CENTER FOR CYBERSIKKERHED

Program

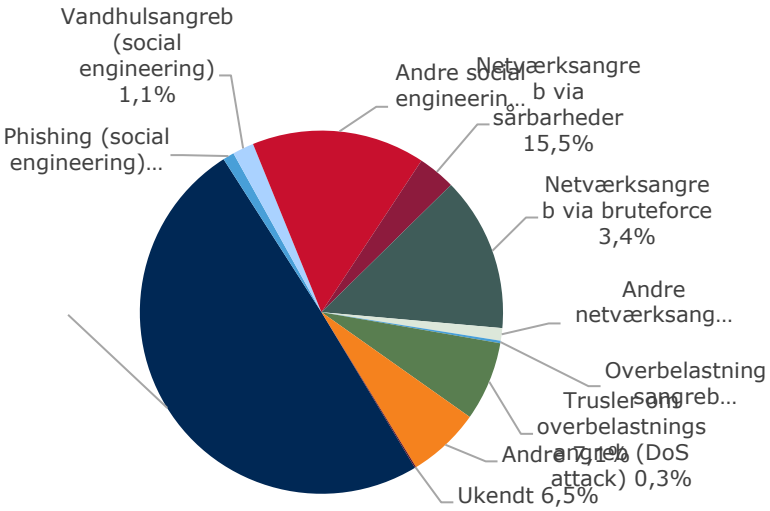
- Cybertruslen – hvad ser vi eksempler på?
- Cybersikkerhed – hvordan?

Eva Leisner, Chef for strategi, formidling og EU, Center for Cybersikkerhed

Cybertruslen – hvad ser vi eksempler på?

- Cybertruslen er meget høj, og myndigheder og virksomheder rammes dagligt af cyberangreb
- Øget digitalisering
- Formål: Økonomisk vinding (cyberkriminalitet) og viden (cyberspionage)
- Angrebsvektorer (veje ind)
- Truslen = intention og kapacitet

IDENTIFICEREDE ANGREBSVEJE 2020



CENTER FOR CYBERSIKKERHED

Eksempler

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra
4. juni 2021 21.58 CEST

ISS

Demant

ritzau

KALUNDBORG FORSYNING

Drikkevand Fjernvarm

Forside » Kalundborg Forsyning ramt af ransomwareangreb

Kalundborg Forsyning ramt af ransomwareangreb

Microsoft | Security Solutions Products Partners Resources

March 2, 2021

HAFNIUM targeting Exchange Servers with 0-day exploits

Microsoft Threat Intelligence Center (MSTIC)
Microsoft 365 Defender Threat Intelligence Team
Microsoft 365 Security

Bauhaus slås for at slippe ud af russiske hackeres kløer: Overvejer nu at betale løsesummen

solarwinds

På trods af ransomware-betaling: Dansk hotelplatform stadig ramt af problemer to uger senere

Den 9. juni blev den danske hotelplatform AK Techotel ramt af et ransomware-angreb, og modvilligt valgte selskabet dagen efter at betale løsepenge. Men i dag to uger efter, bliver der stadigvæk arbejdet på højttryk på de indre linjer, og problemerne er stadigvæk ikke løst fuldstændigt.

