsynligt, at fremmede stater aktuelt har intentioner om at rette destruktive cyberangreb mod Danmark.

Flere stater har dog betydelige kapaciteter til at udføre destruktive cyberangreb, og de udvikler deres kapaciteter løbende. Truslen kan stige i forbindelse med en skærpet politisk eller militær konflikt med lande, der har evnen til at gennemføre destruktive cyberangreb.

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.

Det er her vigtigt at bemærke, at CFCS' definition af destruktive cyberangreb dækker cyberangreb med meget forskellige konsekvenser, rangerende fra ødelæggelse af data til fysisk ødelæggelse og dødsfald. 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.

Destruktive cyberangreb er selv inden for denne brede definition relativt sjældne. CFCS vurderer, at langt størstedelen af de destruktive cyberangreb, som CFCS har kendskab til, sandsynligvis har været udført af stater. Næsten alle disse angreb er udført i forbindelse med konflikter eller geopolitiske spændinger mellem stater. Det er mindre sandsynligt, at fremmede stater har intention om at ramme Danmark.

Det er dog muligt, at danske virksomheder og myndigheder, som har aktiviteter i regioner præget af konflikter, kan blive udsat for følgevirkningerne af et destruktivt cyberangreb, sådan som det eksempelvis skete for A. P. Møller Mærsk ved NotPetya-angrebet i Ukraine i 2017. Indtil nu har de fleste angreb fundet sted i Ukraine og Saudi Arabien.

Danske virksomheder med aktiviteter i særligt Ukraine og Saudi Arabien kan i enkelte tilfælde også blive udset som direkte mål for destruktive cyberangreb. Det blev illustreret af angrebet, der slettede data hos den italienske virksomhed Saipem i 2018.

Saipem er underleverandør til den saudiske nationale olieproducent Saudi Aramco. Saudi Aramco har selv været udsat for destruktive cyberangreb både i 2012, 2016 og 2017.

Stater forsøger at afskrække brugen af destruktive cyberangreb
NATO har, bl.a. som reaktion på NotPetya-angrebet i 2017, slået fast i en fælles erklæring, at cyberangreb mod medlemslandene vil kunne udløse alliancens kollektive forsvarsforpligtigelser i rammen af Atlantpagtens artikel 5, den såkaldte musketer-ed.

Destruktive cyberangreb er indtil videre typisk ikke blevet mødt med militære modsvar. Dog bombede det israelske luftvåben i maj 2019 en bygning i Gaza, som ifølge Israel husede hackere fra Hamas. Der er flere eksempler på, at stater har reageret på destruktive cyberangreb med økonomiske sanktioner.

Stater kan have forskellige formål med destruktive cyberangreb
Stater kan forsøge at opnå forskellige resultater ved hjælp af destruktive cyberangreb. En stat kan ved hjælp af destruktive cyberangreb mod samfundsvigtige sektorer eksempelvis forsøge at sende et signal om, at den anden stat ikke er i stand til at beskytte sin befolkning.

Den angribende stat kan også bruge angrebene til at straffe eller til at signalere, at fremmede stater ikke må agere imod det angribende lands interesser. Destruktive cyberangreb rettet mod virksomheder med aktiviteter i en region præget af geopolitiske spændinger kan også have til hensigt at skræmme udenlandske virksomheder og investorer fra at gøre forretninger i det pågældende land.

Et destruktivt cyberangreb, der ødelægger kritisk infrastruktur eller militære kapaciteter, kan potentielt svække modstandere i tilfælde af en krise eller krig. Der er dog endnu ikke offentligt omtalte eksempler på destruktive cyberangreb, der har haft så vidtrækkende konsekvenser. Det eksempel, der kommer tættest på, er angrebet mod iranske centrifuger til berigelse af uran, der blev offentligt kendt i 2010. Det er også stadig det eneste kendte eksempel på et destruktivt cyberangreb, der har medført fysisk ødelæggelse i større skala.

I det årti, der er gået siden angrebet på de iranske atomcentrifuger, har både industrielle systemer og offensive cyberkapaciteter dog udviklet sig væsentligt, og det er sandsynligt, at der er flere lande, der har kapacitet til at lave lignende angreb.

Få destruktive cyberangreb uafhængigt af konflikter
Hackere benytter i få tilfælde også simple destruktive cyberangreb uafhængigt af politiske og militære konflikter.

