2. Angriberens perspektiv ”Social Engineering”

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.

Angriberens perspektiv

Formål

→At øge forståelsen for social engineering.

→At forstå hvordan angribere tænker og arbejder.

→At blive bedre til at opdage manipulation før skaden sker.

Mental model

→*Cybersikkerhed handler mere om mennesker end teknologi.*

Deltagere

→Alle medarbejdere (administration og produktion).

→Meget velegnet til onboarding og teams med eksterne kontakter.

Input

→Offentligt tilgængelige oplysninger (f.eks. LinkedIn-profiler, mailsignaturer).

→Eksempler på social engineering-angreb.

Case

→I arbejder i en dansk produktionsvirksomhed med ca. 80-100 medarbejdere.

→Virksomheden har:

- → ERP-system.
- → Leverandører i ind- og udland.
- → Produktionsanlæg forbundet til IT-systemer.
- → Medarbejdere med mail, telefon og adgangskort.

→Angriberen vil have:

- → Loginoplysninger.
- → Adgang til systemer.
- → Information om leverandører, ordrer eller produktion.

Fremgangsmåde

→Trin 1 – Tænk som angriberen (10-15 min.)

Opgave: *Forestil jer, at I er en angriber, der vil snyde jer selv eller jeres kolleger. I skal diskutere:*

1. Hvem i virksomheden er lettest at angribe og hvorfor?
2. Hvilke oplysninger kan findes offentligt? (f.eks. hjemmeside, LinkedIn, mails m.v.)
3. Hvilke situationer giver travlhed, stress eller autoritet?

Fremgangsmåde

→Trin 2 – Design angrebet (15 min.)

Opgave: I skal nu designe et social engineering-angreb.

1. Hvordan tager angriberen kontakt (mail, telefon, SMS, fysisk fremmøde m.v.)?
2. Hvilken rolle udgiver angriberen sig for at have (leverandør, IT-support, leder, fragtfirma m.v.)?
3. Hvilken følelse forsøger angriberen at udnytte (hast, frygt, hjælpsomhed, autoritet m.v.)?

Fremgangsmåde

→Trin 3 – Forsvarsperspektivet (10 min.)

Opgave: I skal nu skifte perspektiv og svarer på:

1. Hvilke advarselstegn er der i angrebet?
2. Hvad burde medarbejderen gøre i situationen?
3. Hvem skal kontaktes internt?

Mulige drøftelser: Tænk som angriberen

1. Hvem i virksomheden er lettest at angribe og hvorfor?

→ Typisk lette mål er:

- → Indkøb og økonomi - arbejder med leverandører, fakturaer og ændringer.
- → Reception og administration - vant til at hjælpe og give information.
- → Produktion under tidspres - fokus på drift frem for sikkerhed.
- → Nye medarbejdere - kender ikke procedurer og normer endnu.

👉 **Angriberens logik:** Jeg vælger personer med:

- → Travlhed.
- → Mange eksterne kontakter.
- → Lav sandsynlighed for at stille kritiske spørgsmål.

Mulige drøftelser: Tænk som angriberen

2. Hvilke oplysninger kan findes offentligt? (eksempler)

→Navne, stillinger og e-mails på hjemmeside.
→LinkedIn-profiler (ansvarsområder, relationer, tidligere job).
→Leverandører nævnt i nyheder eller jobopslag.
→Produktionsudstyr og processer nævnt i markedsføring.

👉 **Angriberens logik:** Jo mere virksomheden deler åbent, jo lettere er det at lyde troværdig.

3. Hvilke situationer giver travlhed, stress eller autoritet? (eksempler)

→Månedsskifte/fakturaperioder.
→Produktionsstop eller hasteordrer.
→Leverandørskift eller systemopdateringer.
→Beskeder, der udgiver sig for at komme fra ledelse eller IT.

👉 **Angriberens logik:** Jeg angriber, når medarbejderen ikke har tid til at tænke sig om.

Mulige drøftelser: Design angrebet

1. Hvordan tager angriberen kontakt?

→Typiske valg:

→E-mail (mest brugt og billigst).

→Telefonopkald (skaber pres og autoritet).

→SMS (kort, presserende beskeder).

→Fysisk fremmøde ("jeg er fra leverandøren/IT").

👉 **Angriberens logik:** Jeg vælger den kanal, hvor det er sværest at dobbelttjekke hurtigt.

Mulige drøftelser: Design angrebet

2. Hvilken rolle udgiver angriberen sig for at have?

→ Eksempler på roller:

→Kendt leverandør

→IT-support / systemleverandør

→Leder eller direktionssekretariat

→Fragtfirma eller tekniker

👉 **Angriberens logik:** Jeg vælger en rolle som normalt ikke bliver udfordret.

Mulige drøftelser: Design angrebet

3. Hvilken følelse forsøger angriberen at udnytte?

→Hast: “Det skal gøres nu”
→Frygt: “Ellers stopper systemet”
→Hjælpsomhed: “Kan du lige hjælpe mig?”
→”Autoritet: “Ledelsen har bedt mig om det”

👉 **Angriberens logik:** Hvis jeg styrer følelserne, stopper den kritiske tænkning.

Mulige drøftelser: Forsvarsperspektivet

1. Hvilke advarselstegn er der i angrebet?

→Typiske røde flag:

- → Uventede henvendelser.
- → Tidspres eller trusler.
- → Afvigende sprog, stavefejl eller tone.
- → Anmodninger om login, koder eller ændringer.
- → “Vi plejer ikke at gøre det sådan”.

2. Hvad burde medarbejderen gøre?

→Stoppe op og tage en pause

→Undlade at klikke, svare eller udlevere oplysninger

→Verificere via kendt kontaktvej.

→Kontakte leder, IT eller sikkerhedsansvarlig.

👉 **Vigtig pointe:** Det er professionelt at være skeptisk.

Mulige drøftelser: Forsvarsperspektivet

3. Hvem skal kontaktes internt?

→ Afhænger af virksomheden, men typisk:

- → Nærmeste leder.
- → IT-ansvarlig/service desk.
- → Sikkerheds- eller compliancefunktion.
- → Fælles mail eller telefon til sikkerhedshændelser.