CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod Danmark 2021

1. udgave juni 2021

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave juni 2021

Cybertruslen mod Danmark 2021

Formålet med denne trusselsvurdering er at informere danske beslutningstagere, myndigheder og virksomheder om cybertruslen mod Danmark. Viden om truslen skal bl.a. kunne bruges til at prioritere tiltag hos den enkelte myndighed og virksomhed. Dette produkt vurderer trusselsniveauerne for forskellige typer af cybertrusler, men trusselsvurderingen indeholder ikke konkrete råd og vejledninger til at imødegå disse trusler.

Hovedvurdering

- Truslen fra cyberkriminalitet er **MEGET HØJ**. Alle danske myndigheder, virksomheder og borgere er udsat for en vedvarende og aktiv trussel fra cyberkriminelle. Truslen underbygges af de cyberkriminelles evne til at udvikle og omstille sig til nye virkeligheder samt det specialiserede samarbejde, der foregår på lukkede internetfora.

- Truslen fra cyberspionage er **MEGET HØJ**. CFCS vurderer, at fremmede stater kan og vil forsøge på at stjæle værdifuld information fra Danmark. Særligt interessante mål på det udenrigs- og sikkerhedspolitiske område er udsat for en vedvarende interesse fra statslige aktører. Konkrete hændelser og løbende angrebsforsøg understreger gang på gang denne vurdering.

- CFCS vurderer, at truslen fra destruktive cyberangreb mod danske myndigheder og virksomheder er **LAV**. Flere stater har kapaciteten til at udføre destruktive angreb, men det er mindre sandsynligt, at de aktuelt har intention om at udføre den type angreb mod danske mål.

- Truslen fra cyberaktivisme er **LAV**. De mange protester, der har præget 2020, har ikke ført til en stigning i antallet af cyberaktivistiske angreb på verdensplan. Antallet af angreb ligger således på niveau med de seneste år.

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

Indledning

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) udgiver for sjette gang den årlige vurdering af cybertruslen mod Danmark. Vurderingen af cybertruslen er som i tidligere år opdelt i trusler fra cyberangreb, der understøtter kriminalitet, spionage, destruktive cyberangreb, aktivisme og terrorisme. Analysen har ikke givet anledning til, at CFCS har ændret på trusselsniveauerne i forhold til 2020.

Det betyder bl.a., at CFCS vurderer, at truslen fra cyberkriminalitet og cyberspionage fortsat er **MEGET HØJ**. Når et trusselsniveau ligger på **MEGET HØJ**, betyder det, at der er aktører, der kan, vil og løbende forsøger at angribe Danmark. Både cyberkriminelle og medarbejdere hos statslige aktører arbejder systematisk, vedholdende og målrettet på at ramme mål i Danmark.

Selvom et trusselsniveau ikke har ændret sig, så kommer truslen til udtryk på forskellig vis fra år til år. Det er derfor ikke altid nok at kende et trusselsniveau for at forstå truslen.

Et trusselsniveau fungerer godt til at skabe overblik, og det kan være retningsgivende for hvilke trusler, der kræver en særlig opmærksomhed. Samtidigt kan niveauet give et indtryk af trusselsudviklingen over tid. Hvis en virksomhed, myndighed eller organisation skal opbygge et effektivt cyberforsvar, er det dog nødvendigt at tage skridtet videre og forholde sig til de nuancer, som det enkelte trusselsniveau dækker over.

Selvom trusselsniveauet ikke ændrer sig, kan både aktører, metoder og konsekvenser godt ændre sig. Et eksempel fra årets cyberkriminalitetskapitel illustrerer dette forhold mellem trusselsniveau og trussel. Ligesom sidste år ligger trusselsniveauet fra cyberkriminalitet på det højst mulige. Det skyldes bl.a. de målrettede ransomware-angreb, der de seneste år også er begyndt at ramme danske virksomheder. For at øge presset på deres ofre begyndte flere hackergrupper i løbet af 2020 at true med at lække data, som de havde stjålet i forbindelse med ransomware-angreb. Den form for ekstra afpresning bliver i it-sikkerhedskredse kaldt for dobbelt afpresning.

Dobbelt afpresning har øget de potentielle konsekvenser af et målrettet ransomware-angreb. Ofrene risikerer nu ikke blot at miste tilgængeligheden af vigtige it-systemer. De risikerer samtidig, at forretnings- eller følsomme personoplysninger bliver lækket til offentligheden eller solgt videre. Dobbelt afpresning ændrer ikke på trusselsniveauet, men fænomenet føjer nye nuancer til truslen fra cyberkriminalitet. Og det er vigtigt for virksomheder, myndigheder og organisationer at kende disse nuancer, hvis de skal beskytte sig effektivt og tilstrækkeligt mod truslen.

Cybertruslen skal fortsat tages alvorligt

Det meget høje trusselsniveau for cyberkriminalitet og cyberspionage har været gældende, siden CFCS i 2016 udgav sin første vurdering af cybertruslen mod Danmark. Og de forhold, som understøtter cybertruslen, ser ikke ud til at blive svækket i de kommende år.

Hacking er mulig af flere årsager. Alle it-systemer indeholder sårbarheder, og frit tilgængeligt på internettet findes en overflod af information og værktøjer, der gør det

muligt for hackere at finde og udnytte sårbarhederne. I dagligdagen får oppetid og funktionalitet ofte højere prioritet end it-sikkerhed. Endelig er den menneskelige faktor en sårbarhed, der bl.a. udnyttes i forbindelse med phishing-mails.

Når hackerne angriber, kan de samtidig gøre det med lav risiko for at blive pågrebet. Det skyldes, at det er let at gemme sig og optræde anonymt på internettet. Forsøg på at fange gerningsmanden vil desuden ofte involvere flere lande, hvilket vanskeliggør opklaring og retsforfølgelse.

Det frie og åbne internet betyder, at hackere har uhindret adgang til deres ofre. Danske teleselskaber er forpligtet til uhindret at sende al trafik til deres kunder, også cyberangreb som ikke truer selve teleinfrastrukturen. De skal sikre fri adgang til alle internettjenester, hvilket inkluderer hackernes infrastruktur og hjemmesider.

Så længe der er næsten uhindret adgang til et stigende antal potentielt sårbare enheder, der kan hackes med højt udbytte og lav risiko, er der desværre ikke noget, der tyder på, at den generelle cybertrussel vil blive mindre de kommende år.

Kampen mod hackerne er ikke tabt

Langt de fleste hackerangreb bliver afværget takket være avanceret teknologi samt oplyste og opmærksomme virksomheder og borgere. Men ligesom mange først køber en tyverialarm, efter de har haft indbrud, lykkes mange hackerangreb på grund af et overset eller nedprioriteret cyberforsvar. På samme måde som en god lås, overvågning og opmærksomhed kan holde indbrudstyve væk, kan et grundlæggende cyberforsvar og trænede, årvågne medarbejdere forhindre eller afbøde de fleste angreb fra hackere.

Hackerne har derfor langt fra vundet kampen om det digitale domæne. I takt med at cybersikkerhed indtager en mere central plads hos organisationer, virksomheder og myndigheder, vil robustheden stige. Det mindsker risikoen for alvorlige cyberangreb.

Robustheden underbygges først og fremmest af en nuanceret og detaljeret forståelse af de cybertrusler, der retter sig mod det danske samfund.

God læselyst!

Cyberkriminalitet

Truslen fra cyberkriminalitet er **MEGET HØJ**. Det betyder, at det er meget sandsynligt, at myndigheder, virksomheder og borgere i Danmark bliver 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, der er motiveret af økonomisk berigelse.

Alle danske myndigheder, virksomheder og borgere er udsat for en vedvarende og aktiv trussel fra cyberkriminelle. Truslen underbygges af de cyberkriminelles evne til at udvikle og omstille sig til nye forhold samt det specialiserede samarbejde, der foregår i det cyberkriminelle miljø.

Cyberkriminalitet udgør en bred trussel mod det danske samfund

CFCS vurderer, at cyberkriminalitet er den mest udbredte cybertrussel mod Danmark, og at den fortsat vil være det på langt sigt.

Den mest almindelige type cyberkriminalitet er fortsat baseret på brede cyberangreb rettet mod et stort antal potentielle ofre på tværs af samfundet. Det gælder bl.a. angreb gennem phishing, udnyttelse af kendte sårbarheder i udbredte it-systemer samt misbrug af usikre fjernadgange. Derfor kan langt de fleste danskere forvente at blive udsat for forsøg på cyberkriminalitet.

De kriminelle bruger værktøjer og angrebsteknikker, der typisk er udviklet til specifikke kriminelle formål, eksempelvis til tyveri af personlige oplysninger, afpresning gennem ransomware eller misbrug af it-systemer til kryptomining. Variationen i angrebene betyder, at cyberkriminalitet dækker over flere typer berigelseskriminalitet, herunder både tyveri, afpresning og bedrageri.

Cyberkriminelle er modstandsdygtige og hurtige til at omstille sig

Cyberkriminalitet er drevet af mulighederne for at tjene penge. Derfor omstiller mange cyberkriminelle sig hurtigt, når nye indtjeningsmuligheder opstår, nye værktøjer udvikles, eller de ydre omstændigheder ændrer på forretningsgrundlaget. Det medfører, at truslen fra cyberkriminalitet konstant udvikler sig og hurtigt kan ændre udtryk.

Siden 2019 har flere cyberkriminelle grupper eksempelvis fokuseret på at udføre eller understøtte målrettede ransomware-angreb. Disse hackergrupper har, som beskrevet i indledningen, i 2020

udvidet deres afpresning ved også at true med at lække følsomme oplysninger, stjålet i forbindelse med ransomware-angrebene. Nogle førende hackergrupper har endda holdt længere pauser i foråret 2020 for at udvikle og teste nye værktøjer til disse angreb.

Ransomware-angreb
Ved ransomware-angreb bliver data og systemer gjort utilgængelige for offeret, ofte ved kryptering, og derved holdt som gidsel. Hackeren kræver en løsesum, typisk i form af kryptovaluta, for at give offeret adgang til sine data igen.

Målrettede ransomware-angreb er en særlig type ransomware-angreb. Hackerne forsøger her med en større arbejdsindsats over længere tid at kryptere store dele af it-infrastrukturen i myndigheder eller virksomheder på én gang. Det gør de for at afpresse ofrene for store løsesummer.

Andre hackere, der tidligere primært har fokuseret på tyveri af finansielle oplysninger fra bl.a. restaurations- og hotelbranchen, ændrede i 2020 fokus mod nye mål og angrebsmetoder. Det nye fokus skyldes sandsynligvis det omfattende fald i omsætning i restaurations- og hotelbranchen under COVID-19-pandemien verden over. Eksempelvis begyndte hackergruppen Carbanak at udføre målrettede ransomware-angreb. Gruppen var over en årrække blevet kendt for at kompromittere betalingssystemer i netop restaurations- og hotelbranchen samt detailhandlen for at stjæle kreditkortoplysninger. COVID-19-pandemien tvang gruppen til at tænke nyt.

Cyberkriminalitet er en industri
Carbanaks mulighed for hurtigt at omstille sig til at udføre målrettede ransomware-angreb blev bl.a. understøttet af det samarbejde, der er mellem de cyberkriminelle. Kriminelle hackere samarbejder og udveksler tjenester indbyrdes under markedslignende vilkår. Denne udveksling bliver i it-sikkerhedskredse kaldt Crime-as-a-Service (CaaS). Samarbejdet øger specialiseringen og effektiviteten i det cyberkriminelle miljø, hvilket skaber robuste og organiserede forsyningskæder, der bl.a. understøtter målrettede ransomware-angreb.

Statsstøttede hackere udfører også cyberkriminalitet
Nogle lande bruger cyberkriminalitet for at fremme deres strategiske interesser. Eksempelvis har Nordkorea gennem digitale bankrøverier, cyberangreb mod kryptobørser og distribuering af malware, der kan stjæle kryptovaluta, stjålet værdier, der svarer til milliarder af danske kroner. Pengene er bl.a. blev brugt til at understøtte Nordkoreas atomprogram.

Alene inden for det sidste år har nordkoreanske grupper angrebet organisationer, der handler med kryptovaluta, i mere end 30 lande.

Udvekslingen af værktøjer og tjenester foregår på lukkede internetfora og gennem etablerede, personlige samarbejdsrelationer. Her sælges og udveksles en bred palet af værktøjer som malware, adgang til kompromitterede ofre mv. CaaS gør det muligt for hackere at anskaffe sig de tjenester og adgange, de skal bruge i deres cyberangreb, frem for

selv at skulle udvikle dem. Det skaber værdikæder mellem de kriminelle hackere, der på forskellig vis gør det lettere for hackerne at begå cyberkriminalitet.

Flere kriminelle hackergrupper og netværk samarbejder i dag om målrettede ransomware-angreb, der kan være en meget indbringende forretning. I de tilfælde, hvor samarbejdet antager en mere organiseret form, vil hackerne ofte specialisere sig i at udføre afgrænsede dele af et angreb eller levere afgrænsede tjenester mod at få en andel af det samlede udbytte.

Nogle grupper organiserer endda deres ransomware-angreb som en decideret platformsøkonomi i lighed med kommercielle løsninger som Airbnb. Her leverer bagmændene bag bestemte ransomware værktøjer, infrastruktur og adgang til ofre til et netværk af andre hackere, der får en andel af udbyttet for at udføre selve angrebene.

REvil bruger et netværk af udvalgte hackere
Netværket, der står bag ransomwaren REvil, der også bliver kaldt Sodinokibi, bruger platformsøkonomien som forretningsmodel. Netværkets bagmænd står for udviklingen og driften af deres ransomware, mens de bruger et netværk af udvalgte hackere til at udføre selve angrebene for sig. Bagmændene finder deres hackere på bl.a. russiske hackerfora. Hackerne spores af bagmændene gennem et ID-nummer og får automatisk en del af udbyttet fra angrebene.

Udover målrettede ransomware-angreb truer netværket også med at lække data fra deres ofre, hvis de ikke betaler. Netværket har en hjemmeside, som de kalder "Happy Blog", hvor de truer deres ofre med læk af følsom data. Netværket angriber myndigheder og virksomheder på tværs af landegrænser og har også haft ofre i Danmark. I 2020 truede de eksempelvis med at lække data fra den nordiske brillekæde Synsam, der også ejer ProfilOptik.

Konsekvenserne af cyberkriminelle angreb vokser
De målrettede ransomware-angreb, som nogle hackere samarbejder om at udføre, er en global trend, der netop illustrerer, hvor hurtigt cyberkriminelle tilpasser sig nye indtjeningsmuligheder. Siden 2019 har truslen fra målrettede ransomware-angreb også været en del af normalbilledet i Danmark. Danske organisationer og myndigheder bliver regelmæssigt udsat for forsøg på denne type cyberkriminalitet.

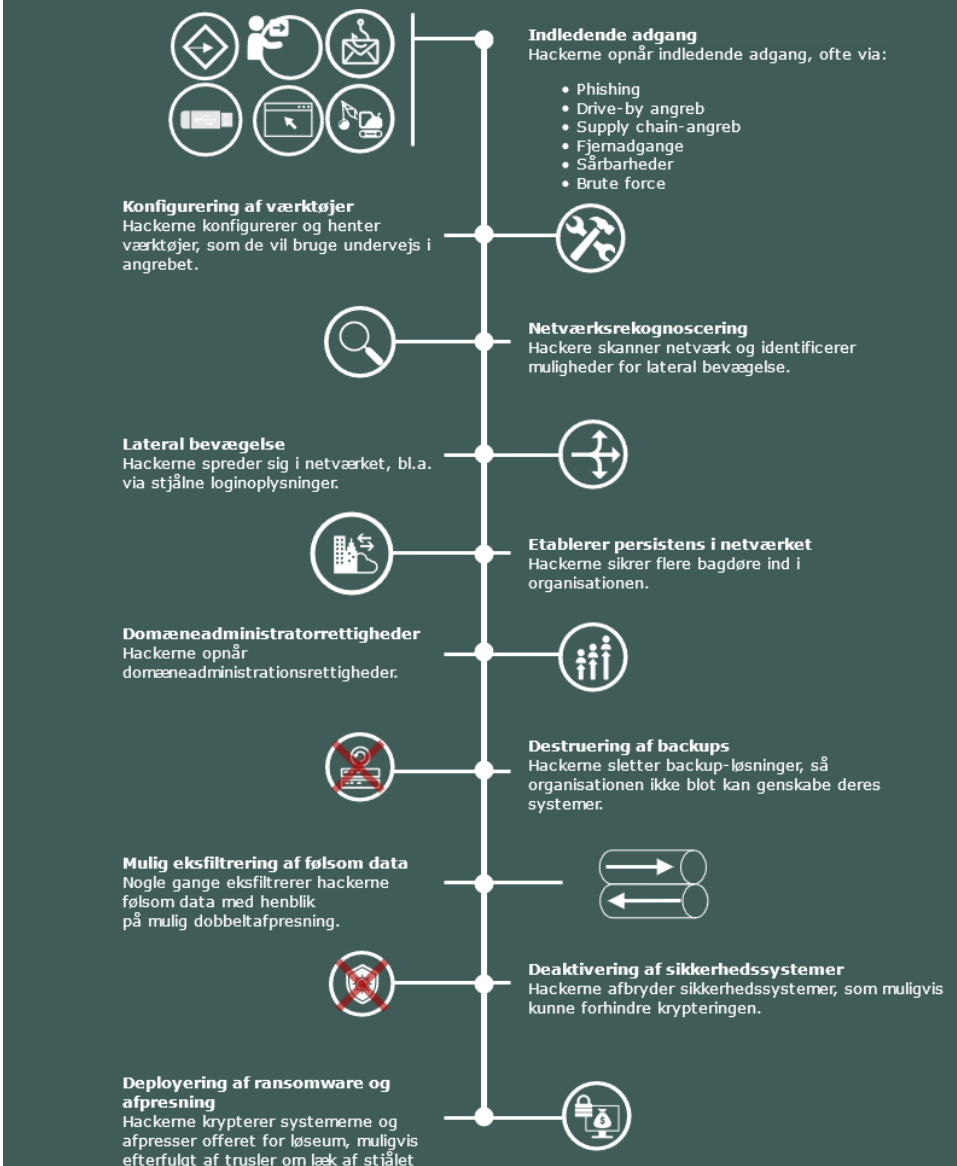
I 2020 voksede de potentielle konsekvenser af de målrettede ransomware-angreb, da de kriminelle på flere områder spændte den digitale tommelskrue. Eksempelvis har dobbelt afpresning øget de potentielle konsekvenser af et målrettet ransomware-angreb, fordi ofrene nu ikke blot mister tilgængeligheden af vigtige it-systemer men også risikerer, at forretnings- eller personfølsomme oplysninger bliver lækket til offentligheden eller solgt videre.

