Henning Mortensen 24. jan 23

# Trusselsbilledet

- fra risici til kontroller

# To aktuelle trusler

**DDoS-angreb**

- 8.dec 2022: Forsvarsministeriet
- 10. jan 2023: En række banker
- 10. jan 2023: Nationalbanken
- 11. januar 2023: Finansministeriet

Kilder: DR.dk

- Russisk hackergruppe Killnet står bag, kendt for bl.a. hack af Ukraine og dets allierede.
- Formål: destabilisere og skabe frygt ved ikke at kunne betale

**Angreb på energisektoren m.v.**

- 750.000 daglige skanninger (blandet landhandel)
- OT-angreb med bl.a. Industroyer2
- Ransomware og DDoS-forsøg

Kilde: EnergiCERT

- Formål: destabilisere og skabe frygt for mangel på energi

# Trusler – et overblik

**Trusler mod SMV og alle andre**

- Phishingkampagner – f.eks. Nets, PostNord, kompromitterede partnere
- Ransomware – f.eks. Vastaamo klinikkerne: tre-trin
- Sårbarheder / virus / malware – f.eks. Log4J
- Fakturabedrageri – f.eks. kompromitterede partnere og fupbutikker
- CEO-fraud
- Compliancebrud på lovgivning – f.eks. GDPR, ePrivacy, NIS2, AI-forordningen,…

**Er i interessante – ud over jeres penge – og større?**

- Leverandører / supply chain – f.eks. SolarWinds
- Anden snyd – f.eks. Deep Fakes med AI
- Insidere
- DDoS-angreb
- Spionage
- Trusler mod produktion og IoT
- Aflytning og genkendelse – f.eks. Pegasus (krypterede apps er nytteløst) og databrokere og Bellingcat med Skripal/Novichok

**Hvem er trusselsaktørerne?**

- Kriminelle
- Fremmede lande
- Idealister
- Leverandører
- Os selv

# Trusler – Hack af IoT

- Mirai malware: inficerede IoT-enheder via standard brugernavn og password => Mirai Botnet og DYN-angrebet (DDoS)
- Hack af Jeep Cherooke, Kilde: https://www.youtube.com/watch?v=MKoSrxBC1xs, 00:00-02:30
- Hack af medicoteknisk udstyr, pacemakers, insulinpumper, m.v.
- Hack af smart TV
- Gætte brugernavn og passwords gennem andre hackede kilder => overtage TV-overvågning og alarmer i private hjem
- Generelt smart home enheder
- Hack af legetøj og sexlegetøj (IoD-projektet)

- Mange af disse eksempler har flere år på bagen!!!
- I dag benytter producenterne typisk ikke ukrypteret kommunikation, ens brugernavn/passwords, autentifikation af den enhed, der giver input (f.eks. iPhone)

# Hvad skal der gøres? - Ledelsen

**1. Ansvarsfordeling**

- CISO, CPO, DPO, intern audit
- Solid forankring i Governance-board (seks gange årligt + en gang bestyrelse)
- Stol på dem og giv dem hvad de beder om, hvis der er sammenhæng med risici

**2. Risikovurdering**

- Kortlæg informationsaktiver og kritikalitet (RTO (max genetablering) / RPO (max datatab))
- Trusselskatalog
- Risiko= sandsynlighed x konsekvens

**3. Ledelsesaccept af risici**

- Mindst årligt
- Guideline for hvad der er brug for af foranstaltninger

# Hvad skal der gøres? - Ledelsen

**4. Brug standarder**

- Kom hele vejen rundt om sikkerhed og compliance
- Lav politikker, procedure og processer, bl.a. beredskabsplan
- Implementer teknologier

**5. Kontroller og rapporter**

- Hvis det ikke er kontrolleret og dokumenteret kan det ikke rapporteres = det er ikke gjort
- Governance: Find ud af, hvorfor noget ikke er mål og ret op på det (ressourcer, kompetencer, modvillighed, andre prioriteter, modstridende interesser,…)

