3. Lag på lag (Defense in Depth)

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.

Lag på lag

Formål

→At forstå, hvorfor sikkerhed er et samspil mellem mennesker, processer og teknologi.

→At fjerne idéen om "det ene rigtige værktøj".

Mental model

→*Ingen sikkerhedsforanstaltning er perfekt - men flere sammen virker.*

Deltagere

→Medarbejdere fra administration og produktion.

→Særligt relevant for ledelse og procesejere.

Input

→Visualisering af flere sikkerhedslag.

→Eksempler på kontroller (multifaktorgodkendelse, procedurer, awareness).

Kort scenarie

A. Kort virksomhedsscenarie

- → En dansk produktionsvirksomhed med ca. 90 medarbejdere:
  - → ERP-system.
  - → Operationel Teknologi (OT).
  - → Leverandører og fjernadgang.
  - → Mail, adgangskort og fælles netværk.
- → Virksomheden vil beskytte:
  - → Produktion.
  - → Kundedata.
  - → Leverancer.
  - → Omdømme.

B. Hændelse:

- → En angriber forsøger at:
  - → Narre loginoplysninger via phishing.
  - → Få adgang til systemer.
  - → Bevæge sig mod produktionen.

Proces: Trin 1 - kortlæg lagene

Opgave: *Hvilke lag af beskyttelse findes der - eller burde findes - i virksomheden?*

- → Der skal identificeres lag inden for f.eks.:
  - → Mennesker (adfærd, opmærksomhed, træning).
  - → Processer (procedurer, godkendelser, eskalation).
  - → Teknik (systemer, adgangskontrol, segmentering).
  - → Fysisk sikkerhed (adgang, låse, gæster) .
- → Eksempler:
  - → Adgangskort.
  - → Multifaktorgodkendelse.
  - → Segmentering.
  - → Awareness.
  - → Backup.
  - → Ledelsesgodkendelse.

Proces: Trin 2 - Fjern et lag

Opgave: *Vælg et lag, der fejler eller mangler*

→Hvad sker der, hvis dette lag ikke virker?
→Hvilke andre lag kan stadig begrænse skaden?
→Hvor bliver virksomheden sårbar?

👉 **Pointe:** Lagene skal overlappe, ikke stå alene.

Proces: Trin 3 – medarbejderens rolle i lagene (10-15 min.)

Spørgsmål:

→Hvilke lag afhænger direkte af medarbejderadfærd?
→Hvor kan en enkelt handling styrke eller svække flere lag?
→Hvad kan medarbejdere konkret gøre for at være et aktivt lag?

→Eksempler:
- → Stoppe op før klik.
- → Følge procedurer, også under pres.
- → Reagere på afvigelser.
- → Melde fejl og mistanke.

Mulige løsninger: Trin 1 – kortlæg lagene

Eksempel på identificerede lag i en dansk produktions-SMV

- → Mennesker:
  - → Medarbejdernes opmærksomhed på mails og opkald.
  - → Awareness-træning i phishing og social engineering.
  - → Kultur hvor det er acceptabelt at stoppe op og spørge.
- → Processer:
  - → Godkendelsesprocedure ved ændring af leverandørdata.
  - → Klar eskalationsvej ved mistanke om sikkerhedshændelser.
  - → Adgangsstyring baseret på rolle og arbejdsopgaver.
- → Teknik:
  - → Multifaktorgodkendelse.
  - → Antivirus og mailfiltrering.
  - → Netværkssegmentering mellem kontor-IT og produktion.
  - → Logning og overvågning.
- → Fysisk sikkerhed:
  - → Adgangskort til bygninger.
  - → Gæsteregistrering.
  - → Adskillelse mellem kontor- og produktionsområder.

👉 **Pointe:** Sikkerhed består af flere overlappende lag, og mange af dem er ikke tekniske, men organisatoriske og menneskelige.

Mulige løsninger: Trin 2 - fjern et lag

Eksempel: Multifaktorgodkendelse virker ikke / er ikke slået til

Hvad sker der, hvis dette lag fejler?
→ Angriberen kan logge ind med stjålne brugernavn og adgangskode.
→ Risikoen for uautoriseret adgang stiger markant.

Hvilke andre lag kan stadig begrænse skaden?
→ Rollebaserede rettigheder begrænser, hvad angriberen kan se og ændre.
→ Netværkssegmentering beskytter produktionssystemerne.
→ Overvågning kan opdage unormal adfærd.
→ Medarbejdere kan reagere på mistænkelig aktivitet.

Hvor bliver virksomheden sårbar?
→ Hvis flere lag mangler samtidig (f.eks. også manglende overvågning).
→ Hvis adgangsrettigheder er for brede.

👉 **Pointe:** Ét lag er aldrig nok. Lagene skal kompensere for hinanden, når noget fejler.

Mulige løsninger: Trin 3 - medarbejderens rolle i lagene

Hvilke lag afhænger direkte af medarbejderadfærd?

- → Phishing-beskyttelse (første klik eller ej).
- → Overholdelse af procedurer og godkendelser.
- → Rapportering af mistænkelige hændelser.
- → Fysisk adgang (lukke døre, følge gæsteregler).

Hvor kan én handling styrke eller svække flere lag?

Eksempel:

- → Hvis en medarbejder klikker på et phishing-link→ Svækker både det menneskelige lag og det tekniske lag.
- → Hvis en medarbejder stopper op og melder en mistænkelig mail→ Styrker både det menneskelige lag, overvågning og processer.

→ Hvad kan medarbejdere konkret gøre?

- → Tage sig tid til at vurdere mails og opkald, især under pres.
- → Følge procedurer, også når det virker besværligt.
- → Reagere på afvigelser og sige noget højt.
- → Acceptere sikkerhedsforanstaltninger som multifaktorgodkendelse og kontroller.

👉 **Pointe:** Medarbejdere er ikke det svageste led, men et aktivt sikkerhedslag, når rammerne understøtter det.