CENTER FOR CYBERSIKKERHED

Trusselsvurdering:

Cybertruslen mod Danmark 2022

2. udgave februar 2023.

Indhold

CENTER FOR CYBERSIKKERHED

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

2. udgave februar 2023.

Cybertruslen mod Danmark 2022

Formålet med denne trusselsvurdering er at informere beslutningstagere i danske myndigheder og virksomheder om cybertruslen mod Danmark. Trusselsvurderingen redegør for de forskellige typer cybertrusler, Danmark står over for. Vurderingen kan bl.a. indgå som en del af grundlaget for myndigheders og virksomheders risikovurderinger på cybersikkerhedsområdet.

Trusselsvurderingen er redigeret i februar 2023. Trusselsniveauet for cyberaktivisme er hævet fra **MIDDEL** til **HØJ,** og de relevante tekststykker i trusselsvurderingen er rettet for at afspejle denne ændring**.** Den resterende tekst er uændret.

Hovedvurdering

- Truslen fra cyberspionage er **MEGET HØJ.** Den vedvarende trussel udgår især fra Rusland og Kina og fører løbende til cyberangreb mod danske mål. Dele af det danske samfund er udsat for en vedvarende, aktiv og alvorlig trussel. Truslen er særligt rettet mod Udenrigs- og Forsvarsministeriets myndighedsområde, men rammer også myndigheder og virksomheder i andre samfundsvigtige sektorer.

- Truslen fra cyberkriminalitet er **MEGET HØJ.** Den mest alvorlige trussel fra cyberkriminalitet mod Danmark kommer fra ransomware-angreb. Cyberkriminelles muligheder for samarbejde, arbejdsdeling og specialisering understøtter truslen og bidrager til at fastholde den meget høje trussel fra cyberkriminalitet.

- Truslen fra cyberaktivisme er **HØJ.** CFCS har hævet trusselsniveauet på baggrund af pro-russiske cyberaktivisters høje aktivitetsniveau mod NATO-lande, herunder Danmark, samt deres mere formaliserede angrebsmodus og øgede kapacitet. Det er sandsynligt, at særligt pro-russiske hackere igen vil gå efter mål i Danmark.

- Truslen fra destruktive cyberangreb er **LAV.** Det er mindre sandsynligt, at fremmede stater aktuelt har intentioner om at udføre destruktive cyberangreb mod Danmark. Destruktive cyberangreb bliver oftest udført af stater i forbindelse med konflikter eller geopolitiske spændinger. Flere stater har kapacitet til at udføre den type angreb.

- Truslen fra cyberterror er **INGEN.** Fraværet af en trussel fra cyberterror skyldes dels at militante ekstremister har begrænset hensigt om at udføre cyberterror. Dels har de ikke den fornødne kapacitet til at udføre cyberangreb, der er så ødelæggende, at de kan sammenlignes med konventionel terror.

- Fremmede stater, herunder Rusland, bruger aktivt cyberangreb i deres forsøg på at påvirke holdninger og adfærd i andre lande. Det er dog sandsynligt, at Danmark aktuelt ikke udgør et prioriteret påvirkningsmål for fremmede stater.

Indledning

Ruslands invasion af Ukraine i slutningen af februar 2022 medførte store forandringer i det sikkerhedspolitiske landskab. Fremtiden tegner på flere områder mere usikker end før invasionen, og denne usikkerhed har også spredt sig til cyberområdet. Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) udgav derfor i marts 2022 trusselsvurderingen "Cybertruslen mod Danmark i lyset af Ruslands invasion af Ukraine", hvori CFCS vurderede, hvordan Ruslands invasion havde påvirket cybertrusselsbilledet.

Når CFCS nu udgiver den årlige vurdering af cybertruslerne mod Danmark, er formålet at vurdere cybertruslerne mod Danmark i en bredere kontekst end den russiske invasion af Ukraine alene. For selvom den usikkerhed og spænding, der kendetegner den nuværende situation, øger risikoen for misforståelser og eskalation, så vurderer CFCS fortsat, at alle trusselsniveauer bortset fra truslen fra cyberaktivisme er uændrede.

Danmark står overfor en række cybertrusler, der også var alvorlige før invasionen af Ukraine, og som vil være gældende uafhængigt af, hvordan situationen i Ukraine udvikler sig. Cybertruslen mod Danmark kommer fortsat særligt fra kriminelle hackere og fremmede stater. Både Rusland, Kina og kriminelle hackergrupper udfører løbende cyberangreb mod danske myndigheder og virksomheder.

Cyberkriminalitet udgør en af de mest alvorlige cybertrusler mod Danmark. Cyberkriminalitet fører til angreb, der har omfattende økonomiske omkostninger for både myndigheder og virksomheder. I enkelte tilfælde har konsekvenserne af cyberkriminalitet også afbrudt leveringen af samfundsvigtige ydelser i udlandet.

Cyberspionage er politisk og økonomisk motiveret. Stater udfører fortsat cyberspionage for at få adgang til sensitiv og værdifuld viden, som danske organisationer ønsker at beskytte. Hvis denne type viden kompromitteres, kan den blive misbrugt til eksempelvis at svække Danmarks udenrigspolitiske indflydelse eller til forberedelse af eventuelle fremtidige konflikter. Begge dele kan i sidste ende få betydning for Danmarks sikkerhed.

Udover cyberkriminalitet og cyberspionage vurderer CFCS også truslerne fra cyberaktivisme, destruktive cyberangreb, cyberterror og belyser også i år truslen fra påvirkning med brug af cyberangreb.

Påvirkning med brug af cyberangreb udgør også en trussel
Cyberangreb er en af flere typer aktiviteter, fremmede stater bruger i deres påvirkningskampagner. Fremmede stater laver også påvirkningsaktiviteter, der ikke involverer cyberangreb.

Truslen fra påvirkning med brug af cyberangreb har ligheder med truslen fra cyberaktivisme, da mange af de samme angrebsmetoder går igen. Truslen fra cyberaktivisme og påvirkning med brug af cyberangreb kommer dog fra trusselsaktører med forskellige kapaciteter, henholdsvis individer og ikke-statslige hackergrupper på den ene side og fremmede stater på den anden. De adskiller sig også ved, at cyberaktivister udfører angreb for at tiltrække sig så meget opmærksomhed som muligt, mens stater udfører den samme type angreb for at påvirke holdninger og adfærd i det skjulte.

Truslen fra cyberaktivisme er hævet til HØJ, mens de øvrige trusselsniveauer er uændrede
CFCS vurderer, at Danmark fortsat står over for en **MEGET HØJ** trussel fra cyberspionage og cyberkriminalitet. CFCS har hævet truslen fra cyberaktivisme fra **MIDDEL** til **HØJ**, bl.a. på baggrund af et øget antal pro-russiske cyberaktivistiske angreb mod mål i europæiske NATO-lande, herunder også i Danmark. Derudover er danske myndigheder og virksomheder også udsat for en **LAV** trussel fra destruktive cyberangreb. Truslen fra cyberterror er fortsat **INGEN**.

Et **MEGET HØJT** trusselsniveau betyder, at det er meget sandsynligt, at cyberangreb vil finde sted. CFCS sætter trusselsniveauer ud fra en vurdering af trusselsaktørers kapacitet og vilje til at udføre cyberangreb for at opnå forskellige formål. Ved en **LAV** trussel er det mindre sandsynligt, at cyberangreb vil blive udført, men ikke usandsynligt. En **LAV** trussel er altså ikke et fravær af truslen. Det er særligt vigtigt at understrege i forhold til truslen fra destruktive cyberangreb, hvor CFCS vurderer, at der er stor kapacitet, men begrænset hensigt. Her skal der kun en ændring i hensigten til at ændre trusselsniveauet, hvilket derfor kan ske med kort eller uden varsel. Det er netop en ændring i CFCS' vurdering af cyberaktivisters hensigt til at udføre cyberangreb mod Danmark, der har medført, at truslen er blevet hævet. Cyberaktivisters kapacitet til at udføre cyberangreb mod Danmark var allerede til stede.

