CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod Danmark 2023

1. udgave maj 2023

EFTERRETNINGSTJENESTERNES ÅRLIGE VURDERINGER AF TRUSLERNE MOD DANMARK

Cybertruslen mod Danmark beskriver og fastsætter de nationale trusselsniveauer for cyberspionage, cyberkriminalitet, cyberaktivisme, destruktive cyberangreb og cyberterror. Cybertruslen mod Danmark er en af fire årlige vurderinger af truslerne i og mod Danmark. De andre er:

- **UDSYN**, hvori FE beskriver de ydre vilkår for Danmarks sikkerhed og danske interesser.
- **Vurderingen af terrortruslen mod Danmark,** hvori Center for Terroranalyse (PET) fastsætter det nationale terrortrusselsniveau og beskriver terrortruslen mod Danmark og danske interesser i udlandet.
- **Vurderingen af spionagetruslen mod Danmark**, der udgives af PET og beskriver fremmede staters efterretningsvirksomhed mod Danmark, dvs. især spionage, påvirkning og forsøg på ulovligt at anskaffe teknologi og viden.

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave maj 2023

Cybertruslen mod Danmark 2023

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.

Hovedvurdering

- Truslen fra cyberspionage mod Danmark er **MEGET HØJ**. Truslen er koncentreret om udenrigs- og sikkerhedspolitiske forhold såsom Arktis, NATO og EU, selvom også kritisk infrastruktur er udsat for truslen.

- Cyberspionage kan underminere danske interesser, både politisk, økonomisk og sikkerhedsmæssigt. Det er sandsynligt, at fremmede stater benytter cyberspionage som forberedelse af destruktive cyberangreb.

- Truslen fra cyberkriminalitet mod Danmark er fortsat **MEGET HØJ**. Velorganiserede ransomware-grupper går efter alle dele af samfundet.

- CFCS vurderer, at langt de fleste cyberkriminelle fortsat er økonomisk motiverede, arbejder opportunistisk og er uafhængige af stater.

- Truslen fra cyberaktivisme mod Danmark er **HØJ**. Det er sandsynligt, at danske virksomheder og myndigheder vil blive ramt af aktivistiske cyberangreb på kort sigt. Pro-russiske cyberaktivister har et højt aktivitetsniveau mod NATO-lande, herunder Danmark, og har i stigende grad formaliseret deres angrebsmodus og forøget deres kapacitet.

- Truslen fra destruktive cyberangreb er **LAV**. Det er mindre sandsynligt, at fremmede stater på nuværende tidspunkt har til hensigt at udføre destruktive cyberangreb mod Danmark. CFCS vurderer dog, at hackergrupper tilknyttet fremmede stater forbereder sig for at kunne udføre destruktive angreb med kort varsel.

- Danske organisationer, der har aktiviteter i Ukraine eller leverer produkter og tjenester relateret til krigen i Ukraine, kan være udsat for en højere risiko for at blive ramt af et destruktivt cyberangreb eller følgevirkningerne af et angreb, der er rettet mod Ukraine.

- Truslen fra cyberterror er **INGEN.** Militante ekstremister har kun begrænset hensigt og ingen kapacitet til at udføre cyberangreb, der kan sidestilles med konventionel terror.

Indledning

Europa og verden står i en ny sikkerhedspolitisk situation som resultat af Ruslands invasion af Ukraine. Krigen ser ud til at blive langvarig og vil være central for udviklingen i forholdet mellem Rusland og Vesten og dermed også Danmark. Det er i det lys, at vi skal forstå det aktuelle trusselsbillede – også i det digitale domæne.

Trusselsbilledet udvikler sig hele tiden, og selvom de fleste cyberangreb stadig bliver udført uden sammenhæng til situationen i Ukraine, er det i dén ramme, mange nu forstår verden. Når strømmen forsvinder på Bornholm eller en anden kritisk funktion oplever et nedbrud, har befolkningen et behov for at få afklaret, om der er tale om et uheld eller en bevidst handling. I de tilfælde, hvor det kan konstateres, at der er tale om et cyberangreb, opstår der et nyt behov, nemlig for at forstå, hvem der står bag. Er der tale om grådige kriminelle, eller er det en fremmed stat, der har rettet sine cybervåben mod Danmark?

CFCS' trusselsvurderinger er opdelt i forskellige formålskategorier – cyberspionage, cyberkriminalitet, cyberaktivisme, destruktive cyberangreb og cyberterror. Vi forsøger altså at fastslå, hvorfor et givent angreb bliver udført. Ofte medfører det en forståelse af, hvilken type aktør der står bag. Vi vurderer eksempelvis, at cyberkriminalitet oftest bliver udført af individer eller grupper, der handler opportunistisk og er økonomisk motiverede – og som ikke bliver styret af en stat. Selvom ransomware-angreb også rammer kritisk infrastruktur, er det altså ikke ensbetydende med, at angrebet har den russiske stat som afsender. Virksomheder, der er en del af Danmarks kritiske infrastruktur, kan nemlig tit have karakteristika, som gør dem til attraktive ofre for kriminelles angreb.

På samme måde vurderer vi, at den bølge af DDoS-angreb, der har ramt både danske og europæiske mål i løbet af det seneste år, er begået af aktiviske hackergrupper, der udtrykker deres politiske sympatier. Særligt de pro-russiske hackere har været aktive i 2022 og starten af 2023.

Det er sjældent enkelt at fastslå formålet med et cyberangreb, og ofte kan der i et angreb være aspekter af flere formål. Kriminelle kan have politiske dagsordener, der påvirker deres måludpegning, eller de kan have løse kontakter til stater, der peger dem i en retning. Lige så vel kan aktivistiske hackere have brug for at tjene penge og benytte deres tekniske færdigheder til det formål.

Selvom udfordringen ikke er ny, er behovet for at forstå, hvilke trusler Danmark står over for, større end tidligere. Den nuværende sikkerhedspolitiske situation har dermed medført et øget behov for at klarlægge, om et cyberangreb bliver begået af kriminelle grupper eller er cyberangreb fra en fremmed stat.

Truslen fra cyberaktivisme er hævet til HØJ, mens de øvrige trusselsniveauer er uændrede

Selvom krigen i Ukraine har ændret meget, forbliver de fleste af trusselsniveauerne i dette års vurdering på samme niveau som sidste år. Det betyder dog ikke, at truslen er uændret. Cybertrusler udvikler sig løbende i takt med bl.a. geopolitiske og teknologiske udviklinger.

CFCS vurderer, at truslen fra cyberspionage forsat er **MEGET HØJ**. Det er meget sandsynligt, at danske myndigheder og virksomheder vil blive ramt af forsøg på cyberspionage inden for de næste to år. Det er særligt Rusland og Kina, der benytter cyberangreb til at få viden, primært om dansk udenrigs- og sikkerhedspolitik.

På samme måde er truslen fra cyberkriminalitet **MEGET HØJ**. Cyberkriminalitet rammer bredt, og vi vurderer, at de økonomisk motiverede cyberkriminelle ofte er velorganiserede og robuste overfor myndighedernes indgriben.

Truslen fra cyberaktivisme er nu **HØJ** – og altså på det højeste niveau, siden CFCS i 2016 udgav den første årlige trusselsvurdering. Truslen kan kædes direkte sammen med krigen i Ukraine og de mange pro-russiske hackere, der tyer til tastaturet for at vise deres støtte til Rusland – hvilket flere gange er gået ud over danske mål. Det er sandsynligt, at mål i Danmark vil blive ramt af cyberaktivistiske angreb, særligt overbelastningsangreb. Ændringen af niveauet betyder dog ikke, at konsekvenserne af aktivistiske cyberangreb er blevet mere alvorlige.

