CENTER FOR CYBERSIKKERHED

Trusselsvurdering

# Hackere misbruger legitime programmer i cyberangreb

# Trusselsvurdering: Hackere misbruger legitime programmer i cyberangreb

Formålet med denne trusselsvurdering er at orientere om en angrebsteknik, som er en del af cybertruslen mod danske virksomheder og myndigheder. Trusselsvurderingen kan bruges af virksomheder og myndigheder til at sætte fokus på angrebsteknikken, og hvordan man beskytter sig mod den. Trusselsvurderingen er primært rettet mod organisationernes it-teknikere og it-ledelse.

Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Tlf: 3332 5580
E-mail: cfcs@cfcs.dk
www.cfcs.dk

1. udgave februar 2020

**Hovedvurdering**

- Hackere anvender ofte en angrebsteknik mod myndigheder og virksomheder i Danmark og i udlandet, hvor de misbruger ofrenes egne programmer til at udføre cyberangreb.
- Angrebsteknikken gør det vanskeligt at opdage angrebet og kræver en proaktiv og helhedsorienteret beskyttelse.
- Både fremmede stater og kriminelle benytter angrebsteknikken som supplement til eller i stedet for at angribe med malware.
- I denne type angreb misbruger hackere ofte forudinstalleret software i Windows, såsom PowerShell.
- Det er relativt nemt for hackere at anvende angrebsteknikken, fordi metoden er blevet integreret i flere såkaldte pentest-værktøjer, som er frit tilgængelige.

## Analyse

Hackere med skadelige intentioner bruger ofte en angrebsteknik mod myndigheder og virksomheder i Danmark og i udlandet, hvor de misbruger ofrenes egne programmer til at udføre cyberangreb. Med egne programmer menes programmer, der enten er forudinstallerede sammen med styresystemet, eller programmer som ofret selv har installeret og anser som legitime. Denne angrebsteknik kaldes også *"living off the land"*, fordi hackerne så at sige opererer ved at udnytte de programmer, de finder på ofrets systemer. Angrebsteknikken er ikke ny, men den bliver brugt i stigende grad og udvikler sig.

Teknikken er effektiv og kan bruges af hackere til at opnå samme mål, som hvis de havde angrebet med malware.

Metoden bliver både benyttet i forbindelse med cyberspionage og cyberkriminalitet, og der har været mange eksempler i udlandet på denne type angreb de seneste år. Der har også været eksempler i Danmark.

**Post-exploit-metode**

Denne trusselsvurdering fokuserer på, hvordan hackere misbruger legitime programmer hos ofret til at opnå deres mål *efter*, de har kompromitteret ofret. Det kaldes ofte for post-exploit. I forhold til Cyber Kill Chain®-modellen er det primært stadierne: afsendelse & udnyttelse, installation og kommando & kontrol. De enkelte stadier kan ses på Lockheed Martins hjemmeside eller i bilag 1. Post-exploit dækker eksempelvis over aktiviteter, hackerne bruger til at opnå administratorrettigheder eller metoder, de bruger til at eksfiltrere data fra ofret.

Hackere kan også misbruge legitime programmer til indledningsvist at kompromittere ofre. De kan f.eks. gøre det via macro'er. Disse metoder er dog ikke en del af denne trusselsvurdering, da den fokuserer på post-exploit metoder.

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) sætter i denne vurdering ikke et trusselsniveau for angrebsteknikken. CFCS vurderer og formidler trusselsniveauer ud fra, hvilket formål anvendelsen af cyberangreb har for de aktører, der anvender dem. Formålet med cyberangreb kan eksempelvis være at udføre spionage, cyberkriminalitet, cyberaktivisme eller cyberterror. CFCS har fastsat trusselsniveauer for det nationale niveau og en række samfundsvigtige sektorer i trusselsvurderinger, der kan findes på CFCS' hjemmeside.