Trusler med samme trusselsniveau kan have meget forskellige konsekvenser
Trusselsniveauer giver et godt overblik over, hvor sandsynligt det er, at danske virksomheder og myndigheder vil blive ramt af forsøg på cyberangreb. Trusselsniveauerne siger til gengæld ikke noget om, hvor sandsynligt det er, at angreb vil lykkes, eller hvilke konsekvenser det vil have, hvis en cybertrussel resulterer i succesfulde cyberangreb.

Eksempelvis er der stor forskel på, hvilke konsekvenser succesfulde aktivistiske og destruktive cyberangreb vil have. Truslen fra destruktive cyberangreb er **LAV**, men destruktive cyberangreb kan, hvis de finder sted, få meget alvorlige konsekvenser, i værste fald i form af død eller personskade og afbrydelse af samfundsvigtige funktioner. Til sammenligning er truslen fra cyberaktivisme **HØJ**, men aktivistiske cyberangreb vil ofte kun påvirke en organisations omdømme eller skabe kortvarige afbrydelser af tilgængeligheden af f.eks. hjemmesider

CFCS bruger Forsvarets Efterretningstjenestes trussels- og sandsynlighedsniveauer, der er beskrevet til sidst i vurderingen. CFCS beskriver i denne vurdering truslen på kort sigt, hvilket svarer til en tidshorisont på 0-2 år.

God læselyst!

Cyberspionage

Truslen fra cyberspionage mod Danmark er fortsat **MEGET HØJ**. Det betyder, at det er meget sandsynligt at danske myndigheder og virksomheder vil blive udsat for cyberspionage inden for de næste to år. Truslen er særligt rettet mod Udenrigs- og Forsvarsministeriets myndighedsområde, men også mod myndigheder og virksomheder i andre samfundsvigtige sektorer. Truslen fra cyberspionage er vedvarende og fører løbende til cyberangreb mod danske mål. Nogle myndigheder og virksomheder vil konstant være udsat for en alvorlig trussel, mens truslen kan variere over tid for andre.

Den alvorlige trussel fra cyberspionage skyldes, at fremmede stater, herunder især Rusland og Kina, har en særlig interesse for viden af udenrigs-, sikkerheds- og forsvarspolitisk karakter. Spionage mod disse områder kan eksempelvis give fremmede stater indblik i danske udenrigs- og sikkerhedspolitiske beslutninger samt militære kapaciteter og planer. I nogle tilfælde har den viden, der efterstræbes, betydning for Danmarks sikkerhed. Når stater stjæler den type viden, kan den blive brugt til eksempelvis at svække Danmarks udenrigspolitiske indflydelse. Cyberspionage kan derfor ikke blot betragtes som almindelige it-sikkerhedshændelser eller driftsproblemer.

CFCS vurderer, at Ruslands invasion af Ukraine ikke har medført en ændring i truslen fra cyberspionage mod Danmark, der allerede var **MEGET HØJ** før invasionen. Det er meget sandsynligt, at Rusland efter invasionen af Ukraine forsat vil have det samme fokus på at udføre cyberspionage mod myndigheder og organisationer i Danmark, der har betydning for dansk udenrigs-, sikkerheds- og forsvarspolitik, som før invasionen.

Truslen fra cyberspionage er især rettet mod forsvars- og udenrigspolitiske mål
Cyberspionage er politisk og økonomisk motiveret. Dele af det danske samfund er udsat for en vedvarende, aktiv og alvorlig trussel. Det gælder særligt Udenrigs- og Forsvarsministeriets myndighedsområde. Myndigheder og virksomheder med en tilknytning til disse myndighedsområder bliver løbende udsat for forsøg på cyberspionage.

Der har igennem en årrække også været en meget høj trussel fra cyberspionage mod myndigheder og virksomheder i søfarts-, og energisektoren samt forsvarsindustrien. Her kan fremmede stater bl.a. være interesserede i bestemte virksomheder, teknologier eller specifik viden. Fremmede stater, herunder Kina, er eksempelvis typisk interesseret i udstyr og teknologi, der både kan bruges civilt og militært. Der har i de seneste år også været en øget trussel mod både transport og forskning.

Truslen fra cyberspionage hænger bl.a. sammen med de udenrigspolitiske udfordringer, som Danmark står over for. Ruslands og Kinas ambitioner i Danmarks nærområde og Arktis er nogle af motiverne bag forsøg på cyberspionage fra landene mod danske myndigheder og organisationer, der beskæftiger sig med disse områder. Danmark indgår desuden i flere udenrigs- og sikkerhedspolitiske sammenhænge, herunder EU og NATO, der også har Kina og Ruslands interesse.

Andre dele af samfundet er udsat for en mere omskiftelig trussel
Truslen fra cyberspionage er også rettet mod andre dele af samfundet. Her varierer truslen fra cyberspionage i højere grad over tid og følger generelt skiftende fokus i fremmede staters efterretningsarbejde.

CFCS hævede i 2021 niveauerne for truslen fra cyberspionage fra **HØJ** til **MEGET HØJ** for både transportsektoren og danske universiteter og forskning.

Den øgede trussel mod universiteter og forskning kommer fra flere fremmede stater, der udfører cyberspionage mod forskning verden over. CFCS har i de senere år set flere forsøg på cyberangreb rettet mod danske universiteter og forskningsinstitutioner. Fremmede stater har forskellige formål med at udføre cyberspionage mod forskningsinstitutioner og universiteter. Cyberspionage er i nogle tilfælde drevet af en interesse for at opnå konkurrencemæssige og strategiske fordele ved at stjæle sensitiv eller værdifuld viden. Nogle fremmede stater spionerer sandsynligvis også for at fremskynde national forskning og udvikling af samfundsmæssige ydelser, såsom bedre kritisk infrastruktur. Det er sandsynligt, at fremmede stater også forsøger at udføre cyberspionage mod universiteter og tænketanke for at få indblik i forskningsbaserede bidrag til aktuelle udenrigs- og sikkerhedspolitiske problemstillinger.

Den øgede trussel mod transportsektoren kan være motiveret af sikkerhedspolitiske interesser. I det omfang at dele af transportsektoren støtter dansk forsvar eller andre landes militær, kan det have fremmede staters interesse. Indhentning af information om transportsektoren, som er en del af dansk kritisk infrastruktur, kan også benyttes i forberedelsen af destruktive cyberangreb eller fysiske angreb rettet mod sektoren.

CFCS har i 2022 sænket trusselsniveauet for cyberspionage mod telesektoren fra **HØJ** til **MIDDEL** i forhold til den tidligere trusselvurdering fra 2019. Ændringen er sket på baggrund af en fornyet analyse, der viser, at selvom det er muligt, at fremmede stater planlægger cyberspionage mod telesektoren i Danmark, så er sektoren i Danmark sandsynligvis ikke et højt prioriteret angrebsmål.

Cyberspionage rammer også mere vilkårlige ofre. Det skyldes, at stater også udfører opportunistiske cyberangreb. Det kan bl.a. ske i forbindelse med offentliggørelsen af sårbarheder eller ved supply-chain angreb, hvor fremmede stater kompromitterer mange organisationer inden for kort tid. Efter den første kompromittering kan staterne derefter tage stilling til, hvilke adgange, data eller konti der er interessante at arbejde videre med.

0-dags sårbarheder i Exchange servere udnyttet bredt

Den 2. marts 2021 udgav Microsoft og det amerikanske firma Volexity en række rapporter og blogs, der beskrev en cyberkampagne mod Microsoft Exchange servere ved hjælp af flere 0-dags sårbarheder. I juli 2021 tilskrev bl.a. USA hackere tilknyttet den kinesiske stat for at stå bag nogle af angrebene mod Microsoft Exchange servere. I forbindelse med denne hændelse blev flere sektorer primært i USA kompromitteret, herunder forskning, uddannelse, tænketanke, NGO'er og forsvarsindustrien. Microsoft kalder hackergruppen HAFNIUM.