Det er blevet fast praksis for flere af de kriminelle grupper at lække stjålen information, hvis de ikke får en løsesum. Flere danske ofre har fået deres data lækket enten i forbindelse med et målrettet ransomware-angreb mod dem selv eller via kompromittering af en samarbejdspartner.

Cyberkriminelle forsøger sig også med andre former for afpresning. CFCS har i 2020 observeret en bølge af såkaldte Ransom Denial of Service-angreb (RDoS) i Danmark, hvor kriminelle truer med overbelastningsangreb, hvis deres offer ikke betaler en løsesum. Det er dog ikke alle kriminelle aktører, der har truet med den form for angreb, som har haft kapaciteten til at føre truslerne ud i livet.

Ransomware-angreb kan afværges

Målrettede ransomware-angreb er som udgangspunkt ikke lette at gennemføre for hackerne. De skal have omfattende kontrol over offerets it-systemer, før de kan kryptere dem. Et målrettet ransomware-angreb kan derfor være undervejs på organisationens it-netværk i flere dage, uger eller måneder, før systemerne rent faktisk krypteres. I den periode kan organisationer nå at reagere og afværge angreb, hvis de kender faresignalerne. Et typisk målrettet ransomware-angreb foregår på følgende vis:



Danske hackere udfører også cyberkriminalitet

CFCS vurderer, at truslen fra cyberkriminalitet især udgår fra organiserede hackergrupper og netværk i udlandet. Disse hackere udfører angreb i stor skala mod ofre verden rundt. Der er dog også eksempler på cyberkriminelle i Danmark.

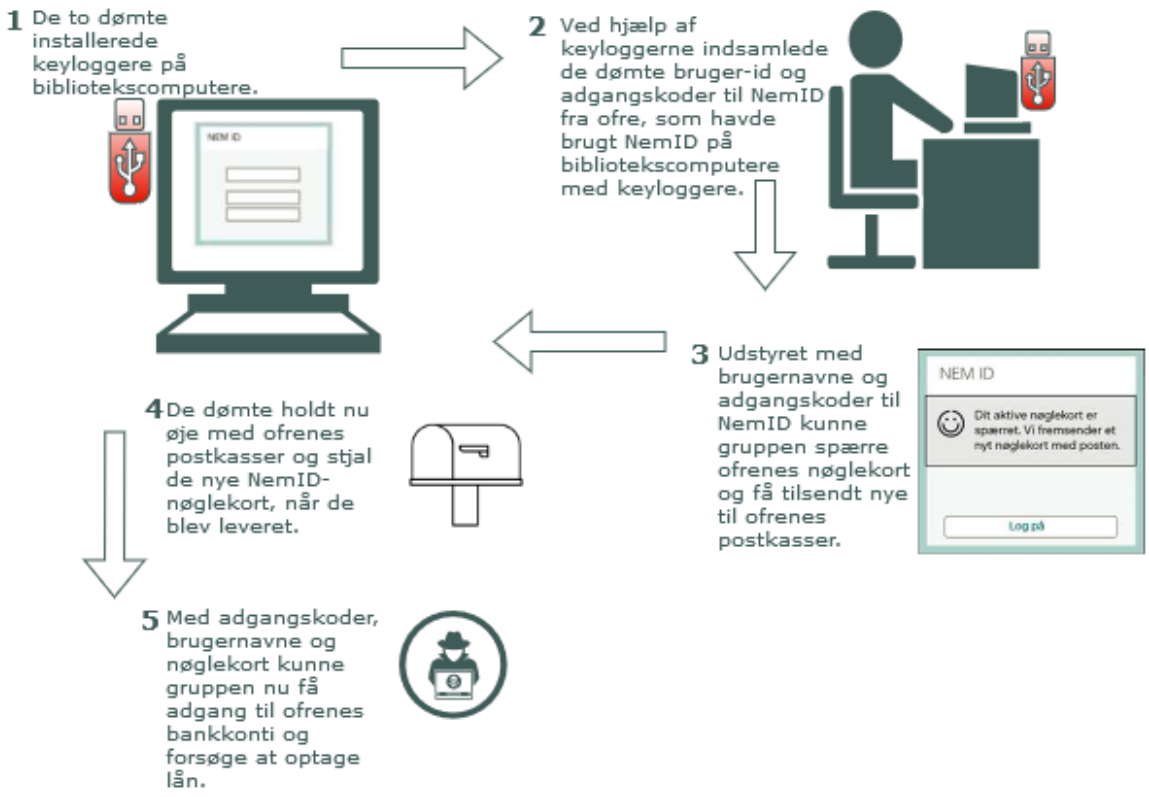
I december 2020 idømte Østre Landsret en 38-årig mand fængsel i tre år og konfiskerede ca. 22,4 mio. for hacking og bedrageri i forbindelse med pokerspil på internettet. Manden blev dømt for at have installeret malware på ofrenes computere, der gav ham adgang til at se deres computerskærme. Det udnyttede han i forbindelse med pokerspil på internettet mod de pågældende.

Kriminelle i Danmark kan i modsætning til udenlandske hackere også udnytte deres fysiske adgang til potentielle ofre og kendskab til det danske sprog og nationale it-sikkerhedsløsninger såsom NemID.

Keyloggere

Keyloggere registrerer tastetryk på tastaturer, som dermed gør det muligt at stjæle personlige oplysninger fra brugerne, herunder indtastede kreditkortoplysninger, brugernavne og kodeord til bl.a. NemID, mailkonti eller sociale medier.

I 2020 anholdte politiet eksempelvis 11 danskere i en sag om groft databedrageri med NemID. De tiltalte er sigtet for at have installeret keyloggere på offentlige bibliotekscomputere med henblik på økonomisk berigelse. Indtil videre er to af de sigtede i sagen blev dømt til henholdsvis to et halvt og tre års fængsel. De resterende ni afventer fortsat dom. Sagen er en del af et større sagskompleks, hvoraf to af de sigtede tidligere er dømt i lignende sager og for terrorplanlægning. I sagen fra 2016-2017 foregik svindlen på følgende måde:



CFCS samarbejder med andre myndigheder og virksomheder om løbende at identificere og nedtage hjemmesider, der bl.a. skal ligne danske myndigheders hjemmesider, og hvor formålet bl.a. er at stjæle brugernavne og kodeord til NemID eller betalingsoplysninger. I 2020 identificerede CFCS omkring 500 hjemmesider, der forsøgte at frarøve danske borgere deres personoplysninger på forskellig vis. Langt de fleste sider er efterfølgende blevet blokeret af politiet eller nedtaget af hosting-udbydere, typisk i udlandet.

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 fra fremmede stater inden for de næste to år.

Cyberspionage er en vedvarende trussel. CFCS har i de seneste seks år vurderet, at truslen fra cyberspionage mod Danmark er på det højeste mulige niveau på skalaen. Det betyder i praksis, at fremmede stater løbende forsøger at stjæle værdifuld information fra Danmark. Konkrete hændelser og angrebsforsøg underbygger gang på gang denne vurdering.

I 2020 kom flere angreb verden over frem i offentligheden, da myndigheder og virksomheder i et forsøg på at beskytte andre mod lignende angreb beskrev og fordømte angrebene.

Stater stjæler viden for at styrke egne interesser
Fremmede staters motiver for spionage kan opdeles i to hovedformål. Dels spionerer stater for at opnå sikkerhedspolitisk relevant viden, fra den helt overordnede strategiske viden til viden relevant for militær planlægning. Dels spionerer stater for at kunne fremme deres egen industri og økonomi.

