CENTER FOR CYBERSIKKERHED

BESKYT DIG MOD DESTRUKTIVE CYBERANGREB

I lyset af det aktuelle trusselsniveau for destruktive cyberangreb anbefaler CFCS, at virksomheder og myndigheder genbesøger deres eksisterende sikkerhedsforanstaltninger. Hvis situationen ændrer sig, og truslen fra destruktive cyberangreb bliver mere udtalt, kan det være for sent at begynde arbejdet med modforanstaltninger. Det drejer sig særligt om nu at sætte ind på tre områder:

1. Forebyg angreb

- Sikkerhedsopdatér alle systemer og tjenester, der kan tilgås fra internettet.
- Beskyt alle fjernadgange med flerfaktor-autentifikation (MFA).
- Sikkerhedsopdatér medarbejdernes klienter og software.
- Brug stærke passwords og undgå især genbrug af passwords.
- Hav offline backup af data og kritiske systemer, og test at der kan reetableres.
- Opdater it-beredskabsplaner og øv dem.

2. Opdag angreb

Slå logning til på alle systemer og tjenester, der kan tilgås fra internettet, og på den centrale interne infrastruktur. Hold øje med logs, og mulige tegn på wiper-angreb som:

- Alarmer fra sikkerhedsprodukter (antivirus mv.).
- Oprettelse af nye, privilegerede brugere.
- Ændringer til group policies.
- Tilføjelse af nye scheduled tasks.
- Sletning af shadow copies og sletning af lokale logs.
- Større antal sletninger, overskrivninger eller omdøbning af filer.

3. Håndtér angreb

Identificeres et igangværende destruktivt angreb (f.eks. et wiper-angreb), bør det håndteres struktureret:

- Isolér ramte klienter og systemer fra det øvrige netværk.
- Aktivér beredskabsplanen, hvis nødvendigt.
- Søg eventuelt ekstern assistance.
- Sørg for at afdække og lukke de sårbarheder, som er blevet udnyttet, inden der reetableres fra backup.

For yderligere inspiration og råd, henvises til CFCS' vejledninger på https://www.cfcs.dk og de tekniske minimumskrav for statslige myndigheder på https://www.sikkerdigital.dk

For mere om logning, se CFCS' vejledning "Logning – en del af et godt cyberforsvar" https://www.cfcs.dk/logning

CFCS' situationscenter kan kontaktes døgnet rundt på tlf. 3332 5580 eller mail cert@cert.cfcs.dk.