MISSION 1: Operation CyberGuard

CyberGuard missionen

Hvad fylder i medierne? Nøgleord som geopolitik, hybrid krig, deep fake og hackergrupper er blevet kendte ord i nyhedsbilledet – både nationalt og internationalt. Derfor skal I på en mission, hvor I skal lave en dybdegående undersøgelse af en hackergruppe efter eget valg for at undersøge og lære om deres motiver, mønstre og angrebstyper.

Fagforslag:
Samfundsfag, International Økonomi, Sprog (research på engelsk), Informatik m.m.

Pro-russiske hackergrupper

Der findes rigtig mange professionelle hackergrupper, og nogle af dem er f.eks. de pro-russiske hackergrupper APT28 (Fancy Bear) og APT29 (Cozy Bear). Grupperne har været involveret i store cyberangreb med politisk indblanding og spionage, og flere af dem modtager sågar økonomisk støtte af den russiske stat.

Deres typiske angrebsmetoder inkluderer **phishing**, **DDoS**, **malware** og andre målrettede angreb på institutioner.

Pro-russiske hackergrupper udfører ofte målrettede phishing-kampagner. Her gør de ofte brug af det, man definerer som **social engineering** for at narre brugere til at klikke på skadelige links eller vedhæftede filer. Social engineering er brugen af bedrag til at manipulere mennesker til at give adgang til eller videregive oplysninger eller data.

Hvad betyder geopolitik for trusselsbilledet?

Geopolitik refererer til forholdet mellem geografi og politik, hvor nationers handlinger og beslutninger formes af deres geografiske placering, territoriale interesser og internationale relationer.

Efter Ruslands invasion af Ukraine i 2022, har det geopolitiske miljø ændret sig markant, og vi ser et øget antal af pro-russiske hackergrupper, der udfører cyberangreb på forskellige lande, som direkte eller indirekte støtter Ukraine.

Hvad betyder en hybrid krig?

En hybrid krig indebærer brugen af forskellige metoder og strategier, både konventionelle og ikke-konventionelle, for at opnå politiske mål.
Dette kan være cyberangreb, propaganda og økonomisk pres, hvorfor hybrid krigsførelse adskiller sig markant fra de traditionelle militære handlinger, som man før brugte i krig. Det har vi også tydeligt kunnet mærke i Danmark efter Ruslands invasion af Ukraine i 2022.

Hvordan vil danske virksomheder kunne mærke, at f.eks. pro-russiske hackergrupper bliver mere aktive?

Danske virksomheder har på flere måder mærket en stigende aktivitet hos pro-russiske hackergrupper.
Det ses ved en stigning i målrettede cyberangreb mod danske virksomheder og organisationer, hvor forsøg på at stjæle fortrolige oplysninger eller forstyrre driften, er blevet langt mere udbredt end tidligere.

Hvordan politik har ændret de cyberkriminelles dagsorden

Politik får stadig større indflydelse på cyberkriminalitet, hvilket ses tydeligt, idet hackergrupper i stigende grad retter deres angreb efter politiske mål og dagsordener for at påvirke geopolitiske forhold. Skiftende politiske dagsordner påvirker i høj grad udviklingen inden for cyberkriminalitet.

Det bliver især institutioner og organisationer med politisk betydning, som bliver gruppernes primære mål for angreb.

Samtidig har de cyberkriminelle udvidet deres angrebsmetoder fra ren politisk spionage til også at involvere sig i økonomisk-motiverede angreb. Denne udvikling understreger behovet for at øge opmærksomheden på cybersikkerhed og evnen til at tilpasse sig den dynamiske trussel fra politiske hackergrupper.

DDOS angreb som følge af Mette Frederiksens udtale om støtte til Ukraine

Et eksempel på et politisk motiveret angreb fra en pro-russisk hackergruppe, finder sted i februar 2024, hvor en række danske virksomheder blev udsat for det, der hedder **DDOS-angreb** (overbelastningsangreb), herunder f.eks. Københavns Lufthavn og Aarhus Kommune. Hackergruppen udførte angrebet som en form for "gengældelse" for den danske støtte til Ukraine.

På Telegram skriver NoName057, at angrebene er gengældelse for Danmarks løfte om at støtte Ukraine økonomisk i ti år, hvilket Mette Frederiksen havde annonceret ugen forinden angrebet.

Selvom et DDoS-angreb på papiret lyder skræmmende, ligger der typisk ikke meget andet i dem end skræmmeeffekten. Selve angrebet er ikke særlig farligt, da de for eksempel ikke får adgang til data/systemer eller andet, og i de fleste tilfælde betyder det derfor "kun" at en hjemmeside er ude af drift i en kortere periode.

Nye trusler opstår med ChatGpT og AI (Deep Fake)

Ny teknologi giver nye trusler. Hackeres anvendelse af Chat GpT og AI, især hvad angår deep fake-teknologien, har markante implikationer på trusselsbilledet.