Der er enkelte eksempler på, at hackere i forbindelse med digitale bankrøverier har slettet eller krypteret finansielle virksomheders data. Formålet har sandsynligvis været at slette deres spor eller forhindre virksomhederne i at reagere på tyveriet. Cyberkriminalitet kan altså potentielt ledsages af cyberangreb, der har en destruktiv effekt. Sletning eller kryptering af data i digitale bankrøverier er foreløbigt et relativt sjældent fænomen, men det kan have store konsekvenser for den enkelte berørte finansielle institution.

Der kan generelt ske fejl, når hackere manipulerer it-systemer. Det betyder, at andre typer cyberangreb også kan få en ødelæggende virkning, selvom det ikke var hackerens hensigt. Inden for søfart er der eksempler på cyberangreb, der har påvirket strømforsyning, navigationssystemer og positioneringssystemer. Konsekvenserne i sagerne, som CFCS har kendskab til, har ikke medført fysisk skade og ulykker, men det er muligt, at sådanne angreb kan få fysiske konsekvenser.

Cyberaktivisme

Truslen fra cyberaktivisme er **LAV**. Det betyder, at det er mindre sandsynligt, at danske virksomheder og myndigheder vil blive udsat for forsøg på cyberaktivisme inden for de næste to år.

På globalt plan er antallet af aktivistiske cyberangreb faldet de seneste år. Cyberaktivister retter sjældent deres fokus mod danske myndigheder og virksomheder. Truslen kommer særligt til udtryk i forbindelse med begivenheder eller enkeltsager, der tiltrækker cyberaktivisters opmærksomhed.

Det er også mindre sandsynligt, at Danmark vil blive ramt af faketivisme, hvor statsstøttede hackere udfører cyberangreb, mens de udgiver sig for at være cyberaktivister. Truslen fra faketivisme vil sandsynligvis stige i forbindelse med militære eller politiske konflikter med fremmede stater.

Fodboldhacker fælder Afrikas rigeste kvinde
Siden 2015 har den portugisiske hacker Rui Pinto hacket og lækket informationer om fodboldverdenen i kampagnen Football Leaks.

I 2018, da Pinto stjal dokumenter til understøttelse af Football Leaks, stødte han ifølge flere åbne kilder ved et tilfælde også på fortrolige dokumenter, der indeholdte inkriminerende informationer om Afrikas rigeste kvinde, Isabel dos Santos.

Pinto gav dokumenterne videre til en afrikansk whistleblowerorganisation, hvilket blev starten på Luanda Leaks. Luanda Leaks har medført, at dos Santos er blevet genstand for strafferetslig efterforskning i Angola, ligesom Portugal har indefrosset hendes bankkonti i landet.

Der er umiddelbart langt fra de europæiske fodboldbaner til de angolanske regeringskontorer, men der findes dog en tematisk fællesnævner. Football Leaks og Luanda Leaks indeholder begge anklager om bl.a. korruption og magtmisbrug. Sagen illustrerer, hvordan både aktivisternes fokus og tilfældigheder kan have betydning for, hvem der bliver ramt af cyberaktivisme.

Rui Pinto blev arresteret i Ungarn i 2019. FOTO: Ferenc Isza/AFP/Ritzau Scanpix

Begivenheder og tilfældigheder kan udløse cyberaktivisme
Formålet med cyberaktivisme er at skabe størst mulig opmærksomhed om en sag. Cyberaktivister opnår dette mål med forskellige midler, og angrebsmetoderne varierer meget i kompleksitet – fra relativt simple DDoS-angreb til mere ressourcekrævende hack og læk af informationer fra myndigheder og virksomheder.

Det sidste cyberaktivistiske angreb i Danmark, der fik stor medieopmærksomhed, var et DDoS-angreb mod bl.a. Udlændinge- og Integrationsministeriet og Udenrigsministeriet i 2017. Angrebet var sandsynligvis en reaktion på en debat om Muhammed-tegningerne kort forinden. Angrebet understreger, at truslen er dynamisk, da angreb fra cyberaktivister ofte er en spontan reaktion på specifikke begivenheder.

DDoS-angreb er relativt nemme at udføre og forudsætter derfor typisk minimal planlægning og teknisk viden. Truslen fra sådanne simple angreb kan derfor stige pludseligt, hvis danske myndigheder eller virksomheder kommer i aktivisternes søgelys, som det eksempelvis skete i 2017. Hack og læk af eksempelvis personfølsomme oplysninger forudsætter til sammenligning længere planlægning og bedre tekniske færdigheder.

