1. Antag kompromittering (”Assume Breach”)

www.cyber-smv.dk

Værktøjet er tilvejebragt i forbindelse med projektet **Cybersikkerhed og Forretningskontinuitet** (www.cyber-smv.dk), støttet af Industriens Fond.
Offentliggjort den 09.01.2026.

Antag kompromittering

Formål

→At skabe realistisk risikoforståelse og fokus på konsekvensreduktion frem for fejlfrihed.

Mental model

→*Spørgsmålet er ikke om, men hvornår noget går galt.*

Deltagere

→Alle medarbejdere.

→Ingen teknisk forudsætning.

Input

→En realistisk case (f.eks. phishing-mail, forkert modtager, mistet enhed) (se de næste sider).

→Kort introduktion til princippet “Assume Breach”.

Case: Baggrund

→En dansk produktionsvirksomhed med ca. 90 medarbejdere producerer komponenter til maskinindustrien. Virksomheden har både:
  → **Informationsteknologi (IT)** (mail, ERP, CRM m.v.).
  → **Operationel teknologi (OT)** (MES, SCADA m.v.).

→IT og OT er delvist forbundet for at understøtte effektiv drift og rapportering.

→Virksomheden har grundlæggende it-sikkerhed, men er ikke en stor virksomhed med eget sikkerhedsteam.

→Ledelsen har besluttet at arbejde efter princippet **"Assume Breach"** – altså at man planlægger sin sikkerhed, som om et angreb allerede er sket.

Case: Hændelsen

→En medarbejder i indkøb modtager en e-mail, der ser ud til at komme fra en kendt leverandør. Mailen indeholder et vedhæftet dokument med en opdateret prisliste. Medarbejderen åbner dokumentet og logger efterfølgende ind på ERP-systemet som normalt.

→Uden at medarbejderen ved det, er loginoplysningerne blevet opsnappet af en angriber, som nu har adgang til medarbejderens konto.

→Angriberen forsøger herefter at:

- → Få adgang til ERP-systemets administrative funktioner.
- → Bevæge sig videre mod produktionssystemerne.
- → Hente oplysninger om ordrer og leverandører.

Case: Diskussionsspørgsmål

1. Identifikation

→ Hvor i casen er virksomheden allerede kompromitteret?

→ Hvilke tegn kunne indikere, at der er sket et sikkerhedsbrud?

2. Assume Breach-tankegang

→ Hvordan adskiller “Assume Breach” sig fra at fokusere på at forhindre alle angreb?

→ Hvilke konkrete foranstaltninger i casen understøtter “Assume Breach”?

3. Konsekvensbegrænsning

→ Hvad kunne konsekvenserne have været uden segmentering og rollebaseret adgang?

→ Hvilke forretningsmæssige risici blev reduceret?

4. Overførsel til egen hverdag

→ Hvor i jeres egen virksomhed kunne et tilsvarende brud ske?

→ Hvad kan medarbejdere konkret gøre for at understøtte “Assume Breach” i praksis?

Case: Mulige løsninger til identifikation

→Hvor i casen er virksomheden allerede kompromitteret?

- → Virksomheden er kompromitteret i det øjeblik medarbejderen åbner det vedhæftede dokument, og angriberen får adgang til medarbejderens loginoplysninger.
- → Bruddet sker altså før der opstår synlige problemer.

→Hvilke tegn kunne indikere, at der er sket et sikkerhedsbrud?

- → Login fra usædvanlig lokation eller tidspunkt
- → Forsøg på adgang til funktioner, som medarbejderen normalt ikke bruger
- → Flere fejlede loginforsøg eller gentagne forespørgsler
- → Alarmer fra overvågning og logning

👉 **Vigtigt læringspunkt:** Et brud opdages sjældent ved selve hændelsen, men via afvigende adfærd.

Case: Mulige løsninger til Assume Breach-tankegang

→Hvordan adskiller "Assume Breach" sig fra at fokusere på at forhindre alle angreb?

→ I stedet for at tro, at man kan forhindre alle angreb, tager "Assume Breach" udgangspunkt i, at angriberen allerede er inde. Fokus flyttes fra perfektion til robusthed og skadesbegrænsning.

→Hvilke foranstaltninger i casen understøtter "Assume Breach"?

→ Rollebaserede rettigheder (angriberen får kun samme begrænsede adgang som medarbejderen).
→ Netværkssegmentering (kontor-it kan ikke frit tilgå produktions-it).
→ Multifaktorgodkendelse (forhindrer eskalering af adgang).
→ Logning og overvågning (bruddet opdages hurtigt).

👉 **Pointen er**, at systemerne ikke stoler blindt på, at en bruger er legitim.

Case: Mulige løsninger til konsekvensbegrænsning

→Hvad kunne konsekvenserne have været uden segmentering og rollebaseret adgang?

- → Adgang til produktionssystemer og risiko for produktionsstop.
- → Manipulation eller sletning af ordrer og styklister.
- → Datatyveri af leverandør- og kundeoplysninger.
- → Økonomiske tab og leveringsproblemer.

→Hvilke forretningsmæssige risici blev reduceret?

- → Risiko for nedetid i produktionen.
- → Risiko for tab af kundetillid.
- → Risiko for økonomiske tab og kontraktbrud.
- → Risiko for regulatoriske konsekvenser (f.eks. i forhold til NIS2).

👉 **"Assume Breach"** beskytter forretningen – ikke kun IT.

Case: Mulige løsninger til overførsel til egen hverdag

→**Hvor i virksomheden kunne et tilsvarende brud ske?**

- → Typisk i funktioner med:
  - → Meget e-mail-kontakt (f.eks. indkøb, salg, økonomi).
  - → Adgang til centrale systemer.
  - → Samarbejde med eksterne leverandører.

→**Hvad kan medarbejdere konkret gøre for at understøtte "Assume Breach"?**

- → Reagere hurtigt på mistænkelig adfærd og melde det.
- → Acceptere sikkerhedsforanstaltninger som multifaktorgodkendelse.
- → Følge princippet om mindst mulige rettigheder.
- → Være opmærksomme på, at "normale" handlinger kan misbruges af angribere.

→ 👉 **Budskab:** Medarbejdere er en aktiv del af sikkerheden, ikke kun en risiko.