Truslen fra destruktive cyberangreb er **LAV**. Vi vurderer fortsat, at det er mindre sandsynligt, at danske myndigheder og virksomheder vil blive mål for et destruktivt cyberangreb. Det er dog sandsynligt, at statsstøttede hackergrupper forbereder sig på at kunne udføre destruktive cyberangreb mod kritisk infrastruktur i Danmark. I og med at flere stater besidder kapaciteten til at udføre destruktive cyberangreb, er truslen i høj grad afhængig af, hvilken hensigt disse stater har. Derfor kan truslen mod Danmark stige med kort eller intet varsel.

Endelig er truslen fra cyberterror fortsat **INGEN.** Cyberterror er alvorlige cyberangreb, der skal opnå samme effekt som konventionelle terrorangreb. Truslen har været **INGEN** flere år i træk, men CFCS følger den tæt, fordi Center for Terroranalyse ved PET vurderer, at truslen fra konventionel terror mod Danmark er i niveauet alvorlig.

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**, og det er meget sandsynligt, at danske myndigheder og virksomheder vil blive udsat for cyberspionage inden for de næste to år.

Fremmede stater forsøger vedvarende at kompromittere danske virksomheder og myndigheder for at stjæle viden. Fremmede stater udfører primært cyberspionage mod Danmark for at få adgang til viden om udenrigs- og sikkerhedspolitik, samt information om Forsvaret. Det er sandsynligt, at Danmark bl.a. er et mål for politisk motiveret cyberspionage pga. Danmarks medlemskab af NATO og EU. Derudover bidrager Danmarks geografiske placering og rolle i forhold til Arktis også til truslen fra fremmede stater.

Udover politisk motiveret cyberspionage udfører fremmede stater også cyberspionage for at fremme deres økonomiske interesser og få adgang til viden, der kan understøtte teknologiske udviklingsmål. Succesfuld cyberspionage kan underminere danske interesser, både politisk og økonomisk.

Endelig vurderer CFCS, at cyberspionage er en forudsætning for destruktive cyberangreb. Det er derfor sandsynligt, at fremmede stater, der bedriver cyberspionage mod Danmark, også kan benytte den indsigt, de opnår ved cyberspionage, til at forberede fremtidige, destruktive cyberangreb.

Rusland og Kina forsøger at stjæle viden om dansk forsvar og udenrigspolitik
Truslen fra cyberspionage kommer især fra Rusland og Kina. Begge stater har betydelige cyberkapaciteter, som de bruger til at kompromittere ofre verden over, herunder i Danmark.

Staterne er særligt interesserede i at få adgang til viden om dansk udenrigs- og sikkerhedspolitik samt Forsvarets kapaciteter, materiel og personel. Viden om militær- og dual-use-teknologi samt forskning bl.a. i Danmark er også udsat for truslen fra cyberspionage

Cyberspionage drevet af militære interesser kan også ramme kritiske sektorer, der enten aktuelt eller potentielt i fremtiden understøtter Forsvaret. Det gælder særligt transport-, energi-, forsknings- og søfartssektorene.

Det er desuden sandsynligt, at organisationer med en mindre åbenlys eller indirekte forbindelse til Forsvaret eller det udenrigs- og sikkerhedspolitiske område kan blive ramt af politisk motiveret cyberspionage. Det gælder f.eks. danske virksomheder, myndigheder, forskningsinstitutioner, NGO'er og tænketanke. Det kan ske, hvis de af modstanderen bliver opfattet som organisationer, der understøtter dansk forsvar eller udenrigspolitik, f.eks. ved at levere ydelser, viden eller produkter til danske aktører inden for disse områder.

Udover organisationer, der på den ene eller anden måde kan forbindes til dansk udenrigspolitik og forsvar, er der også en trussel rettet mod virksomheder og myndigheder, der leverer ydelser til flere forskellige sektorer og myndigheder. Cyberspionage kan f.eks. blive rettet mod virksomheder, der leverer it-ydelser på tværs af sektorer og organisationer. Leverandører kan også blive brugt som trædesten til yderligere cyberspionage.

Fremmede stater forsøger bl.a. at få adgang til viden om kommunikation indenfor de organisationer, der kompromitteres, ved at angribe deres mailsystemer. Udover indholdet i de enkelte mails kan kompromitteringer af mailsystemer også give fremmede stater et indblik i de samarbejdsrelationer, danske virksomheder eller myndigheder indgår i. Den viden kan blandt andet bruges til at iværksætte nye angreb mod andre ofre.

Stater spionerer både målrettet og bredt mod Danmark
CFCS vurderer, at Danmark er et mål for cyberspionage på linje med andre NATO- og EU-lande. Det skyldes, at fremmede stater generelt er interesserede i sikkerheds- og udenrigspolitik herunder Vestens syn på internationale dagsordner, konflikter og begivenheder.

Der er derudover forhold, der gør Danmark til et særligt interessant mål for cyberspionage. Det er bl.a. sandsynligt, at Danmarks geografiske placering i Østersøen og tæt ved Baltikum bidrager til spionagetruslen fra især Rusland.

Både Rusland og Kina har desuden betydelige interesser relateret til Arktis. Cyberspionage kan blive misbrugt af begge lande til at fremme deres handlemuligheder og interesser i Arktis, potentielt på bekostning af grønlandske, færøske og danske interesser.

Cyberspionage mod grønlandsk mål påvirkede borgervendte tjenester

Grønlandske mål bliver løbende udsat for forsøg på cyberspionage. Eksempelvis opdagede Naalakkersuisuts digitaliseringsstyrelse et sikkerhedsbrud i centraladministrationen d. 25. marts 2022. Kommunikation ind og ud af landet til administrationens servere blev derfor blokeret. Det gik bl.a. ud over adgangen til hjemmesider ved brug af NemID samt forsinkede udbetalingen af sociale ydelser og regninger. Formanden for Naalakkersuisut, Múte B. Egede, udtalte til grønlandske medier, at hændelsen skyldtes et cyberangreb, der havde spionage som formål.

Stater udfører cyberspionage for at fremme egne interesser
Fremmede stater bruger cyberspionage til at fremme deres egen sikkerhed og interesser på den internationale scene og i bilaterale forhold. Både Rusland og Kina benytter cyberspionage for at få adgang til forskellige typer viden, de kan bruge til at udfordre vestlige normer og styrke deres internationale indflydelse. Cyberspionage kan f.eks. give fremmede stater indsigt i Danmarks forhandlingspositioner og udenrigspolitiske dagsorden.

Cyberspionage bruges både strategisk til at opbygge viden over længere tid og taktisk til at opnå mere specifik viden f.eks. om konkrete begivenheder eller områder.

Ud over Rusland og Kina udfører flere regionale aktører i bl.a. Asien, Mellemøsten og Latinamerika cyberspionage. Disse aktører anvender hovedsageligt deres kapaciteter mod rivaliserende stater i deres nærområde. En del af dem overvåger, ligesom eksempelvis Kina, også personer og organisationer, der er regimekritiske, eller som på anden vis bliver opfattet som en trussel.

Stater spionerer også for at fremme økonomiske og teknologiske interesser
CFCS vurderer, at fremmede stater også benytter cyberspionage mod danske mål for at fremme egne økonomiske interesser og teknologiske udviklingsmål. Økonomisk drevet spionage kan f.eks. ramme danske virksomheder og myndigheder i forbindelse med store udbud. Forskning, teknologi og innovationsrelaterede organisationer bliver også ramt af økonomisk drevet cyberspionage.

Stater spionerer mod førende virksomheder

Økonomisk motiveret cyberspionage kan eksempelvis blive rettet mod danske virksomheder, der er internationalt førende inden for deres felt. Eksempelvis forsøgte flere fremmede stater at kompromittere udenlandske medicinalvirksomheder, der udviklede COVID-19 vacciner i 2020.