Truslen fra cyberspionage kommer især fra Rusland og Kina

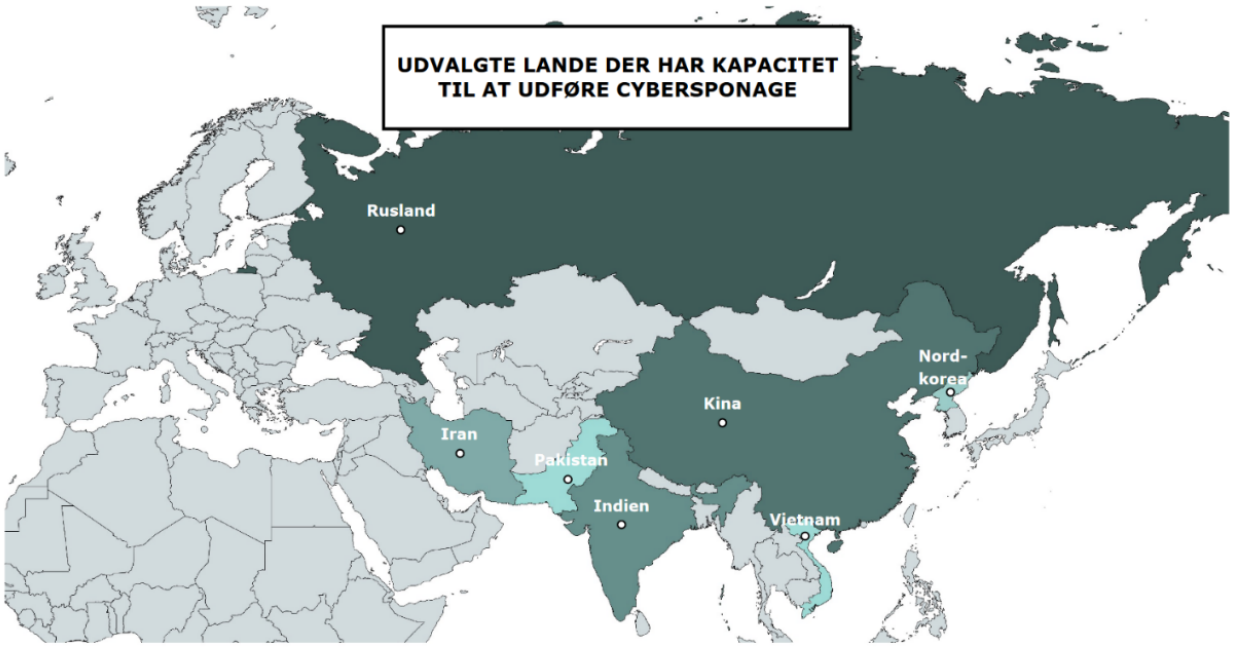
Truslen fra cyberspionage kommer især fra Rusland og Kina, der råder over betydelige kapaciteter til at udføre cyberspionage. Begge lande udgør en konstant trussel mod danske myndigheder og virksomheder.

Rusland har meget store cyberkapaciteter, som landet bruger systematisk til at understøtte sine nationale interesser. Cyberspionage kan også blive brugt til at forberede destruktive cyberangreb.

Kina udfører omfattende cyberspionage verden over, også mod danske myndigheder, virksomheder og organisationer. Kinas militær og efterretningstjenester har meget væsentlige kapaciteter og evner til at skaffe sig fuld og vedvarende adgang til organisationers informationer. Der er tale om en konstant og langsigtet aktivitet, der gavner Kinas sikkerheds- og udenrigspolitiske samt økonomiske og kommercielle interesser.

Samtidig prioriterer andre lande end Rusland og Kina også at udvikle deres cyberkapacitet. Det er meget sandsynligt, at flere stater i fremtiden vil udgøre en cybertrussel mod Danmark.

CFCS vurderer, at blandt andre Iran, Nordkorea, Vietnam, Pakistan og Indien også har kapacitet til at udføre cyberspionage. Det er sandsynligt, at disse stater generelt ikke har en særlig interesse i at ramme danske mål. Aktuelt bruger staterne primært deres kapaciteter mod lande i deres nærområde. Danske virksomheder og myndigheder, der er tilstede i eller omkring de lande, kan dog blive ramt af cyberspionage. Enten fordi kompromitterede mål, kan blive brugt som trædesten i videre cyberangreb, eller fordi staterne er interesserede i at få adgang til viden om f.eks. dansk udenrigs- og sikkerhedspolitik i regionen samt viden om det land eller den region, organisationen ligger i. Danske universiteter og forskningsinstitutioner, der har viden, samarbejdspartnere eller forskning, som er interessant for et eller flere af disse lande, er også udsat for truslen fra cyberspionage.



Kort over udvalgte lande med kapacitet til at udføre cyberspionage

Stater bruger flere metoder i forsøg på at udføre cyberspionage

Cyberspionage er typisk målrettet it-systemer og netværk, der indeholder information såsom mails og dokumenter, som har fremmede staters interesse. Fremmede staters muligheder for at få adgang til disse informationer varierer og er bl.a. afhængige af offerets it-systemer og angriberens evner og værktøjer. Fremmede stater bruger derfor flere forskellige angrebsmetoder.

Helt simple angreb kan eksempelvis være såkaldte brute force-angreb, hvor hackerne forsøger at trænge ind i it-netværk ved at afprøve et stort antal mulige brugernavne og passwords. Hackere opretter også falske hjemmesider, hvor ofrene bliver lokket til at indtaste deres brugernavne og kodeord. Derudover er det stadig meget udbredt, at hackere bruger phishing i deres forsøg på til at sprede malware.

Mere avancerede angreb kan ske gennem organisationernes leverandører. Det kan eksempelvis ske ved software supply chain-angreb, hvor aktører gemmer malware i ellers legitime opdateringer, som leverandører derefter distribuerer til deres kunder. Cyberspionage kan også blive rettet mod andre leverandører og samarbejdspartnere, der kan misbruges som trædesten i angreb mod de organisationer, staterne er interesserede i. Kompromitterede organisationer kan også blive brugt som ufrivillig infrastruktur i fremtidige angreb udført af hackerne.

Angrebene kan være rettet mod hele eller dele af netværk hos de organisationer, fremmede stater har interesse i. Der kan være tale om organisationernes samlede netværk, f.eks. et ministeriums it-systemer, eller netværk serviceret af en ekstern leverandør. I mindre skala kan der også være tale om angreb rettet mod specifikke computere og mailkonti.

Cyberangreb kan også blive udført ved at misbruge sårbarheder i it-systemerne, såsom fejl i hard- og software, manglende opdateringer eller fejlopsætninger. I nogle tilfælde betyder opdagelsen af sårbarheder i udbredte it-systemer, at en bred vifte af organisationer udgør mulige mål.

Fremmede stater gør – i lighed med andre typer hackere – ofte brug af de samme værktøjer og fremgangsmåder i angreb mod flere mål. Genbrug af metoder og værktøjer gør det muligt for angriberne at økonomisere med deres ressourcer og forsøge at ramme mange mål på én gang eller over længere tid. Rusland og Kina har kapacitet til samtidigt at udføre flere spionagekampagner mod mål verden rundt, bl.a. i Danmark. Genbrug af metoder og værktøjer gør det imidlertid også nemmere at identificere angrebene og overføre erfaringen fra tidligere angreb til beskyttelsen af andre potentielle mål.

Fremmede stater udfører brute force-angreb, også mod Danmark

Selvom fremmede stater, såsom Rusland og Kina, råder over avancerede cyberkapaciteter, bruger de også mere simple angrebsmetoder.

Britiske og amerikanske myndigheder offentliggjorde i sommeren 2021 en såkaldt Cyber-security Advisory, hvori de beskrev, hvordan den russiske militære efterretningstjeneste GRU fra 2019 til 2021 har stået bag en global brute force-kampagne. Brute forcekampagnen gjorde det muligt for GRU at få adgang til beskyttet information, bl.a. loginoplysninger og mails.

CFCS vurderer, at danske organisationer løbende bliver ramt af forsøg på cyberspionage ved brug af brute force-angreb udført af fremmede stater.

Cyberkriminalitet

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

CFCS bruger begrebet cyberkriminalitet som en fællesbetegnelse for handlinger, hvor hackere bruger cyberangreb til at begå kriminalitet, der er motiveret af økonomisk berigelse.

Danmark bliver løbende udsat for mange forskellige typer cyberkriminalitet, der – ligesom andre typer kriminalitet – generelt baserer sig på forskellige former for tyveri, bedrageri og afpresning.

Lige nu fylder afpresning gennem ransomware-angreb meget i trusselbilledet. Truslen fra cyberkriminalitet er dog dynamisk, og den vil sandsynligvis udvikle sig i fremtiden. Der er flere drivere, der skubber denne udvikling fremad, eksempelvis ændringer i brug af digitale tjenester, som kriminelle kan misbruge, og nye samarbejdsmuligheder for de kriminelle. Udviklingen vil sandsynligvis fortsat bevæge sig inden for spektret af tyveri, bedrageri og afpresning.

Ruslands invasion af Ukraine har skabt flere reaktioner internt i det kriminelle miljø, men CFCS vurderer, at invasionen ikke i væsentlig grad har påvirket truslen fra cyberkriminalitet mod Danmark.

Cyberkriminalitet rammer alle dele af det danske samfund
Der er tale om en meget aktiv trussel, som rammer alle dele af det danske samfund, og det vil den blive ved med på lang sigt. Kriminelle har generelt gode betingelser for at begå cyberkriminalitet. De har bl.a. gode muligheder for at arbejde anonymt samt samarbejde og dele værktøjer og teknikker via internettet.

Det er meget sandsynligt, at næsten alle danske borgere og virksomheder vil blive udsat for forsøg på cyberkriminalitet. Det skyldes, at nogle typer cyberkriminalitet går efter at ramme så mange ofre som muligt, eksempelvis gennem phishing spredt til tusinder af modtagere i Danmark og andre lande. Andre typer cyberkriminalitet går mere målrettet efter myndigheder og virksomheder, hvor udbyttet fra det enkelte offer kan løbe op i millioner af kroner.

Danmark står samlet set over for en international kriminel milliardindustri, der løbende tiltrækker nye hackere, som udgør en vedvarende trussel mod Danmark.

Ransomware-angreb kan have alvorlige konsekvenser
Afpresning gennem ransomware-angreb er aktuelt den mest synlige og alvorlige trussel fra cyberkriminalitet mod det danske samfund. Her krypterer kriminelle centrale it-systemer hos myndigheder og virksomheder for derefter at afpresse ofrene en løsesum mod at låse systemerne op igen. Ofrene bliver også ofte truet med offentliggørelse af stjålet data, hvis løsesummen ikke betales. Målrettede ransomware-angreb mod myndigheder og virksomheder har været en fast del af trusselsbilledet i Danmark i de seneste par år.

I 2021 er flere virksomheder på tværs af samfundet i Danmark blevet ramt af ransomware-angreb. Eksempelvis har kriminelle hackere angrebet Kalundborg Forsyning, vindmølleproducenten Vestas, it-virksomheden AK Techotel og nordens største hotelkæde, Nordic Choice Hotels, der også har hoteller i Danmark.

Ransomware-angreb kan ikke kun gøre stor skade på ramte myndigheder og virksomheder, men kan også have alvorlige konsekvenser for samfundsvigtige funktioner.

I maj 2021 blev det amerikanske olieselskab Colonial Pipeline eksempelvis udsat for et ransomware-angreb. Angrebet medførte, at Colonial Pipeline i seks dage måtte holde virksomhedens rørledninger lukket, mens køerne ved tankstationer langs den amerikanske østkyst voksede. Angrebet illustrerede, hvordan ransomware-angreb kan true kritiske forsyningskæder.

Flere faktorer underbygger den aktuelle trussel fra ransomware
Hackerne bag ransomware-angreb er velorganiserede og arbejder ud fra velafprøvede måder at udføre cyberangreb på. Samtidig er ransomware-angreb i dag en så profitabel kriminel aktivitet, at det brødføder et stort og højt specialiseret økosystem af kriminelle hackere. Det betyder generelt, at hackerne kan udføre flere og mere effektive ransomware-angreb.

Hackerne har udviklet profitable forretningsmodeller, eksempelvis såkaldte Ransomware-as-a-Service-platforme, hvor bagmænd står for udviklingen og serviceringen af specifikke ransomware og deres infrastruktur, som de stiller til rådighed for andre hackere mod en andel af profitten fra løsesummer. De servicerede platforme betyder bl.a., at barren, for hvem der kan lave ransomware-angreb, er blevet sænket, så flere kriminelle kan udføre disse angreb.

Kriminelle hackere har hidtil vist sig modstandsdygtige over for eksternt pres og ændrede betingelser. Indgreb fra myndigheder og it-sikkerhedsfirmaer, afhængigheden af online markeder og tjenester fra andre hackere samt hyppige opbrud internt i det kriminelle miljø skaber kontinuerligt væsentlige udfordringer for hackerne. Hackerne er dog generelt i stand til at tilpasse sig ved eksempelvis at lancere nye ransomwarevarianter og udvikle deres måder at samarbejde på.

Kriminelle hackere bruger en bred vifte af metoder til at begå berigelses-kriminalitet

Ransomware-angreb er kun én måde, kriminelle hackere begår cyberkriminalitet på. Kriminelle hackere forsøger eksempelvis også at bruge cyberangreb til at stjæle finansielle og personlige oplysninger, som de selv kan misbruge eller sælge videre til andre kriminelle.

Tyveri, misbrug og videresalg af kreditkortoplysninger har gennem mange år været en fast del af det kriminelle hackermiljø med digitale markeder på det mørke net.

For at modvirke truslen har den finansielle sektor i bl.a. Danmark styrket beskyttelsen mod misbrug gennem eksempelvis flerfaktorbeskyttelse af transaktioner. På trods af dette er der stadig et meget stort marked for videresalg af kreditkortoplysninger på det mørke net.

Der er flere måder, hackerne kan stjæle disse oplysninger på, bl.a. gennem kompromitteringer af virksomheder, der har finansielle oplysninger fra deres kunder, gennem kompromitteringer af betalingssystemer eller hjemmesider, hvor der er online betaling, eller ved at ramme mere eller mindre tilfældige ofre gennem eksempelvis phishing.

Kriminelle hackere går også efter nyere typer af digitale værdier, eksempelvis kryptovalutaer og virtuelle værdier knyttet til online spil.

Mens afpresning og tyveri er meget udbredte metoder for kriminelle hackere at berige sig på, er der fortsat også hackere, der specialiserer sig i bedrageri. Blandt andet i form af såkaldte Business Email Compromise (BEC), hvor kriminelle typisk hacker ledende medarbejdere i en virksomhed eller myndighed for derefter at udgive sig for at være den ledende medarbejder og bede om overførsler af penge til hackernes egne konti.

Med de meget forskellige typer cyberkriminalitet bruger kriminelle hackere en tilsvarende bred vifte af angrebsmetoder. For at hacke deres ofre spreder kriminelle eksempelvis malware gennem phishing eller misbruger kendte sårbarheder og lækkede brugernavne og passwords. Når cyberkriminelle har kompromitteret et offer, vil de i nogle tilfælde sælge denne kompromittering videre til andre kriminelle eller selv installere yderligere værktøjer og malware for at få bred adgang til offerets netværk.

Hackerne tilpasser sig og nyder godt af et robust og anonymiseret miljø

Der er i dag et veludviklet cyberkriminelt miljø, der er i stand til at tiltrække nye hackere og tilbyde forskellige muligheder for samarbejde, arbejdsdeling og specialisering. Disse gunstige betingelser for cyberkriminalitet vil sandsynligvis fortsat være til stede i de kommende år. Det er med til at fastholde den meget høje trussel fra cyberkriminalitet.

Hackerne har generelt gavn af et miljø præget af anonymitet og fortrolighed. De bliver bl.a. hjulpet af teknologier som kryptovalutaer, anonymiseringstjenester som TOR-netværket og VPN-tjenester samt hackerfora og markedspladser på det mørke net. Den anonymiserede og netværksbaserede måde at samarbejde på gør miljøet robust mod indgreb fra myndigheder. Bliver et netværk slået ned, kan det hurtigt blive overtaget af andre eller nye netværk kan opstå.

Anonymiteten, der beskytter hackerne, betyder dog også, at det er relativt nemt for hackerne at snyde hinanden. Hackerne forsøger derfor at skabe tillid ved at opbygge et positivt omdømme. Nogle grupper deponerer millionbeløb hos mellemmænd på hackerforaerne som synlig garanti til deres samarbejdspartnere. Nogle grupper, typisk de mere veletablerede, har dannet længerevarende relationer med udvalgte samarbejdspartnere.

Afhængigheden af bestemte teknologier og tjenester kan gøre de kriminelle sårbare over for indgreb mod eksempelvis kryptovalutaer og hackerfora. Udviklingen i bl.a. målrettede ransomware-angreb har dog vist, at de kriminelle hackere generelt er hurtige til at tilpasse sig nye forhold. Nye måder at angribe og afpresse på såvel som nye måder at organisere sig bliver relativt hurtigt kopieret og udbredt i miljøet.

Da amerikanske myndigheder lagde pres på bestemte hackergrupper efter angrebet på bl.a. Colonial Pipeline i 2021, var flere hackere eksempelvis hurtige til at flytte deres aktiviteter over på andre ransomware-platforme.

Ruslands invasion af Ukraine har ikke i væsentlig grad ændret truslen fra cyberkriminalitet

Der har været flere reaktioner fra kriminelle hackere på Ruslands invasion af Ukraine. Især Rusland er hjemland for flere kriminelle hackergrupper og netværk.

Hackere bag ransomwaren Conti har eksempelvis truet med gengældelse, hvis Vesten angriber kritisk infrastruktur i Rusland eller russisktalende lande. CFCS vurderer dog, at Conti-gruppen på trods af udtalelserne forsat hovedsageligt er finansielt motiveret.

Hackerne bag Conti-gruppen blev efter udtalelserne udsat for læk, der eksponerede flere af gruppens medlemmer og værktøjer. Flere konkurrerende ransomware-grupper har meddelt, at de er apolitiske og henviser til, at deres netværk består af hackere i bl.a. Rusland og Ukraine. Der er også kriminelle hackerfora, der har forbudt diskussioner om krigen eller udelukket russiske hackere.

På trods af fra Conti-gruppens udtalelser kender CFCS endnu ikke til eksempler, hvor veletablerede kriminelle hackergrupper har givet afkald på deres muligheder for profit ved at lave destruktive angreb. Organiserede kriminelle hackere lever af deres indtægter fra cyberkriminalitet og indgår i integrerede kriminelle forsynings- og værdikæder, hvor udbyttet fra bl.a. ransomware bliver fordelt mellem mange aktører. Hvis kriminelle hackere bruger disse kapaciteter på at lave destruktive angreb, vil det som udgangspunkt være et brud på værdikæden. Det kan skade deres muligheder for at indgå i et fremtidigt samarbejde med andre kriminelle, der har fokus på profit.

Ruslands invasion af Ukraine har derfor ikke i væsentlig grad ændret truslen fra cyberkriminalitet mod Danmark.

Cyberaktivisme

OPDATERET FEBRUAR 2023

Truslen fra cyberaktivisme mod Danmark er **HØJ**. CFCS hævede d. 31. januar 2023 trusselsniveauet fra **MIDDEL** til **HØJ**, bl.a. på baggrund pro-russiske aktivistiske hackergruppers høje aktivitetsniveau mod NATO-lande, herunder Danmark, samt deres mere formaliserede angrebsmodus og øgede kapacitet.

Når trusselsniveauet fra cyberaktivisme er **HØJ**, betyder det, at det er sandsynligt, at danske virksomheder og myndigheder vil blive ramt af aktivistiske cyberangreb på kort sigt.

Den resterende del af kapitlet er ikke ændret.

Cyberaktivisme udføres af individer og hackergrupper, der udfører cyberangreb for at få mest mulig opmærksomhed til deres dagsorden eller for at straffe organisationer. Cyberaktivisme er typisk drevet af forskellige ideologiske eller politiske motiver, der strækker sig fra politiske enkeltsager til modstand mod magthavere. Cyberaktivister angriber både ofre, de ser som symbolske mål, og modstandere af deres sag.

Cyberaktivister er i stand til at udføre forskellige typer cyberangreb, fra simple overbelastningsangreb og defacement-angreb til mere ressourcekrævende hack og læk-operationer.

Krigen i Ukraine presser trusselsniveauet op
Særligt Ruslands invasion af Ukraine har medført en øget aktivitet i de cyberaktivistiske miljøer.

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

De pro-russiske cyberaktivistiske gruppers forhøjede aktivitetsniveau øger også truslen for cyberaktivistiske angreb mod Danmark.

Pro-russiske Killnet står bag cyberangreb
Den pro-russiske hackergruppe Killnet hævder at stå bag en række cyber-aktivistiske angreb i forbindelse med krigen i Ukraine. Killnet har f.eks. udført DDoS-angreb mod myndighedshjemmesider, banker og TV-stationer i flere europæiske lande.

Selvom truslen mod Danmark hæves på baggrund af pro-russiske aktiviteter, udgør aktører på begge sider af konflikten dog en trussel for aktivistisk motiverede cyberangreb mod Danmark. Pro-russiske aktivister kan være interesserede i at straffe

eller påvirke dansk støtte til Ukraine, mens pro-ukrainske aktivister kan være interesserede i enten at straffe organisationer med tilknytning til Rusland eller angribe mål i lande, som de mener ikke gør nok for at støtte Ukraine.
Truslen gælder dermed også for danske organisationer eller personer med relationer til Ukraine, der kan blive ramt af angreb rettet mod mål i Ukraine. Danske ofre kan f.eks. få lækket følsomme oplysninger i forbindelse med hack og læk-angreb rettet mod organisationer i Ukraine.

Truslen fra danske cyberaktvistiske miljøer er fortsat meget begrænset
Aktivistiske cyberangreb kommer yderst sjældent fra Danmark, og der er generelt kun få eksempler på, at konventionel aktivisme og protester i Danmark har ført til cyberangreb. Indenfor de seneste år har uenigheder om sociale eller politiske emner i Danmark ikke medført cyberaktivistiske angreb mod danske mål. Eksempelvis afholdt protestbevægelsen "Men in Black" flere demonstrationer i Danmark i 2021, men deres aktiviteter inkluderede ikke aktivistiske cyberangreb.

Destruktive cyberangreb

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

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
Det er mindre sandsynligt, at fremmede stater aktuelt har intentioner om at udføre destruktive cyberangreb mod Danmark. Stater udvikler dog løbende deres kapaciteter til at kunne udføre destruktive cyberangreb med kort varsel.

Selvom det er mindre sandsynligt, at fremmede stater har intentioner om at udføre destruktive cyberangreb, kan det få alvorlige konsekvenser, hvis intentionen ændrer sig, og stater udfører succesfulde destruktive cyberangreb.

Krigen i Ukraine har understreget, at destruktive cyberangreb hovedsageligt bliver brugt af stater i forbindelse med konflikter. Flere stater, herunder Rusland, har kapacitet til at udføre den type angreb. Det betyder, at truslen mod Danmark kan stige med kort eller uden varsel, hvis den sikkerhedspolitiske situation, eksempelvis som følge af krigen mellem Rusland og Ukraine, eskalerer i retning af en militær konfrontation mellem Rusland og NATO.

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 i 2017 rettet mod Ukraine, der bredte sig og ramte ofre verden over i 2017.

Destruktive cyberangreb kan have meget alvorlige konsekvenser
Selvom truslen fra destruktive cyberangreb aktuelt er **LAV**, er der tale om en væsentlig trussel mod Danmark, da destruktive cyberangreb kan have meget alvorlige konsekvenser.

