Appendiks 6. Cyber respons under COVID-19

COVID-19 har påvirket trusselsbilledet ift. hvilke angrebsmetoder, hackerne vælger. Særlige cybertrusler, risici og angreb relateret til COVID-19 er bl.a.:

Phishingangreb, ondsindede internetsider og angreb på organisationens e-mailsystemer.

- Cyber-kriminelle anvender i høj grad den stigende interesse i den globale epidemi til at sprede spam kampagner relateret til COVID-19.

Ransomware, afpresning, IP rettigheder og skade på virksomhedens omdømme.

- Cyber-kriminelle målretter angreb mod de organisationer, som anses at være under pres fra COVID-19.
- Handlinger eller udtalelser anset som upassende fra organisationen kan være årsag til hacktivisme.

Operationelle forstyrrelser fra cyberangreb

- Organisationer bliver i højere grad udsat for et COVID-19 tematiseret angreb, såsom falske donationslinks, hvilket leder til et ransomware angreb, hvor cyber-kriminelle krypterer kritiske IT aktiver og kræver en betaling for dekrypteringen af disse.

Virtualisering af tidligere fysiske aktiviteter og **decentralisering** af processer

- Ændring i netværks-baseline:

1. Fjernadgang til høj-risiko handlinger giver alarmer
2. Al trafik vil være udsvingsgivende indtil en ny baseline kan etableres
3. Pres på helpdesk

Center for Cybersikkerhed har specifikt set på cybertruslen mod Danmark under COVID-19: https://cfcs.dk/da/temasider/covid-19/cybertruslen-mod-danmark-under-covid-19/

Følgende handlinger kan mitigere disse trusler og beskytte organisationen imod særlige indenfor cyber relateret til COVID-19:

- **MFA**. Implementering af multifaktor-autentifikation (MFA) på samtlige VPN forbindelser til at øge den generelle sikkerhed. Hvis MFA ikke kan anvendes, kan der bruges længere og mere komplekse adgangskoder.
- **Opdatering**. Opdatering af VPN, netværksinfrastrukturenheder og enheder for at opnå fjernadgang til organisationens miljø med de seneste softwareopdateringer og sikkerhedskonfigurationer.
- **Adgange**. Monitering af privilegerede adgange ved optimering af adfærdsanalytiske værktøjer for at identificere mistænksomme aktiviteter.
- **Filtrering**. Web og e-mailbeskyttelse ved implementering af web-filtrering. Således blokeres ondsindede hjemmesider. E-mailfiltreringen kan implementeres og anvendes til at blokere spam og phishing e-mails.
- **Overvågning**. Øge monitoreringskapaciteten og identificeringen af potentielle malware eller kampagner, som anvender de nuværende COVID-19 scenarier, f.eks. via blacklisting eller markering af udefrakommende e-mails. Øge organisationens end point-monitorering.
- **Falske hjemmesider og e-mails**. Minimere indvirkningen af forsøg på besvigelser i kritiske betalingssystemer relateret til COVID-19. En række COVID-19 relaterede websider og e-mails anvendes til phishingkampagner med henblik på at stjæle adgange og sprede malware.
- **Værktøjer**. Support for anvendelsen af samarbejdsværktøjer, såsom Microsoft Teams, Skype eller Cisco Webex.
- **Ressourcer og back-up**. Forøge kapaciteten til krisehåndtering ved at øge allokeringen af ressourcer. Evaluering af backupsystemer og failover kapaciteter. Helpdesk skal forberedes til at håndtere et øget antal af events.
- **Forberedelse**. Forbered værste scenarier, evaluering af krisehåndtering og interne eventresponskapaciteter. Ligeledes bør tilgængeligheden af tredjeparter evalueres.
- **SOC/SIEM**. Forstærkning af sikkerhedsinformation- og eventhåndteringssystemer (SIEM) samt sikkerhedsoperationscentre (SOC) og monitoreringsteams til at kunne håndtere en øget mængde sikkerhedsalarmer. Alarmer sorteres efter risici og procedurer for at skelne falske-positive fra reelle mistænksomme events.

BESTYRELSESFORENINGEN
Center for Cyberkompetencer

KROMANN REUMERT

FE CENTER FOR CYBERSIKKERHED

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation