Igang med cyber- og informationssikkerhed

Henning Mortensen
CISO/CPO, AO; Fmd., Rådet for Digital Sikkerhed; Privacy Evangelist, Wired Relations

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,…

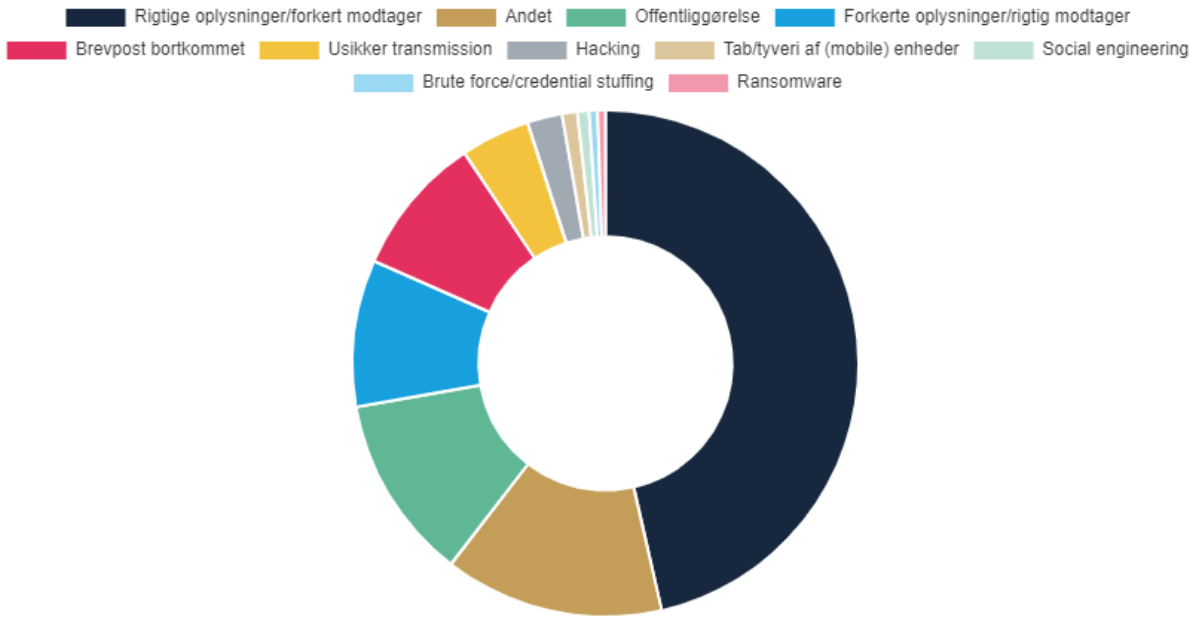
Er i interessante – ud over jeres penge – og større?

- 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

”Kedelige” hændelser



Langt de fleste hændelser skyldes os selv

- Rigtige oplysninger / forkert modtager
- Offentliggørelse
- Forkerte oplysninger / rigtig modtager
- **67,6% er fuldstændigt trivielle hændelser**
- Når vi fokuserer på de ”eksotiske” hændelser skyldes det, at de koster på bundlinjen.
- Kilde: https://www.datatilsynet.dk/sikkerhedsbrud/statistik-over-anmeldte-sikkerhedsbrud

Hvad skal der gøres?

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?

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

Teknisk appendiks

Til dialog når i kommer hjem

- Er der antivirus, firewall, kryptering, data loss prevention på relevant udstyr?
- Har vi HELT airgapped backup og virker den og hvor lang tid tager det?
- Er der begrænsninger på administrative rettigheder (IT-afdeling og lokalt)?
- Er der stærke adgangskoder, fler-faktor adgangskoder også remote og hos leverandører?
- Er medarbejderne trænet og aware og ved dem hvem de skal underrette?

- 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?
- Har vi politikker, procedurer (herunder beredskab), processer, teknologier og kontroller i fornødent omfang?