Cyberspionage mod kritiske sektorer bliver mere udbredt i fremtiden
Det er sandsynligt, at truslen fra cyberspionage fremover vil blive skærpet mod mål inden for flere kritiske sektorer. Det skyldes bl.a., at international politik bliver mere præget af konkurrence og modsætninger, hvilket skaber en tendens til, at beslutninger, der tidligere blev betragtet som af civil, teknisk eller økonomisk karakter, bliver sikkerhedspolitiske. Dette gælder forhold som f.eks. forsyningskæder, energi og teknologiudvikling.

Cyberspionage-aktører udfører også andre typer cyberangreb

Truslen fra cyberspionage er kompleks, fordi cyberangreb, der umiddelbart har til formål at indsamle information, også kan føre til andre typer cybertrusler. Eksempelvis kan hackere, der i første omgang udfører cyberspionage, senere bruge deres adgange til kompromitterede systemer til andre typer angreb.

Der er bl.a. eksempler på, at flere statsstøttede hackergrupper, der udfører cyberspionage, også står bag andre typer angreb i udlandet, bl.a. destruktive cyberangreb og påvirkning med brug af cyberangreb.

Ifølge Microsoft har en enkelt statsstøttet hackergruppe stået bag både cyberspionage, destruktive cyberangreb og påvirkning med brug af cyberangreb mod mål i Ukraine. Microsoft har givet gruppen navnet DEV-0586 og beskriver i deres rapporter, hvordan hackere fra DEV-0586 både udførte cyberspionage mod ukrainske mål og siden også destruktive wiper-angreb og defacement-angreb mod ukrainske hjemmesider.

Cyberkriminalitet

Truslen fra cyberkriminalitet mod danske myndigheder og virksomheder er fortsat **MEGET HØJ**. Det er den mest synlige cybertrussel mod Danmark, der fylder både i trusselslandskabet samt i danskernes hverdag. Truslen vil fortsat have mærkbare konsekvenser for virksomheder, myndigheder og borgere. Blandt andet i form af afbrudte services, ydelser og økonomiske tab.

CFCS bruger begrebet cyberkriminalitet som en fællesbetegnelse for økonomisk motiveret it-kriminalitet begået via cyberangreb.

Hvad er ransomware-angreb?

I ransomware-angreb forsøger kriminelle at afpresse myndigheder og virksomheder ved at gøre deres data og systemer utilgængelige, ofte ved at kryptere data. De kriminelle kræver en løsesum typisk i form af kryptovaluta for at gøre data og systemer tilgængelige igen. Ofrene bliver ofte også truet med, at informationer, der kan være stjålet i angrebet, bliver offentliggjort, hvis løsesummen ikke betales.

Cyberkriminelle truer alle dele af samfundet

Alle kan komme i de cyberkriminelles søgelys. Visse ransomware-aktører går bevidst efter kritisk infrastruktur, hvor de kan skabe alvorlige driftsforstyrrelser i forsøget på at presse virksomheden eller myndigheden til at betale en høj løsesum. Andre hackere går i den modsatte retning og går bevidst udenom kritisk infrastruktur, sandsynligvis i håbet om at undgå opmærksomhed fra myndighederne.

En anden faktor, der har betydning for ransomware-aktørers udvælgelse af mål, er de potentielle ofres omsætning. En højere omsætning betyder, at ransomware-aktørerne forventer at kunne afpresse offeret for et større beløb.

Små- og mellemstore virksomheder går dog ikke fri af truslen fra ransomware. Opportunistiske cyberkriminelle går efter ofre, de nemt kan kompromittere. Der er ikke nødvendigvis samme fokus på cybersikkerhed i mindre virksomheder, og de kan derfor udgøre lavthængende frugter for cyberkriminelle.

En helt almindelig arbejdsplads – og så alligevel ikke

Det er meget sandsynligt, at danske virksomheder og myndigheder fortsat vil blive ramt af hyppige forsøg på cyberkriminalitet. Det cyberkriminelle miljø er robust og består af grupper og individer, der samarbejder og handler med hinanden på tværs af landegrænser.

Samarbejdet mellem cyberkriminelle har flere negative effekter for deres potentielle ofre. Samarbejdet øger de kriminelles kapaciteter, bl.a. fordi de har mulighed for at specialisere sig og effektivisere deres angreb. Samarbejdet på tværs af landegrænser bidrager også til, at miljøet er relativt robust over for enkelte landes forsøg på at afskrække eller straffe de kriminelle.

Dygtig ransomware-aktør oplærer andre kriminelle

I både 2021 og i 2022 blev en cyberkriminel gruppe, der var kendt som Conti, udsat for læk af deres interne informationer. I lækket fremgik bl.a. interne chatbeskeder og trin-for-trin guides til at udføre ransomware-angreb. Disse guides har sandsynligvis været anvendt til at hjælpe og træne kriminelle, der var tilknyttet gruppen - også kaldet affiliates. Instruktionerne var så præcise og brugervenlige, at de kunne hjælpe hackere med begrænset teknisk viden til at udføre relativt avancerede ransomware-angreb.

Conti var en meget aktiv ransomware-gruppe, som stod bag flere alvorlige angreb verden over. De nedlagde størstedelen af deres infrastruktur i foråret 2022.

En del af de cyberkriminelle grupper forsøger på mange måder at organisere sig som virksomheder. Lækket af informationer fra den cyberkriminelle gruppe Conti understregede dette. Interne chats viste, at Conti havde flere afdelinger med forskellige ansvarsområder og budgetter, regelmæssige lønudbetalinger til op til 80 medarbejdere, løbende rekruttering af nye medarbejdere via jobopslag på onlinefora, og klare interne hierarkiske strukturer.

Meget handel og samarbejde mellem cyberkriminelle foregår på russisktalende online-fora. Det er ikke ensbetydende med at alle medlemmerne på foraene er russere eller opholder sig i Rusland. Cyberkriminelle opholder sig verden over.

Cyberkriminalitet kender ingen grænser.

De kriminelle kan opholde sig verden over og anvende it-infrastruktur, der er spredt over flere lande. Men når flere stater samarbejder, kan de lykkes med at gøre livet sværere for de kriminelle. I januar 2023 blev infrastruktur fra ransomware-gruppen Hive taget ned i en koordineret indsat mellem flere lande. Blandt andet overtog FBI den hjemmeside, hvor gruppen plejede at offentliggøre sine ofre.

Foto: Andre M. Chang/Zuma/Ritzau Scanpix

Forbindelser mellem cyberkriminelle og stater
CFCS vurderer, at langt de fleste cyberkriminelle er økonomisk motiverede, arbejder opportunistisk og er uafhængige af stater.

Det er dog sandsynligt, at der i enkelte tilfælde er forbindelser mellem fremmede stater og cyberkriminelle. Disse forbindelser varierer i forhold til, hvor formelle og tætte de er. Et særligt tilfælde i denne forbindelse er Nordkorea, hvor statslige hacker-grupper sandsynligvis udfører cyberkriminalitet for at skaffe økonomiske midler til staten.

Det er sandsynligt, at enkelte fremmede stater har rekrutteret cyberkriminelle til at udføre cyberspionage. CFCS vurderer, at der, når bl.a. medier og it-sikkerheds-selskaber har italesat forbindelser mellem eksempelvis den russiske stat og cyber-kriminelle, som udgangspunkt er tale om, at de cyberkriminelle har bidraget til cyberspionage.

Rekruttering af kriminelle personer kan tjene flere formål. For det første kan det være for at øge statens cyberkapaciteter relativt nemt og billigt. Derudover kan det give en stat mulighed for at lægge afstand til cyberangreb, som er udført af personer, der ikke officielt er ansat af staten.

