CENTER FOR CYBERSIKKERHED

4. juni 2024

TRUSSELSVURDERING

CFCS hæver trusselsniveauet for destruktive cyberangreb mod Danmark fra **LAV** til **MIDDEL**

Trusselsvurderingen skal informere organisationer og beslutningstagere i Danmark om en skærpet trussel fra destruktive cyberangreb. Viden om truslen er bl.a. relevant for beskyttelsen af digitale systemer i samfundsvigtige sektorer.

HOVEDVURDERING

- CFCS hæver trusselsniveauet for destruktive cyberangreb mod Danmark fra **LAV** til **MIDDEL**. Det er muligt, at organisationer i Danmark vil blive udsat for destruktive cyberangreb.

- Trusselsniveauet hæves, fordi Rusland sandsynligvis er blevet mere risikovillig i forhold til at bruge hybride virkemidler med destruktive effekter i europæiske NATO-lande. CFCS vurderer, at denne risikovillighed også omfatter destruktive cyberangreb.

- CFCS hæver trusselsniveauet fra destruktive cyberangreb for Danmark generelt. Såfremt Rusland vil rette destruktive cyberangreb mod Danmark, vil Rusland sandsynligvis vælge blandt et bredt udsnit af mål i samfundsvigtige sektorer.

- Det er mindre sandsynligt, at Rusland i den nuværende situation vil gennemføre destruktive cyberangreb mod Danmark, hvor hensigten er at skabe alvorlige og omfattende konsekvenser for samfundsvigtige funktioner. Mindre omfattende cyberangreb kan dog også få betydelige konsekvenser for offeret og for samfundet.

- Truslen fra destruktive cyberangreb kommer særligt fra russiske statslige hackere, men også fra ikke-statslige hackere med forskellige grader af forbindelser til den russiske stat.

ANALYSE

CFCS hæver trusselsniveauet for destruktive cyberangreb fra **LAV** til **MIDDEL**. Det er muligt, at organisationer i Danmark vil blive udsat for destruktive cyberangreb.

Trusselsniveauet hæves, fordi Rusland sandsynligvis er blevet mere risikovillig i forhold til at bruge hybride virkemidler med destruktive effekter i europæiske NATO-lande. CFCS vurderer, at den øgede risikovillighed også omfatter destruktive cyberangreb. Russiske statslige hackergrupper har i årevis haft kapacitet til at udføre destruktive cyberangreb.

Truslen fra fysisk sabotage er skærpet
PET meddelte den 8. maj 2024, at der er en skærpet trussel fra fysisk sabotage fra Rusland mod militære og civile mål i Danmark med tilknytning til støtten til Ukraine.

Den skærpede trussel skyldes ifølge PET, at personer med mulig forbindelse til de russiske efterretningstjenester har stået bag sabotage i en række europæiske lande. PET vurderer, at Rusland med disse aktiviteter udviser en højere risikovillighed i forhold til at gøre brug af såkaldte hybride virkemidler mod og i Europa. Formålet med de russiske aktiviteter er bl.a. at skabe frygt og usikkerhed, og at svække den folkelige opbakning i Europa til den fortsatte støtte til Ukraine.

Truslen gælder for Danmark generelt

CFCS hæver trusselsniveauet for destruktive cyberangreb for Danmark generelt. CFCS vurderer, at mange typer af organisationer i samfundsvigtige sektorer vil kunne blive udvalgt som mål for eventuelle destruktive cyberangreb.

Det skyldes, at et destruktivt cyberangreb sandsynligvis vil have til formål at påvirke befolkningen og beslutningstagere. Eksempelvis er det sandsynligt, at et formål med destruktive cyberangreb mod Danmark vil være at svække danskernes opbakningen til Ukraine.

Den konkrete fysiske effekt af angrebene vil dermed sandsynligvis være sekundær i forhold til, om angrebene skaber opmærksomhed, hvilket efterlader en lang række potentielle mål.

Udvælgelsen vil dog sandsynligvis været påvirket af, hvor hackerne har adgang eller nemt kan få det.

Destruktive cyberangreb kan få betydelige konsekvenser

Det er mindre sandsynligt, at Rusland i den nuværende sikkerhedspolitiske situation vil gennemføre destruktive cyberangreb, hvor hensigten er at skabe alvorlige og omfattende konsekvenser for samfundsvigtige funktioner. Selvom disse angreb er mindre sandsynlige, vurderer CFCS, at hackergrupper knyttet til Rusland løbende forbereder sig på at kunne udføre den form for destruktive cyberangreb mod Danmark. Sandsynligheden for den type angreb kan derfor stige med kort eller uden varsel.