Truslen fra cyberspionage retter sig derfor især mod danske myndigheder og organisationer, som arbejder med udenrigs- og sikkerhedspolitik i bred forstand. Ved hjælp af cyberspionage kan fremmede stater opnå viden om danske interesser, overvejelser og beslutninger i forbindelse med større internationale sager eller udenrigspolitiske forhandlinger. Den viden kan staterne bl.a. udnytte til at modarbejde danske interesser eller sætte danske forhandlere og beslutningstagere under pres.

Truslen er derudover særligt rettet mod virksomheder, der besidder en viden, som andre stater har interesse i. Det kan eksempelvis være kommercielle forretningshemmeligheder, herunder viden om kontrakter, udbud, ny teknologi, forskning eller anden intellektuel ejendom. Det kan skade Danmarks konkurrenceevne og dansk økonomi, hvis danske virksomheder udsættes for cyberspionage.

Cyberspionage retter sig også i nogle tilfælde mod virksomheder og myndigheder, som kan blive værdifulde for fremmede stater at have adgang til i fremtiden. Det kan f.eks. være i forbindelse med militære konflikter, hvor private virksomheder spiller en rolle for bl.a. forsyningssikkerheden og militæret. Fremmede stater kan med andre ord bruge cyberspionage mod virksomhederne til at opbygge kapacitet til at kunne gennemføre destruktive cyberangreb mod dem i forbindelse med en alvorlig konflikt.

COVID-19 står fortsat højt på den globale dagsorden i 2021

Forskning relateret til COVID-19 er et eksempel på viden, der kan have værdi for fremmede stater, og som derfor er et attraktivt mål for cyberspionage.

I løbet af det sidste år har der været flere cyberangreb mod organisationer, der arbejder med COVID-19. Eksempelvis anklagede den sydkoreanske nationale efterretningstjeneste, NIS, nordkoreanske hackere for at have forsøgt at hacke medicinalvirksomheden Pfizers databaser. Formålet var, ifølge NIS, at tilgå oplysninger om COVID-19 vacciner.

Flere lande herunder USA, Canada og Storbritannien har gentagne gange anklaget andre lande for at stå bag cyberspionage mod COVID-19 forskning.

Stater forsøger at udnytte alle veje ind

Når de aktører, der udfører cyberspionage, først har udset sig et mål, er de meget vedholdende i deres forsøg på at trænge ind i ofrenes systemer. De giver ikke op, hvis den direkte vej ind ikke lykkes, men finder i stedet alternative angrebsvinkler.

Leverandører bliver eksempelvis brugt som angrebsvinkel i de såkaldte supply-chain-angreb. Ved at kompromittere leverandører kan hackerne få adgang til mål, der ellers er godt beskyttet, og de kan få adgang til mange mål på én gang. De leverandører, der har en legitim og privilegeret adgang til deres kunders it-systemer, er særligt attraktive for hackerne. Det kan f.eks. være software-leverandører eller it-serviceudbydere. Det kan både være svært at opdage og at imødegå angreb via en leverandør, og det udnytter hackerne.

Hacket af SolarWinds var en alvorlig trussel

I december 2020 opdagede sikkerhedsfirmaet FireEye et af de mest omfattende offentligt kendte cyberspionageangreb nogensinde. Organisationer verden over, herunder i Danmark, var blevet kompromitterede via softwaren Orion fra virksomheden SolarWinds. Bl.a. har Mircrosoft og flere centrale amerikanske myndigheder offentligt meldt ud, at de er blevet ramt af angrebet. Virksomheder som Microsoft er selv leverandør til virksomheder verden over, og adgangen til dem kunne potentielt misbruges i angreb mod deres kunder i et dobbelt supply chain-angreb.

CFCS vurderer, at kompromitteringen via SolarWinds' software var en meget alvorlig trussel. Det er sandsynligt, at formålet med kompromitteringen er spionage.

Angrebet blev ifølge åbne kilder udført ved, at hackere kompromitterede virksomheden SolarWinds, som leverer software til organisationer verden over. Hackerne tilføjede i marts 2020 ondsindet kode i legitime opdateringer til SolarWinds' software Orion. Ifølge SolarWinds downloadede op imod 18.000 kunder verden over de kompromitterede opdateringer. Den ondsindede kode gav hackerne en indledende adgang til ofrenes systemer, som de kunne udnytte yderligere. CFCS vurderer, at aktøren kun udnyttede adgangene mod de mest interessante ofre.

CFCS er bekendt med, at mere end 50 organisationer i Danmark har anvendt den kompromitterede version af Orion og dermed fik installeret en bagdør i deres netværk. CFCS undersøger fortsat, om bagdøren har været udnyttet til at kompromittere ofrene yderligere med henblik på at stjæle data.

En anden alternativ angrebsvinkel er medarbejderes private konti, som stater kan angribe for at få adgang til deres arbejdsplads. Mange medarbejdere bruger den samme computer eller mobil både privat og arbejdsmæssigt, og nogle genbruger samme passwords til private og arbejdsmæssige adgange. Det udnytter hackerne. Hjemsendelserne under COVID-19 betyder samtidig, at det private og det professionelle digitale liv er blevet tættere forbundet. Konsekvenserne af, at den digitale frontlinje så at sige er rykket hjem i stuen, bliver uddybet i kapitlet omkring trends med betydning for cybertruslen.

Stater er oftest meget tålmodige i deres cyberspionage. En statsstøttet hackergruppe, der først er kommet ind i et system, spionerer som regel i det skjulte, længe før de laver mere risikable aktiviteter, der potentielt udløser alarmer i ofrenes systemer. Det kan derfor være vanskeligt at opdage statsstøttede hackergrupper i ens systemer.

APT28 – hackergruppen, der ikke altid går under radaren

APT28 er en af de mest omtalte hackergrupper. De blev bredt kendt i offentligheden, efter at amerikanske myndigheder anklagede APT28 for i 2016 at have hacket Demokraternes Nationale Komité (DNC). Ifølge anklagerne lækkede APT28 de stjålne informationer fra DNC for at påvirke det amerikanske præsidentvalg i 2016. APT28 er, ifølge de amerikanske myndigheder, tilknyttet den militære russiske efterretningstjeneste GRU.

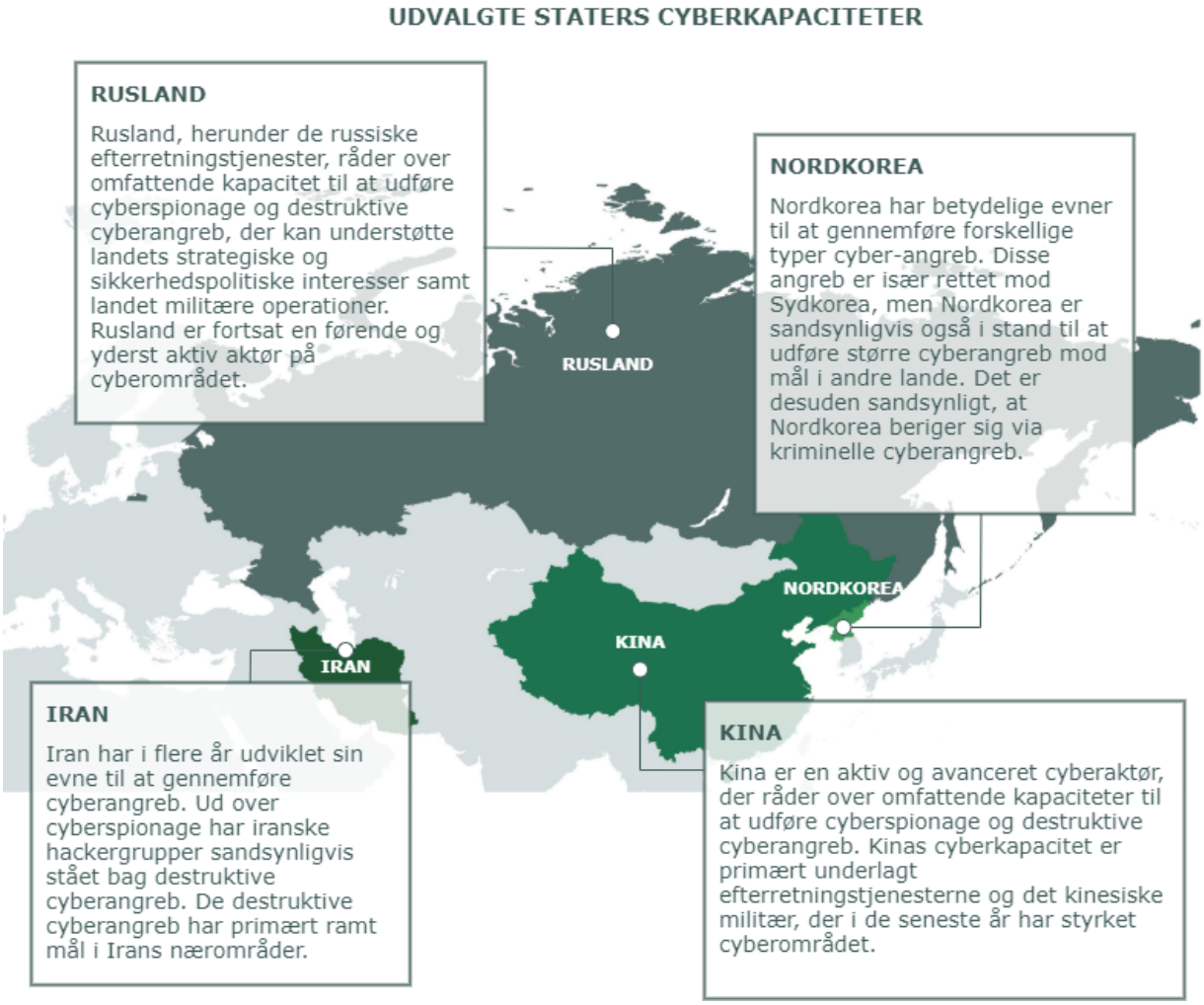
Nye cyberangreb bliver løbende tilskrevet APT28. I december 2020 udtalte den norske sikkerhedstjeneste PST, at APT28 sandsynligvis stod bag et cyberangreb mod det norske parlament.

