CENTER FOR CYBERSIKKERHED

Trusselsvurdering: CFCS hæver trusselsniveauet fra cyberaktivisme mod Danmark fra LAV til MIDDEL

Maj 2022 1. udgave

Denne vurdering orienterer om ændringen af trusselsniveauet for truslen fra cyberaktivisme mod Danmark. Formålet med vurderingen er at give en uddybende begrundelse for det forhøjede trusselsniveau, der hæves på baggrund af den seneste tids cyberaktivistiske angreb mod vesteuropæiske NATO-lande.

Hovedvurdering

- Truslen fra cyberaktivisme mod Danmark er **MIDDEL**. CFCS hæver dermed trusselsniveauet fra **LAV** til **MIDDEL** på baggrund af aktivistiske cyberangreb udført i forbindelse med krigen i Ukraine.

- Cyberaktivistiske angreb ramte i krigens indledende fase hovedsageligt mål i Rusland, Ukraine og Belarus, men har i de seneste uger også ramt mål i vesteuropæiske NATO-lande.

- CFCS vurderer, at det er muligt, at særligt pro-russiske hackere vil gå efter mål i Danmark. Det er en ændring af trusselsbilledet sammenlignet med de seneste år, hvor CFCS har vurderet, at cyberaktivister ikke har udvist intention om at ramme danske mål.

Analyse

Truslen fra cyberaktivisme mod Danmark er **MIDDEL**. CFCS hæver dermed trusselsniveauet fra **LAV** til **MIDDEL**. Når trusselsniveauet fra cyberaktivisme hæves til **MIDDEL** betyder det, at der er en generel trussel mod Danmark, og at det er muligt, at danske virksomheder og myndigheder på kort sigt rammes af aktivistiske cyberangreb.

CFCS hæver trusselsniveauet på baggrund af aktivistiske cyberangreb udført i forbindelse med Ruslands invasion af Ukraine og efterfølgende reaktioner på krigen. Når trusselsniveauet for cyberaktivisme hæves på grund af konkrete aktiviteter udført af pro-russiske cyberaktivister forbundet med situationen i Ukraine, betyder det ligeledes, at niveauet kan ændre sig igen med kort varsel afhængigt af krigens udvikling.

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 skete i direkte forlængelse af krigen og var fokuseret mod Rusland, Ukraine og Belarus, har cyberaktivistiske angreb nu også ramt europæiske NATO-lande.

Flere vesteuropæiske NATO-lande er mål for cyberaktivisme
Inden for de seneste uger har cyberaktivistiske angreb ikke længere kun ramt aktive parter i konflikten i Ukraine, Rusland og Ukraine, men også omkringliggende lande. Angrebene har hovedsageligt ramt lande i Ukraines nærområde, hvor pro-russiske aktivistgrupper har angrebet virksomheder og myndigheder i eksempelvis Tjekkiet, Polen og Estland.

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

Cyberaktivistiske angreb kan antage forskellige former og målrettes forskellige typer symbolske ofre. Senest er der set eksempler på overbelastningsangreb mod myndigheders hjemmesider i blandt andet Estland, Rumænien og Letland, banker i Polen og TV- og radiostationer i Tjekkiet. Cyberaktivisme kan ligeledes finde sted i form af hack og læk-angreb og defacement af hjemmesider.

Truslen fra cyberaktivisme kommer særligt fra pro-russiske hackere
CFCS hæver trusselsniveauet på baggrund af truslen fra aktører, hvis motivation for at ramme Danmark med cyberangreb er drevet af den aktuelle krig i Ukraine. CFCS vurderer, at det er muligt, at særligt pro-russiske hackere vil gå efter mål i Danmark. Det er en ændring af trusselsbilledet sammenlignet med de seneste år, hvor CFCS har vurderet, at cyberaktivister ikke har udvist intention om at ramme danske mål.

Selvom truslen hæves på baggrund af konkrete pro-russiske cyberangreb på europæiske NATO-lande, udgør aktører på begge sider af konflikten, herunder pro-russiske og pro-ukrainske aktører, begge en trussel for aktivistisk motiverede cyberangreb mod Danmark.

Pro-russiske aktivister kan være interesserede i at straffe eller påvirke dansk støtte til Ukraine eller dansk pres på Rusland. Anti-russiske hackere, såsom hackere affilieret med Anonymous, kan være interesserede i enten at straffe organisationer med tilknytning til Rusland eller straffe mål i lande, som de mener ikke gør nok for at støtte Ukraine eller sanktionere Rusland.

Killnet

Killnet er et eksempel på en hackergruppe, der er gået aktivt ind i krigen ved at erklære sit tilhørsforhold til Rusland.

Gruppen har indtil krigens start forsøgt at tjene penge på at udleje sit botnet til brug for andre hackeres overbelastningsangreb. Men efter krigens udbrud har Killnet selv udført aktivistiske overbelastningsangreb til støtte for Rusland.

Killnet hævder bl.a. at have udført overbelastningsangreb mod tyske og lettiske regeringshjemmesider og mod Polens Nationalbank.

Truslen gælder derfor 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.

Kriser i Danmark medfører sjældent cyberaktivistiske angreb
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.

Når CFCS hæver trusselsniveauet, sker det på baggrund af en øget trussel fra aktører uden for Danmark. Der er i mindre grad et cyberaktivistisk miljø i Danmark og generelt kun få eksempler på, at konventionel aktivisme og protester i Danmark har ført til cyberangreb. Situationen i Ukraine vurderes ikke at ændre truslen fra danske cyberaktivistiske miljøer.

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.