Cyberaktivistiske angreb dækker således over en mangfoldig gruppe af aktiviteter, der spænder fra opportunistiske angreb til mere organiserede kampagner. En fællesnævner på tværs af dette spektrum er dog, at mens angrebene ofte er en reaktion på specifikke begivenheder, så findes der en kontinuitet i de temaer, som de forskellige aktivister forfølger.

Stater bruger cyberaktivisme som dække for påvirkning
I nogle lande ledsager cyberaktivisme den traditionelle politiske aktivisme. Cyberaktivister har eksempelvis suppleret den seneste bølge af protester og civile uroligheder i Sydamerika og Catalonien med cyberangreb. Denne typer aktivisme sker typisk inden for rammerne af lokale konflikter og uroligheder.

Fremmede stater kan have interesse i at forstærke disse lokale konflikter og uroligheder ved selv at lave cyberangreb, der ligner cyberaktivisme. I populær tale kaldes dette for faketivisme.

Faketivisme repræsenterer typisk forsøg på at afspore og aflede den offentlige debat i de ramte samfund og kultivere en polarisering i samfundet. Det kan være vanskeligt at bevise, hvilke lande der står bag faketivismen. Staterne kan på den måde forsøge at unddrage sig et ansvar for påvirkningskampagner i andre lande.

Det er mindre sandsynligt, at Danmark vil blive ramt af faketivisme. Det er dog muligt, at truslen vil stige ved sager af særlig politisk, strategisk eller økonomisk karakter, som fremmede stater har en væsentlig interesse i at påvirke. Det er sandsynligt, at truslen vil stige ved en skærpet politisk eller militær konflikt mellem Danmark og fremmede stater.

Hackere plantede flere falske nyheder i Litauen
Den 19. juni 2019 dukkede en falsk nyhed op på flere litauiske internetmedier. I nyheden stod der, at NATO ved et uheld havde forurenet en flod i Litauen med radioaktive materialer under øvelsen "Iron Wolf". Det viste sig dog efterfølgende, at internetsiderne var blevet kompromitteret, og nyhederne var plantet af hackere.

Et par måneder senere i oktober 2019 gentog mønsteret sig. Et litauisk internetmedie kunne rapportere om amerikanske planer for at flytte atomvåben til Litauen, men igen viste det sig at være en falsk historie, der var blevet plantet, efter at mediet var blevet hacket.

I november 2019 udtalte det litauiske forsvar, at de mente, at hændelserne var en del af en større russisk påvirkningskampagne, hvis formål bl.a. var at skabe tvivl om NATO's tilstedeværelse i landet.

I april 2020 blev en fabrikeret e-mail, der udgav sig for at komme fra NATO's generalsekretær, sendt til bl.a. litauiske medier, med falske påstande om at NATO ville trække sig ud af landet.

Cyberterror

Truslen fra cyberterror er **INGEN**. Det betyder, at det er usandsynligt, at Danmark, herunder danske virksomheder og myndigheder, 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 mere konventionel terror, f.eks. 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.

Der er endnu ingen terrorgrupper, som har udført cyberangreb, der lever op til CFCS's definition på cyberterror, mod hverken danske eller udenlandske mål. Der findes heller ingen hændelser, hvor terrorgrupper har taget ansvaret for at udføre cyberterror.

Manglende kapacitet ledsages af en meget begrænset hensigt
Der er kun få eksempler på, at militante ekstremister har opfordret til cyberterror. Militante ekstremister har heller ikke hævdet at stå bag nogle af de destruktive cyberangreb, som verden hidtil har set. Selvom det nogle gange er tilfældet, at terrorgrupper ikke offentligt påtager sig ansvaret for deres terrorhandlinger, vurderer CFCS, at et vellykket alvorligt cyberangreb ville være blevet fulgt op af propaganda for at understrege den nye trussel.

Den manglende hensigt skyldes sandsynligvis, at de etablerede terrorgrupper ikke anser cyberangreb som en realistisk og effektiv måde til at skabe den samme frygt og kaos, som konventionelle terrorangreb skaber.

Militante ekstremister står i stedet bag cyberaktivisme
Cyberangreb udført af militante ekstremistiske grupper har primært manifesteret sig som cyberaktivisme. Det fremgår af de opfordringer og vejledninger til cyberangreb, som militante ekstremister har udsendt. Angreb og ønsker om angreb har typisk drejet sig om defacement- og overbelastningsangreb på hjemmesider samt hack og læk af personoplysninger ledsaget af opfordringer til drab i form af såkaldte drabslister.