Det er også meget sandsynligt, at enkelte fremmede stater udnytter det cyber-kriminelle miljø ved eksempelvis at anskaffe sig malware fra cyberkriminelle. Fremmede stater kan udnytte de online fora, hvor kriminelle anonymt handler med hinanden til dette. De kriminelle ved derfor ikke nødvendigvis, at de samarbejder med eller sælger til en statsstøttet aktør. Ligesom ved rekruttering af kriminelle er der her tale om en måde for stater at udvide deres kapacitet på. Også her vil staten kunne skabe forvirring ved at få cyberangreb til at ligne cyberkriminalitet.

Russiske FSB-officerer anklaget for at betale cyberkriminelle for at hacke Yahoo

Amerikanske myndigheder tiltalte i 2017 to officerer fra den russiske sikkerhedstjeneste, FSB for at have hyret en russisk og en canadisk-khasakhisk cyberkriminel til at stjæle følsom viden.

FSB-officererne, hvoraf den ene ifølge åbne kilder selv havde en fortid som cyberkriminel, betalte ifølge anklagerne de kriminelle for at hacke sig ind i bl.a. Yahoos netværk samt Yahoo- og Google-mailkonti.

Hackerne delte ifølge amerikanske myndigheder oplysninger fra udvalgte mailkonti med FSB-officererne. Herunder informationer fra regeringskritiske russiske journalisters mailkonti samt data fra amerikanske virksomheder, embedsmænd og diplomater.

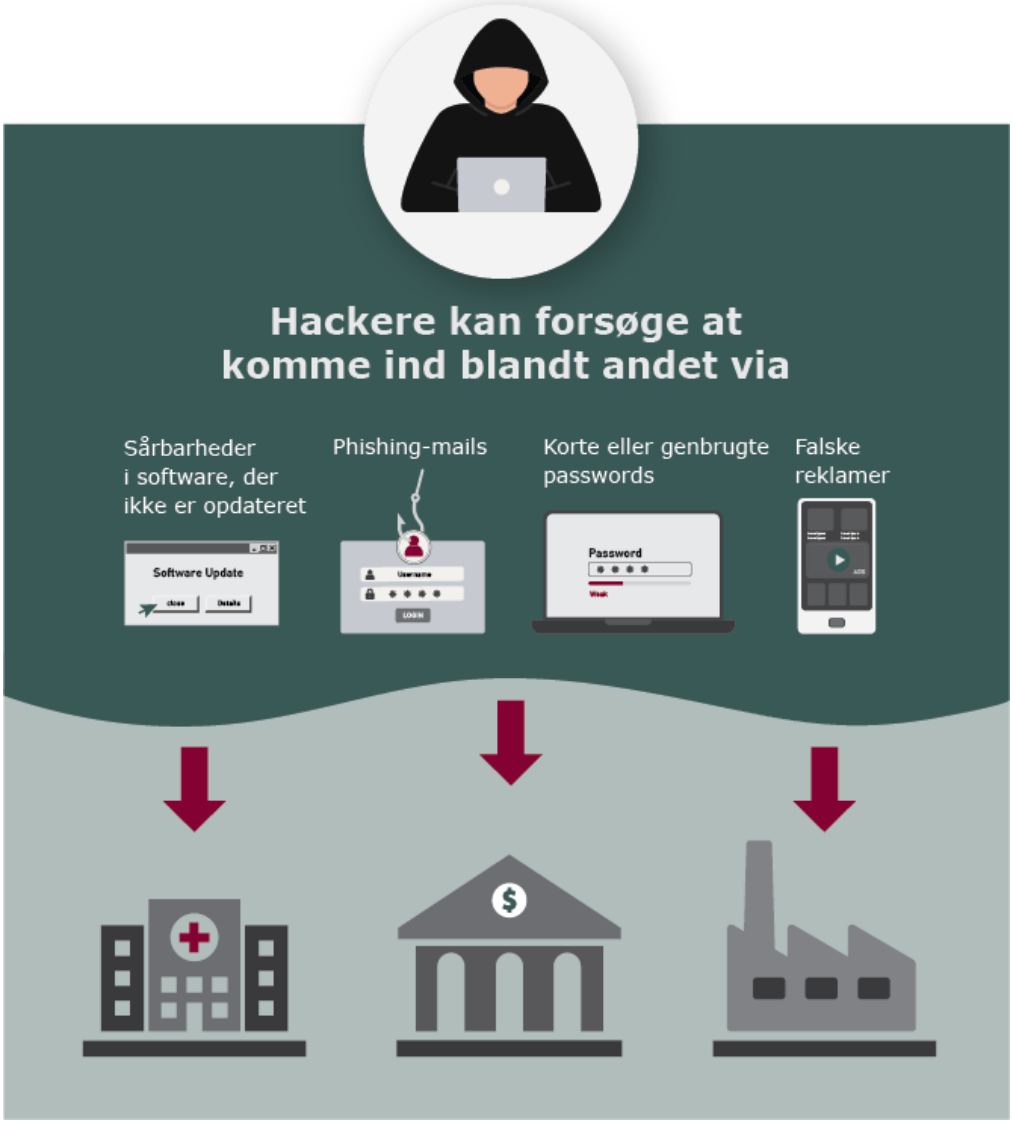
Den russiske hacker berigede samtidig sig selv bl.a. ved at stjæle kreditkortoplysninger og gavekort fra de kompromitterede mailkonti. Ifølge anklageskriftet hjalp FSB-officererne ham med at undgå at blive anholdt.

Den canadiske hacker blev anholdt og udleveret til USA, hvor han erklærede sig skyldig. I 2018 blev han idømt fem års fængsel.

Et andet aspekt af forholdet mellem stater og cyberkriminelle er, hvorvidt stater gør nok for at bekæmpe cyberkriminelle i deres respektive lande, eller om de med vilje undlader at gribe ind, så længe de cyberkriminelle primært retter deres angreb mod udlandet. USA har anklaget Rusland og Kina for i flere tilfælde at have kendskab til cyberkriminelle aktørers aktiviteter og identitet uden at gribe ind overfor dem.

Kriminelle afpresser også uden at kryptere data

Cyberangreb, der krypterer data, har fået meget opmærksomhed de seneste år, men cyberkriminelle afpresser også virksomheder og myndigheder uden at kryptere data. Nogle kriminelle stjæler viden fra virksomheder og truer med at lække eller sælge den, hvis offeret ikke betaler. Selvom denne type angreb ikke påvirker driften i samme grad, som hvis data blev krypteret, kan det stadig skade offeret betragteligt. Ud over de umiddelbare konsekvenser, såsom eventuelle GDPR-bøder og tab af omdømme og derved kunder eller markedsværdi, kan angrebene også give mere langsigtede tab, hvis forretningshemmeligheder bliver delt.



Visse cyberkriminelle specialiserer sig i at få adgange til systemer, som de sælger videre til andre hackere. De kan dermed bruge al deres tid og kompetencer på at komme ind og derefter hurtigt bevæge sig videre til næste offer. Køberne af adgangene kan eksempelvis bruge dem i ransomware-angreb.

Aktører, der udfører denne type afpresning, bruger mange af de samme teknikker, som ransomware-aktører ift. at presse offeret til at betale. Blandt andet offentliggør de kriminelle deres ofre på hjemmesider, de kontrollerer, der også kaldes "Dedicated Leak Sites". It-sikkerhedsselskaber har beskrevet flere eksempler fra udlandet på cyberkriminelle, der har kontaktet offerets medarbejdere eller kunder om den stjålne information. I andre tilfælde forsøger kriminelle at gøre de stjålne informationer lette at finde gennem almindelige internetsøgninger.

BEC-svindel medfører fortsat store økonomiske tab

Business E-mail Compromise (BEC)-svindel er stadig en hyppig angrebsmetode, der koster ofrene mange penge. Ved BEC-svindel forsøger kriminelle at franarre virksomheder og organisationer penge gennem falske anmodninger om penge-overførelser. I nogle tilfælde kompromitterer cyberkriminelle en legitim mailkonto hos en virksomhed eller hos en virksomheds samarbejdspartnere for derefter at manipulere medarbejdere til at overføre penge til de kriminelles konti. De kriminelle kan eksempelvis sende falske fakturaer eller ændre oplysningerne i ellers legitime fakturaer. Det er nærmest kun fantasien, der sætter grænser for, hvordan de kriminelle forsøger at bedrage organisationer og individer via kompromitterede mails.

Kommune svindlet for 277.000 kroner

Næstved Kommune meldte i juli 2022 ud, at kommunen var blevet svindlet for 277.000 kroner. En medarbejders kommunale mailkonto var blevet hacket og misbrugt til at sende falske fakturaer til en økonomimedarbejder i kommunen. Hackeren havde fået adgang til medarbejderens mail via en phishingmail sendt fra en lokal elektriker, som hackeren også havde kompromitteret. Medarbejderen havde tidligere haft kontakt til elektrikeren og mistænkte derfor ikke mailen for at være ondsindet. Det kan være særligt svært at opdage phishing-mails, hvis de er sendt som led i en eksisterende og legitim dialog. Dette kaldes også e-mail thread hijacking.

Kriminelle hackere udfører BEC-svindel for at tjene penge nemt og hurtigt. Ofte behøver de cyberkriminelle end ikke at kompromittere en mailkonto. I stedet kan de blot få en mail til ofret til at se legitim ud på overfladen. De kan eksempelvis oprette en mailadresse, der ligner en legitim mailadresse fra modtagerens arbejdsplads. De kriminelle kan også bruge viden om virksomheden eller myndigheden og dens medarbejdere til at få deres mails til at virke overbevisende.

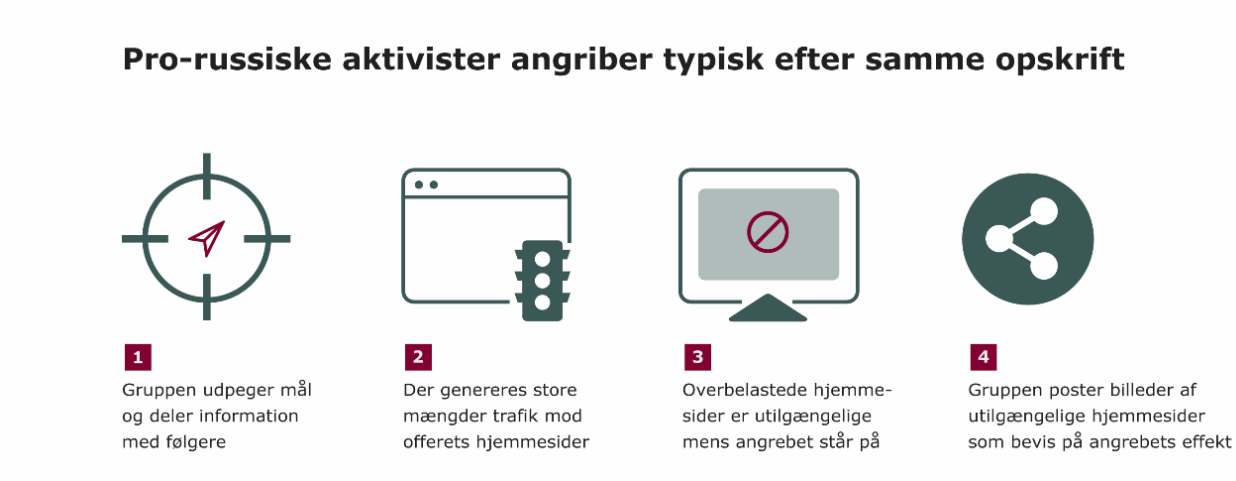
Ligesom med andre former for cyberkriminalitet er der et vedvarende kapløb mellem organisationerne, der forsøger at opsætte sikkerhedsforanstaltninger mod BEC-svindel, og de kriminelle, der forsøger at omgå disse foranstaltninger. De kriminelle er kreative og samarbejder for at få succes med deres angreb.

Cyberaktivisme

Truslen fra cyberaktivisme mod Danmark er **HØJ**. CFCS hævede trusselsniveauet fra **MIDDEL** til **HØJ** i januar 2023.

Det er sandsynligt, at danske virksomheder og myndigheder vil blive ramt af aktivistiske cyberangreb på kort sigt. CFCS hævede trussels-niveauet fra cyberaktivisme på baggrund af pro-russiske aktivistiske hacker-gruppers høje aktivitetsniveau mod NATO-lande, herunder Danmark, samt deres mere formaliserede angrebsmodus og øgede kapacitet.

Cyberaktivisme udføres af individer og grupperinger, der bruger cyberangreb for at få mest mulig opmærksomhed til deres dagsorden eller for at straffe organisationer, som de anser som modstandere af deres sag. Cyberaktivister er typisk drevet af ideologiske eller politiske motiver, der strækker sig fra politiske enkeltsager til modstand mod magthavere.



De DDoS-angreb, som også har ramt Danmark, følger ofte den samme fremgangsmåde.

Pro-russiske hackere rammer mål i Danmark
Det er sandsynligt, at danske organisationer også i fremtiden vil blive mål for cyber-aktivistiske angreb. Når de cyberaktivistiske angreb er en del af det aktuelle trussels-billede for Danmark skyldes det særligt, at pro-russiske cyberaktivister angriber mål i Europa og NATO i konteksten af de fortsat øgede spændinger mellem Rusland og Vesten. Truslen fra danske cyberaktivistiske miljøer er derimod fortsat meget begrænset.

Forsvarets hjemmesider udsat for aktivistisk DDoS-angreb

Det er sandsynligt, at en pro-russisk cyberaktivistisk hackergruppe stod bag DDoS-angreb mod flere af Forsvarsministeriets hjemmesider d. 8. december 2022. Gruppen er en af mange pro-russiske grupper, der har udført DDoS-angreb mod mål i europæiske NATO-lande siden Ruslands invasion af Ukraine i februar 2022.

Gruppen går ofte efter at ramme offentlige myndigheder. Forud for angreb opfordrer gruppen sine følgere på Telegram til at deltage i fælles DDoS-angreb mod udpegede mål. Gruppen stiller værktøjer og mållister til rådighed for følgere, der ønsker at deltage i angrebene.

I nogle tilfælde angriber cyberaktivister mål, som de anser for at være anti-russiske eller symbolske for andre landes støtte til Ukraine. Det seneste år har de pro-russiske cyberaktivister mere eller mindre konstant udført kortere angrebskampagner, hvor de grupperer målene under bestemte tematikker enten i et specifikt land eller på tværs af lande. Det udpegede tema kan i begge tilfælde eksempelvis være organisationer i en udvalgt sektor. Hackerne er især gået efter myndigheder og virksomheder inden for transport-, finans- og forsvarssektoren. Danske mål er blevet ramt i forskellige typer kampagner, bl.a. i et angreb, hvor temaet var europæiske forsvarsministerier, samt i en kampagne, hvor temaet var den danske finanssektor.

Cyberaktivister udgør en trussel mod danske virksomheder og myndigheder

Pro-russiske hackere angriber løbende mål i samfundsvigtige sektorer i vestlige lande. Det er sandsynligt, at danske mål igen vil blive ramt, særligt hvis Danmark tiltrækker sig pro-russiske hackergruppers opmærksomhed f.eks. i forbindelse med håndhævelse af sanktionerne mod Rusland eller Danmarks militære støtte til Ukraine.