Deep Fake gør det muligt at skabe overbevisende manipuleret indhold som falske videoer og lydoptagelser.

Denne teknologi øger mængden af desinformation og underminerer troværdigheden i offentlige oplysninger.

I har måske set kendte danske profiler, hvor der bliver manipuleret med deres billeder, så der på Facebook, eksempelvis florerer budskaber om, at de er syge, døde eller har været udsat for andre tragiske hændelser. Billederne ser helt troværdige ud, får masser af likes og pludselig florerer falske budskaber digitalt.

Den teknologiske udvikling vil kræve skærpet opmærksomhed på at bekæmpe misinformation samtidig med, at digitale autentifikationsmetoder skal styrkes for at bevare integriteten af det digitale rum.

Hvem truer os?

Vi kan gruppere aktører, som truer cybersikkerheden i følgende grupperinger:

- **Insiders** – Betroede medarbejdere med onde intentioner
- **Cyberkriminelle** – Folk og organiserede grupper med onde hensigter
- **Script kiddies** – Nybegynder-hackere, der bruger andres ideer og kode
- **Gray hats** – Folk, der arbejder med cybersikkerhed, men kan finde på at bryde loven
- **Hacktivists** – Onlineaktivister, der hacker sig til deres mål, ofte om at få viden frem om en sag eller situation
- **Statsstøttede hackere** – Hackere fra andre lande, der ofte har mange ressourcer, som de får tildelt af deres regering. Man plejer at sige: "hvis de vil ind, så kommer de ind!"

Hvordan angriber cyberkriminelle?

Man plejer at inddele et cyberangreb i følgende forskellige trin:

- **Informationsindsamling** - de kriminelle finder ud af, hvordan og hvor de bedst kan angribe et digitalt mål med success.
- **Network mapping/scanning** - her forsøger de kriminelle af få overblik over, hvordan det digitale mål er opbygget.
- **Sårbarhedssøgning** - hvor er hjemmesiden f.eks. svagest, er det i netværket, er det ved brug af hjemmesiden eller noget tredje?
- **Udnyttelse af sårbarheder (indbrud)** - udforskning af systemet – kan være en lang fase!
- Udførelse af skadelig aktivitet - hacke, overtage en profil på systemet eller andet.
- **Etablering af malware/backdoor**. Malware er ondsindet software, og hackerne bruger ofte en "backdoor", når de skal installere det. En "backdoor" er som ordet refererer til en alternativ adgang til fx et system, netværk eller applikation, der omgår de normale sikkerhedsforanstaltninger.
- **Sletning af sporene**. Gerningsstedet forlades

HUSK, at brugeren tit er det svageste led, og det er der, de første angreb sker!

Jeres mission

I skal nu påbegynde jeres mission, som skal gøre jer meget klogere på hackerne - hvad der motiverer dem, og hvilken trussel de kan udgøre!

Missionen består af følgende fem trin:

1. I skal nu forsøge at identificere 2-3 hackergrupper, der potentielt kan udgøre en trussel mod Danmark, og kort begrunde jeres svar.
2. I skal derefter udvælge én gruppe og undersøge, hvem de er, hvad deres motiv for deres angreb er, hvilke mål de forfølger og hvilke typer angrebsvektorer, de bruger.
3. Undersøg et af deres tidligere angreb og angrebsmønstre (hvad gjorde de? hvorfor gjorde de det? hvad var skadens omfang?).
4. Analysér, hvilke danske organisationer eller virksomheder, som kunne være i deres søgelys.
5. Diskutér hvordan brugen af Chat GPT og AI kommer til at påvirke trusselsbilledet og overvej, hvordan AI-assistance kunne have ændret angrebet fra pkt. 3.

Jeres præsentation

I skal forberede en præsentation, hvor I redegør for, hvad I er kommet frem til i jeres arbejde med de fem trin. Præsentér den information, I har fundet, og hvilke tanker I gør jer om det.

Præsentationen må max tage 5 minutter.

Det er helt op til jer, hvordan I præsenterer: Det kunne f.eks. være med en **PowerPoint** præsentation, gennem et kort **skuespil**, en **videopræsentation** eller noget **helt andet**. Det vigtigste er, at I får formidlet jeres arbejde med missionen tydeligt og grundigt.

Deltag i en national konkurrence

Cybermissionen er en national konkurrence, hvor alle ungdomsuddannelser har mulighed for at være med. Alle klasser må deltage i konkurrencen med ét løsningsforslag. Man deltager i konkurrencen ved at lave en videooptagelse af sin præsentation og sende den til Styrelsen for It og Læring. Alle videoer vurderes af Cybermissionens dommerpanel.

Videoen skal uploades af den underviser, som har tilmeldt jer Cybermissionen. I finder link til uploadfunktionen på konkurrencens hjemmeside: https://cybermissionen.cyberskills.dk, hvor I kan læse mere.