CENTER FOR CYBERSIKKERHED

Cybertruslen mod Danmark i lyset af Ruslands invasion af Ukraine

Formålet med denne trusselsvurdering er at informere danske beslutningstagere, myndigheder og virksomheder om cybertruslen mod Danmark i lyset af Ruslands invasion af Ukraine. Formålet er bl.a. at give en uddybende forklaring på, hvorfor CFCS fastholder trusselsniveauerne for cybertruslen mod Danmark og en forståelse for de faktorer, som kan få betydning for, hvordan truslen udvikler sig.

Hovedvurdering

- Ruslands invasion af Ukraine forandrede det sikkerhedspolitiske landskab og skabte en usikkerhed, der også har spredt sig til cyberområdet. Selvom CFCS fastholder de nuværende trusselsniveauer, så betyder det tempo og den spænding, som den nuværende situation foregår i, at de sikkerhedspolitiske forhold – og derved trusselsniveauerne – hurtigt kan ændre sig.

- Cybertruslen fra cyberspionage mod Danmark er fortsat **MEGET HØJ.** CFCS vurderer, at Danmark i den nuværende situation fortsat står over for en vedvarende, aktiv og alvorlig trussel fra cyberspionage. CFCS vurderer, at invasionen ikke i væsentlig grad har ændret Ruslands og Kinas vedholdende fokus på at udføre cyberspionage mod Danmark.

- Cybertruslen fra cyberkriminalitet mod Danmark er fortsat **MEGET HØJ**. Cyberkriminalitet udgør en alvorlig trussel, der er rettet mod myndigheder, virksomheder og borgere på tværs af samfundet. Ruslands invasion af Ukraine har ikke i væsentlig grad påvirket truslen fra cyberkriminalitet mod Danmark.

- Truslen fra destruktive cyberangreb mod Danmark er fortsat **LAV.** CFCS vurderer, at stater, der har kapaciteter til at bruge destruktive cyberangreb, herunder Rusland, fortsat ikke har intentioner om at rette denne type angreb mod Danmark.

- Truslen fra cyberaktivisme mod Danmark er fortsat **LAV**. Selvom Ruslands invasion af Ukraine har medført en øget aktivitet i de cyberaktivistiske miljøer, så har aktivismen hidtil i vid udstrækning foregået i direkte forlængelse af krigen og været fokuseret mod Rusland, Ukraine og Belarus.

- Truslen fra cyberterror er **INGEN**. Truslen er upåvirket af Ruslands invasion af Ukraine.

Indledning

Forsvarets Efterretningstjenestes Center for Cybersikkerhed udgiver en ny trusselsvurdering, der vurderer cybertruslen mod Danmark i lyset af Ruslands invasion af Ukraine. Formålet med vurderingen er at give en kort opdateret forståelse af trusselsbilledet og de faktorer, som kan få betydning for, hvordan truslen udvikler sig.

Efter Ruslands invasion af Ukraine den 24. februar 2022 står Danmark overfor et forandret sikkerhedspolitisk landskab, hvor fremtiden på flere områder tegner mere usikker end før. Denne usikkerhed spreder sig også til cyberområdet, hvor trusselsbilledet hurtigt kan ændre sig, hvis eksempelvis forholdet mellem NATO-landene og Rusland bliver væsentligt forværret.

Det tempo og den spænding, som den nuværende situation foregår i, øger risikoen for misforståelser. Det medfører, at de sikkerhedspolitiske forhold – og derved trusselsniveauerne – hurtigt kan ændre sig.

Således er situationen i Ukraine med til at understrege, at cybertruslen skal tages alvorligt. Selvom CFCS ikke på nuværende tidspunkt justerer på trusselsniveauerne, opfordrer CFCS danske myndigheder og virksomheder til at sikre, at organisationens risikovurdering er opdateret, og at de mitigerende tiltag fortsat er tilstrækkelige.