Cyberaktivister slår tilbage

Aktivistiske hackere udfører også gengældelsesangreb mod myndigheder og virksomheder i lande, der håndhæver sanktioner mod Rusland. I mange tilfælde retter hackerne angreb mod organisationer inden for samme sektor, som sanktionerne rammer i Rusland.

I juni 2022 opfordrede en pro-russisk cyberaktivistisk hackergruppe på sin Telegram-kanal til DDoS-angreb på litauisk infrastruktur som gengæld for Litauens håndhævelse af restriktioner på fragt af gods med jernbanen til Kaliningrad. På samme måde gennemførte en pro-russisk aktivistisk hackergruppe et DDoS-angreb på et finsk militærakademi som gengældelse for Finlands militærtræning af ukrainske soldater. Også Tyskland og Letland har været udsat for gengældelsesangreb fra pro-russiske cyberaktivister.

De pro-russiske cyberaktivister retter bl.a. deres angreb mod sektorer med forbindelse til forsvaret som f.eks. logistikvirksomheder, der bl.a. arbejder med transport af materiel. Eksempelvis udførte en pro-russisk aktivistgruppe i oktober 2022 DDoS-angreb mod lufthavne, marineterminaler og logistikvirksomheder i USA. Forud for angrebet lagde gruppen et opslag på deres Telegramkanal, hvor de opfordrede følgere til at generere trafik til de pågældende virksomheders hjemmesider, der som resultat blev sat ud af drift.

I krigens indledende måneder udgjorde cyberaktivister på både den pro-ukrainske og den pro-russiske side af konflikten en trussel mod Danmark. Efter krigens udbrud blev mange cyberaktivistiske angreb også rettet mod Rusland eller udenlandske virksomheder, som pro-ukrainske hackere anså som Ruslands-venlige. Pro-ukrainske cyberaktivister er stadig aktive, men den største trussel mod Danmark udspringer fra pro-russiske cyberaktivister.

Det cyberaktivistiske landskab er komplekst
Selvom cyberaktivister ikke er statslige aktører, men handler på eget initiativ, kan der være forbindelser mellem nogle aktivister og forskellige landes myndigheder. Den mulige tilknytning mellem cyberaktivister og fremmede stater samt hyppigheden i cyberaktivistiske angreb på tværs af landegrænser skaber en gråzone, der kan sprede og forværre konflikter. Det kan eksempelvis ske, hvis angrebene får en ødelæggende effekt eller forstyrrer kritisk infrastruktur.

Forud for Ruslands invasion af Ukraine var antallet af aktivistiske cyberangreb faldende, men krigen har skabt stor aktivitet i dele af det aktivistiske miljø.

I løbet af krigen har cyberaktivistiske hackergrupper udført angreb, der har haft til formål at forstærke konsekvenserne af konventionelle angreb. Eksempelvis udførte en pro-russisk hackergruppe et overbelastningsangreb på en ukrainsk online-forhandler af nødgeneratorer. Angrebet skete i kølvandet på en række russiske missilangreb på kraftværker. Målet var at forhindre ukrainere i at indkøbe private strømgeneratorer. Et andet eksempel er en pro-ukrainsk hackergruppe, der påstod at have rettet et aktivistisk angreb mod jernbanen i Belarus. Angrebet skulle have forstyrret signal-systemerne og betød, at man måtte gå over til manuel drift. Målet var sandsynligvis at forstyrre russisk transport af materiel til Belarus forud for invasionen af Ukraine.

Aktivister angriber primært med DDoS
Cyberaktivistiske hackere benytter sig oftest af DDoS-angreb, sandsynligvis fordi det er en type cyberangreb, der ikke kræver avancerede tekniske færdigheder og samtidig tiltrækker opmærksomhed til aktivisternes dagsorden. Denne type angreb virker forstyrrende, men har ikke varige eller destruktive konsekvenser for ofrenes systemer.

Den stigende tilslutning til de aktivistiske angreb betyder, at grupperne får flere medlemmer, der stiller ressourcer til rådighed i botnet, der bruges til DDoS-angreb. De ekstra ressourcer, som tilslutningen giver, kan øge DDoS-angrebs styrke og gøre dem sværere at mitigere.

Udover DDoS-angreb er en række pro-russiske hackergrupper også involveret i udførelsen og promoveringen af informationskampagner. Her forsøger grupperne ved hjælp af manipuleret eller fabrikeret information at påvirke bestemte befolknings-grupper i en retning, der tjener Ruslands strategiske interesser. Hack og læk-angreb kan i disse operationer være med til at forstærke kampagnens effekt.

Pro-russiske grupper har også angrebet med metoder, som oftest bruges af andre typer aktører. Eksempelvis har en aktivistisk gruppe udført ransomware-angreb mod vestlige mål. Her bliver brugerens data krypteret som ved et økonomisk motiveret angreb, men i stedet for at efterlade offeret med en note med information om betaling

af løsesum, efterlader hackerne et link til en Telegramkanal, der spreder pro-russisk propagandamateriale.

I andre tilfælde anvender aktivistiske hackere defacement-angreb, hvor de ændrer offerets hjemmeside ved f.eks. at indsætte en tekst eller et billede på forsiden. Både pro-russiske og pro-ukrainske hackere har anvendt denne type angreb. De pro-ukrainske hackere har særligt brugt det til at sprede information om Ruslands invasion af Ukraine til den russiske befolkning.

Cyberaktivister bruger sociale medier til at opfordre til angreb
Cyberaktivisme er typisk drevet af ideologiske eller politiske motiver. Med krigen i Ukraine er der opstået aktivistiske miljøer, der på den russisk-udviklede applikation Telegram opfordrer hinanden til og koordinerer aktivistiske cyberangreb.

De pro-russiske hackergrupper er en del af et foranderligt onlinemiljø, hvor grupperinger løbende opstår, varierer i aktivitetsniveau over tid og i nogle tilfælde forsvinder igen. De pro-russiske cyberaktivister angriber med afsæt i samme anti-vestlige dagsorden, men koordinerer ikke nødvendigvis på tværs af grupperne.

CFCS vurderer, at de pro-russiske hackere også motiveres af medieomtale. Hackerne følger løbende med i mediedækningen af deres cyberangreb. Grupperne deler bl.a. opslag om omtale med deres følgere. Der er desuden intern konkurrence mellem de forskellige pro-russiske hackergrupper. Den interne konkurrence mellem grupperne viser sig bl.a. ved deres ønske om, at medier og andre hackergrupper tydeligt til-skriver dem æren for angreb, de udfører. Omfattende mediedækning af cyber-aktivistiske angreb mod danske mål kan derfor bidrage til at gøre Danmark til et mere attraktivt mål for cyberaktivister.

Det er sandsynligt, at de pro-russiske aktivistiske grupper vil være motiverede til at angribe mål i Vesten og i Danmark, så længe den aktuelle krise mellem Rusland og Vesten står på.

Destruktive cyberangreb

CFCS vurderer, at truslen fra destruktive cyberangreb mod Danmark fortsat er **LAV**. Det er mindre sandsynligt, at danske virksomheder og myndigheder vil blive udsat for destruktive cyberangreb på kort sigt.

Det er dog sandsynligt, at statsstøttede hackergrupper forbereder sig på at kunne udføre destruktive cyberangreb mod kritisk infrastruktur i Danmark. Truslen mod Danmark kan stige med kort eller uden varsel, hvis f.eks. den sikkerhedspolitiske situation eskalerer i retning af en militær konfrontation mellem Rusland og NATO.