Hackerne bag disse cyberangreb har typisk udvist støtte til Islamisk Stat. Fire hackergrupper slog sig i 2016 sammen og dannede United Cyber Caliphate (UCC), sandsynligvis for at styrke deres kapacitet. Det militære pres på Islamisk Stat har medført, at hackergrupperne ikke har kunnet etablere sig som en fysisk samlet enhed, men stadig er overladt til at operere som løst forbundne enkeltpersoner.

Radikalisering og rekruttering kan øge truslen
Truslen fra cyberterror kan stige, hvis det lykkes militante ekstremister at radikalisere og rekruttere dygtige hackere eller insidere med adgang til kritiske it-systemer. Der er i udlandet eksempler på, at insidere i enkelte tilfælde har tilbudt deres it-ekspertise til militante ekstremister.

På mellemlangt sigt kan den øgede sammensmeltning af det fysiske og digitale domæne medføre en stigende risiko for, at et cyberangreb medfører skade på materiel eller mennesker. Det kan potentielt øge truslen fra cyberterror.

Fraværet af cyberterror betyder ikke, at internettet er uden betydning for terrortruslen. Militante ekstremister anvender krypterede chattjenester og lukkede internetfora til at rekruttere og radikalisere nye ekstremister på tværs af landegrænser. I de lukkede fora deles også opfordringer og vejledninger til udførelse af konventionelle terrorangreb samt råd om hvorledes mobil- og internetkommunikation kan skjules for myndighederne.

Kunstig intelligens og kvanteteknologi forandrer cybersikkerheden

En række teknologiske gennembrud har i de seneste år givet os et væld af nye digitale muligheder. Personlige assistenter er en del af manges hjem, vores ansigt kan bruges til autentifikation, og selvkørende biler testes allerede i flere storbyer.

Med hastige fremskridt følger dog også nye udfordringer, som vil forme vores digitale sikkerhed i de kommende år. Særligt har gennembrud indenfor kunstig intelligens og kvanteteknologi åbnet op for nye muligheder og udfordringer.

Kunstig intelligens: Automatisering af forsvar og angreb
Udviklingen inden for kunstig intelligens har givet langt bedre muligheder for at opdage cyberangreb end tidligere. Algoritmer, drevet af machine learning, danner i dag kerneforretningen for mange private cybersikkerhedsfirmaers it-sikkerhedsløsninger. Flere firmaer tilbyder aktiv monitorering af netværkstrafik, som løbende træner deres algoritmer til at identificere og standse ondsindet aktivitet i realtid. Særligt er der sket fremskridt inden for identificeringen af phishing-mails, hvor langt de fleste i dag bliver opdaget og frasorteret automatisk af machine learning algoritmer.

På den anden side har kunstig intelligens skabt en række nye udfordringer. Hackere er eksempelvis begyndt at udnytte samme algoritmer til automatisk at generere langt mere troværdige phishing-mails netop for at slippe forbi disse avancerede machine learning algoritmer. Det sker i stigende grad ved, at algoritmerne aktivt indarbejder informationer om deres mål fra sociale medier for at virke mere troværdige.

Kunstig intelligens
Teknologier, som efterligner menneskelig intelligens herunder sprog, syn, læring og evnen til at generalisere.

Machine Learning
IT-systemer, som behandler nye data på baggrund af maskinelle analyser af et tidligere datasæt (læring) frem for gennem eksplicit programmering (instrukser).

Kunstig intelligens giver også nye muligheder for at udføre langt mere målrettede hackerangreb. Under it-sikkerhedskonferencen Black Hat i 2018 demonstrerede IBM for eksempel, hvordan det er muligt at indlejre machine learning algoritmer i malware, som udnytter ansigts- og talegenkendelse til kun at frigive malwaren, hvis den genkender et specifikt ansigt eller en specifik stemme. Det åbner for særligt målrettede cyberangreb, der retter sig mod udvalgte enkeltpersoner eller grupper. Kunstig intelligens har med andre ord bl.a. gjort det muligt at misbruge vores biometriske data mod os selv. I takt med at kunstig intelligens tages i brug, også i systemer indenfor kritisk infrastruktur, er det derfor vigtigt, at cybersikkerhed tænkes ind i både udviklings- og anvendelsesfasen.