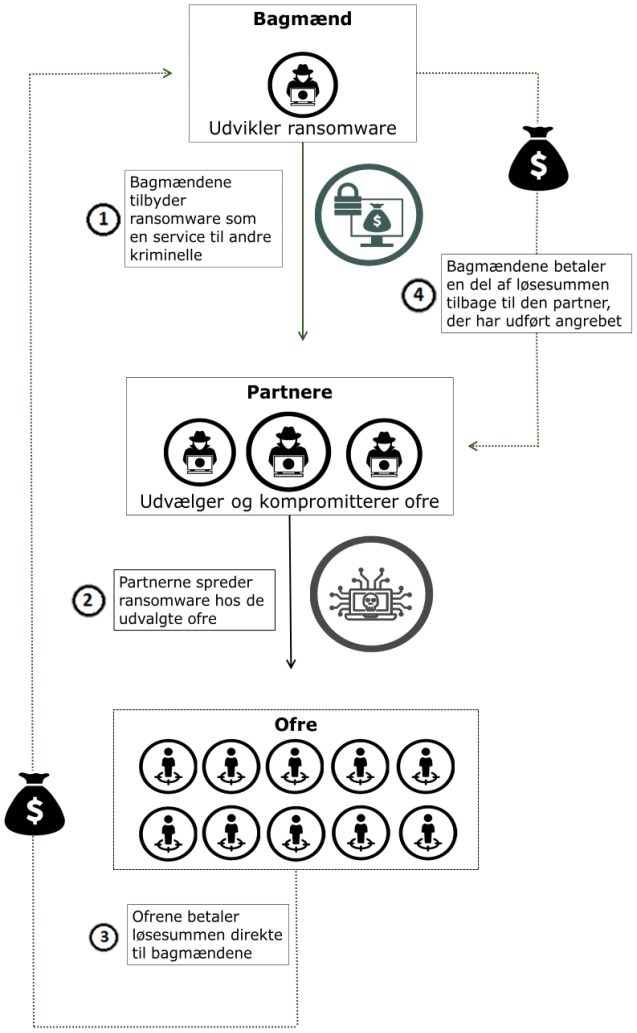
24. juni 2021 kl. 15.57

HSE cyber-attack: Irish health service still recovering months after hack

By Michael Sheils McNamee
BBC News NI

5 September

Cyberkriminalitet



Figur: Illustration af en typisk Ransomware-as-a-Service-forretningsmodel

- Truslen er MEGET HØJ og den mest udbredte trussel
- Hackere forsøger at afpresse penge ved at lamme it-systemer gennem phishing, udnyttelse af kendte sårbarheder og misbrug af usikre fjernadgange
- Målrettet ransomware og trussel om at lække data (dobbelt afpresning)
- Crime-as-a-Service/platformsøkonomi

Og vi ser et lignende billede fra udenlandsk rapportering…

Microsoft Digital Defense Report (oktober 2021)

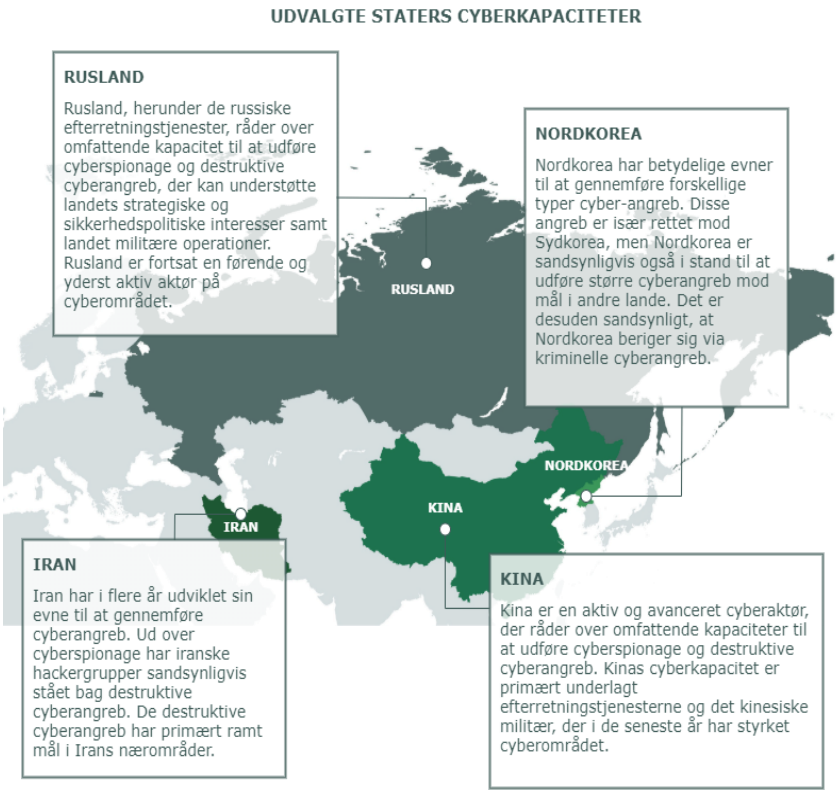
- Alle samfundsvigtige områder angribes, kriminelle arbejder også for statslige aktører
- Moden forsyningskæde af kriminelle tjenester