Vurderingen af cybertruslen er opdelt i trusler fra cyberangreb, der understøtter spionage, kriminalitet, destruktive cyberangreb, aktivisme og terrorisme.

Når Forsvarets Efterretningstjeneste vurderer et trusselsniveau, vurderer vi det ud fra to grundlæggende parametre. For det første de potentielle trusselsaktørers kapaciteter og for det andet de potentielle trusselsaktørers hensigter. Den samlede vurdering af trusselsaktørernes kapaciteter og hensigt resulterer i en femtrins skala, der spænder fra **INGEN** trussel til en **MEGET HØJ** trussel.

Danske virksomheder og myndigheder vil meget sandsynligt fortsat løbende blive udsat for cyberspionage og cyberkriminalitet, både uafhængigt af og i forlængelse af den nuværende krise.

CFCS vurderer, at hensigten om at ramme danske mål med destruktive cyberangreb fortsat er begrænset. Flere stater, herunder Rusland, besidder kapaciteten til at udføre destruktive cyberangreb. Hvis et sådant angreb bliver rettet mod for eksempel kritisk infrastruktur med det formål at skade samfundsvigtige funktioner, kan det tilsvare et militært angreb mod et dansk mål. CFCS vurderer på nuværende tidspunkt, at det er mindre sandsynligt, at Rusland har til hensigt at rette den type angreb mod Danmark. Derfor er truslen fra destruktive cyberangreb fortsat vurderet til at være **LAV**.

Cyberspionage

Cybertruslen fra cyberspionage mod Danmark forbliver **MEGET HØJ.** CFCS vurderer, at invasionen ikke i væsentlig grad har ændret Ruslands og Kinas vedholdende fokus på at udføre cyberspionage mod Danmark.

CFCS vurderer, at Danmark i den nuværende situation fortsat står over for en vedvarende, aktiv og alvorlig trussel fra cyberspionage. Danske myndigheder og virksomheder bliver løbende udsat for cyberangreb, der har til formål at give fremmede stater adgang til sensitiv og værdifuld viden, som danske organisationer ønsker at beskytte. Der har i de seneste år også været en øget trussel mod både transport og forskning.

Allerede inden Ruslands invasion af Ukraine var truslen fra cyberspionage mod Danmark særligt rettet mod udenrigs- og forsvarsministeriets myndighedsområde. Den vedvarende trussel mod organisationer med tilknytning till disse myndighedsområder skyldes, at fremmede stater, herunder Rusland, har en særlig interesse for viden af udenrigs-, sikkerheds- og forsvarspolitisk karakter.

Det er meget sandsynligt, at Rusland med invasionen af Ukraine forsat vil have et særligt fokus på at udføre cyberspionage mod myndigheder og organisationer i Danmark, der har betydning for Danmarks udenrigs-, sikkerheds- og forsvarspolitik.

Cyberspionage mod den type viden vil fortsætte, og kan eksempelvis give fremmede stater, herunder Rusland, indblik i danske udenrigs- og sikkerhedspolitiske beslutninger samt militære kapaciteter og planer. En viden der kan blive misbrugt til eksempelvis at svække Danmarks udenrigspolitiske indflydelse, bl.a. i relation til krigen i Ukraine og samarbejdet i eksempelvis EU og NATO.

Truslen fra cyberspionage kommer fortsat også fra andre stater end Rusland. CFCS vurderer, at den aktuelle sikkerhedspolitiske situation ikke ændrer på den vedvarende trussel fra bl.a. Kina. Kina udfører bl.a. cyberspionage for at få adgang til viden om udstyr og teknologi, der både kan bruges civilt og militært.

Cyberkriminalitet

Truslen fra cyberkriminalitet er fortsat **MEGET HØJ**. Truslen er rettet mod myndigheder, virksomheder og borgere på tværs af samfundet. Ruslands invasion af Ukraine har skabt flere reaktioner internt i det kriminelle miljø, men ikke i væsentlig grad påvirket truslen fra cyberkriminalitet mod Danmark.

