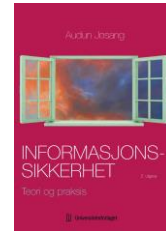


Informasjonssikkerhet: Teori og praksis

Audun Jøsang

2. utgave 2023

Universitetsforlaget



Oppgaver

Kapittel 1: Grunnleggende sikkerhetsbegreper

Oppgave 1: Tilgangsautorisering

- 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?
- Hvordan er autorisering definert på Wikipedia?
<https://en.wikipedia.org/wiki/Authorization>
- Forklar om definisjoner av konfidensialitet, integritet og tilgjengelighet (KIT) i standardene X.800 og ISO/IEC 27000 gir mening på bakgrunn av Wikipedias definisjon av autorisering.

Oppgave 2: 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*».

- Konfidensialitet
- Integritet
- Tilgjengelighet

Oppgave 3: 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?».

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

Oppgave 4: Brukerautentisering og data-autentisering

En bruker har autentisert seg til et nettsted på Internett ved starten av en økt, og bruker tjenester på webtjeneren via klientcomputeren. Forklar mulige scenarier som gjør at nettsted/webtjener i løpet av økten mottar falske data fra klientcomputeren, dvs. data som **ikke** er autentisk sent av brukeren, på tross av at brukeren er korrekt autentisert.

Oppgave 5: 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 å bruke laptoppen mens du eier den.

Oppgave 6: ISO/IEC 27000 ISMS – Oversikt

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

https://www.uio.no/studier/emner/matnat/ifi/IN5080/v23/dokumenter/iso_iec_27000_2018.pdf

Bruk oversettelsene på 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 informasjonssikkerhetsmålsetting? Foreslå en alternativ generell informasjonssikkerhetsmålsetting.