Notater fra IN1020 gruppetime uke 42

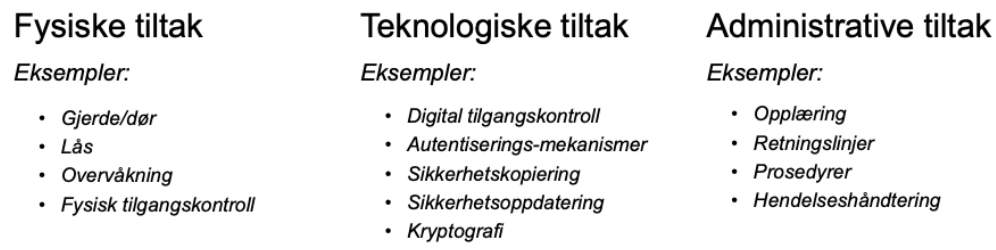
Hva er informasjonssikkerhet?

- Handler om å gjøre de systemene som brukes til å behandle all informasjon sikre, slik at informasjonen ikke blir synlig for uvedkommende, den ikke blir endret eller slettet av uvedkommende, og at den skal være tilgjengelig for de rette personene til rett tid.
- Informasjonssikkerhet er en kontinuerlig prosess for å oppdage og hindre trusler og å fjerne sårbarheter.

Sikkerhetsmål – stikkorda som inngår i informasjonssikkerhet (lag en fin modell på tavla): Det er 6 mål som vi har innen informasjonssikkerhet slik at vi ønsker at alle sikkerhetsaspektet av alle tjenester skal oppnå disse målene.

Sikkerhetstiltak - tiltak vi gjør for å nå sikkerhetsmålene. Vi kan dele sikkerhetstiltak i flere kategorier:

- Fysiske, teknologiske og administrative tiltak er en måte å gruppere på.
- Forebyggende, detekterende, korrigerende tiltak er en annen måte å gruppere på.



De viktigste målene er:

- **Konfidensialitet**:
    - Handler om at kun de som skal ha rett til å se informasjonen gitt i en tjeneste skal ha tilgang til å se denne informasjonen.
    - Det vil si, ingen uvedkommende skal kunne se informasjon som skal være skjult for allmenheten.
    - Viktig mål fordi: Vi vil at kun de som har rett skal kunne få tak i informasjon, siden sensitiv informasjon kan fort misbrukes om den faller i feil hender.
    - Sikkerhetstiltak: kryptering, tilgangskontroll (hvem har tilgang til hva), skallsikring (feks brannmur men også fysiske tiltak).

- **Integritet**:
    - Informasjon skal ikke endres eller slettes av uvedkommende.
    - Det vil si at kun de som har rettigheter skal kunne endre og slette informasjon, og ingen andre.
    - Skal stole på at dataen som er tilgjengelig er korrekt.
    - Viktig fordi: Vi vil vite at den informasjonen vi har er korrekt og at ingen med onde hensikter eller noen med et uhell endrer eller sletter viktig data.
    - Sikkerhetstiltak: tilgangskontroll, endringskontroll, skallsikring, kryptering

- **Tilgjengelighet**:
    - Informasjon skal alltid være tilgjengelig for de som har rett til å få tak i den.
    - I praksis betyr det at informasjonen skal være «brukbar» for de som har rett til den uavhengig av feil, angrep, vedlikehold etc.
    - Viktig fordi: I noen situasjoner trenger vi at informasjon er tilgjengelig til alle tider. Som et eksempel er det viktig å ha tilgang til pasientjournaler (?) til enhver tid, slik at denne informasjonen er tilgjengelig i tilfelle medisinsk personell trenger den.
    - Sikkerhetstiltak: sikkerhetskopier, rutinger for håndtering av data, gjenoppretting

Andre sikkerhetsmål er:

- **Autentisering**:
    - Sjekke at noen er de de utgir seg for å være.
    - Det vil si at man skal kunne verifisere at en person er den de sier de er, for eksempel i en innloggingssituasjon.
    - Viktig for eksempel når man vil logge inn i nettbanken, så er det viktig at kun den rette personen får tilgang før man får tilgang til sensitiv data. Det er (relativt) lett å få tak i brukernavn og passord for kontoer, så derfor er det viktig av vi setter inn mer avanserte mekanismer for å beskytte informasjonen vår.
    - Det gjelder også at for eksempel nettsider er de de utgir seg for å være, og ikke kopier styrt av personer med onde hensikter.
    - Sikkerhetstiltak: 2-faktorautentisering, sertifikat på nettsider (?)

- **Uavviselighet**:
    - Kommer fra u- avvise, eller ikke-avvise.
    - Man skal ikke kunne fornekte en handling.
    - Fra IN1020 ukesoppgaver 2018: Det skal ikke være mulig å påstå at man ikke har gjort noe man har gjort, og at man har gjort noe man ikke har gjort.
    - For eksempel om du har signert en kontrakt, skal ikke du eller den andre parten kunne nekte for at du har signert kontrakten.
    - Sikkerhetstiltak: Digitale signaturer (skal se på hvordan de fungerer senere)

- **Sporbarhet**:
    - Man vil kunne knytte en identitet til en gitt hendelse.
    - Poenget er at alle handlinger skal kunne spores tilbake til en identitet, og at sporene skal bevares til senere.
    - Dette er viktig for at vi skal kunne spore tilbake til en kriminell person, om en kriminell handling skulle være utført, og denne personen kan bli holdt ansvarlig.
    - Sikkerhetstiltak: autentisering (slik at man skal finne den ansvarlige personen), logging av hendelser, etterforskning (korrigerende).

- **Personvern**:
    - Ikke egentlig et sikkerhetsmål, men fortsatt så viktig at vi tar det med.
    - Handler i hovedsak om personopplysninger.
    - Det stilles altså krav til behandling og oppbevaring av personopplysninger som alle må følge.
    - Viktig fordi vi ikke vil at personopplysninger om oss skal komme på avveie og at uvedkommende skal ha tilgang til å se slik informasjon.
    - Sikkerhetstiltak: lovverket som tjenester må følge når det gjelder behandling og lagring av data.

Verdier, trusler og trusselaktører –viktige stikkord