CENTER FOR CYBERSIKKERHED

Trusselsvurdering

CFCS hæver trusselsniveauet fra cyberaktivisme mod Danmark fra **MIDDEL** til **HØJ**

Formålet med vurderingen er at orientere om, at CFCS hæver truslen fra cyberaktivisme mod Danmark fra **MIDDEL** til **HØJ** på baggrund af pro-russiske aktivistiske hackergruppers høje aktivitetsniveau samt vilje og kapacitet til at angribe danske mål.

Hovedvurdering

- Truslen fra cyberaktivisme mod Danmark er **HØJ**. CFCS hæver dermed trusselsniveauet fra **MIDDEL** til **HØJ**. Når trusselsniveauet fra cyberaktivisme hæves til **HØJ**, betyder det, at det er sandsynligt, at danske virksomheder og myndigheder vil blive ramt af aktivistiske cyberangreb på kort sigt.

- CFCS hæver truslen fra cyberaktivisme, bl.a. på baggrund af pro-russiske aktivistiske hackergruppers høje aktivitetsniveau mod NATO-lande, herunder Danmark, samt deres øgede kapacitet.

- De pro-russiske hackere angriber løbende mål i sektorer, de anser for at være symbolske for andre landes støtte til Ukraine. Hackerne er særligt gået efter myndigheder og virksomheder inden for transport-, finans- og forsvarssektoren.

- Pro-russiske hackere udfører især simple overbelastningsangreb. Denne type angreb virker forstyrrende og tiltrækker sig opmærksomhed, men har ikke varige eller destruktive konsekvenser for ofrenes systemer.

- Pro-russiske hackere er drevet af en patriotisk dagsorden og motiveres bl.a. af medieomtale.

Analyse

Det er sandsynligt, at danske organisationer igen vil blive mål for cyberaktivistiske angreb. Det skyldes, at pro-russiske cyberaktivister i konteksten af de fortsat øgede spændinger mellem Rusland og Vesten udfører mange angreb mod skiftende mål, som de særligt udvælger inden for en bred vifte af NATO-lande. De pro-russiske hackere angriber løbende bl.a. mål i sektorer, de anser for at være symbolske for andre landes støtte til Ukraine. Hackerne er særligt gået efter myndigheder og virksomheder inden for transport-, finans- og forsvarssektoren.

De pro-russiske cyberaktivister har ikke et særligt fokus på Danmark relativt til andre NATO-lande. De seneste cyberangreb mod danske mål viser dog, at aktivisterne er opmærksomme på danske organisationer som potentielle mål for deres cyberangreb. Det seneste år har de pro-russiske cyberaktivister mere eller mindre konstant udført kortere angrebskampagner, hvor de grupperer målene under bestemte tematikker. Danske mål har eksempelvis både indgået i en angrebskampagne, hvor temaet var europæiske forsvarsministerier, samt i en kampagne, hvor temaet var den danske finanssektor.

Cyberaktivisme udføres af individer og hackergrupper, der udfører cyberangreb for at få mest mulig opmærksomhed på deres dagsorden eller for at straffe organisationer.

Cyberaktivisme er drevet af forskellige ideologiske eller politiske motiver, der strækker sig fra politiske enkeltsager til modstand mod magthavere. Cyberaktivistiske angreb kan derfor også udføres som reaktion på enkelthændelser. Det er sandsynligvis tilfældet med de overbelastningsangreb, der blev udført i slutningen af januar 2023 mod flere danske hjemmesider. Cyberaktivistiske aktører har på sociale medier hævdet at stå bag, og begrundet deres angreb på hjemmesider med bl.a. koranafbrændinger i Sverige og Danmark.

Stigende tilslutning betyder større kapacitet

De pro-russiske cyberaktivistiske hackergrupper formaliserer i stigende grad deres planlægning og eksekvering af angreb. Flere af de mest aktive pro-russiske grupper har desuden oprettet platforme dedikeret til at mobilisere ressourcer til DDoS-angreb.

Pro-russiske hackere udfører især overbelastningsangreb. Denne type angreb virker forstyrrende og tiltrækker sig opmærksomhed, men har ikke varige eller destruktive konsekvenser for ofrenes systemer.

CFCS vurderer, at antallet af følgere og aktive deltagere i de pro-russiske cyberaktivistiske grupper er steget løbende efter Ruslands invasion af Ukraine.

Det er sandsynligt, at den øgede tilslutning til de pro-russiske aktivistiske hackergrupper betyder, at grupperne får kapacitet til at udføre flere og kraftigere angreb.

Den stigende tilslutning betyder eksempelvis, at grupperne får flere medlemmer, der stiller ressourcer til rådighed i botnet, der bruges til DDoS-angreb. De øgede ressourcer, som tilslutningen giver, kan øge DDoS-angrebs styrke og gøre dem sværere at mitigere. DDoS-angrebene vil dog fortsat ikke have en varig eller ødelæggende effekt på systemerne.

DDoS-angreb
DDoS står for Distributed Denial of Service og er et overbelastningsangreb. Hackere udnytter kompromitterede computere til at generere usædvanligt store mængder datatrafik mod en hjemmeside (webserver) eller et netværk, så hjemmesiden eller netværket ikke er tilgængeligt for legitim trafik, mens angrebet står på.

Patriotisk dagsorden og medieomtale driver truslen

De forskellige pro-russiske hackere er alle drevet af den samme patriotiske dagsorden. 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.

Hackernes specifikke gruppetilhørsforhold påvirker ikke truslen i nogen særlig grad, da grupperne angriber med afsæt i samme politiske dagsorden og med de samme angrebsmetoder.

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 tilskriver dem æren for angreb, de udfører. Det er derfor muligt, at en omfattende mediedækning af cyberaktivistiske angreb mod danske mål kan bidrage til at gøre Danmark til et mere attraktivt mål for pro-russiske cyberaktivister.

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 plan-lægning. 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.