Konsekvenser af et angreb kan eksempelvis være, at adgangen til samfundsvigtige funktioner og ydelser, såsom strøm, transport eller internet bliver afbrudt eller forstyrret. Et destruktivt cyberangreb kan også medføre omfattende ødelæggelse af data og enheder.

Destruktive cyberangreb kan tjene andre formål end "blot" at ødelægge et specifikt mål. Et motiv for destruktive cyberangreb kan eksempelvis være at sende et politisk signal

til et offer, potentielle ofre eller et land. Destruktive cyberangreb kan også have et militært sigte. Militært kan destruktive cyberangreb eksempelvis bidrage til at begrænse Forsvarets evne til at kommunikere og manøvrere. Det er ofte vanskeligt at vurdere præcis, hvilken hensigt der ligger bag et destruktivt cyberangreb, og angreb kan også tjene flere formål.

Destruktive cyberangreb i Ukraine i 2022

Flere åbne kilder har løbende rapporteret om destruktive cyberangreb, der har ramt Ukraine op til og under krigen. Listen er ikke udtømmende:

- **WhisperGate/WhisperKill** – Wiper-angreb mod ukrainske myndigheder mv. i januar 2022
- **AcidRain** – Udbyderen af satellitkommunikation Viasat blev dagen før den russiske invasion udsat for et destruktivt cyberangreb. Angrebet vanskeliggjorde ukrainsk militærs kommunikation, da tusindvis af satellitmodemmer særligt i Europa fik slettet sin opsætning.
- **HermeticWiper** – Dette angreb blev iværksat dagen før den russiske invasion mod ukrainske myndigheder, it-virksomheder og samfundskritiske sektorer
- **CaddyWiper** – I marts 2022 blev en ny wiper-malware opdaget i Ukraine. Denne wiper er en lille og simpel malware, og det er endnu uklart hvilke ofre i Ukraine, der har været ramt.

Destruktive cyberangreb bliver hovedsageligt brugt i konfliktområder

Indtil Ruslands invasion af Ukraine i februar 2022 har der de senere år ikke været mange eksempler på cyberangreb, som svarer til CFCS' definition på destruktive cyberangreb. De relativt få eksempler, der har været, er blevet udført i områder præget af politiske spændinger og konflikt som Mellemøsten og Ukraine.

I konfliktområder kan truslen fra destruktive cyberangreb derfor være højere. Det er muligt, at danske virksomheder og myndigheder, der er til stede i særligt i Ukraine og Mellemøsten, vil blive ramt af destruktive cyberangreb eller følgevirkninger deraf, såsom strømafbrydelser og manglende internetadgang.

Ukraine er op til og siden invasionen i 2022 blevet ramt af flere forskellige typer af destruktive angreb lige fra meget simple wiper-angreb til mere avancerede angreb mod satellitkommunikation.

Størstedelen af de destruktive angreb, som har ramt Ukraine i krigens første måneder, har været afgrænsede og har ikke spredt sig ud over landets grænser. Det var dog ikke tilfældet med cyberangrebet mod Viasat, en amerikansk udbyder af satellit-kommunikation. Selvom målet for angrebet sandsynligvis var ukrainsk militær kommunikation, fik det følgevirkninger langt ud over dette.

Angrebet mod Viasat viser, at virksomheder, der enten er fysisk til stede i eller på anden vis er knyttet til Ukraine, kan blive ramt af destruktive cyberangreb. Det skyldes, at konsekvenserne af disse angreb spreder sig til virksomhedens kunder på tværs af landegrænser. Den samme risiko gælder for angreb, hvor der benyttes malware, der spreder sig på tværs af enheder og maskiner.

Viasat blev ramt i et destruktivt cyberangreb, der havde konsekvenser udover Ukraines grænser

Stater udvikler løbende deres kapacitet til at udføre destruktive cyberangreb
Stater udvikler løbende deres kapaciteter til at kunne udføre destruktive cyberangreb med kort varsel. Stater bruger bl.a. cyberspionage til at forberede destruktive cyberangreb, der f.eks. vil kunne iværksættes i tilfælde af en eskalerende krise eller krig.

Cyberspionage kan give adgang til kritisk infrastruktur, som stater kan forsøge at ødelægge eller forstyrre i en alvorlig krise eller krig. Ukrainske myndigheder afværgede eksempelvis i april 2022 et russisk destruktivt cyberangreb, der havde til formål at skabe strømafbrydelser i dele af Ukraine. Flere it-sikkerhedsfirmaer har forbundet angrebet med russiske hackere, der ifølge it-sikkerhedsfirmaerne også tidligere har rettet deres malware mod industrielle kontrolsystemer i den ukrainske energisektor.

Forberedelsen af destruktive cyberangreb vil ofte bestå i en kortlægning af organisationer, systemer og netværksenheder, f.eks. industrielle kontrolsystemer. 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.

Amerikanske myndigheder udsendte i marts 2022 en advarsel om, at russiske hackere, der tidligere har benyttet malwaren Triton, stadig aktivt søger at kompromittere virksomheder i energisektorer verden over. Triton er en destruktiv malware, som påvirker sikkerhedsmekanismer i industrielle kontrolsystemer, og som derfor potentielt kan påvirke fysiske processer i eksempelvis energiproduktion. Statsstøttede hackergrupper har i mange år udvist en interesse for energisektoren, også i Danmark.

Cyberterror

Truslen fra cyberterror mod Danmark er **INGEN**. Det betyder, at det er usandsynligt at danske myndigheder og virksomheder, 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.

CFCS vurderer, at militante ekstremister har begrænset hensigt til at udføre cyberangreb, der har samme effekt som konventionel terror, samt at de ikke har den fornødne kapacitet.

Selvom der er en alvorlig trussel fra konventionel terror, og militante ekstremister i årevis har udnyttet internettet til at understøtte deres eksistens, planlægge konventionel terror og udføre simple aktivistiske cyberangreb som DDoS-angreb og defacement, har der endnu ikke været nogen eksempler på, at terrorister har udført cyberangreb med en effekt, der svarer til konventionel terror.

Påvirkning med brug af cyberangreb

Påvirkning med brug af cyberangreb dækker i denne trusselsvurdering over fremmede staters cyberangreb, der bliver udført med det formål at påvirke meningsdannelsen.

Fremmede staters brug af cyberangreb til påvirkning er blot ét af flere midler, der bliver brugt til at påvirke holdninger og adfærd i andre lande. Samlet set foregår påvirkning både online og offline, i det åbne og i det skjulte. CFCS vurderer ikke staters øvrige påvirkningsaktiviteter gennem internettet.

Ghostwriter – en bred vifte af påvirkningsaktiviteter
En af de mest omfattende påvirkningskampagner inden for de seneste år har fået tilnavnet Ghostwriter. Ghostwriter dækker over en række påvirkningsaktiviteter, der bl.a. er blevet rettet mod mål i Litauen, Letland, Polen og Tyskland. Aktørerne bag Ghostwriter har bl.a. brugt cyberangreb, f.eks. til at kompromittere hjemmesider og konti på sociale medier, for efterfølgende at bruge dem til at dele manipuleret eller fabrikeret information. CFCS vurderer, at statsstøttede hackere står bag dele af Ghostwriter-aktiviteterne.

Påvirkning med brug af cyberangreb udgør en indirekte trussel mod Danmark
Fremmede stater, herunder Rusland, bruger aktivt cyberangreb i deres forsøg på at påvirke holdninger og adfærd i andre lande. Eksempelvis er det meget sandsynligt, at Rusland har brugt cyberangreb til at lave påvirkning mod Ukraine i forbindelse med Ruslands invasion af landet.

CFCS vurderer, at Danmark aktuelt ikke udgør et prioriteret påvirkningsmål for stater, der har kapacitet til at udføre påvirkning gennem cyberangreb.

