CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Beskyttelse af intellektuel ejendomsret

www.cyber-smv.dk

Værktøjet er tilvejebragt i forbindelse med projektet **Cybersikkerhed og Forretningskontinuitet** (www.cyber-smv.dk), støttet af Industriens Fond.
Offentliggjort den 08.01.2026.

Formål, deltagere og anvendelse

- **Formål**
  - At understøtte etablering og koordinering af cybersikkerhedsforanstaltninger til beskyttelse af intellektuel ejendomsret (IP).
- **Deltagere**
  - Data- og IT-chefer, leverandører samt andre relevante eksterne samarbejdspartnere.
- **Anvendelse**
  - Bør gennemføres med en passende hyppighed.

Fremgangsmåde

1. Klassificering af eksisterende intellektuelle ejendomsrettigheder (IP).
2. Kortlægning af viden blandt medarbejdere.
3. Iværksættelse af passende cybersikkerhedsforanstaltninger.
4. Udarbejdelse af genopretnings- og kontinuitetsplaner.

Særlige SMV-karakteristika tages i betragtning:

- Begrænsede IT-ressourcer.
- Afhængighed af eksterne IT-leverandører.
- Behov for omkostningseffektive sikkerhedsløsninger.

Klassificering af eksisterende intellektuel ejendom (IP)

Metoder

- **Forskellige niveauer af fortrolighed, som minimum:** Offentlig, intern, fortrolig (begrænset).
- **Bevidsthed om IP og fortrolighed:** Ikke kun for medarbejdere, men også for konsulenter/kontraktansatte.
- **Kronjuveler:** IP, der er nødvendig for virksomhedens eksistensgrundlag, og som udgør mål af høj værdi.

Politik

- **Målgruppe:** Medarbejdere, konsulenter/kontraktansatte og leverandører.
- En politik, der fastholder definitioner af dataklassifikationsniveauer, herunder kriterier for hvert niveau.
- Politikken bør indeholde eksempler, der illustrerer anvendelsen af kriterierne og klassifikationsniveauerne.

Kortlægning af viden blandt medarbejdere

Overvejelser

- Personer har behov for forskellige niveauer af kendskab til fortrolige oplysninger.
- **Kortlægning af højrisikoroller:** Balance mellem afhængighed af nøgle-/ekspertmedarbejdere og den tilhørende risiko.
- **Fortrolighedsaftaler (NDA'er):** For medarbejdere og konsulenter/kontraktansatte, men bør ikke stå alene.
- **Overvågning af efterlevelse:** Aktiv kontrol af overholdelse af politikker og aftaler for at forebygge brud.
- **Etikpolitik:** Dataklassifikation samt ansvar for efterlevelse hos medarbejdere og konsulenter/kontraktansatte.
- **Retlige skridt:** Vær forberedt på at iværksætte juridiske tiltag i tilfælde af videregivelse.

Trusler

- Forsætlig eller utilsigtet videregivelse.
- **Insidertrusler:** utilfredse medarbejdere, tidligere medarbejdere eller konsulenter/kontraktansatte.
- **Eksterne trusler:** ondsindede aktører.

Iværksæt passende cybersikkerhedsforanstaltninger

Overvejelser

- **Risikoomfang:** Al infrastruktur (ERP, e-mail, samarbejdsværktøjer m.m.) kan indeholde fortrolig IP.
- **Databeskyttelse:** Beskyt data i hvile, under overførsel og i brug med kontroller, der er tilpasset den enkelte tilstand.
- **Anvendelse af AI/LLM (Large Language Models):** Behandl (offentlige og private) LLM'er som databehandlere med høj risiko; fastlæg tilladte datatyper, licensmæssige begrænsninger og klassifikationsregler før anvendelse.
- **Leverandørintelligens:** Leverandørvurderinger og indhold i ERP-systemer er værdifulde mål og bør beskyttes for at undgå at muliggøre kompromittering længere nede i forsyningskæden.

Trusler

- **Dataeksfiltration via samarbejdsværktøjer** – lækage gennem e-mail, Slack, Teams eller fildelingsløsninger.
- **Menneskelige mål** – social engineering, tyveri af loginoplysninger, phishing og utilsigtet videregivelse.
- **Teknologiske svagheder** – fejlkonfiguration (f.eks. utilstrækkelig kryptering) og forældede systemer.

Udarbejde genopretnings- og kontinuitetsplaner

Overvejelser

- **Synlighed og telemetri (fjernmåling/overførsel af måledata via telekommunikation):** Effektiv forebyggelse af datatab og overvågning kræver fuld synlighed.
- **Afhængigheder i forsyningskæden:** Kortlæg tredjepartsleverandører, deres sikkerhedsniveau samt alternative leverandører eller afbødende tiltag ved leverandørkompromittering.
- **Test og tabletop-øvelser:** Planlæg regelmæssige øvelser for scenarier med IP-lækage/-tab og overtagelse af leverandører.
- **Backup-integritet og adgang:** Etabler og valider effektive sikkerhedskopier af IP, og sikre at procedurerne testes og afprøves.

Trusler

- **Angreb på forsyningskæden** – angribere udnytter lækkede leverandørvurderinger eller udgiver sig for at være leverandører.
- **Ufuldstændig indsamling af retsmedicinske data** – genopretningshandlinger, der overskriver bevismateriale, som er nødvendigt for at kunne fastslå årsagen til bruddet, hvilket hæmmer juridiske tiltag eller afhjælpning.