APT28 har ifølge anklagerne betydelige ressourcer, men de har også brugt relativt simple angrebsmetoder, såsom spear phishing-mails og brute force-angreb.

APT28 er også kendt under andre navne, bl.a. Fancy Bear, Sofacy og Pawn Storm.

Ovenstående understreger, hvor målrettede og ihærdige fremmede stater kan være i deres forsøg på at trænge ind i organisationers systemer. I særlige tilfælde anvender fremmede stater også personer til fysisk at facilitere cyberspionage. Denne type angreb bidrager til, at cybertruslen også er alvorlig for systemer, der ellers er segmenterede fra internettet.

Fremmede staters angreb er dog i nogle tilfælde også præget af en vis opportunisme. De scanner efter sårbare systemer og ser, hvor de kan komme ind. Det kan bl.a. være for at opbygge infrastruktur, som de kan bruge til angreb mod andre mål. Men hvis hackerne finder interessant information på netværket, så stjæler de det. CFCS kender til flere eksempler på cyberangreb fra stater, hvor listen med ofre meget tyder på, at de fleste af ofrene alene blev angrebet, fordi de har haft den pågældende sårbarhed i deres netværk, og ikke fordi de var et prioriteret mål.



APT41 – hackergruppen der tager lidt til sig selv.
Fem medlemmer af APT41 blev i september 2020 anklaget af det amerikanske justitsministerium for at have stået bag flere års omfattende cyberspionage mod amerikanske og andre landes virksomheder og organisationer. Åbne kilder kæder også gruppen til omfattende cyberspionage mod bl.a. flere store tyske medicinalvirksomheder. Hackergruppen har bl.a. stjålet kildekode, digitale certifikater og anden værdifuld forretningsinformation. Gruppen har primært brugt forskellige offentligt tilgængelige hackerværktøjer. De har brugt både spear phishing, kendte sårbarheder og supply chain angreb til at opnå en indledende kompromittering af ofrene.

Ifølge det amerikanske anklageskrift har hackergruppen en tilknytning til den kinesiske stat. Hackerne har dog også brugt den statsstøttede hacking for egen vinding ved at bruge de indledende kompromitteringer til at udføre cyberkriminalitet.

APT41 er også kendt under andre navne, bl.a. Winnti, Wicked Panda, og Wicked Spider.

Private aktører benytter også cyberspionage

CFCS vurderer, at det i sjældne tilfælde ikke er fremmede stater, men private aktører, såsom virksomheder eller privatdetektiver, der benytter sig af cyberspionage. Det kan betyde, at organisationer, der normalt ikke vil komme i fremmede staters søgelys, kan blive mål for cyberspionage. Det er dog fortsat oftest stater, der udfører cyberspionage eller hyrer civile hackere til at udføre cyberspionage på statens vegne. En af årsagerne til, at cyberspionage sjældent bliver brugt af private, er sandsynligvis, at de har begrænset vilje og kapacitet. Hvis private aktører har viljen, kræver det ofte, at de betaler andre for at hacke for sig. Involveringen af en tredjepart er en risiko, som det sandsynligvis kun er få virksomheder, der vil løbe.

I de få udenlandske sager omhandlende privat cyberspionage, der er blevet offentligt kendt, har cyberspionagen været rettet mod forretningshemmeligheder eller følsomme informationer, der f.eks. kunne hjælpe virksomheden til at undergrave deres kritikere eller konkurrenter.

Kritikere af WireCard blev forsøgt hacket i årevis

I sommeren 2020 kom det frem, at en indisk virksomhed, BellTroX Infotech Services, sandsynligvis har udført cyberspionage for forskellige kunder igennem flere år. Det er ikke klart, hvem disse kunder er, men virksomheden har sandsynligvis arbejdet for bl.a. privatdetektiver.

Nogle af de ofre, som virksomheden sandsynligvis har angrebet, var journalister og shortsellere, der havde anklaget den tyske virksomhed WireCard for at begå svindel. Et af ofrene, der igennem flere år modtog spear phishing-mails, blev også opsøgt og udspurgt af privatdetektiver hyret af WireCard. WireCard erklærede sig konkurs i juni 2020, efter det kom frem, at store dele af virksomhedens forretninger var vildledende. Virksomheden efterforskes for omfattende økonomisk svindel.

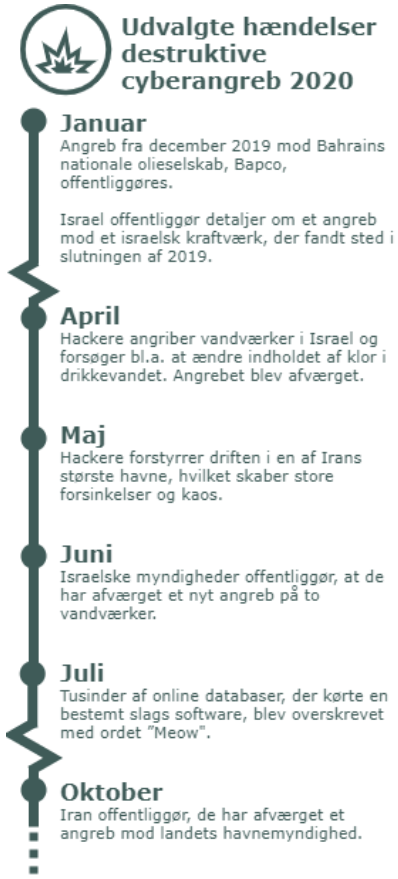
Hacking-kampagnen, der tilskrives BellTroX, er beskrevet i en rapport fra the Citizen Lab med titlen Dark Basin. I rapporten beskriver Citizen Lab også, hvordan bl.a. kritikere af den amerikanske virksomhed Exxon var mål for BellTroX' angreb.

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 bliver udsat for forsøg på destruktive cyberangreb inden for de næste to år.

Flere stater har kapaciteten til at udføre destruktive angreb, men det er mindre sandsynligt, at de aktuelt har intentioner om at udføre den type angreb mod danske mål.

Destruktive cyberangreb er stadig sjældne globalt. Langt de fleste destruktive cyberangreb, der har fundet sted indtil nu, har ikke medført fysisk skade, men har ødelagt data ved at slette eller kryptere dem uden mulighed for at genskabe dem.



Hvad er destruktive cyberangreb?

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

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

Stater har ikke intention om at udføre destruktive cyberangreb mod Danmark

Succesfulde destruktive cyberangreb kan have meget alvorlige konsekvenser, f.eks. i form af afbrudt adgang til samfundsvigtige funktioner, såsom strøm, transport eller internet eller omfattende ødelæggelse af data og enheder. Der er derfor tale om en potentiel trussel, som kan have alvorlige konsekvenser.

Det er mindre sandsynligt, at fremmede stater aktuelt har intentioner om at udføre destruktive cyberangreb mod Danmark. Flere stater har dog kapacitet til at udføre den type angreb. Det betyder, at truslen kan stige, hvis intentionen ændrer sig. Truslen kan ændre sig i forbindelse med en skærpet konflikt eller geopolitiske spændinger mellem Danmark og stater, der har kapacitet til at udføre destruktive cyberangreb.

CFCS vurderer, at de fleste destruktive cyberangreb har været udført af stater. Eksempelvis har Rusland, Kina, Iran og Nordkorea kapacitet til at udføre destruktive cyberangreb.

Indtil nu er der ingen kendte tilfælde, hvor danske myndigheder og virksomheder har været udsat for destruktive cyberangreb, der har været specifikt rettet mod dem. Dog blev f.eks. A.P. Møller-Mærsk ramt af det omfattende NotPetya-angreb, der ramte ofre verden over i 2017.

Stater udvikler kapaciteten til at udføre destruktive cyberangreb
Det er sandsynligt, at stater udvikler deres kapacitet til at udføre destruktive cyberangreb. Stater bruger bl.a. cyberspionage i forberedelsen af destruktive cyberangreb.