Et af de mest kendte eksempler på påvirkning med brug af cyberangreb er hack og læk-angrebet mod Demokraternes Nationale Komité (DNC), der blev udført i forbindelse med det amerikanske præsidentvalg i 2016. Amerikanske myndigheder anklagede Rusland for at stå bag angrebet.

Danmark er ikke direkte blevet udsat for den type angreb, men påvirkning med brug af cyberangreb udgør en indirekte trussel mod Danmark. Det skyldes, at cyberangreb, der udføres med det formål at undergrave tilliden til demokratiske værdier og svække sammenhængskraften i allierede lande og internationale organisationer af betydning for Danmark, såsom NATO, potentielt kan få langsigtede politiske konsekvenser, også for Danmark.

Danske organisationer eller personer med relationer til lande, hvor der er et højt antal forsøg på påvirkning med brug af cyberangreb, særligt de baltiske lande, Polen og Ukraine, kan også blive ramt af angreb rettet mod mål i disse lande.

Det er sandsynligt, at cyberangreb løbende bliver udført bl.a. for at svække sammenhængskraften i NATO. Der er flere eksempler på angreb mod de baltiske lande, der har haft til formål at underminere opbakningen til NATO's tilstedeværelse i regionen.

Ukraine er også blevet ramt af en række cyberangreb, der sandsynligvis har haft til formål at påvirke og presse den ukrainske befolkning i forbindelse med Ruslands invasion af landet med angrebsmetoder, der ligner dem, cyberaktivister ofte bruger.

Eksempelvis er flere ukrainske regeringshjemmesider blevet udsat for defacement-angreb flere gange i løbet af 2022, både før og efter invasionen. Den 14. januar 2022 blev op imod 70 ukrainske regeringshjemmesider lagt ned i et omfattende defacement-angreb. Angrebet ramte Ukraines Udenrigs- og Energiministerium, ministerkabinet og den nationale beredskabsstyrelse. Defacement-angrebet erstattede det originale indhold på siderne med en tekst på ukrainsk, russisk og polsk, hvoraf det fremgik, at ukrainske borgeres personfølsomme data ville blive offentliggjort, samt en advarsel om at forberede sig på det værste.

Inden for de seneste år har de fleste tilfælde af påvirkning med cyberangreb i Europa, som CFCS har kendskab til, været rettet mod mål i Ukraine, Polen og de baltiske lande. Formålet med disse angreb har oftest været at afspore eller aflede den offentlige debat for derved at fremme polarisering i de ramte samfund.

Fremmede stater har i flere tilfælde udgivet sig for at være cyberaktivister, formentlig som et forsøg på at skjule at de står bag påvirkningsaktiviteter. I populær tale kaldes det for faketivisme. Formålet med faketivisme er det samme som ved staters øvrige påvirkning ved brug af cyberangreb.

Skærmbilledet set ved defacement-angrebet mod op mod 70 ukrainske hjemmesider

Begrænset hensigt til at påvirke Danmark
Det er sandsynligt, at Danmark aktuelt ikke udgør et prioriteret påvirkningsmål for stater, der har kapacitet til at udføre påvirkning gennem cyberangreb.

Truslen fra påvirkningsangreb kommer fra statsstøttede hackere med betydelige kapaciteter. Rusland er en af de stater, der har avancerede cyberkapaciteter, som de bl.a. bruger til at udføre påvirkningscyberangreb. Viden indsamlet og opbygget gennem cyberspionage kan blive anvendt i forbindelse med eventuelle fremtidige påvirkningskampagner. Det kunne f.eks. ske i en eventuel fremtidig interessekonflikt i Arktis, hvor Danmark og Rigsfællesskabet får en mere fremtrædende rolle i en konflikt over for Rusland.

Påvirkning mod Rigsfællesskabet
Et eksempel på et påvirkningsforsøg mod Rigsfællesskabet er sagen om et falsk brev fra Grønlands daværende minister for udenrigsanliggender Ane Lone Bagger til den amerikanske senator Tom Cotton i november 2019. Brevet cirkulerede på internettet og omtalte bl.a. grønlandsk-amerikansk samarbejde, en fremtidig afstemning om grønlandsk selvstændighed og en specifik aftale om Grønlands status og amerikansk økonomisk støtte. Det er meget sandsynligt, at formålet var at skabe splid i Rigsfællesskabet og mistillid mellem Danmark og USA vedrørende USA's intentioner i Arktis.

Stater bruger meget andet end cyberangreb i påvirkningskampagner
Cyberangreb er blot en af flere typer aktiviteter, fremmede stater bruger i deres påvirkningskampagner. Fremmede stater laver også påvirkningsaktiviteter, der ikke involverer cyberangreb. For eksempel tilbyder statslige aktører borgere penge, rejser eller lignende for at hjælpe med at sprede misinformation. En anden måde, hvorpå statslige aktører kan påvirke meningsdannelsen, er at benytte sig af falske profiler og bots på sociale medier for at promovere særlige budskaber. Formålet med den metode er at skabe en illusion af folkelig opbakning eller foragt for bestemte mærkesager i overensstemmelse med den statslige aktørs udenrigspolitiske mål.

Task Force Påvirkning
I september 2017 nedsatte den daværende regering en task force bestående af Justitsministeriet (formand), Udenrigsministeriet, Forsvarsministeriet, Politiets Efterretningstjeneste og Forsvarets Efterretningstjeneste. Task forcens opgave er at koordinere den danske indsats mod statslige påvirkningskampagner og sikre, at myndighederne samlet agerer effektivt og velkoordineret.

Task Force Påvirkning definerer påvirkning mod Danmark som statslige aktørers åbne eller skjulte aktiviteter med henblik på at påvirke meningsdannelsen i Danmark og omverdenens syn på Danmark for at fremme egne interesser på bekostning af danske interesser. Det er dog vigtigt at tilføje, at påvirkning mod Danmarks allierede og mod internationale organisationer som NATO og EU også kan skade Danmarks interesser.

Udbredte cyberangrebsmetoder som bruges til påvirkning

Stater gør brug af en række forskellige typer cyberangreb i deres forsøg på at påvirke meningsdannelsen i andre lande. Nedenfor er nogle af de mest udbredte angrebsmetoder fremhævet.

Hack og læk

Hack og læk er blandt de mest udbredte typer cyberangreb, der bruges til påvirknings-aktiviteter. Der er forskellige typer hack og læk-angreb. I nogle tilfælde stjæler hackere følsom information fra deres offer og offentliggør den, enten uændret eller i en manipuleret version, med henblik på at skade offeret. Der er også eksempler på påvirkningsforsøg, hvor hackere har kompromitteret nyhedssider og indsat falske nyheder, for på den måde at sprede misinformation.

Misbrug af stjålne brugernavne og kodeord

Hackere udfører også angreb, hvor de forsøger at kompromittere brugernavne og kodeord til mailkonti og sociale medier. I forlængelse af dette har hackere i flere tilfælde videresendt falsk information via de kompromitterede konti. Kompromitteringen af brugernavne og kodeord kan også blive brugt i den første fase af hack og læk-angreb, hvor hackere forsøger at stjæle information.

Defacement

Defacement af en hjemmeside er et angreb, der ændrer hjemmesidens visuelle udtryk. For eksempel kan angriberen indsætte en tekst eller et billede på hjemmesidens forside.

Tendenser

I dette kapitel beskrives eksempler på tendenser og udvikling, som har eller forventes at få, en betydning for cybertruslen mod Danmark.

Den digitale koncentration har betydning for cybersikkerheden
It og internettet har fået stor betydning for, hvordan vores samfund fungerer, og internettets udvikling har stor betydning for både sikkerhed og tilgængelighed af de onlinetjenester, vi alle er blevet afhængige af. Dette afsnit skitserer udviklinger, som har betydning for cybertruslen, og de mulige konsekvenser af et cyberangreb mod en af de store virksomheder, der understøtter internettet.

Internettet domineres af færre, men større teknologi-virksomheder
Siden internettets spæde start i 1960'erne er der ikke kun sket en voldsom teknisk udvikling, men også en konsolidering, der betyder, at færre teknologi-virksomheder leverer og kontrollerer en stadig større del af internettets infrastruktur og den software, som bl.a. mange danske virksomheder og myndigheder er afhængige af.