Kriminelle hackere er forsat hovedsageligt finansielt motiverede og opportunistiske i deres cyberangreb, og cyberkriminelle netværk vil fortsat angribe danske mål uafhængigt af Ruslands invasion af Ukraine. Konflikten har på kort sigt derfor ikke en direkte betydning for truslen fra cyberkriminalitet. Den alvorligste trussel kommer fortsat fra målrettede ransomware-angreb, der kan påvirke samfundsvigtige tjenester.

Der er eksempler på, at kriminelle hackere har misbrugt opmærksomheden på konflikten i spredningen af phishingmails. Det gælder eksempelvis mails om humanitær hjælp til Ukraine. Kriminelle hackere misbruger ofte samfundsaktuelle emner i phishingangreb. Det skete eksempelvis også i forbindelse med Covid-19-pandemiens udbrud i 2020.

Der har været flere reaktioner fra kriminelle hackere på invasionen af Ukraine. Dette er ikke overraskende, da der er et stort russisktalende kriminelt hackermiljø. Hackere bag ransomwaren Conti har truet med gengældelse, hvis Vesten angriber kritisk infrastruktur i Rusland eller russisktalende lande. Conti-gruppen er efter udtalelserne blevet udsat for læk, der har skadet gruppens aktiviteter. 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. CFCS vurderer, at Conti-gruppen på trods af udtalelserne forsat hovedsageligt er finansielt motiveret.

Destruktive cyberangreb

Truslen fra destruktive cyberangreb mod Danmark er fortsat **LAV.** CFCS vurderer, at det er mindre sandsynligt, at Rusland eller andre stater har intentioner om at rette denne type angreb mod Danmark. Rusland har på nuværende tidspunkt ikke intentioner om at udvide krigen til også at omfatte NATO.

Danske myndigheder og virksomheder, der er til stede i Ukraine, kan blive ramt af destruktive cyberangreb målrettet ukrainsk it-infrastruktur. Det skete f.eks. ved NotPetya-angrebet i 2017, hvor A.P. Møller Mærsk bl.a. blev ramt.

Hvad er destruktive cyberangreb?
CFCS definerer destruktive cyberangreb som cyberangreb, hvor den forventede effekt er:
- Død eller personskade,
- betydelig skade på fysiske objekter eller
- ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning.

Danske virksomheder og myndigheder, der er til stede i Ukraine, kan også blive ramt af følgevirkninger af destruktive angreb i Ukraine, selvom Rusland ikke har intention om at ramme danske mål specifikt. Følgevirkninger kan f.eks. være strømafbrydelser eller tab af netværksforbindelse.

En række forhold kan få indflydelse på, hvordan trusselsbilledet kan bevæge sig. Hvis f.eks. den sikkerhedspolitiske situation som følge af krigen mellem Rusland og Ukraine eskalerer i retning af en militær konfrontation mellem Rusland og NATO, vil truslen fra destruktive cyberangreb mod Danmark stige. Det konkrete trusselsniveau vil i den situation afhænge af en sådan krises karakter og videre udvikling.

Ukraine er blevet ramt af flere typer cyberangreb i 2022
Ukraine er i januar og februar 2022 blevet ramt af mange cyberangreb. Indtil videre indbefatter angrebene især gentagne såkaldte DDoS-, defacement- og wiper-angreb med forskellige typer destruktiv malware bl.a. rettet imod den ukrainske regering og institutioner knyttet hertil.

Flere af de destruktive wiper-angreb, der indtil videre har været anvendt mod Ukraine, har sandsynligvis haft til formål at skabe panik i den ukrainske befolkning og nedbryde Ukraines funktions- og forsvarsevne. DDoS og defacement-angreb falder ikke inden for CFCS' definition på destruktive cyberangreb, da de oftest har en mere forstyrrende end reelt ødelæggende karakter.

Der er fortsat usikkerhed omkring omfanget og effekten af de aktuelle destruktive angreb i Ukraine. Der kan også være cyberangreb, der ikke bliver omtalt i medier eller offentliggjort af ukrainske myndigheder.

Statslige aktører kan forsøge at sløre deres cyberangreb som kriminalitet
Ukrainske myndigheder har været udsat for cyberangreb, hvor der har været brugt destruktiv malware, der udgiver sig for at være ransomware. Det skete i Ukraine i 2017

med NotPetya-angrebet og igen i januar 2022 i forbindelse med angreb med den destruktive malware WhisperGate.

Statslige aktører bruger også cyberkriminelle tjenester og værktøjer i cyberangreb. Brug af kriminelle tjenester kan medvirke til at sløre, hvem der står bag angrebene.

Formålet med denne sløring kan være at skabe usikkerhed om angrebenes formål og derved gøre en tilskrivning til specifikke lande mere vanskelig. Hvis statslige aktører vurderer, at de effektivt kan sløre destruktive cyberangreb som cyberkriminalitet, kan det øge risikovilligheden hos de statslige aktører til at lave sådanne angreb.

Cyberaktivisme

Truslen fra cyberaktivisme mod Danmark er fortsat **LAV.**

Cyberaktivisme er typisk drevet af forskellige ideologiske eller politiske motiver. Cyberaktivistiske angreb udføres af ikke-statslige individer eller grupper for at få mest mulig opmærksomhed på deres dagsorden eller for at straffe organisationer.

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. Aktivistiske netværk har fortsat kapacitet til at udføre cyberangreb.

Det er dog flere år siden, at der har været væsentlige aktivistiske cyberangreb rettet mod danske mål. CFCS vurderer, at der fortsat er begrænset intention blandt cyberaktivister til at angribe mål i Danmark. Aktivismen i forbindelsen Ruslands invasion er hidtil i vid udstrækning foregået i direkte forlængelse af krigen og hovedsageligt været fokuseret mod Rusland, Ukraine og Belarus.

Hackergruppen Cyber Partisans har udført aktivistiske angreb rettet mod bl.a. jernbanen i Belarus, hvor de forstyrrede signalsystemerne, både før og efter Rusland havde igangsat invasionen af Ukraine.

Det er cyberaktivistiske angreb af denne type, som i øjeblikket fylder meget i mediebilledet. Aktivister, der hævder at tilhøre hackergruppen Anonymous, har erklæret cyberkrig mod Rusland. I tiden efter erklæringen har der været en række forskellige aktivistiske cyberangreb, hvor cyberaktivister har ramt bl.a. russiske medier. Eksempelvis tog Anonymous på Twitter ansvaret for en aktion mod en række af russiske tv-kanaler, hvor de afbrød udsendelserne for at vise optagelser fra krigen i Ukraine. Efterfølgende blev flere statslige nyhedskanaler i Rusland ramt af defacement-angreb, hvor der blev vist beskeder, som kritiserede den russiske regering og krigen i Ukraine.

Stater udfører påvirkning under dække cyberaktivisme
Truslen fra påvirkning med brug af cyberangreb dækker alene over truslen fra fremmede staters cyberangreb, der bliver udført med det formål at påvirke meningsdannelsen.

Fremmede stater, herunder Rusland, bruger aktivt cyberangreb i deres forsøg på at påvirke holdninger og adfærd i andre lande. I Ukraine er flere af landets regeringshjemmesider blevet udsat for defacement-angreb, hvor falske meddelelser bekendtgjorde, at Kyiv skulle have overgivet sig og underskrevet en frederklæring med Rusland.

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

Cyberterror

Truslen fra cyberterror er **INGEN**. Truslen er upåvirket af Ruslands invasion af Ukraine.

Alvorlige cyberangreb, hvor hensigten er at skabe samme effekt som mere konventionel terror, forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister fortsat ikke har. Hensigten er samtidigt begrænset.

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

Usandsynligt | **Mindre sandsynligt** | **Muligt** | **Sandsynligt** | **Meget sandsynligt**

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