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/

Oplæg DS Cyberdag

29. september 2022

Dagsorden

- Hvem er ViSikrer:
- Standarden:
    1. Vores erfaring med at arbejde med standarder
    2. Derfor gør vi det
    3. Udfordringer
    4. Hvilken værdi har det tilført jeres virksomhed?
    5. Gode råd til andre virksomheder i opstarten

Enkel, troværdig, ansvarlig og prisrelevant

- ViSikrer er startet den 15. november 2019 og vil være den ledende anerkendte sikringsorganisation.
- Vores fokus er havne og anden kritisk infrastruktur.
- ViSikrer har operatører tilknyttet over hele landet, og de har baggrund i politiet, forsvaret og specialoperationsstyrkerne.
- ViSikrer ejes og ledes af Johnny Dalgaard og Eigil Schjønning.
- ViSikrer er medlem af Danske Shipping- og Havnevirksomheder/Dansk Industri og af SikkerhedsBranchen

Vi arbejder med sikring af kritisk infrastruktur i Danmark

- Risikovurderinger
- Beredskabsplaner
- Udbud / tilbud / Implementering / kontrol
- Uddannelse

Trusselsvurdering - Risikovurdering

Cyber trussel er overvældende

Remote – Social ingeneering

Hvorfor har I valgt det?

Definitioner

TERRORTRUSSELSNIVEAU

CTA anvender følgende trusselsniveauer (fremhævet med **BRUN** i teksten):

- **Meget alvorlig** - Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse.
- **Alvorlig** - Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning.
- **Generel** - Der er kapacitet og/eller hensigt og mulig planlægning.
- **Begrænset** - Der er en potentiel trussel. Der er begrænset kapacitet og/eller hensigt.
- **Minimal** - Der er ingen indikationer på en trussel. Enten hensigt, kapacitet eller begge dele er ikke erkendt.

SANDSYNLIGHEDSGRADER

CTA anvender følgende sandsynlighedsgrader (fremhævet med **BLÅ** i teksten):

Meget sandsynligt	**>= 85%**
Sandsynligt	**60-85%**
Muligt	**40-60%**
Mindre sandsynligt	**15-40%**
Usandsynligt	**<= 15%**

Vores erfaring med standarder

- ISO 9001; Kvalitetsledelse
- ISO 27001; Dokumentsikkerhed
  (Digitale dokumenter)

Derfor gør vi det

- Vores kerneforretning er andres virksomheders sikring af værdier
- Vores fokus ligger på, at gøre andre virksomheder sikre

➢ Vi risikerer at glemme vores egen sikkerhed, når vi har travlt med at sikre andre virksomheders sikring

➢ Hvis vi ikke sikrer vores egen virksomhed, kompromitterer vi vores kunders sikring i udvekslingen af digital information

➢ Hvis vores papirer ligger og flyder, risikerer vi, at de kommer til uvedkommendes kendskab og kompromitterer dermed

  ➢ vores egen virksomhed – og sikring
  ➢ vores kunders sikring
  ➢ Vores forretning

Udfordringer

- 1. Vi har selv skrevet standarden
  - ➢ Tidskrævende
- 2. En pokkers masse procedurer og dokumentationskrav
  - ➢ Tidskrævende

Værdi for ViSikrer

1. Vi har beskrevet en procedure, der kan overtages i tilfælde af bortfald af interne ressourcer
2. Vi tvinges til at udføre de oplagte – og korrekte sikringsaktiviteter
3. Vi giver vores kunder tryghed for, at vi passer på deres – og vores værdier
4. Reduktion af risici for cyber-kriminalitet mod ViSikrer og vores kunder
5. Kommunikation med kunder om det vigtige, hvad kan vi gøre for dem
6. Vores forretning

Gode råd

1. Sæt god tid af
2. Lav selv jeres standard, så I har den under huden og så ved I hvad proceduren er
3. Gør det I skriver i jeres 27001, at i gør
   - Kommer I bag ud, så indhent det forsømte snarest
4. Uddan jeres medarbejdere i at overholde reglerne
5. Fortæl jeres kunder, at I anvender standarden, så I hurtigt kommer til at tale om jeres kunders behov

Tak for ordet

- Husk, at jeres virksomheder er under angreb fra cyberkriminelle og folk der synes, at det er spændende at hacke i hele verden.

- Husk, at man kan angribe jeres IT gennem PC, mobiltelefoner, IOT enheder (fx overvågningskameraer, tyverialarmer og ”kinesiske gadgets”