Det er muligt, at fremmede stater har forsøgt at kompromittere danske samfundsvigtige virksomheder for at kunne opbygge kapacitet til at udføre destruktive cyberangreb i Danmark på et senere tidspunkt. CFCS ser derfor med alvor på, at der i 2017 var flere målrettede forsøg på at få uautoriseret adgang til organisationer i den danske energisektor.

Forberedelsen af destruktive cyberangreb vil ofte bestå i en kortlægning af organisationer, systemer og netværksenheder, f.eks. industrikontrolsystemer. Ved at opnå viden om organisationer og systemer kan hackere udvikle specialiseret malware. Derudover kan hackere etablere såkaldte bagdøre på kompromitterede systemer, som de kan benytte i senere destruktive angreb. Hvis hackere allerede har en bagdør i et system, vil de hurtigere kunne iværksætte et destruktivt angreb mod systemet. Derfor kan en bagdør være en alvorlig sikkerhedsbrist, selvom den ikke bliver udnyttet nu og her.

Sandworm – hackerne bag flest kendte destruktive cyberangreb
Sandworm er en hackergruppe, som ifølge amerikanske myndigheder arbejder for den russiske stat. De er anklaget for at stå bag flere alvorlige destruktive cyberangreb, herunder strømafbrydelserne i Ukraine i 2015 og 2016, NotPetya-angrebet i 2017 og Olympic Destroyer-angrebet mod vinter-OL i Sydkorea i 2018.

Gruppen bliver kaldt Sandworm, fordi der er fundet referencer i deres malware til Science Fiction-bogen *Dune* af Frank Herbert fra 1965, hvor kæmpe sandorme spiller en afgørende rolle. Sandworm er også kendt under andre navne, bl.a. Voodoo Bear og Telebots.

15. oktober 2020: Amerikanske myndigheder anklager seks navngivne russiske statsborgere for at have været en del af Sandworm. (Pool/AFP/Ritzau Scanpix)

Motiverne bag destruktive cyberangreb varierer
Formålet med destruktive cyberangreb er at ødelægge og skade, men der er forskellige mere specifikke motiver bag de enkelte angreb. Et bagvedliggende motiv for destruktive cyberangreb kan eksempelvis være sabotage. Sabotage kan bl.a. indebære, at en aktør udfører et angreb for at forstyrre eller forhindre en modstanders adgang til et system, en teknologi eller information. Motivet kan også være en straffeaktion i forbindelse med en konflikt, hvor målet med angrebet er at påføre offeret økonomiske eller andre ressourcemæssige omkostninger. Et motiv for destruktive cyberangreb kan derudover være at sende et signal til offeret samt andre potentielle ofre. Endelig kan et destruktivt cyberangreb også blive udført for at teste og potentielt udvikle en kapacitet.

Det er ofte vanskeligt at vurdere præcis, hvilken hensigt der ligger bag et destruktivt cyberangreb. Det er desuden sandsynligt, at mange angreb tjener flere formål.

NotPetya, der var et af de mest omfattende destruktive cyberangreb i verden, kan have tjent flere formål. Angrebet startede i Ukraine i 2017 og spredte sig derefter globalt. Flere lande har tilskrevet angrebet til Rusland. Angrebet kan dels tolkes som en straf af Ukraine, som Rusland var i konflikt med. Men det kan også tolkes som et signal til omverdenen, om at der er risici forbundet med at drive virksomhed i Ukraine.

Destruktive cyberangreb bruges oftest i forbindelse med konflikter
CFCS vurderer, at destruktive cyberangreb oftest bliver udført af stater i forbindelse med konflikter eller geopolitiske spændinger.

I konfliktområder, hvor stater har brugt destruktive cyberangreb mod civile mål, eksempelvis i Mellemøsten eller i Ukraine, kan truslen fra destruktive cyberangreb være højere. Danske virksomheder, der arbejder globalt, kan blive ramt af angreb, der ikke er rettet mod Danmark, men mod virksomheder der opererer i konfliktområder.

Truslen fra destruktive cyberangreb kan også blive skærpet for virksomheder, som arbejder for organisationer eller stater, der i øvrigt er mål for destruktive cyberangreb.

Det er muligt, at danske virksomheder og myndigheder, der er til stede i konfliktområder, særligt i Ukraine og Mellemøsten, kan blive ramt af følgevirkninger af destruktive cyberangreb, såsom strømafbrydelser eller ødelæggelse af data.

Angreb mod industrikontrolsystemer kan medføre fysisk ødelæggelse
Destruktive cyberangreb mod industrikontrolsystemer, der understøtter leveringen af samfundsvigtige funktioner, kan få særligt alvorlige samfundsmæssige konsekvenser. Dels kan angreb på den type systemer afbryde leveringen af vitale ydelser såsom strøm og internet, men de kan også medføre ødelæggelse af fysiske objekter og personskade.

Det kan ske, fordi industrikontrolsystemer styrer, overvåger og kontrollerer industriprocesser, f.eks. sikkerhedsmekanismer, der kan skabe farlige situationer, hvis de forstyrres eller manipuleres.

Det er dog fortsat kun få eksempler, hvor det er sandsynligt, at destruktive cyberangreb er blevet udført med det formål at forårsage egentlig fysisk ødelæggelse.

Der er kun få eksempler på destruktive cyberangreb, hvor formålet har været egentlig fysisk ødelæggelse

Stuxnet (2010) Det eneste kendte destruktive cyberangreb, der har medført reel fysisk ødelæggelse, ramte Iran i 2010. Hackere brugte malwaren Stuxnet mod iranske centrifuger til berigelse af uran. Angrebet ødelagde centrifugerne.

Strømafbrydelser i Ukraine (2016) Det destruktive cyberangreb, der ramte Ukraines elforsyning i 2016, kunne også have medført fysisk skade på udstyr, og dermed potentielt længerevarende strømafbrydelser. It-sikkerhedseksperter har bl.a. beskrevet indikationer på, at angrebet var planlagt til at ramme kontrolswitches og beskyttelsesrelæer med overbelastningsangreb. Hackerne havde dog ikke succes med den del af angrebet**.**

Triton (2017) Det er muligt, at cyberangrebet mod industrikontrolsystemet Triconex i Saudi Arabien i 2017 kunne have skabt fysisk ødelæggelse. Angrebet var rettet mod en petrokemisk industrivirksomhed og systemet Triconex, som den ramte virksomhed brugte. Triconex sørger bl.a. for, at produktionssystemer bliver lukket ned på en kontrolleret og sikker måde, hvis der opstår kritiske fejl eller problemer. Angrebet kunne potentielt have medført fysisk ødelæggelse, men sikkerhedssystemerne lukkede ned på en ufarlig måde. Nedlukningen betød også, at malwaren blev opdaget. Hvis sikkerhedsmekanismerne var blevet slået fra eller manipuleret med, kunne det have øget risikoen for personskade eller død på og omkring virksomheden, som følge af enten udslip af farlige gasser eller eksplosioner.

Stater udfører også omfattende forstyrrende cyberangreb

Stater udfører også alvorligt forstyrrende cyberangreb, der ikke falder ind under CFCS' definition af destruktive cyberangreb, men alligevel har betydelige konsekvenser. Den type angreb er sjældne, men har i få tilfælde i udlandet resulteret i afbrydelse og forstyrrelser af adgangen til og driften af mange eller vitale digitale systemer og tjenester.

De alvorligt forstyrrende angreb befinder sig typisk i en gråzone mellem destruktive cyberangreb og cyberaktivisme, bl.a. fordi angrebsmetoderne minder en del om hinanden. Det var tilfældet, da den georgiske web-hostingudbyder Pro Service blev ramt af et alvorligt forstyrrende angreb i efteråret 2019. Både amerikanske og britiske myndigheder har offentligt anklaget russiske statsstøttede hackere for at stå bag angrebet. De britiske myndigheder udtalte bl.a., at angrebet blev udført med det formål at skabe ustabilitet og underminere Georgiens suverænitet.

Cyberangrebet mod Pro Service førte til, at over 2.000 georgiske hjemmesider, der bl.a. tilhørte den georgiske regering, præsidentkontoret, civile domstole, lokale byråd, banker, NGO'er samt større virksomheder og nyhedsmedier i Georgien, blev udsat for såkaldte defacement-angreb. Det originale indhold på de mange hjemmesider blev erstattet af et foto af Georgiens tidligere præsident Mikheil Saakashvili med teksten "I'll be back". Herefter lukkede hackerne hjemmesiderne, der dog var online igen efter 24 timer.

Billedet af den tidligere præsident Mikheil Saakashvili, der blev brugt til at deface hjemmesiderne.

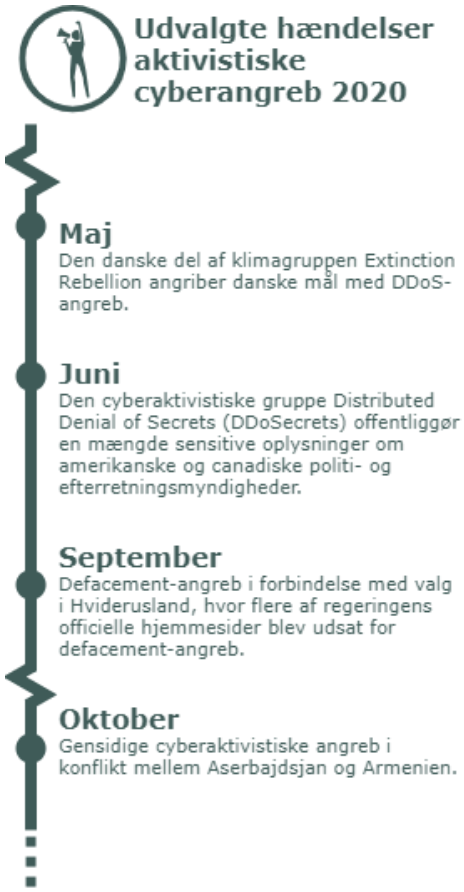
Cyberaktivisme

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

I 2020 har der været enkelte, mindre alvorlige aktivistiske cyberangreb mod danske mål. Truslen fra cyberaktivisme kommer typisk til udtryk i forbindelse med begivenheder eller enkeltsager, der tiltrækker cyberaktivisters opmærksomhed.

De mange protester, der har præget 2020, har ikke ført til en stigning i antallet af cyberaktivistiske angreb på verdensplan. Antallet af angreb har således ligget på niveau med de seneste år.

Det er mindre sandsynligt, at Danmark vil blive ramt af faketivisme, hvor stater udfører cyberangreb under dække af at være cyberaktivister.



Flere forskellige typer aktivister udfører cyberangreb
Formålet med cyberaktivisme er, ved hjælp af cyberangreb, at skabe størst mulig opmærksomhed om en sag. Aktivisterne anvender forskellige angrebsmetoder for at opnå dette. Angrebene varierer meget i kompleksitet – fra relativt simple overbelastningsangreb til mere ressourcekrævende hack og læk operationer. Derfor findes der forskellige kategorier af cyberaktivister.

En type af aktivister supplerer i sjældne tilfælde demonstrationer, SoMe kampagner og happenings med simple cyberangreb som eksempelvis overbelastningsangreb, også kaldet DDoS-angreb.

DDoS-angreb er relativt nemme at udføre og forudsætter typisk ikke meget planlægning og teknisk viden. Det er imidlertid også forholdsvis nemt for virksomheder og myndigheder at beskytte sig mod denne type angreb.

COVID-19 tvinger klimaaktivister til at tænke nyt
Corona-nedlukningen af samfundet i foråret 2020 havde også betydning for miljøaktivister. Den danske del af klimagruppen Extinction Rebellion, som tidligere har lavet klassisk aktivisme, gennemførte ifølge deres eget nyhedsbrev i maj 2020 meget simple overbelastningsangreb mod en række organisationer.

Aktivisterne angreb hver dag et nyt offer, som de mente, var en stor miljøforurener. Blandt de angrebne organisationer var BP, Shell, A.P. Møller Mærsk og Finansministeriet i Danmark. Sidstnævnte angreb de, fordi den danske stat havde givet finansiel støtte til flyselskabet SAS.

Aktivisterne benyttede sig af et let tilgængeligt værktøj. Fra deres hjemmecomputere sendte aktivisterne tusindvis af beskeder med dele af FN's klimarapport til virksomhedernes hjemmesider. Aktivisterne ville overbelaste hjemmesiderne og få dem til at lukke ned.

En anden type aktivister bruger cyberangreb som et mere centralt værktøj i deres aktivisme. Denne gruppe besidder ofte veludviklede tekniske kompetencer, der gør dem i stand til at udføre avancerede cyberangreb. Et eksempel på det er hack og læk angreb, hvor hackere stjæler følsom information fra deres offer og offentliggør den med henblik på at skade offeret.

Den form for angreb er typisk sværere at beskytte sig imod, og konsekvenserne af et veludført angreb kan blive mere kritiske.

Cyberaktivisme kommer således til udtryk i en mangfoldig gruppe af aktiviteter, der spænder fra simple angreb til mere organiserede kampagner. En fællesnævner på tværs af det 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 og aktivistiske grupper forfølger. Det er eksempelvis klima eller dyrevelfærd.

Protestbevægelser er kun i begrænset omfang gået online
De mange konventionelle protester, der har præget 2020, har ikke været ledsaget af en tilsvarende stigning i cyberaktivisme.

Protester mod håndteringen af COVID-19-pandemien, Black Lives Matter-bevægelsen, MeToo-bølgen og præsidentvalget i USA har fået tusindvis af demonstranter på barrikaderne både i udlandet og herhjemme. Samtidigt betød COVID-19-pandemien, at flere lande har indført forsamlingsforbud og restriktioner, der i praksis har gjort det mere besværligt at afholde konventionelle demonstrationer.

Den mobilisering og de besværlige forhold, den har udfoldet sig under, har dog ikke ført til en generel stigning i antallet af cyberaktivistiske angreb globalt. På trods af bl.a. Blue Leaks og Extinction Rebellions cyberaktivisme ligger antallet således på samme lave niveau som de foregående år.

BlueLeaks: Black Lives Matter bevægelsen vækker Anonymous til live
I juni 2020 offentliggjorde hackergruppen Distributed Denial of Secrets (DDoSecrets) flere hundrede gigabytes data fra amerikanske og canadiske politimyndigheder og efterretningstjenester. Lækket bestod bl.a. af over 16 millioner rækker data om politiarbejde og inkluderede persondata om mere end 700.000 betjente.

Det offentliggjorte data stammer ifølge åbne kilder fra 251 politihjemmesider, hvoraf mange var beregnet til at dele data mellem forskellige dele af de amerikanske politimyndigheder. Alle websites kørte på den samme software fra virksomheden Netsentiel, som også hostede data. Ved at udnytte en svaghed ved leverandøren Netsentiel fik hackeren sandsynligvis adgang til de mange hjemmesider.

Ifølge grundlæggeren af DDoSecrets har de modtaget BlueLeaks-data fra en hacker, der er tilknyttet hackergruppen Anonymous.

Uro og konflikter afføder fortsat cyberaktivisme
Det er flere år siden, at der har været avancerede aktivistiske cyberangreb rettet mod danske mål. I udlandet er der dog flere eksempler på, at avancerede cyberaktivistiske angreb har været brugt i forbindelse med konflikter og politisk uro i 2020.

Det skete eksempelvis med læk af oplysninger om politiet i de såkaldte BlueLeaks i USA og Canada samt i forbindelse med valget i Hviderusland, hvor flere af regeringens officielle hjemmesider blev hacket i september 2020. Her indsatte hackere tekster og billeder, som rettede kritik mod præsident Aleksandr Lukasjenko og regeringen.

Nagorno-Karabakh-konflikten mellem Armenien og Aserbajdsjan affødte også cyberaktivistiske angreb. Her stjal armenske cyberaktivister bl.a. klassificeret information om medlemmer af Aserbajdsjans flådestyrke og lækkede informationen på internettet. Derudover udførte armenske cyberaktivister løbende DDoS-angreb på flere regeringsportaler i Aserbajdsjan.

Hackere forsøger at undergrave tilliden til COVID-19 vacciner
I december 2020 meddelte det Europæiske Lægemiddelagentur, EMA, at de var blevet kompromitteret.

Hackerne tilgik bl.a. viden om Pfizers og BioNTech samt Modernas vacciner mod COVID-19. EMA har senere beskrevet, hvordan hackerne, der stjal dokumenter og fortrolige mails, samtidigt manipulerede med indholdet i disse og lækkede dem på nettet i et forsøg på at undergrave tilliden til vaccinerne.

Stater bruger cyberaktivisme som dække for påvirkning

Under dække af at være cyberaktivister bruger nogle stater en kombination af cyberangreb og andre typer propagandaværktøjer i påvirkningskampagner.

Det var eksempelvis tilfældet, da flere nyhedsmedier i Litauen over en længere periode i 2019 blev kompromitteret af hackere, der plantede falske nyheder på deres hjemmesider. Nyhederne centrerede sig især omkring NATO's tilstedeværelse i landet. 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 alliancens tilstedeværelse i landet.

I populær tale kaldes det for faketivisme. Formålet med faketivisme er oftest at afspore eller aflede den offentlige debat og derved at kultivere en polarisering i de ramte samfund.

Det er mindre sandsynligt, at Danmark vil blive ramt af faketivisme. Det er dog muligt, at truslen vil stige i forbindelse med 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.

Cyberterror

Truslen fra cyberterror er **INGEN**.

Det betyder, at det er usandsynligt, at Danmark, herunder danske virksomheder og myndigheder, bliver 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.

Cyberangreb i den skala forudsætter it-kompetencer og organisatoriske ressourcer, som CFCS vurderer, at militante ekstremister aktuelt ikke har.