### Denne type angreb er generelt svære at opdage

Denne angrebsteknik er særligt problematisk, da den er svær at opdage. Idet hackerne misbruger legitime programmer, som allerede er installeret på ofrets systemer, opdages den ondsindede aktivitet ofte ikke af typiske antivirusprogrammer hos virksomheder og myndigheder.

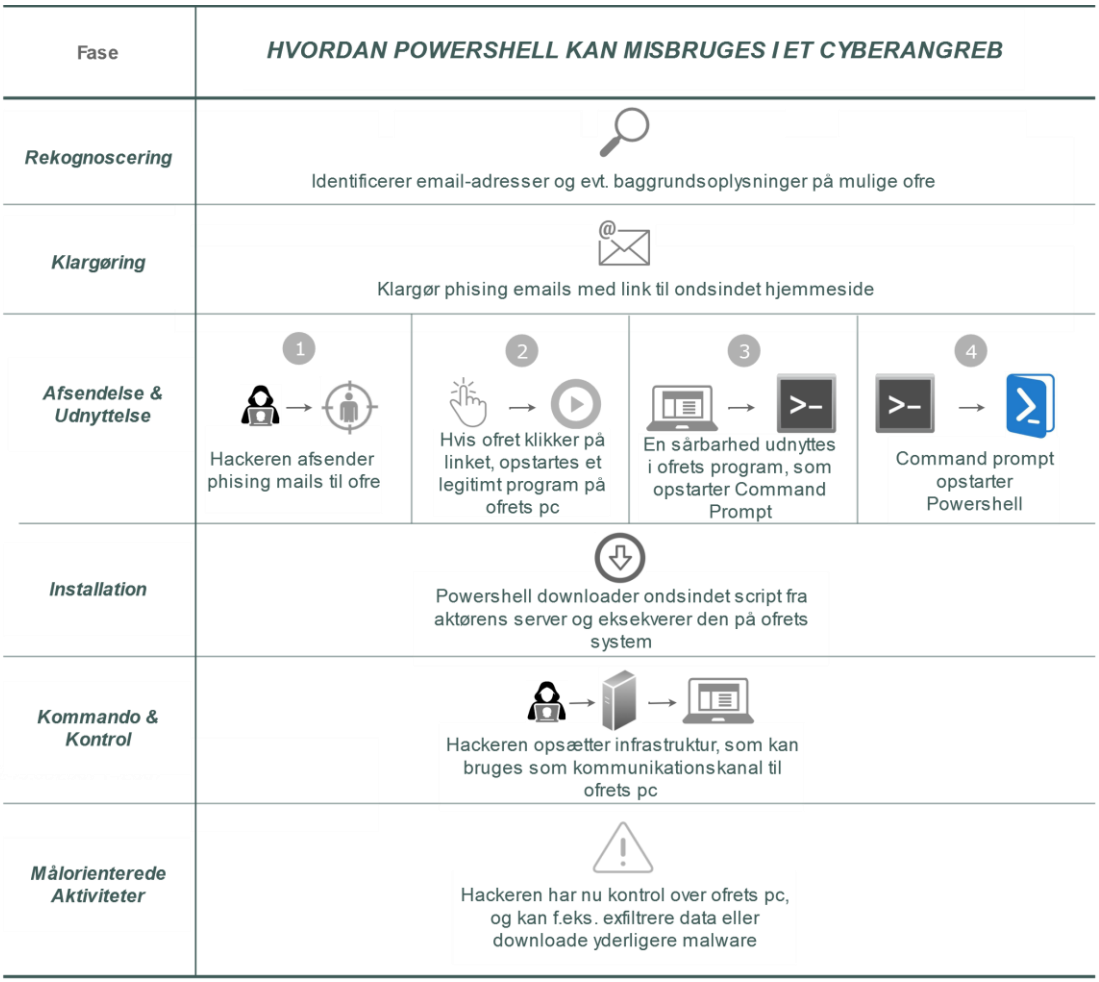
Denne type angreb er ydermere svær at opdage, fordi de ofte er filløse. I filløse angreb anvender hackerne ikke deres egne eksekverbare filer til at udføre skadelig kode, men de misbruger derimod legitime ekse-

kverbare filer, der allerede er på ofrets systemer, til at udføre koden. Det gør, at den ondsindede aktivitet kun foregår i hukommelsen på ofrets system og ikke på harddisken.