I 2022 blev der på verdensplan set et hidtil uset højt antal destruktive cyberangreb sammenlignet med tidligere år. Hovedparten af de kendte angreb har været rettet mod Ukraine og udført af Rusland.

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.

Begrænset intention om destruktive cyberangreb mod Danmark

Det er mindre sandsynligt, at fremmede stater, herunder Rusland, aktuelt har intentioner om at udføre destruktive cyberangreb mod Danmark. Danske organisationer, der har aktiviteter i Ukraine eller leverer produkter eller tjenester relateret til krigen i Ukraine, kan dog være udsat for en højere risiko for at blive ramt af et angreb eller følgevirkningerne af et angreb, der er rettet mod Ukraine.

Destruktive cyberangreb bliver hovedsageligt brugt af stater op til og under væbnede konflikter, hvilket krigen i Ukraine er seneste eksempel på. Flere stater har kapacitet til at udføre destruktive cyberangreb.

Stater opbygger destruktive kapaciteter i fredstid – også mod Danmark.

Selvom det er mindre sandsynligt, at fremmede stater aktuelt har intention om at udføre destruktive cyberangreb mod Danmark, er det alligevel sandsynligt, at statsstøttede hackergrupper, særligt fra Rusland, forbereder sig på at kunne udføre destruktive angreb mod kritisk infrastruktur i Danmark. På den måde kan hackergrupperne med kort eller intet varsel iværksætte destruktive angreb, såfremt intentionen skulle ændre sig.

Stater bruger bl.a. cyberspionage til at forberede destruktive cyberangreb, der f.eks. vil kunne iværksættes i tilfælde af en eskalerende krise eller krig. Forberedelsen af destruktive cyberangreb består ofte 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. På den måde er grupperne forberedte på at kunne udføre destruktive angreb med kort varsel, såfremt hensigten fra stater med destruktive kapaciteter skulle ændre sig.

Wiper-malware er det foretrukne værktøj

I langt de fleste destruktive cyberangreb er der brugt såkaldt wiper-malware, der bruges til at ødelægge systemerne eller netværket. Wiper-malware fungerer ved, at den sletter eller krypterer filer på det system eller netværk, det rettes imod, så det ikke virker og er svært at genskabe.

Sådan virker wiper-malware

Når filer på en harddisk slettes, fjernes de ikke umiddelbart fra disken med det samme. Pladsen, hvor filen var gemt, bliver i stedet markeret som ledig til at gemme nye filer på. Når nye filer gemmes, overskrives den data, der tidligere befandt sig på pladsen, og derfor er den oprindelige data først nu reelt slettet. Derfor kan man ofte genskabe en fil, der er blevet slettet ved en fejl.

Wiper-malware sletter derfor ikke bare, men overskriver også med ny og ubrugeligt data. Det er der flere metoder til at gøre, og der er generelt et trade-off mellem hastighed og grundighed i angrebet. Hvis wiperen overskriver data meget hurtigt, er det muligt, at data kan genskabes. Hvis wiperen er meget grundig og dermed langsom, kan sikkerheds-løsninger nå at opdage og stoppe malwaren.

Der findes enkelte historiske eksempler på avancerede destruktive angreb, der sigtede mod at skabe decideret fysisk ødelæggelse ved at ramme industrielle kontrolsystemer. Disse typer af angreb kræver typisk specialfremstillet malware, som er ressource-krævende at udvikle. CFCS vurderer, at flere stater vedligeholder og udvikler kapaciteter til også at kunne udføre den type komplicerede angreb.

Selvom wiper-angreb umiddelbart kan lyde mindre alvorlige end angreb, der sigter mod fysisk ødelæggelse, kan de have omfattende konsekvenser. Hvis angrebet effektivt sletter eksempelvis kritiske systemfiler hos en organisation, vil det ofte påvirke organisationens drift. Det kan samtidig tage uger eller endda måneder at genskabe et velfungerende netværk. Hvis det sker for organisationer, der leverer kritiske ydelser til samfundet, kan angrebet ende med at få store konsekvenser.

At wiper-angreb kan have store konsekvenser, illustreres for eksempel af wiper-angrebet mod Viasat. På dagen for Ruslands invasion af Ukraine blev virksomheden Viasat ramt af et wiper-angreb kaldet AcidRain, der blandt andet resulterede i, at tusindvis af satellitmodemmer, særligt i Europa, fik slettet deres opsætning. Viasat er en amerikansk udbyder af satellitkommunikation. Den manglende satellit-kommunikation førte bl.a. til nedbrud i fjernstyringen af flere vindmøller i Tyskland. Det er sandsynligt, at målet med angrebet var ukrainske militære styrkers satellitkommunikation.

Danmark har sammen med EU og en række nære allierede vurderet, at Rusland stod bag cyberangrebet, og at Rusland var vel vidende om, at angrebet ville have destruktive konsekvenser uden for Ukraine.

Wiper-angreb i krigen mod Ukraine i 2022

Ukraine er op til og siden invasionen i februar 2022 blevet ramt af flere forskellige destruktive wiper-angreb, lige fra meget simple til mere avancerede angreb som det nævnte mod satellitkommunikation. Fælles for angrebene mod ukrainske organisationer er, at de var konstrueret, så de alene har ramt de organisationer, der var målet. De aktører, der udførte angrebene, gjorde således en indsats for at sikre sig, at angrebene ikke ville sprede sig udenfor Ukraine.

Viasat-angrebet ramte som nævnt mål udenfor Ukraine. Selvom målet for angrebet sandsynligvis var ukrainsk militærkommunikation, fik det følgevirkninger langt ud over dette. Angrebet viser, at virksomheder, der enten er fysisk til stede i eller på anden vis er knyttet til Ukraine, kan blive ramt af destruktive cyberangreb

Strømafbrydelser i Ukraine

I april 2022 offentliggjorde den ukrainske CERT, at et ukrainsk energiselskab havde været udsat for et forsøg på destruktivt cyberangreb. I angrebet brugte hackerne en ny version af den såkaldte Industroyer-malware, der i 2016 også var rettet mod energisektoren i Ukraine. Ifølge den ukrainske CERT blev angrebet mod energiselskabet i april 2022 afværget inden, at aktøren havde held med at forårsage strømafbrydelser. Private cybersikkerhedsfirmaer har dog beskrevet, at der fandt en kortere strømafbrydelse sted, og at angrebet sandsynligvis blev udført af den russiske statsstøttede hackergruppe Sandworm.

Microsoft har i en rapport offentliggjort beskrivelser af et destruktivt angreb mod organisationer i både Ukraine og Polen i efteråret 2022. Rapporten beskriver et falsk ransomware-angreb mod transportsektoren i Ukraine og Polen. Det var et angreb, der krypterede filer som i et ransomware-angreb, men hvor det reelt ikke var muligt at dekryptere filerne igen. Sammen med Viasat-angrebet er de sjældne eksempler på destruktive cyberangreb, der ramte både Ukraine og et NATO-land.

De wiper-angreb, der har været anvendt i Ukraine, har været rettet mod meget forskellige dele af det ukrainske samfund. Der har været adskillige angreb mod kritisk infrastruktur og regeringsorganisationer. Men også mange andre sektorer, som eksempelvis detailhandel og landbrug, har været ramt. Det er dog vanskeligt at få pålidelig information om effekterne af de forskellige cyberangreb under krigen.

Hvornår er cyberangreb destruktivt?

