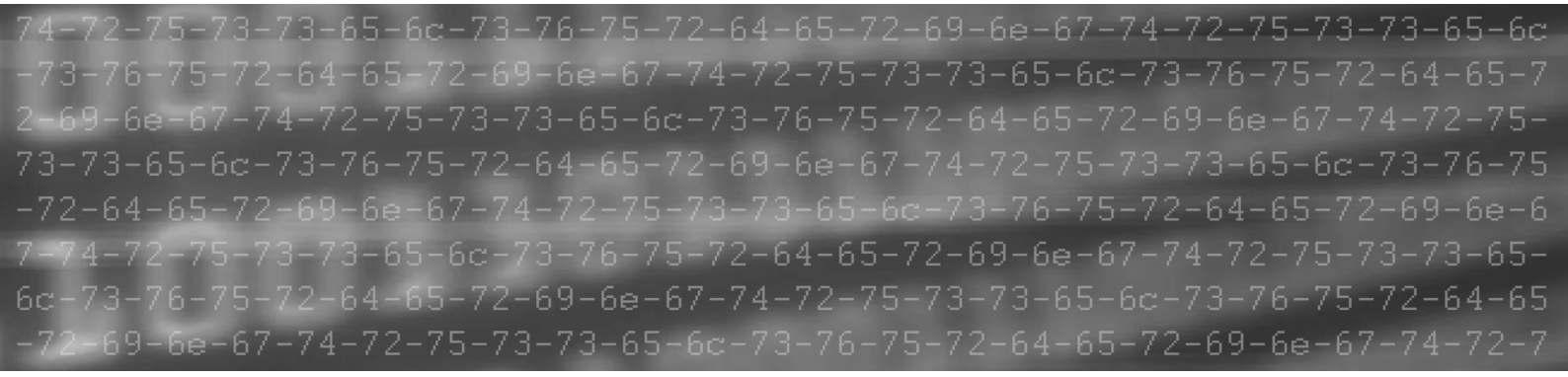
CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Destruktive cyberangreb kan ramme danske virksomheder og myndigheder



Trusselsvurderingsenheden ved Center for Cybersikkerhed

Juli 2017

CENTER FOR CYBERSIKKERHED

6. juli 2017

Trusselsvurdering: Destruktive cyberangreb kan ramme danske virksomheder og myndigheder

Formålet med denne vurdering er at gøre danske virksomheder og myndigheder opmærksomme på, at risikoen for at blive ramt af destruktive cyberangreb er forhøjet, hvis de er til stede i særlige konfliktområder. Virksomheder bør arbejde risikobaseret og segmentere netværk, begrænse administratorrettigheder samt sikre backup og patching.

Hovedvurdering

- Danske virksomheder og myndigheder kan blive ramt af destruktive cyberangreb fra fremmede stater eller organiserede hackergrupper. Det gælder især for virksomheder, der er til stede eller samarbejder i konfliktområder med en større risiko for destruktive cyberangreb.
- Det er sandsynligt, at fremmede stater udfører destruktive cyberangreb forklædt som andre typer angreb, f.eks. ransomwareangreb.
- Det er mindre sandsynligt, at fremmede stater med kapacitet dertil vil rette et egentligt destruktivt cyberangreb mod et industrielt system eller kritisk infrastruktur i Danmark.

Analyse

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) vurderer, at det er muligt, at danske virksomheder og myndigheder kan blive ramt af destruktive cyberangreb fra fremmede stater eller organiserede hackergrupper. Dette gælder særligt virksomheder og organisationer, der arbejder i konfliktområder, hvor der er en større risiko for destruktive cyberangreb, eller hvor der tidligere er forekommet destruktive cyberangreb. I sådanne konfliktområder kan organisationerne blive ramt som følgevirkning af destruktive cyberangreb mod andre mål eller som delmål i større kampagner rettet mod en bredere målgruppe i området.

CFCS har i sin generelle trusselsvurdering beskrevet, hvordan fremmede stater har rettet cyberangreb mod f.eks. industrielle kontrolsystemer i udlandet. Virksomheder, der samarbejder eller på anden vis er til stede i konfliktområder eller områder, hvor fremmede stater med store cyberkapaciteter har interesser, eksempelvis dele af Mellemøsten, fx GCC-landene, Sydkorea i Asien og dele

af Østeuropa, fx Ukraine, bør være opmærksom på truslen fra hackere, der har evnen til at udføre destruktive cyberangreb.