**6. Husk mennesker**

- IT-afdelingen: Det er super svært!!!
- Øvrige medarbejdere: Hvorfor? “Handlinger udført i den bedste mening”, Sprog, “neards call reality”
- Løbende træning, awareness, kurser og efteruddannelse, afprøvninger

# Særligt om kontroller

**Der skal struktur på de ting der skal gøres!**

- Brug standarder
- ISO27002:2022
  - Organisatorisk
  - Menneskeligt
  - Fysisk
  - Teknisk
- Map med andre standarder og krav – f.eks. ISO27701 og statens tekniske minimumskrav
- Map regulering ind – f.eks. NIS2, artikel 21
- Resultatet er eet stor governanceframework, som samler alle de ting vi skal
- Hver gang vi skal noget, skal vi også kontrollere grundigt at vi har gjort det
  - Vi skal tage backup
  - Har vi taget backup, testet at den virker, af data og systemer, airgapped og …

# Tekniskspørgsmål

## Til dialog når i kommer hjem

- Har vi HELT airgapped backup og virker den og hvor lang tid tager det?
- Skanner vi efter sårbarheder på alt udstyr og opdaterer vi og med hvilken frekvens?
- Logger vi alt udstyr og opsamler vi logs og analyserer dem?
- Har vi opdelt vores netværk i segmenter med regler for kommunikation?
- Er der begrænsninger på administrative rettigheder (IT-afdeling og lokalt)?
- Er der stærke adgangskoder, fler-faktor adgangskoder også remote og hos leverandører?
- Er der antivirus, firewall, kryptering, data loss prevention på relevant udstyr?
- Har vi politikker, procedurer (herunder beredskab), processer, teknologier og kontroller i fornødent omfang?
- Er medarbejderne trænet og aware og ved dem hvem de skal underrette?

# RfDS om IoT

## Til brugerne før køb

Har vi behov for at få enheden på internettet?

Er enhederne certificeret, mærket m.v.?

Kan du selv skifte password?

Kan du selv opdatere?

Sendes der data ud af enheden og til hvem?

Er data krypteret under lagring og transmission?

Kilde:
https://www.digitalsikkerhed.dk/wp-content/uploads/2021/02/IoT-tjekliste-.pdf

## Til brugerne efter køb

Skift adgangskoder

Opdater

Sluk, når det ikke bruges

Slå kryptering til

Slå Universal Plug and Play fra

Asset inventory – også af IoT

Risikovurdering: Hvad sker der hvis enheden hackes?

Segmenter IoT-enheder ud for sig selv

Ekstern hjælp til implementering

Husk fysisk sikkerhed

# Det betaler sig at beskytte sig

**Dataansvarlighed = Informationssikkerhed + databeskyttelse + dataetik**

- 39% af de danske SMV'er i undersøgelsen vurderer, at datasikkerhedsniveauet har betydning for virksomhedens konkurrenceevne.
- 63% af de danske SMV'er i undersøgelsen vurderer, at deres virksomhed er blevet styrket af at efterleve lovgivningen om persondatabeskyttelse.
- 56 % af de danske SMV'er i undersøgelsen vurderer, at deres virksomhed bliver styrket, når de viser kunder og potentielle kunder, hvordan de arbejder med dataetik.
- 8% af virksomhederne i undersøgelsen vurderer, at arbejdet med dataansvarlighed som et konkurrenceparameter giver en øget omsætning.
- Virksomheder, der har meromsætning, har forankret og implementeret it-sikkerhed.
- Gennemsigtighed i dataanvendelsen udgør et væsentligt konkurrenceparameter.

**Kilde:** https://www.digitalsikkerhed.dk/ansvarlig-dataanvendelse/

# Kontakt

hmo@ao.dk

https://www.linkedin.com/in/henning-mortensen-343b0/