Det er ofte svært at konkludere med sikkerhed, om et cyberangreb har haft et destruktivt formål, hvis angrebet afværges, inden den destruktive effekt er opnået. Forskellige typer af cyberangreb gennemgår ofte de samme, indledende faser, og det er først i de afsluttende faser, at man kan se, hvad formålet med angrebet egentlig er. Dog kan et forsøg på destruktive cyberangreb muligvis detekteres, hvis der bliver benyttet malware, som i forvejen er kendt som værende destruktiv. På samme måde kan den infrastruktur, som hackerne benytter, til tider indikere, hvem der står bag. Man skal dog være varsom med at bruge infrastruktur som eneste indikator, da

hackere ofte kompromitterer andre servere og således hacker fra dem for at sløre eget ophav.

Typisk er det stater, der har kapaciteterne og potentielt interessen i at udføre destruktive cyberangreb mod andre stater. Aktivister har indtil videre ikke haft kapaciteter til at udføre wiperangreb. Det er dog sandsynligt, at nogle aktivistiske grupper forsøger at udvikle kapaciteter til at udføre wiper-angreb, bl.a. i form af modificeret ransomware, så filerne på et system krypteres, men ikke nødvendigvis kan dekrypteres.

Cyberterror

Truslen fra cyberterror mod Danmark er **INGEN**. Det er usandsynligt, at danske myndigheder og virksomheder på kort sigt vil blive udsat for forsøg på cyberterror.

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

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

Militante ekstremister har i årevis udnyttet internettet til at understøtte deres aktiviteter, planlægge konventionel terror og udbrede deres radikale budskaber. Der har dog endnu ikke været nogle eksempler på, at terrorister har udført cyberangreb med en effekt, der svarer til konventionel terror.

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

Perspektiv: **Cyberangreb med flere formål**

CFCS' vurdering af cybertruslen mod Danmark er bygget op omkring en række formålskategorier, såsom cyberspionage og cyberkriminalitet. Det er altså motivet bag et cyberangreb, der afgør, hvilken kategori CFCS placerer et cyberangreb i.

Hackere har dog ikke nødvendigvis kun ét, afgrænset formål, og som offer kan det være svært at slå fast, hvilken type angreb man er udsat for.

I 2022 er udfordringen med at forstå de enkelte angreb og dermed den samlede trussel ikke blevet mindre kompliceret. Krigen i Ukraine og udviklingen i konflikten mellem Rusland og Vesten har tydeliggjort behovet for at forstå cyberangreb og de bagvedliggende formål.

Cyberkriminalitet i en ny sikkerhedspolitisk virkelighed
CFCS vurderer, at langt de fleste cyberkriminelle fortsat handler opportunistisk og uafhængigt af stater. Ransomware-grupper har det seneste år ramt virksomheder i Vesten og Danmark, og kritisk infrastruktur er ikke gået fri. Selvom krigen i Ukraine har forværret forholdet mellem Danmark, som en del af NATO, på den ene side og Rusland på den anden, er det ikke ensbetydende med, at cyberangreb mod dansk kritisk infrastruktur har den russiske stat som afsender.

En del cyberkriminelle opholder sig, ifølge it-sikkerhedsselskaber og amerikanske myndigheder, i Rusland. Det har i offentligheden ført til spekulationer om forbindelser mellem den russiske stat og cyberkriminelle samt spekulationer om, hvorvidt ransomware-angreb kan være motiveret af andet end ønsket om økonomisk vinding. Det bidrog til disse spekulationer, da der i kølvandet på Ruslands invasion i Ukraine var cyberkriminelle grupper, der åbent erklærede deres støtte til Rusland.

Som beskrevet under kapitlet om cyberkriminalitet er det sandsynligt, at cyberkriminelle i enkelte tilfælde har forbindelser til fremmede stater. Når bl.a. medier og it-sikkerhedsselskaber har italesat forbindelser mellem den russiske stat og cyberkriminelle, er der dog som udgangspunkt tale om, at de cyberkriminelle har bidraget til cyberspionage.

Tekniske og menneskelige fejl kan medvirke til, at ofre for eksempelvis ransomware-angreb bliver i tvivl om, hvad de har været udsat for. Det er nemlig ikke altid, at de kriminelle bag et ransomware-angreb følger op med det samme og afkræver offeret løsepenge. Nogle gange går der lidt tid, eller de kriminelle vender slet ikke tilbage. I sådanne tilfælde kan det for offeret virke som om, at motivet bag angrebet ikke er økonomisk vinding. Men der kan også blot være tale om fejl eller sjusk fra de kriminelles side.

Ransomware med politiske dagsordner
CFCS vurderer, at langt de fleste ransomware-angreb er økonomisk motiverede. Der har dog været enkelte eksempler på cyberangreb, der mudrer dette billede.

I foråret 2022 rettede kriminelle hackere eksempelvis omfattende ransomware-angreb mod flere af Costa Ricas ministerier. Ifølge åbne kilder forsøgte hackerne at lægge pres på regeringen ved at opfordre befolkningen til at gå på gaden og kræve, at man betalte løsesum. Angrebet førte til, at regeringen erklærede national undtagelsestilstand, men nægtede at betale løsepenge til gruppen. Som konsekvens gik hackerne så langt som at true med at afsætte Costa Ricas regering. På trods af disse politiske trusler var det dog sandsynligt, at angrebets egentlige formål var økonomisk vinding.

Mere mudret bliver det, når stater benytter angrebsformer, der kan minde om kriminalitet, men som har et helt andet formål. Her er det særligt problematisk med destruktive cyberangreb, der anvendes under dække af at være ransomware, nogle gange kaldet "fake ransomware". Det mest kendte eksempel på dette er NotPetya-angrebet i 2017. NotPetya var et cyberangreb, der havde sit udspring i Ukraine, men spredte sig globalt og også havde ofre i Danmark.

CFCS vurderer, at NotPetya med stor sandsynlighed var et destruktivt cyberangreb forklædt som et ransomware-angreb.

Senest har Microsoft, som tidligere beskrevet, advaret om, at Rusland i 2022 har anvendt "ransomware-lignende" angreb mod Ukraine og Polen. Sådanne angreb kan netop medvirke til, at ofre for cyberkriminalitet bliver i tvivl om formålet med de enkelte angreb.

Destruktiv aktivisme
Krigen i Ukraine har medført en bølge af aktivistiske cyberangreb. Ikke mindst de pro-ukrainske hackere, der i konfliktens begyndelse blev opfordret til at gribe tastaturet som en del af Ukraines overlevelseskamp, har været meget aktive.

Jo tættere cyberaktivister tilknyttes til en stat, desto vanskeligere bliver det at definere et givent cyberangreb – er der tale om aktivisme eller et cyberangreb begået af en stat? Hackere er ikke fastlåst i bestemte kategorier, og dygtige hackere begrænser ikke nødvendigvis deres talenter til én form for aktivitet i det digitale domæne. En statsligt ansat hacker kan meget vel udføre aktivistiske cyberangreb i sin fritid – ligesom en aktivist måske tjener penge som cyberkriminel.

CFCS vurderer, at aktivisme oftest vil bestå af mindre avancerede angreb som defacement, DDoS eller hack- og læk-angreb. Men der er visse tegn på, at aktivistiske cyberangreb muligvis udvikler sig i en mere avanceret retning, hvilket kan komplicere vores forståelse af cyberangreb yderligere.

Flere aktivistiske grupperinger har under Ukraine-krigen vist interesse i angreb med fysiske, destruktive konsekvenser. Der er eksempler på, at aktivistiske grupper har påstået at have ramt kontrolsystemer i kritisk infrastruktur i Rusland med destruktive konsekvenser. Uanset om disse angreb har været succesfulde eller ej, viser de en udvikling i aktivisternes intention. Det er altså tegn på, at aktivistisk motiverede,

destruktive cyberangreb kan blive en del af fremtidens trusselsbillede, i hvert fald i relation til den igangværende krig i Ukraine.

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

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

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