En positiv side af udviklingen er, at de store leverandører af software, datacentre, cloud computing og internetinfrastruktur ofte hæver it-sikkerheden for de organisationer, der anvender tjenesterne. Det skyldes, at de store teknologi-virksomheder generelt bruger flere ressourcer og har større ekspertise end mindre organisationer, når det drejer sig om at overvåge og sikre deres infrastruktur og tjenester mod hackere.

Udviklingen betyder imidlertid også, at nedbrud eller cyberangreb rettet mod en af disse store leverandører eller enkelte af deres produkter kan ramme mange kunder verden over på samme tid. En sikkerhedshændelse hos en enkelt leverandør kan derfor have alvorlige konsekvenser, ikke blot for enkelte kunder og brugere af internettet, men potentielt for hele samfundet og i flere lande på én gang.

Den digitale koncentration giver hackere adgang til mange ofre på samme tid
Globaliseringen og den teknologiske udvikling har ført til, at relativt få leverandører dominerer det globale it-landskab. Udbredelsen af visse teknologier, som hurtigt bliver de dominerende inden for deres felt, skaber en selvforstærkende effekt, hvor en stadig større koncentration af teknologi og internettjenester samles hos få meget store virksomheder.

Eksempelvis benytter langt de fleste virksomheder i dag Microsoft Windows i deres administrative netværk. Det kan være en fordel, fordi en stor global leverandør har mulighed for at bruge mange ressourcer på at sikre sit produkt mod hackere. Imidlertid betyder den udbredte brug af Windows også, at hackerne kun behøver at udvikle metoder, malware og exploits, der er målrettet Windows, for at få adgang til et stort antal ofre på samme tid. Den sikkerhedsudfordring gælder ikke kun for egentlige softwareprodukter, men også for de mange funktioner, der indgår på tværs i softwareprodukter fra forskellige leverandører. Det var eksempelvis tilfældet, da en alvorlig sårbarhed i den såkaldte Log4j-kode blev fundet og udnyttet i november 2021.

Sårbarhed i Log4j-kode udnyttes mod ofre verden over

I november 2021 blev der fundet en alvorlig sårbarhed i Log4j-koden. Koden anvendes til at logge sikkerhedshændelser i applikationer og på hjemmesider.

Sårbarheden kan udnyttes til at eksekvere ondsindet kode på den enhed eller server, hvor Log4j-koden anvendes. Sårbarheden er let at udnytte. Samtidig indgår Log4j-koden i mange applikationer fra mange forskellige leverandører, og anvendes derfor på millioner af servere verden over. Hackere kan altså ramme mange sårbare servere verden over, ved hjælp af en enkelt angrebsmetode, der udnytter sårbarheden. Det har skabt et globalt kapløb mellem hackere, der forsøger at udnytte sårbarheden og organisationerne, der forsøger at fjerne sårbarheden.

Virksomheders produktion, mail og digitale kontorværktøjer er flyttet i skyen

80 procent af danske virksomheder med mere end 100 ansatte anvender cloud computing. Som eksempel leveres en virksomheds mail og digitale kontorværktøjer ofte fra én cloud-udbyder. Brugen af cloud giver en enkel og fleksibel løsning for mange organisationer, men betyder samtidig, at fejl på internettet kan gøre det svært at udføre sit arbejde. I Danmark er det oftest Microsoft, der leverer mail og digitale kontorværktøjer til virksomheder via skyen. Et nedbrud eller en fejl i Microsofts cloudløsning kan derfor påvirke en stor del af alle større danske virksomheder.

De dominerende udbydere af cloud computing i Europa er de amerikanske virksomheder Amazon, Microsoft og Google. De tre virksomheder tilsammen står for cirka to tredjedele af hele markedet for cloud-tjenester. Det betyder, at et antal internettjenester og produktionen i mange europæiske, herunder danske virksomheder, på samme tid kan blive afbrudt eller forstyrret af en teknisk fejl eller et cyberangreb, der rammer en af disse udbyderes cloud-infrastruktur. Konsekvensen kan være særlig alvorlig, hvis et nedbrud hos en cloud-leverandør påvirker virksomheder i en samfundsvigtig sektor.

Nedbrud hos Amazon påvirkede virksomheder verden over

Den 7. december 2021 medførte et nedbrud hos verdens største cloud-virksomhed, Amazon Web Services, at en række af verdens helt store internetbaserede virksomheder gik i sort. Nedbruddet ramte bl.a. store dele af Netflix, Disney+, Amazon.com, Amazon Prime samt en lang række andre tjenester.

Content Delivery Networks er blevet kritiske for internettets funktion

Tidligere blev data mellem en bruger og en internettjeneste overført direkte mellem brugerens computer og leverandørens webserver. I dag går 60-70 procent af al internettrafik via et såkaldt Content Delivery Network (CDN).

CDN-leverandører driver transmissionssystemer og servere verden over. De anvendes til at optimere svartider og hastighed på kunders internettjenester ved løbende at kopiere indholdet fra kundernes webservere, der typisk kun er placeret et sted i verden, til servere verden over, som er tættere på brugerne. Selvom der findes mange CDN-udbydere, så er det kun en håndfuld udbydere, der står for at håndtere langt den største del af CDN-datatrafikken. Disse udbydere er blevet særlig kritiske for internettets funktion.

Fejl hos CDN-udbydere afbrød internettjenester i bl.a. Danmark

Den 8. juni 2021 oplevede CDN-udbyderen Fastly et timelangt globalt nedbrud, som skyldtes en softwarefejl i udbyderens servere. Nedbruddet afbrød forbindelsen til internettjenester og hjemmesider verden over. I Danmark blev bl.a. TV2's hjemmeside ramt.

Den 22. juli 2021 udløste en softwareopdatering en fejl i DNS-systemet hos CDN-udbyderen Akamai. Fejlen betød, at virksomheden i en time ikke kunne sende internettrafik til flere af kundernes hjemmesider og internettjenester, herunder flere banker.

Kontrollen med adgang til hjemmesider er måske på vej til udlandet

Et sidste eksempel på internettets udvikling, der kan få stor betydning for sikkerheden, handler om den måske mest centrale funktion af internettet kaldet Domain Name System (DNS). DNS fungerer som internettets telefonbog ved at oversætte navnet på en hjemmeside til en IP-adresse, brugerens computer kan forbinde til. Uden DNS fungerer internettet ikke.

I dag er det typisk en brugers internetudbyder, der sørger for oversættelsen. Flere populære browsere, herunder Google Chrome, Microsoft Edge og Mozilla Firefox har imidlertid fået tilføjet en funktion, der kan kryptere DNS-trafik og sende den til en anden virksomhed f.eks. i udlandet.

For nuværende er de populære browsere kodet til, som standard i Danmark, at anvende internetudbyderens DNS-server. Det kan leverandøren af browseren dog vælge at ændre med en opdatering af den. I USA sender Mozilla Firefox som standard brugernes DNS-opslag til en server hos det amerikanske teknologivirksomhed Cloudflare.

Hvis DNS-opslag fremover sendes til servere, der kontrolleres af en virksomhed i udlandet, flytter det samtidig data og kontrollen med adgang til hjemmesider, herunder danske, til den udenlandske virksomhed. En konsekvens kan blive dårligere sikkerhed, fordi de blokeringer af eksempelvis kriminelle svindleres hjemmesider eller andet ulovligt eller skadeligt indhold på internettet, som danske myndigheder, via domstolene, pålægger danske internetudbydere at etablere, vil blive omgået. Det gælder også de blokeringer, der skete under coronapandemien, hvor kriminelle hackere forsøgte at udnytte krisen til at stjæle oplysninger og penge fra danske borgere.
En yderligere konsekvens kan blive, at eventuelle forstyrrelser pga. fejl eller hackere, på den udenlandske virksomheds DNS-tjeneste potentielt kan medføre, at mange brugere verden over mister adgangen til internettet.

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.