Mindre omfattende cyberangreb kan få betydelige konsekvenser for offeret og for samfundet. Det kan f.eks. være angreb, der påvirker samfundsvigtige funktioner i begrænset omfang. Selv hvis destruktive cyberangreb ingen konsekvenser har for samfundsvigtige funktioner, kan de skabe utryghed og påvirke samfundet.

CFCS' definition af 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

De hyppigst forekommende destruktive cyberangreb er wiper-angreb, der sletter, overskriver eller krypterer data.

Russiske hackergrupper har før stået bag flere destruktive cyberangreb mod Ukraine og sandsynligvis også mod andre lande. Eksempelvis har Ukraine været udsat for mange wiper-angreb, men også angreb hvor operationelle systemer i kritisk infrastruktur er blevet manipuleret, hvilket har medført strømafbrydelser.

Ruslands øgede risikovillighed vil også kunne komme til udtryk som omfattende DDoS-angreb mod centrale systemer. DDoS-angreb er ikke destruktive, men omfattende DDoS-angreb mod centrale systemer vil potentielt kunne afbryde eller forstyrre samfundsvigtige funktioner i kortere eller længere tid og derved påvirke befolkningen og beslutningstagere på samme måde som destruktive cyberangreb.

Truslen kommer især fra Rusland
Truslen fra destruktive cyberangreb kommer især fra russiske, statslige hackere. CFCS vurderer, at Rusland i den nuværende situation vil forsøge at sløre sin forbindelse til eventuelle destruktive cyberangreb. Derved kan Rusland gøre det vanskeligere for lande, der rammes af de hybride aktiviteter, at reagere med et modsvar.

De russiske statslige hackere kan eksempelvis gøre dette ved at udføre angreb, der ligner kriminelle ransomware-angreb, hvor data bliver krypteret, men efterfølgende ikke kan dekrypteres. Der har tidligere været eksempler på sådanne falske ransomware-angreb.

Det er dog meget sandsynligt, at de ransomware-angreb, der har ramt danske organisationer inden for de seneste år, har været udført af kriminelle hackere, hvis formål var at tjene penge og ikke at ødelægge data eller infrastruktur. CFCS forventer, at ransomware-angreb også fremadrettet vil blive udført af økonomisk motiverede kriminelle hackere i langt de fleste tilfælde.

Statslige hackere kan også forsøge at skjule deres forbindelse til destruktive angreb ved at udgive sig for at være aktivistiske hackere. Det kan de gøre ved eksempelvis at oprette hjemmesider eller konti på forskellige platforme, hvor de udgiver sig for at være cyberaktivister og tager ansvar for destruktive cyberangreb.

Truslen fra ikke-statslige hackere
En anden måde Rusland kan sløre sin involvering i destruktive cyberangreb er ved at forsøge at få andre aktører til at udføre dem. Derfor er der også en potentiel trussel fra ikke-statslige hackere.

Pro-russiske cyberaktivister er et godt eksempel på, hvordan ikke-statslige hackere kan understøtte staters interesser. Det er dog ikke ensbetydende med, at de arbejder direkte for staten. CFCS vurderer, at nogle pro-russiske cyberaktivistiske grupper har forbindelse til den russiske stat.

Den typiske cyberaktivisme er drevet af ideologiske eller politiske motiver og bliver som udgangspunkt udført uafhængigt af stater. Det kan dog være vanskeligt at vurdere en cyberaktivistisk aktørs tilhørsforhold til fremmede stater. I nogle tilfælde er det derfor ikke entydigt, om cyberaktivister handler overvejende på eget eller på en stats initiativ.

Iran udgør også en trussel
Selvom truslen primært kommer fra Rusland, udgør Iran også en potentiel trussel.

En gruppe, der kaldte sig CyberAv3ngers, har f.eks. taget æren for en række destruktive cyberangreb mod dårligt beskyttet operationelt teknisk udstyr, også kaldet OT-udstyr, i vestlige lande. I den forbindelse udpegede gruppen alt udstyr produceret i Israel som legitime mål i konteksten af konflikten mellem Israel og Hamas.

Den amerikanske myndighed Cybersecurity and Infrastructure Security Agency har offentligt attribueret CyberAv3ngers til Irans Revolutionsgarde (IRGC) og sanktioneret seks personer fra IRGC grundet gruppens destruktive cyberangreb mod USA. Angrebene er således et eksempel på, at statslige hackere slører deres angreb som aktivisme.

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.