Militante ekstremister udfører dog andre former for cyberangreb end cyberterror, eksempelvis cyberaktivisme.

Manglende kapacitet ledsages af en meget begrænset hensigt
Militante ekstremister har endnu ikke udført angreb, der lever op til CFCS' definition af cyberterror. Dels skyldes det, at de mangler ressourcerne. Men det skyldes sandsynligvis også, at de etablerede terrorgrupper generelt ikke anser cyberangreb som en realistisk og effektiv måde at skabe den samme frygt og kaos, som konventionelle terrorangreb gør.

Den manglende hensigt understreges af, at der kun er 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.

Crime-as-a-Service kan hjælpe militante ekstremister med at udføre visse typer cyberangreb
Et fænomen som CaaS, hvor hackerværktøjer og tjenester kan købes på internettet, vil muligvis kunne øge militante ekstremisters cyberkapaciteter.

Terroristerne kan derved potentielt købe sig til services, værktøjer, tjenester og adgange, som de ikke selv har kapaciteten til at udvikle eller udnytte.

Det er dog tvivlsomt, om CaaS kan understøtte angreb, der lever op til CFCS' definition af cyberterror. De værktøjer, som kriminelle udveksler på nettet, er udviklet til cyberangreb, der fortrinsvist understøtter berigelseskriminalitet og ikke cyberangreb, der ville kunne kategoriseres som cyberterror.

En anden barriere er sprog og kultur. Flere kriminelle netværk og hackerfora er eksempelvis russisksprogede og skeptiske over for samarbejde med ikke-russisktalende hackere.

Terrorister udfører andre former for cyberangreb
Der er eksempler på, at militante ekstremister udfører andre former for cyberangreb end cyberterror til at fremme deres sag.

Disse angreb er typisk simple cyberaktivistiske angreb, der har til formål at skabe opmærksomhed om deres sag gennem eksempelvis hacking af hjemmesider og indsættelse af militante ekstremistiske budskaber.

Ligesom terrorgrupper kan benytte sig af cyberaktivisme, kan de også bruge cyberkriminalitet til at finansiere terror, men heller ikke her er der tale om cyberterror.

Trends og tendenser

Pandemien har flyttet virksomhedernes cyberforsvar hjem i stuen
Pandemien har medført en pludselig øget digitalisering af arbejdspladsen for rigtig mange mennesker. Nedlukningen af samfundet i foråret 2020 skabte et akut behov for at opretholde produktion og serviceniveau hjemmefra i de fleste myndigheder og virksomheder. Dén omstilling krævede for mange organisationer hurtige beslutninger om etablering eller udvidelse af fjernadgange og digitale løsninger til online samarbejde.

Denne digitale omstilling har vist sig at have flere fordele. Organisationer er blevet mere fleksible i deres arbejdsgange, og flere har fået øjnene op for, at mange mødeaktiviteter, som traditionelt er foregået fysisk, med fordel kan gennemføres online. Det er sandsynligt, at mange af de nye digitale arbejdsgange og fjernadgange vil fortsætte selv efter sundhedskrisen.

Hjemmearbejde har flyttet den digitale frontlinje hjem i stuen
Samtidigt skaber det også visse udfordringer for it-sikkerheden, når arbejdspladserne flytter hjem i stuen. Det kan for eksempel ske, hvis fjernadgange ikke opdateres eller er sat op i en fart, uden hensyn til sikkerhed. Hackere skanner hele tiden efter disse huller, og forsøger at komme ind via kendte sårbarheder eller usikre adgangskoder.

En hackergruppe har eksempelvis under pandemien tilføjet et nyt modul til deres malware, som specifikt søger og angriber eksponerede fjern-adgange (RDP) for senere at udføre målrettede ransomware-angreb mod interessante ofre. CFCS har flere gange advaret om, at hackere misbruger RDP-adgange. Alligevel er der i andet kvartal af 2021 fortsat mere end 4.000 potentielt sårbare RDP-adgange åbne mod internettet i Danmark og næsten fem millioner på verdensplan.

Når computere uden for organisationens digitale perimeter får adgang til dens it-netværk, kan de blive en genvej ind for hackere og øger derved organisationens angrebsflade. Når den digitale frontlinje rykkes hjem i medarbejdernes stue, bliver cybertruslen mod hjemmecomputere og hjemmearbejdspladser noget, som organisationer skal forholde sig mere aktivt til.

Når arbejdet foregår fra hjemmet, vil nogle medarbejdere have mindre opmærksomhed på it-sikkerhed. De opfatter måske ikke sig selv som et interessant mål for hackere, eller tænker ikke på, at deres private computer er blevet en del af arbejdsgiverens it-infrastruktur, hvis de bruger den til arbejdsrelaterede aktiviteter som mails eller møder.

Hvis en computer, der anvendes til hjemmearbejde, har adgang til den centrale del af virksomhedens it-netværk, for eksempel via med VPN-forbindelse, kan malware og hackere sprede sig fra computeren ind i virksomhedens it-netværk. Hjemmearbejdspladser med den type adgang bør derfor sikres lige så godt som computere på arbejdspladsen.

5G's ankomst til Danmark kan på mellemlangt sigt ændre det digitale landskab og cybertruslens betydning

2020 blev året, hvor 5G kom til Danmark. De selskaber, som har mobilinfrastruktur i Danmark (dvs. TDC, 3 og TT Network, som ejes af Telenor og Telia), nåede alle at tænde for 5G, inden året var omme. Endnu er det kun ét enkelt selskab, der tilbyder 5G i hele landet, mens de øvrige selskaber stadig er i gang med udrulningen.

Hidtil er udviklingen i samfundet gået mod en konstant øget mobilitet og digitalisering, og der er intet, som tyder på, at den tendens stopper. 5G er det bedste bud på en teknologi, der vil løfte den udvikling til næste niveau.

Hvor 4G primært har forbundet mennesker med internettet, lover 5G teknologien høj hastighed, hurtig respons, håndtering af mange samtidige enheder og mobilnetværk dedikeret til eksempelvis IoT, industri og autonome systemer. På kort sigt adskiller 5G sig dog i praksis primært ved at tilbyde en højere datahastighed. Det skyldes, at 5G indledningsvis genbruger meget af teknologien fra de eksisterende 4G-netværk.

5G medfører flere og nye angrebsflader for hackerne

5G lover bedre sikkerhed i mobiltjenesterne. Erfaringerne fra 4G viser imidlertid, at ny teknologi altid indeholder sårbarheder, så fremtiden må vise, om løftet kan holde. Det er derimod sikkert, at 5G's kompleksitet vil medføre nye angrebsflader i teleinfrastrukturen. Decentraliseret netværksstruktur, edge- og cloud computing samt software, der erstatter fysisk hardware, er forudsætninger for 5G's høje ydeevne, men det øger samtidig angrebsfladen.

De mange sensorer, produkter og apparater, der sandsynligvis vil blive forbundet til internettet via en 5G-forbindelse, vil også åbne op for flere og nye angrebsflader. Det er i første omgang en trussel mod brugerne af udstyret, men udstyret kan også kompromitteres og anvendes til cyberangreb mod andre internetbrugere eller teleinfrastruktur.

Fysisk udstyr, der bliver styret digitalt, for eksempel via en 5G-forbindelse, øger koblingen mellem den fysiske og digitale verden og kan hæve risikoen for, at et cyberangreb fører til fysisk skade. Der kan eksempelvis være tale om maskiner i industrien, autonome fartøjer eller udstyr i sundhedssektoren.

5G's fulde funktionalitet vil tidligst være til rådighed om 2-4 år. Det skyldes, at teleudbyderne skal bruge tid på at udbygge 5G-dækningen og ikke mindst indføre de ændringer i infrastrukturen, som understøtter de avancerede 5G-tjenester. Det er derfor mindre sandsynligt, at 5G på kort sigt vil ændre det digitale landskab væsentligt.

5G skaber behov for nye måder at imødegå cybertruslen på

Bliver 5G den forventede succes, vil samfundsvigtige funktioner samt virksomhedernes produktion og økonomi blive afhængige af tilgængeligheden, fortroligheden og integriteten i 5G-tjenesterne.

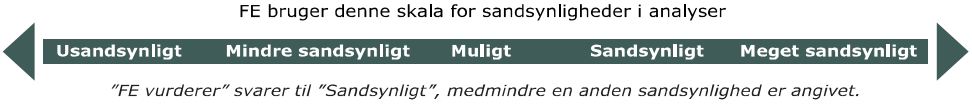
Det gælder især for de services, der bliver afhængige af de funktioner og ydelser, som kun 5G kan levere. Her vil det ikke være muligt at sikre tilgængeligheden ved brug af redundante forbindelser til traditionelle teknologier som 4G eller faste internetforbindelser. Diskussionerne omkring 5G viser, hvordan nye teknologier og de muligheder, der følger med, også kan få indflydelse på cybertruslen.

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 sandsynligheder i analyser



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