Det er særligt ift. det forhold, at angrebsteknikken adskiller sig fra mere traditionelle cyberangreb med malware. Ved cyberangreb med malware installerer aktører skadelige filer på ofrets system, som efterfølgende skal eksekveres. Når aktører i stedet misbruger ofrets programmer, er der ingen udefrakommende eksekverbare filer i den del af angrebet.

Misbrug af ofrets egne programmer kan dog også udføres i kombination med malware. Aktøren kan f.eks. skaffe sig relevante adgange i et netværk via ofrets egne programmer for at lukke ned for ofrets antivirus, og derefter kan hackerne ubemærket installere malware. Malwaren kan f.eks. være ransomware.

I cyberangreb, som misbruger ofrets egne programmer, kan den indledningsvise adgang til ofret også ske på mange forskellige måder. Det kan eksempelvis ske med almindelige kendte metoder som links i phishing-mails, kompromittering af leverandører eller f.eks. ved at udnytte sårbarheder i programmer.




Figur 1: Illustration af, hvordan PowerShell kan misbruges i et cyberangreb

**Cyberangreb, som misbruger ofrets programmer, kræver en mere aktiv beskyttelse**
Det kræver en mere proaktiv og helhedsorienteret tilgang til beskyttelse af ens netværk, hvis man skal imødegå og opdage angreb, hvor hackere misbruger ens legitime programmer. Det nødvendiggør, at man som organisation dels forsøger at forebygge, at hackere misbruger ens systemer, men i høj grad også at man har ressourcer til at opdage det, hvis det sker.

Nogle af modforanstaltningerne kan kræve mange ressourcer, men en relativ nem måde at imødegå denne type angreb kan være at begrænse brugen af visse programmer til relevante personer i organisationen. Mange brugere i f.eks. myndigheder har sædvanligvis ikke brug for programmer til it-administration på deres enheder, hvorfor man kan fjerne disse programmer og mindske angrebsfladen.

Når det, trods ovenstående tiltag, alligevel lykkes hackere at misbruge legitime programmer, kræver det ofte mere beskyttelse end en antivirus-program typisk leverer. Det skyldes, at traditionel antivirusbeskyttelse primært identificerer ondsindet aktivitet i netværk eller på enheder på baggrund af analyser af filer og i nogle tilfælde processer. Et antivirusprogram analyserer således, om filer på enheden eller netværket er ondsindede på bagrund af signaturer. Antivirussen kan efterfølgende slette filer eller sætte dem i karantæne på baggrund af signaturen, hvis der f.eks. er tale om malware.

Det kan give en udfordring i forhold til angreb med ofrets egne programmer, fordi programmerne netop er legitime og som regel har tilladelse af antivirusprogrammer til f.eks. at eksekvere kommandoer. Herudover kan den ondsindede aktivitet helt eller delvist udføres filløst, som beskrevet ovenfor.

