

Cybersikkerhet - teknologier og styring

Audun Jøsang

3. utgave 2025

Universitetsforlaget



Oppgaver

Kapittel 1: Grunnleggende sikkerhetsbegreper

Oppgave 1: Kjært barn har mange navn

Diskuter følgende begreper, hva de betyr og om de er forskjellige:

- Informasjonssikkerhet
- Datasikkerhet
- IT- og IKT-sikkerhet
- Digital sikkerhet
- Cybersikkerhet
- Sikring (<https://nso.no/industrivern/sikring-security/>)

Oppgave 2: Digitale verdier

- a. [Cybersikkerhet](#) defineres som beskyttelse av digitale verdier mot skade ([Jøsang, 2025](#)). Hvor dekkende er denne definisjonen?
- b. [Cyberforsvarsmatrisen](#) gir en enkel kategorisering av digitale verdier. Beskriv de fem kategoriene av digitale verdier i cyberforsvarsmatrisen.
- c. Diskuter om det kan være noen typer (digitale) verdier som ikke passer inn under kategoriseringen fra cyberforsvarsmatrisen og som er relevant for cybersikkerhet?

Oppgave 3: Eksempler på angrep som kan gi brudd på KIT

Beskriv eksempler på angrep som kan forårsake sikkerhetsbrudd for hvert KIT-sikkerhetsmål, og mulige tiltak som kan forhindre angrepene. Angrepsbeskrivelsene skal være svært abstrakte, som f.eks. «*en hacker stjeler et passord og overtar brukerkontoen til en annen person*».

- a. Konfidensialitet
- b. Integritet
- c. Tilgjengelighet

Oppgave 4: Trusler mot IAM (Identitets- og tilgangshåndtering)

En enkel metode for å identifisere trusler er å spørre «Hva kan gå galt?» eller «Hvordan kan dette angripes?».

- a. Nevn relevante trusler mot (trinnene i) konfigureringsfasen av IAM (identitets- og tilgangshåndtering).
- b. Nevne relevante trusler mot (trinnene i) bruksfasen av IAM (identitets- og tilgangshåndtering).

Oppgave 5: Tilgangsbetragtig

- a. X.800 er en standard for sikkerhetstjenester i OSI (Open Systems Interconnection). Søk og finn X.800-standarden, eller besøk <https://www.itu.int/rec/T-REC-X.800-199103-I/en>
Les definisjonene av konfidensialitet, integritet og autorisering i X.800. Er definisjonene av konfidensialitet og integritet fra X. 800 meningsfulle i forhold til hvordan autorisering er definert? Hvorfor eller hvorfor ikke?
- b. Hvordan er autorisering definert p  Wikipedia?
<https://en.wikipedia.org/wiki/Authorization>
- c. Forklar om definisjoner av konfidensialitet, integritet og tilgjengelighet (KIT) i standardene X.800 og ISO/IEC 27000 gir mening p  bakgrunn av Wikipedias definisjon av autorisering..

Oppgave 6: Brukerautentisering og data-autentisering

En bruker har autentisert seg til et nettsted p  Internett ved starten av en  kt, og bruker tjenester p  webtjeneren via klientcomputeren. Forklar mulige scenarier som gj r at nettsted/webtjener i l pet av  kten mottar falske data fra klientcomputeren, dvs. data som **ikke** er autentisk sent av brukeren, p  tross av at brukeren er korrekt autentisert.

Oppgave 7: Sikkerhetspolicy for personlig laptop

Artikulere en enkel (2-3 setninger) sikkerhetspolicy for din personlige laptop, som uttrykker hvem som er eller som kan bli autorisert til   bruke laptoppen mens du eier den.

Oppgave 8: ISO/IEC 27000 ISMS – Oversikt

Se p  standarden ISO/IEC 27000 Information security management systems — Overview and vocabulary;

https://www.mn.uio.no/ifi/forskning/grupper/sec/sikkerhetsledelse/iso_iec_27000_2018.pdf

Bruk oversettelsene p  nettsiden:

<https://www.mn.uio.no/ifi/forskning/grupper/sec/oversettelse/>

- a. Hva er forskjellen mellom en *sikkerhetshendelse* og en *sikkerhets-event/-episode*?
- b. Hva er et styringssystem for informasjonssikkerhet (ISMS)?
- c. Gi en tolkning av begrepet «informasjonsverdi»?
- d. Forklar om KIT for informasjonsverdier er dekkende som en generell informasjonssikkerhetsm lsetting? Foresl  en alternativ generell informasjonssikkerhetsm lsetting.