

▯ Øvelse 3 (Gruppeøvelse) – *Hvad er sikkerhed?*

▯ Information

Formålet med denne øvelse er at definere, hvad *sikkerhed* er, og hvornår der er behov for det. Øvelsen lægger op til refleksion over, hvordan vi forstår sikkerhed i forskellige kontekster – både fysisk og digitalt – og hvorfor sikkerhed altid skal vurderes i forhold til det, man ønsker at beskytte.

▯ *Eksempel: En husforsikring er sikkerhed for en husejer – men giver ingen mening for en, der ikke ejer et hus. Sikkerhed er altså kontekstafhængig.*

▯ I klassens opsamling samles der op på:

- ▯ En fælles definition af *sikkerhed*
- ▯ Eksempler på, hvordan sikkerhedsbehov afhænger af situation og kontekst
- ▯ En begyndende kobling til *software*: Hvordan kan jeres definition af sikkerhed kombineres med definitionen af software fra Øvelse 2 – så vi sammen kan begynde at definere *software-sikkerhed*?

▯ Instruktioner

Sammen i gruppen skal I diskutere følgende spørgsmål:

1. ▯ **Hvad er sikkerhed?**

- Formulér en definition, som hele gruppen er enige om.

2. ▯ **Hvornår er der behov for sikkerhed?**

- Giv eksempler på situationer, hvor sikkerhed er vigtig.
- Giv eksempler på situationer, hvor sikkerhed er mindre vigtig
- Diskutér, hvorfor behovet for sikkerhed er forskelligt i forskellige kontekster.

3. ▯ **Hvad sker der, hvis man undervurderer behovet for sikkerhed?**

- Hvilke konsekvenser kan det få? For individ, organisation eller samfund?

▯ Lav en kort liste med jeres bud på "*hvad god sikkerhed indebærer*" – både i forebyggelse og i håndtering af hændelser.

□ Til sidst

I den fælles klassedialog samler vi op på jeres definitioner og refleksioner og formulerer i fællesskab:

- □ En samlet definition af sikkerhed
 - □ En fælles liste over egenskaber ved god sikkerhed
 - □ En begyndende fælles forståelse af, hvad *software-sikkerhed* kan betyde
-

□ Bonus: Sikkerhedsstandarder og kontekst

I mange officielle sikkerhedsstandarder samt vejledninger er *kontekst* afgørende for, hvordan man vælger at arbejde med sikkerhed:

- **ISO/IEC 27005:** Understreger at risikovurdering altid skal tage udgangspunkt i systemets og organisationens kontekst.
- **ASVS 5.0.0:** Krav afhænger af, hvad systemet bruges til – og hvor store konsekvenser et brud kan have.
- **ISO/IEC 27002:** Sikkerhedsforanstaltninger (kontroller) vælges ud fra risikovurderingen – ikke som “one size fits all”.

□ Sikkerhed indenfor IT handler altså ikke kun om teknologi – men om at *beskytte det rigtige, på det rigtige tidspunkt, i den rigtige sammenhæng*.

Last update: 2026-09-01 17:08:12