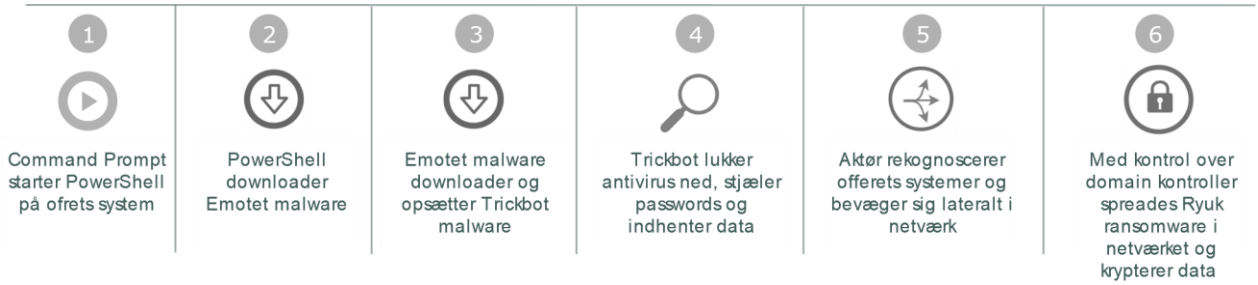
For at opdage denne type angreb er det altså ikke tilstrækkeligt blot at scanne filer, som downloades og eksekveres. Detektering af angrebsteknikken kræver analyse af aktiviteten i legitime programmer, som virksomheden eller myndigheden normalt anvender. Det kan være ved såkaldte endpoint-baserede programmer, som overvåger de enkelte brugeres PC. Intrusion Detection Systems (IDS) kan også bruges til at overvåge netværkstrafik og til at detektere dele af angrebsteknikken, f.eks. når aktøren bevæger sig mellem maskinerne på netværket. Se flere anbefalinger ift., hvordan man kan imødegå disse angreb afslutningsvist i trusselsvurderingen.

**Angreb, som misbruger ofrenes programmer, sker hyppigere**
Der har været adskillige cyberangreb de seneste år, hvor aktører har misbrugt ofres egne programmer til cyberangreb, heriblandt også mod danske mål.

Teknikken anvendes både i målrettede avancerede cyberangreb og i simplere, mindre målrettede angreb fra aktører med relativ få it-kompetencer. Det er sandsynligt, at angrebsteknikken bliver brugt oftere fremover.

**Cyberangreb, der har misbrugt ofrets programmer**
Den norske softwareleverandør Visma offentliggjorde i februar 2019, at den var blevet kompromitteret. It-sikkerhedsfirmaet, som offentliggjorde en større rapport om cyberangrebet, pegede på, at aktøren havde misbrugt programmer i Vismas systemer i angrebet. Det fremgik af rapporten, at aktøren tidligere har brugt samme angrebsteknik mod andre ofre.

Ifølge åbne kilder misbrugte aktøren bag malwaren Lockergoga, som blandt andet ramte Norsk Hydro i marts 2019, også ofrets egne programmer i angrebet. Aktøren misbrugte i dette tilfælde windows-programmer til at sprede malwaren.




Figur 2: Eksempel på cyberangreb, hvor ofrets egne programmer misbruges til at sprede ransomware på ofrets netværk

**Windows-software udnyttes ofte i cyberangreb**
Der findes mange legitime programmer, som misbruges i cyberangreb udført af statsstøttede hackere og kriminelle. Når disse programmer misbruges, er det ikke, fordi programmerne er mere sårbare end andre. Det skyldes i højere grad, at de er meget effektive værktøjer i hænderne på hackere, at de ofte er tilgængelige hos mange ofre, og at de er relativt simple at betjene. Herudover skjuler de hackernes aktivitet, da det er værktøjer, som ofret selv har installeret og bruger.

Ofte misbruger hackere programmerne til at forsøge at opnå større rettigheder, så de kan lave deres egne administratorkonti. Målet med dette kan blandt andet være at kunne bevæge sig videre til andre maskiner i miljøet. Dette kaldes også lateral bevægelse i netværk.

**Eksempler på programmer, som kan misbruges i cyberangreb**
PowerShell: Windows PowerShell har i flere år været en del af Microsoft Windows. Det er udviklet til brug for it-administratorer til f.eks. at udføre konfigurationer og automatisere simple opgaver.

PowerShell kan misbruges til at opnå fuld kontrol over mange systemmæssige funktioner i Windows. Herudover kan aktører misbruge PowerShell til at udføre skadelige kommandoer direkte i hukommelsen på ofrets system.