ENISA threat landscape (oktober 2021)

- Ransomware primære trussel. Kryptovaluta den mest almindelige udbetalingsmetode
- Målrettede og vedvarende DDoS-kampagner. IoT resulterer i en ny bølge
- COVID-19-pandemien multiplikator for menneskelige fejl og systemfejlkonfigurationer

Cyberspionage

- Truslen er MEGET HØJ og vedvarende. Virksomheder og myndigheder angribes. Mange, mange flere forsøges angrebet.
- Udenrigs- og sikkerhedspolitik, fremme egen økonomi og industri f.eks. ny teknologi og forskning (også COVID-vacciner), forsyningssikkerhed
- Supply-chain-angreb f.eks. SolarWinds og Microsoft Exchange Server



Også her et lignende billede fra udenlandsk rapportering…

Microsoft Digital Defense Report (oktober 2021)

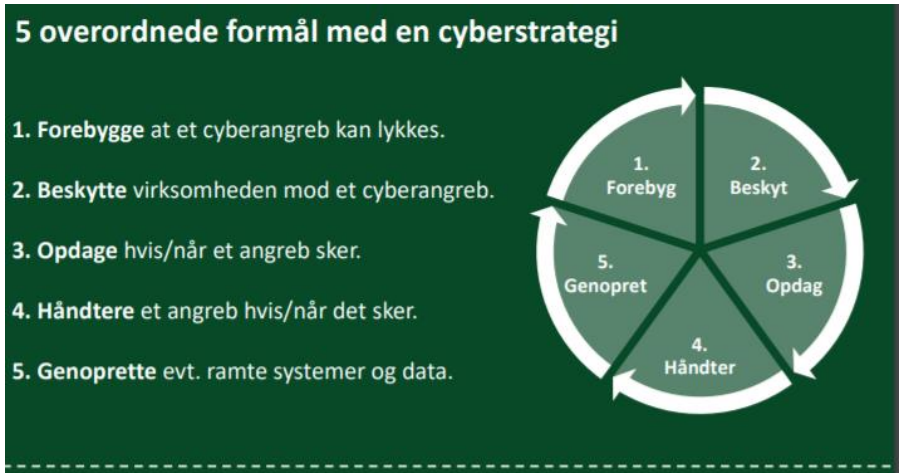
- Offentlige myndigheder, IGOer, NGOer, tænketanke men også private mål f.eks. COVID-vacciner er mål for cyberspionage
- Angriber bl.a. forsyningskæder (f.eks. Solarwinds og Microsoft Exchange Server)

Bestyrelsens rolle

- **Meget alvorlig cybertrussel**
- Bestyrelsen har ansvaret, da den ejer **forretningsrisikoen**

Bestyrelsen skal

- kende aktiverne
- erkende truslerne
- vurdere konsekvenserne
- fastlægge virksomhedens risikoappetit



CENTER FOR CYBERSIKKERHED

Cybersikkerhed – hvordan?

- Ledelsesforankret risikostyring, implementering af organisatoriske og tekniske foranstaltninger og styr på beredskabet, så organisationen er i stand til hændelseshåndtering (før, under og efter)

- Viden om truslen og sårbarheder

- Meget kan gøres ved helt grundlæggende sikkerhed og god cyberhygiejne MEN assume breach - > zero trust architecture

Spørgsmål?

WWW.CFCS.DK

@cybersikkerhed

Center for Cybersikkerhed