CFCS vurderer det sandsynligt, at hackergrupper udfører destruktive cyberangreb under dække af andre formål, eksempelvis økonomisk kriminalitet. Det er sandsynligt, at NotPetya-kampagnen, der 27. juni 2017 ramte flere internationale virksomheder, herunder danske, er et eksempel på dette. Foreløbige analyser af den anvendte malware samt fraværet af muligheden for at betale løsesum indikerer, at NotPetya var et destruktivt cyberangreb forklædt som et ransomwareangreb.

NotPetya-angrebet 27. juni 2017 er i så fald et af de største destruktive cyberangreb set i Europa og tyder på en øget villighed hos hackere til at benytte dette værktøj.

CFCS vurderer det dog fortsat mindre sandsynligt, at fremmede stater med kapacitet dertil vil rette et egentligt destruktivt cyberangreb mod et industrielt system eller kritisk infrastruktur i Danmark. Men hvis en politisk eller militær konflikt opstår mellem Danmark og en sådan fremmed stat kan infrastruktur og systemer blive mål for denne type cyberangreb.

Et destruktivt cyberangreb er et værktøj, der kan anvendes af forskellige aktører med forskellige formål. Det er altså den ønskede effekt af et cyberangreb, som er afgørende for, om det er destruktivt. CFCS definerer et destruktivt cyberangreb som et cyberangreb, hvor den forventede effekt af angrebet er død, personskade, betydelig skade på fysiske objekter, store økonomiske konsekvenser eller ødelæggelse eller forandring af informationer, data eller software, så de ikke længere kan anvendes.

Anbefalinger

På baggrund af den konkrete trussel har CFCS opstillet følgende anbefalinger, som virksomheder bør inddrage i arbejdet med risikovurderinger og implementering af konkrete sikringstiltag.

- CFCS anbefaler, at organisationens topledelse sikrer, at den beskrevne trussel indarbejdes i organisationens risikovurderinger. Forudsætningerne for at kunne indarbejde specifikke trusler er, at der er overblik over forretningsprocesser, it-infrastruktur og it-processer, og hvor der er sårbarheder.
- Det er hensigtsmæssigt, at adskillelse eller segmentering af it-infrastrukturen/netværk afspejler organisationens involvering på forskellige fysiske lokationer. Segmentering betyder, at netværk opdeles i mindre enheder. På hver enkelt af de mindre enheder/segmenter, bør der implementeres et regelsæt, der definerer de enkelte it-enheders tilladelse til at kommunikere med andre it-enheder i infrastrukturen.
- Brugerrettigheder og administrative rettigheder bør i den sammenhæng begrænses mest muligt, og systempassword og andre password bør være forskellige fra segment til segment.
- Organisationer bør foretage systematisk backup af kritiske informationer, centrale konfigurationsfiler og andre opsætningsdata. Backup-rutinen bør gennemføres med høj frekvens og det

bør løbende kontrolleres, at genetablering af backup fungerer efter hensigten. Samtidig bør placering af backupdata overvejes. Det giver god mening at have off-line backup, som derved ikke er sårbar overfor den beskrevne trussel.

- Følg anbefalingerne i vejledningen fra maj 2017 "Ransomware-angrebet WannaCry – fjernelse af malware". Vær særlig opmærksom på sårbarheder i anvendelse af visse versioner af SMB. CFCS har i publikationen "Cyberforsvar der virker", beskrevet en konkret og prioriteret plan for at mindske risikoen for og håndtere de værste konsekvenser ved cyberangreb. CFCS pointerer her, at særligt opdatering (patch) er vigtig i forhold til den konkrete trussel og vil kunne reducere risikoen væsentligt.
- Gennemprøvede planer for genopretning efter et systemnedbrud kan medvirke til, at en organisation under en hændelse kan implementere de nødvendige og hensigtsmæssige modforanstaltninger, og genoprette forretningen så hurtigt som muligt.
- For at organisationen kan opdage og reagere på afvigelser fra normalbilledet skal organisationen løbende udføre overvågning og logning af relevante netværk og systemer. CFCS har udgivet vejledningen "Logning – en del af et godt cyberberedskab", der kan bidrage med yderligere viden på området.
- Trusselsbilledet på cyberområdet er meget dynamisk og kan ændre sig hurtigt. Organisationer bør derfor følge den politiske udvikling i de områder, hvor man er til stede og være beredt på at tilpasse netværk og sikkerhed til nyopståede trusler.

FE bruger denne skala for sandsynlighed i analyser: