Disse notatene tar utgangspunkt i tema i pensumboka, videoer om sikkerhet på emnesiden og foilene til forelesere

Verdier er hva som er viktig for noen i et gitt tilfelle: helse, miljø, informasjon, sensitiv informasjon, penger, gjenstander, omdømme (dom, vurdering).

Sikkerhetstiltak er basert på spesifikk implementering. De benyttes for å forebygge (forhindre og avskrekke angrepsforsøk), oppdage/avdekke/detektere (varsle angrep som forsøkes eller som allerede har skjedd) eller gjenopprette (gjenopprette skade på informasjonsressurser etter angrep). Informasjon kan være i ulike tilstander: Når den *lagres,* under *overføring,* når den er *i bruk.* Tiltak:

- Fysisk sikring
- Sikker lagring
- Datamaskiner og IT-systemer uten sårbarheter
- Sikre nettverk
- Sikker kommunikasjon
- Bevisste brukere
- Gode arbeidsrutiner
- Tydelig plan for eventuell gjenoppretting

Klassifisering av informasjon

Åpne informasjon: Tilgjengelig for alle (kategori: *grønn*)

Begrenset informasjon: Data som ikke er sensitivt, men som likevel skal beskyttes etter lov eller forskrift. Og dermed ikke skal ut i allmuen (kategori: *gul*)

Sensitive informasjon: Ingen uvedkommende skal ha tilgang til *rød* informasjon

Sikkerhetsmål: Noe vi ønsker å oppnå eller tilby. Ulike **sikkerhetstiltak** brukes for å oppnå sikkerhetsmålene:

Konfidensialitet: Informasjonen bør være tilgjengelig for dem som har rettmessig behov for tilgang. Bakveier til informasjonen bør ikke finnes. Konfidensialitet omfatter alle typer informasjon (grønn, gul, rød). Trussel: Tyveri og lekkasje. Sikkerhetstiltak er:

- Kryptering: Det å gjøre informasjonen uleselig for alle som ikke har en nøkkel for dekryptere informasjon. Vi må sørge for at modifikasjon av data oppdages. Det understøtter *konfidensialitet og integritet.*

- Utfordringer: Krypteringsnøkkel på avveie. Kryptering og dekryptering er ressurskrevende.

- Tilgangskontroll: To typer fins: **Fysisk tilgang** og **digital tilgang**. Tilgangskontroll har disse *grunnleggende* komponentene: Identifikasjon, autentisering, autorisering

  - Autorisering: Spesifisering av tilgangsrettigheter (*policy*). Autorisering håndterer forespørsler om tilgang etter at brukere har autentisert seg
  (Autentisering + autorisering). Det følger et forhåndsdefinert regelsett (policy)
  - Tilgangstyring: Ethvert datasystem må ha en funksjon, hvis oppgave er å håndtere tilgangsforespørsler:
    - Kontrollere forespørsel mot gjeldende policy
    - Innvilge eller avvise tilgang
    - Logge hendelsen til hendelseslogg (ivaretar sporbarhet)
  - Perimetersikring/Skallforsvar: Beskytte en virksomhets dataressurser mot uautorisert tilgang fra omverdenen:

Disse notatene tar utgangspunkt i tema i pensumboka, videoer om sikkerhet på emnesiden og foilene til forelesere

- Brannmur: Den slipper inn eller avviser trafikk inn i og/eller ut fra et nettverk basert på forhåndsdefinerte regelsett. Den fungerer som *tilgangskontroll* for nettverket. Kan være et dataprogram eller maskinvare.
- Innbruddsdeteksjon: Overvåker nettverkstrafikk og kan detektere både forsøk på og suksessfulle innbrudd, datavirus og annen ondsinnet programvare, tjenestenektangrep.

- Fysisk sikring av endenoder

Integritet: Informasjonen bør ikke endres eller fjernes utilsiktet. Integritet omfatter alle typer informasjon (grønn, gul, rød).Trussel: Korrupsjon av data og systemer. Sikkerhetstiltak er:

- Tilgangskontroll
- Endringskontroll
- Kryptografisk sjekksumalgoritme
- Perimetersikring/Skallforsvar
- Digital signering av programvare

Tilgjengelighet: Informasjonen bør være tilgjengelig *når* det trengs for dem som har autorisert tilgang (tilgjengelig for rett person til rett tid). Trussel: Tjenestenektangrep, systemfeil, feilkonfigurasjon (en ansatt har ikke fått riktige tilganger pga. manuell feilregistrering), naturkatastrofer eller strømbrudd. Sikkerhetstiltak er:

- Sikkerhetskopier: En strategi for å ta vare på informasjon over tid. Bidrar til økt tilgjengelighet ved å være i stand til å gjenopprette systemer og data ved uønskede hendelser som endrer eller sletter informasjon.
  - De tar vare på flere ulike versjoner av informasjon.
  - Sikkerhetkopien må også sikres: Lagres trygt adskilt fra opprinnelige disker/data, utilgjengelig for uvedkommende
  - Ta kopi av alle **kritiske** data som en virksomhet trenger for å fungere.
  - Ta kopi av all programvare og konfigurasjon som er **nødvendig** for å behandle en virksomhets data.
  - Sikkerhetskopiering er **ikke** datasynkronisering (synkronisering av data på og fra en rekke enheter)
  - Utfordring: Hvordan kvitte seg med fysiske enheter som inneholder data, uten å potensielt lekke data? Når data slettes fra disk, slettes som regel kun referanse til data. Vi må finne egnede verktøy for å sikre at kassert datautstyr ikke inneholder data som ikke skal komme på avveie.
- Redundante tjenester
- Gode rutiner for hendelseshåndtering og gjenoppretting.

Autentisitet: Skap tillit til ekteheten av en gitt identitet. En *bruker*, et *system*, en *organisasjon* kan autentiseres. Autensitet har en interessant sammenheng til opprinnelsen av *data* også. Den benyttes både om prosessen med å bekrefte en påstått identitet (den eller det noen eller noe er) og om prosessen med å bekrefte at informasjonen er ekte og uendret. Trussel: Nettfisking

- Identifisering: Å gi seg til kjenne, etablere identitet for hvem/hva noen/noe er.
- Identifikator: Noe kjent, ikke hemmelig (alminnelige personlige opplysninger).

Ønsker som regel entydig identifikator.

Autentisering: Å bekrefte en hevdet identitet.

- Organisasjonsautentisering: Verifiser at en virksomhet/organisasjon er ekte, altså den den utgir seg for å være, i en online interaksjon. Dette oppnås ved bruk av *kryptografi*.

Disse notatene tar utgangspunkt i tema i pensumboka, videoer om sikkerhet på emnesiden og foilene til forelesere

- Systemautentisering: Verifiser at et datasystem er det det utgir seg for å være. Dette oppnås ved bruk av *kryptografi*.
- Autentisering av dataopprinnelse (data-origin authentication/message authentication): Verifiser at meldingen/data man mottar kommer fra en hevdet sender og at innholdet er ikke endret underveis i forsendelsen. Dette oppnås ved bruk av *kryptografi*.
- Brukerautentisering: Verifiser en hevdet identitet for en bruker som ber om å aksessere et system eller et program ved bruk av *autentiseringsfaktorer.* For eksempel: brukernavnet (identitet), passordet (autentisering):
  - Autentiseringsfaktorer:
  - Noe du vet: For eks: passord til IT-system, kode til elektronisk dørlås
    - Fordel: Du har det alltid med deg
    - Ulemper: Lett å glemme, lett å gjette for uvedkommende, lagres på datamaskin/nedskrevet (ikke fysisk sikret), lagres hos tjenesteleverandøren
  - Noe du har: For eks: Nøkkel til lås, SIM-kort, kontaktløse-brikker, engangspassord fra kodegenerator
    - Fordel: Du slipper å huske
    - Ulemper: Lett å miste, kan stjeles eller "lånes"
  - Noe du er: For eks: Ganglag, signatur, scanning av øyet, fingeravtrykk, ansiktsgjenkjenning
    - Fordel: Du slipper å huske det, du har det alltid med deg
    - Ulemper: Er det unikt, permanent eller sikkert nok? Ressurskrevende å sammenligne.
  - Autentisering av attributter: Det kan være behov for å autentisere en attributt, i stedet for en identitet, for eksempel alder.
  - Flerfaktorautentisering:
    - Kombinasjon av to eller flere ulike faktorer
    - Øker sikkerheten betydelig, men autentisering blir mer tungvint for den som skal autentisere seg.
    - Økende antall tjenester tilbyr to-faktor-autentisering (2FA), mens svært kritiske systemer også benytter seg av kombinasjoner med ennå flere faktorer.
  - Bruk av 2FA oppfordres
- Aktører tilbyr elektronisk identitet og autentisering som en tjeneste:
  - F. eks: Feide, Google, Facebook, BankID
  - Fordeler: God kompetanse, ekspertise og dermed økt sikkerhet i tjenesten som tilbys. Brukerne må forholde seg til færre brukeridentiteter/passord.
  - Ulemper: Hvis autentiseringsfaktorene knekkes, får hackeren tilgang til flere tjenester.