Windows Management Instrumentation (WMI):Er et administratorværktøj, som bruges til at administrere servere eller enheder på netværk. Værktøjet kan f.eks. bruges til opsætning af forskellige system-sikkerhedsindstillinger.

WMI kan misbruges til flere ting eksempelvist at udføre rekognoscering eller lateral bevægelse i netværk.

PsExec: Er et værktøj, som via fjernadgang kan bruges til at eksekvere processer direkte på andre enheder. Kommandoer kan sendes via Windows Command Prompt.

PsExec kan misbruges til lateral bevægelse i ofrets netværk.

PowerShell er et af de foretrukne programmer for hackere til at angribe med, og det er sandsynligt, at PowerShell bliver misbrugt mere i cyberangreb fremover. PowerShell har desuden den fordel for angriberne, at angreb med dette værktøj kan udføres filløst, hvilket gør detektering af ondsindet aktivitet endnu vanskeligere for ofret.

PowerShell kan f.eks. bruges til at udføre rekognoscering eller eksekvere kode direkte på ofrets enhed. Hackere kan bruge det til bl.a. at omgå en firewall, lukke antivirus ned, installere skadelige programmer eller forsøge at bevæge sig videre til andre af virksomhedens eller myndighedens netværk.

Ofte forsøger aktører også at skjule deres aktivitet i netværket ved at tilsløre det ondsindede PowerShell-kode, som eksekveres på ofrets system. Hackerne forsøger dermed at undgå, at koden er manuelt læsbar. Det kan f.eks. være kodet som Base64.

**Pentest-værktøjer anvender også angrebsteknikken**

PowerShell er i de seneste år blevet indarbejdet som en central del af flere pentest-værktøjer. Det gør det relativt nemt for ondsindede hackere at anvende denne angrebsteknik.

**Pentest**
En penetrationtest er en øvelse, hvor et hold af etiske hackere udfører cyberangreb mod udvalgte systemer for at teste og evaluere cybersikkerheden. En pentest kan dermed være med til at danne grundlag for en risikovurdering af en virksomheds it-sikkerhed.

Der findes i dag flere forskellige pentest-værktøjer, som er udviklet til at hacke med. Værktøjerne er udarbejdet af it-sikkerhedseksperter til at udføre sikkerhedsundersøgelser og teste it-sikkerhed i organisationer. Værktøjerne kan dog også misbruges. Pentest-værktøjer er tilgængelige for alle og flere kan findes gratis på internettet, mens andre koster penge.

Indarbejdelsen af PowerShell i pentest-værktøjer har gjort det meget nemt at misbruge programmet til cyberangreb.

**Populære pentest-værktøjer, som kan misbruge PowerShell**

Cobalt Strike

Er software, som er udviklet til simulering af avancerede angreb til brug for legitime sikkerhedsundersøgelser. Det består af flere moduler med forskellige egenskaber til at udføre cyberangreb i alt fra rekognoscering, phishing og post-exploit værktøjer mm. Post-exploit kan Cobalt Strike blandt andet bruges til at eksekvere kommandoer, key-logging, overførsel af filer, eskalering af privilegier og lateral bevægelse i netværk.

PowerShell Empire

Blev designet til sikkerhedsundersøgelser som et værktøj, der skulle simulere statsstøttede hackerangreb. Værktøjet giver mulighed for lateral bevægelse i netværk, herunder at eskalere privilegier, key-logging og at eksfiltrere passwords eller information.

PowerShell Empire anvendes primært post-exploit og er baseret på PowerShell, men det har også andre moduler som f.eks. giver mulighed for at udføre angreb med ondsindede DLL-filer.

Mimikatz

Et værktøj, som er designet til at stjæle passwords og eskalere privilegier ved forskellige metoder, f.eks. pass-the-hash. Mange af Mimikatz' funktioner kan automatiseres med PowerShell, hvilket giver hackere mulighed for at bevæge sig hurtigt rundt i ofrets netværk.

Mimikatz indgår også som modul i andre pentest-værktøjer, f.eks. Cobalt Strike og PowerShell Empire.

Der findes mange andre effektive pentest-værktøjer end de, som er nævnt overfor, f.eks. værktøjerne Kerberoast og Dumpert.

Pentest-værktøjer tilpasses også løbende. Nogle udviklere af pentest-værktøjer er begyndt at skrive i f.eks. .NET C# i stedet for PowerShell. Det gælder for open-source værktøjet BloodHoundAD. Det skyldes sandsynligvis, at flere organisationer er begyndt at begrænse adgangen til PowerShell i deres netværk.

Det er attraktivt for hackere at bruge pentest-værktøjer. Med pentest-værktøjer kan hackerne bruge de programmer, som i forvejen findes på det pågældende netværk, f.eks. PowerShell, til at udbygge deres forståelse og adgang til netværket, ofte uden de behøver avanceret malware til at opnå deres endelige målhandlinger. Dette svarer til trin syv i Lockheed Martins Cyber Kill Chain®. Både statslige aktører og cyberkriminelle bruger værktøjerne til at udføre cyberangreb med.

I februar 2019 blev den maltesiske bank, Bank of Valletta, angrebet i et digitalt bankrøveri. Aktøren forsøgte at stjæle 13 mio. EUR, hvilket svarer til omtrent 100 mio. kroner. Det er sandsynligt, at aktøren misbrugte PowerShell i angrebet.

Pentest-værktøjer bliver også anvendt af grupper eller individer med relativt få it-færdigheder, da værktøjerne er intuitive og lette at benytte.

Udviklerne af pentest-værktøjer er ofte hurtige til at understøtte nye sårbarheder i deres værktøjer kort efter, de er offentliggjort eller først set anvendt af hackere. Eksempelvist blev sårbarheden BlueKeep, som blev offentliggjort af Microsoft i midten af maj 2019, inkorporeret i et pentest værktøj allerede i løbet af juli 2019.

## Rådgivning

På trods af karakteren af de beskrevne angreb kan en organisation stadig begrænse risikoen for at blive ramt. Det primære fokus bør som udgangspunkt være at holde potentielle angribere ude af organisationens systemer og netværk. Det kan bedst ske ved eksempelvis at følge anbefalingerne i Center for Cybersikkerhed's vejledning "Cyberforsvar der virker". Herved vil man kunne afværge en meget stor del af angrebene.

Selv om man følger de bedste råd, kan man dog ikke afværge alle angreb. Derfor er der en række yderligere sikkerhedstiltag, som en organisation med fordel kan gennemføre. På trods af, at mange af dem kan omgås, er de dog stadig relevante at overveje, da de kan forsinker angriberen i sit forehavende og dermed øger chancen for, at man opdager det.

Generelt bør myndigheder og virksomheder løbende overveje behovet for at have værktøjer installeret, som ikke anvendes. Nedenstående forhold er fokuseret på PowerShell, ligesom trusselsvurderingen generelt har fokus på værktøjet. Mange af forholdene gælder dog også for andre værktøjer end PowerShell.

Vurder, om der er et reelt behov for at have Powershell på den enkelte pc eller server. Er der ikke dette, bør Powershell afinstalleres. Er der et reelt behov, så sørg for at begrænse adgangen til og funktionaliteten af Powershell. Funktionaliteten kan eksempelvis begrænses ved brug af "Constrained Language mode", der er tilgængelig i Powershell fra og med version 5. Her ved begrænser man mulighederne for afvikling af ondsindede scripts som eksempelvis Invoke-Mimikatz. Det anbefales, at man altid anvender seneste version af PowerShell og afinstallerer tidligere versioner.

I forhold til at beskytte passwords i systemet findes der en funktion i Windows Defender, Windows Defender Credential Guard, som kan gøre det sværere for aktører at stjæle og udnytte passwords. På Microsofts hjemmeside findes mere information om, hvordan funktionen bruges under emnet: "Manage Windows Defender Credential Guard"

I vejledningen "Cyberforsvar der virker" er et af de grundlæggende sikringstiltag "whitelistning" af programmer. Til det kan man f.eks. anvende AppLocker, der er inkluderet i Windows 10. Man kan bruge AppLocker til at begrænse hvilke Powershell-scripts, der kan afvikles. Vær dog opmærksom på de begrænsninger i AppLocker, som desværre gør, at denne form for beskyttelse kan omgås.

I PowerShell Version 5 har man mulighed for at aktivere og opsamle en række logs. Herved kan uønsket aktivitet potentielt blive opdaget. Logningen bør ske på flere niveauer, således at man øger chancen for at opdage uønskede aktiviteter. Man bør aktivere:

- Script block tracing, der opsamler alle blokke af PowerShell kode, der afvikles.
- Module/Pipeline logging, der registrerer alle detaljer om det som PowerShell afvikler herunder hvilke kodemoduler der inddrages.
- Transcription, der sikrer oprettelse af en post i loggen for hver PowerShell session og inkluderer al input og output, der optræder i den sammenhæng.
- Engine Lifecycle logging, der sikrer logs over opstart og terminering af PowerShell værter samt alle parametre (værdier), der sendes og modtages fra værten. Engine Lifecycle logging er som udgangspunkt aktiveret.

Generelt gælder det at logning, og opsamling af disse fra udstyr og systemer i organisations infrastruktur, er afgørende for myndigheder og virksomheders evne til at opdage et cyberangreb hurtigt og efterfølgende effektivt afdække konsekvensen. For mere information om brug af logning henvises til CFCSs vejledning: "Logning – en del af et godt cyberforsvar", som kan findes på CFCS hjemmeside.

For yderligere information om opsætning af PowerShell henvises der til Australian Cyber Security Centres vejledning "Securing PowerShell in the Enterprise", som løbende opdateres.

Herudover kan det også generelt anbefales at læse Australian Cyber Security Centres vejledning "Essential Eight", som er en række kortere konkrete anbefalinger om, hvordan man kan mindske angrebsfladen for hackere.

**Segmentering af netværk**

Et andet tiltag kan være at se på topologien i ens netværk og om muligt iværksætte en opdeling af dette i en række segmenter (sikkerhedszoner). Segmentering af netværk giver meget sikkerhed for begrænsede midler. Formålet med at segmentere netværk er at skabe to eller flere uafhængige miljøer, således at en angriber, virus eller malware ikke har adgang til hele netværket samtidig. Derudover giver segmentering mulighed for implementering af forskellige sikkerhedsprocedurer og tekniske tiltag i forskellige segmenter på baggrund af det enkelte segments kritikalitet.

CFCS anbefaler, at man ved valg af segmentering anvender disse fire skridt:

1. Identificer grupper af komponenter eller netværk, som har et forretningsmæssigt behov for at kommunikere.

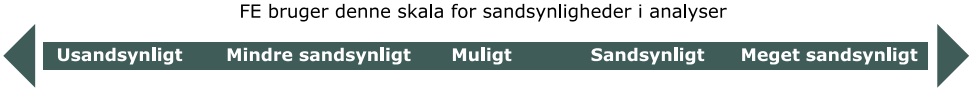
2. Vurder om der er behov for yderligere opdeling i sikkerhedszoner i de forretningsmæssige fællesskaber betinget af forskellige sikkerhedsbehov.

3. Definer de forbindelser mellem sikkerhedszoner, der er nødvendige for at tilgodese forretningsbehovet.

4. Etabler og vedligehold et overblik, således at der kun er én forbindelse eller ét punkt for dataudveksling mellem forskellige segmenter eller sikkerhedszoner.

Efter at have valgt segmenteringen kan man gå i gang med at vurdere, hvordan forbindelserne beskyttes bedst, herunder valg af tekniske tiltag, opsætning af jump-stations, demilitariserede zoner, lognings- og detektionsmekanismer. Backup og systemgenoprettelse bør have en særlig overvejelse i forbindelse med segmentering. Som udgangspunkt bør backup opbevares i separate netværk.

FE bruger denne skala for sandsynligheder i analyser



## **Bilag 1:** Cyber Kill Chain®-modellen

Cyber Kill Chain®-modellen giver en ramme til at analysere og forebygge cyberangreb. Modellen er oprindeligt udviklet af den amerikanske forsvars- og sikkerhedskoncern Lockheed Martin. Modellen anvendes bredt i både den offentlige og private sektor, og fastlægger oprindeligt syv kronologiske faser, som en hacker typisk gennemgår under et cyberangreb. I denne rapport er faserne "afsendelse" og "udnyttelse" imidlertid lagt sammen til én fase for at lette formidlingen. Ved at operationalisere en hackers aktiviteter som én sammenhængende 'kæde' af nødvendige aktiviteter, er det muligt at kortlægge angriberens specifikke angrebsmønster og udvikle skræddersyede sikkerhedsforanstaltninger til hver fase. De syv faser er:

- **Rekognoscering:** Hackeren planlægger sit angreb, og foretager den nødvendige research og identificerer potentielle ofre, som giver hackeren mulighed for at indfri sine mål. Ofre kan være alt fra en tilfældig sårbar server til målrettede angreb mod enkeltindivider eller organisationer af særlig interesse.
- **Klargøring:** På baggrund af den indledende rekognoscering gør hackeren sig klar til angreb ved at identificere eller selv udvikle de ondsindede redskaber, som kan bruges til at kompromittere sit offer.
- **Afsendelse:** Hackeren afsender ondsindede redskaber til sit offer f.eks. via e-mail, kompromitterede hjemmesider eller gennem USB-adgange.
- **Udnyttelse:** Redskaberne udnytter identificerede sårbarheder hos offeret.
- **Installation:** Når en hacker har tilegnet sig adgang, vil vedkommende typisk installere yderligere redskaber for at sikre sig en mere langsigtet adgang samt placere andre typer redskaber, som kan indfri mere specifikke mål.
- **Kommando & Kontrol:** De forskellige redskaber placeret hos offeret vil ofte etablere en kommunikationskanal, som angriberen anvender til at monitorere og styre sine operationer fra.
- **Målorienterede Aktiviteter:** Først efter at have gennemgået de seks indledende faser kan angriberen agere på sine oprindelige målsætninger. Disse varierer bredt fra spionage eller berigelseskriminalitet til direkte ødelæggelse af hardware.

## Bilag 2: Illustration af, hvordan PowerShell kan misbruges i et cyberangreb

| Fase | *HVORDAN POWERSHELL KAN MISBRUGES I ET CYBERANGREB* |
|---|---|
| ***Rekognoscering*** | Identificerer email-adresser og evt. baggrundsoplysninger på mulige ofre |
| ***Klargøring*** | Klargør phising emails med link til ondsindet hjemmeside |
| ***Afsendelse & Udnyttelse*** | 1 Hackeren afsender phising mails til ofre<br>2 Hvis ofret klikker på linket, opstartes et legitimt program på ofrets pc<br>3 En sårbarhed udnyttes i ofrets program, som opstarter Command Prompt<br>4 Command prompt opstarter Powershell |
| ***Installation*** | Powershell downloader ondsindet script fra aktørens server og eksekverer den på ofrets system |
| ***Kommando & Kontrol*** | Hackeren opsætter infrastruktur, som kan bruges som kommunikationskanal til ofrets pc |
| ***Målorienterede Aktiviteter*** | Hackeren har nu kontrol over ofrets pc, og kan f.eks. exfiltrere data eller downloade yderligere malware |

**Bilag 3: Eksempel på cyberangreb, hvor ofrets egne programmer misbruges til at sprede ransomware på ofrets netværk**