Cybersikkerhed efter kvantespringet
Udviklingen af kvanteteknologi vil også påvirke vores cybersikkerhed de kommende år. Forskere og virksomheder forsøger at overføre kvantefysiske fænomener til den digitale verden bl.a. med henblik på at udvikle universelle kvantecomputere og skabe kvantesikrede kommunikationskanaler.

Kvantecomputere bygger på såkaldte ”qubits”, som har langt flere frihedsgrader til at foretage beregninger relativt til klassiske computere. Faktisk fordobles computerkraften hos en kvantecomputer for hver qubit, der tilføjes. En kvantecomputers regnekraft vokser med andre ord dobbelteksponentielt, mens klassiske computere kun vokser eksponentielt. Det er en meget stor forskel, som sandsynligvis vil få betydelige konsekvenser i fremtiden.

Udviklingen af kvantecomputere udgør en potentiel trussel mod cybersikkerheden i Danmark, da kvantecomputernes øgede maskinkraft kan misbruges i cyberangreb. Udviklingen af kvantecomputere udfordrer især vores datasikkerhed på internettet. Kommunikation over internettet krypteres i øjeblikket med meget komplicerede beregninger, som beskytter vores data på en måde, som en klassisk computer skal bruge flere tusinde år på at bryde. I fremtiden kan kvantecomputere muligvis bryde disse krypteringer på få sekunder, og krypteret information, som vi i dag sender over internettet, kan således potentielt blive læsbar.

En af de mest udbredte krypteringsmetoder i dag hedder RSA. Ifølge det amerikanske forskningsinstitut National Institute of Standards and Technology (NIST) vil kvantecomputere sandsynligvis kunne bryde RSA om ti år. Derfor igangsatte NIST i 2017 en international konkurrence om udviklingen af en ny krypteringsmetode, som skal erstatte RSA og være såkaldt ”kvantesikret”. Udfordringen ligger nu i at udpege en erstatning og implementere denne, inden kvantecomputerne kan bryde RSA.

Selvom udviklingen i dag er i en tidlig fase, er de første prototyper på kvantecomputere allerede begyndt at levere resultater. Google byggede eksempelvis en kvantecomputer i 2019, som på lidt over 3 minutter løste et regnestykke, som en klassisk computer skulle bruge cirka 10.000 år på. Der er stadig betydelige udfordringer forbundet med kvantecomputere, men nogle sammenligner Googles bedrift med Wright-brødrenes første flyvning, der på trods af den begrænsede præstation åbnede døren til en ny fremtid.

Udviklingen af kvantesikret kommunikation præsenterer imidlertid en mulig løsning på nogle af udfordringerne. Ideen bag kvantesikret kommunikation bygger på muligheden for at dele ’nøgler’, som legitimt bruges til at afkode meddelelser af modtagere, på en ny og sikker måde baseret på kvantefysik. Det særlige er, at nøgleudvekslingen sker på en måde, hvor datasikkerheden ikke længere er afhængig af begrænset computerkraft, og at både afsenderen og modtageren altid vil kunne opdage, hvis nogen forsøger at opfange nøgleudvekslingen under forsendelsen.

Udviklingen af kvantesikker kommunikation er aktuelt længere fremme relativt til kvantecomputeren. Kina har på forsøgsbasis eksempelvis etableret en 2.000 km lang kommunikationslinje baseret på kvanteteknologi, som via fiberkabel forbinder Beijing,

Jinan, Hefei og Shanghai. I 2016 opsendte Kina desuden en satellit ved navn ”Micius”, som kan facilitere kvantekommunikation på tværs af landegrænser.

Implementering af kvantekommunikation i stor skala på internettet vil imidlertid kræve enorme omstruktureringer af internettets nuværende opbygning.

Medarbejder inspicerer IBM's kvantecomputer "Q". FOTO: Connie Zhou/Ritzau Scanpix

Kommercielle interesser driver udviklingen
Udviklingen af både kunstig intelligens og kvanteteknologi i den vestlige verden bliver primært drevet af store private teknologivirksomheder.

For virksomhederne understøtter teknologierne betydelige kommercielle interesser bl.a. i form af first-mover-fordele ved udviklingen af selvkørende biler, videreudvikling af digitale assistenter og yderligere optimering af machine learning algoritmer.

Der er en risiko for, at kommercielle interesser overskygger behovet for at imødegå de nævnte sikkerhedsmæssige udfordringer for fremtidens samfund.

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 plan-lægning. 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 sandsynligheder i analyser