UKE 35
Gruppe 7 og 18 - IN1020
Introduksjon til informasjonssikkerhet
Jehan Khodabocus

PLAN FOR TIMEN

- Bli kjent
- Kort repetisjon av pensum
- Twitter-hack case oppgave
- Ukeoppgave

BLI KJENT



SIKKERHET

- Beskyttelse av **verdier** mot skade og ødeleggelse.

- Verdi har en svært vid betydning. Hva som er en verdi kan **variere fra person til person** og handler om **hva som er viktig for noen i et gitt tilfelle.**





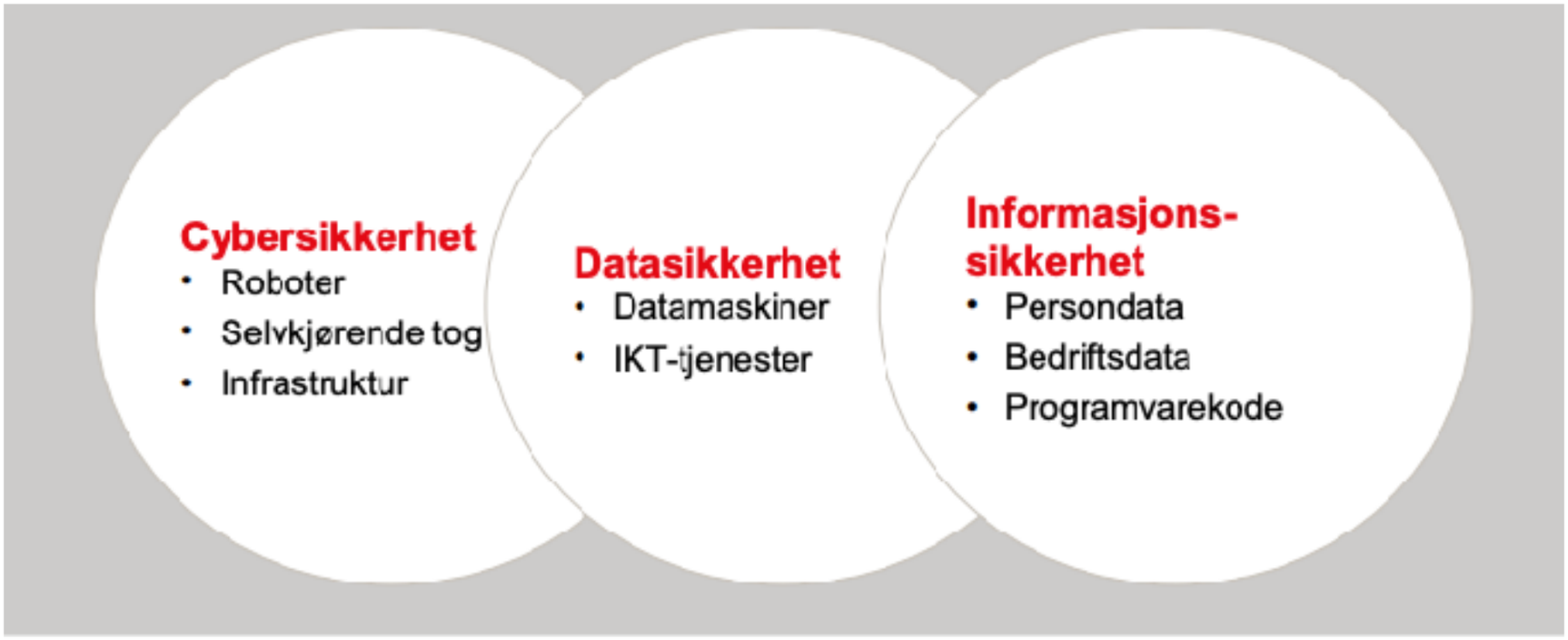




- Bekymringen er **skadelige hendelser**, tilsiktet eller utilsiktet.
  - Naturkatastrofer, krig, ulykker, skade påført med hensikt

- Hva som utgjør en trussel kan defineres ulikt i ulike situasjoner.

DIGITAL SIKKERHET – FLERE BEGREPER



- **Informasjonssikkerhet**: Beskytte ***informasjon*** og ***informasjonsressurser.*** Informasjonen kan være analog (papir) eller digital (filer på et datasystem). Dekker både tilsiktede og utilsiktede hendelser.
- **Datasikkerhet**: Fokus på sikring av IT-tjenester eller systemer og datamaskiner.
- **Cybersikkerhet**: Beskytte ***ting som er sårbare*** via IKT. Tolkes ofte som sikkerhet for alt som har å gjøre med Internett og som er koblet til Internett.

DIGITALE TRUSLER ØKER

- Flere tjenester går digitalt. Det betyr at man også vil se stadig nye digitale trusler. Trenden er at datakriminaliteten økes.
    - Datakriminalitet, sabotasje, industrispionasje, etterretning
- Vanlig å kategorisere trusselaktører
- Drivkraft bak angrep kan være økonomisk vinning, tilgang til hemmeligheter, svekke konkurrenter eller stater, politiske interesser, ideologi, anerkjennelse.
- **Konklusjon**: Informasjonssikkerhet er en kontinuerlig prosess for å hindre trusler og fjerne sårbarheter



SIKKERHETSMÅL OG SIKKERHETSTILTAK

- ***Sikkerhetsmål***
  - En egenskap man kan ønske å oppnå eller tilby
  - Kan oppnås og ivaretas med ulike sikkerhetstiltak
  - Uavhengig av spesifikk implementering
- ***Sikkerhetstiltak***
  - Tiltak for å oppnå/ivareta sikkerhetsmål
  - Basert på spesifikk implementering
  - Benyttes for å forebygge, oppdage eller gjenopprette



SIKKERHETSMÅL FOR INFORMASJONSSIKKERHET

- ***Konfidensialitet:*** Å sikre at informasjon ikke blir gjort tilgjengelig eller vist til uautoriserte individer, entiteter eller prosesser.
  - **Sikkerhetstiltak**: Kryptering, tilgangskontroll, skallsikring.
- ***Integritet:*** Å sikre at informasjon alltid er korrekt, og ikke endres eller slettes utilsiktet.
  - **Sikkerhetstiltak**: Tilgangskontroll, endringskontroll, kryptografisk algoritmer, skallsikring.
- ***Tilgjengelighet:*** Å sikre at en informasjon alltid er tilgjengelig for rett person til rett tid.
  - **Sikkerhetstiltak**: Sikkerhetskopier, redundante systemer, gode rutiner for hendelseshåndtering og gjenoppretting.

SIKKERHETSMÅL

- ***Autentisitet:*** Å legitimere at noen eller noe er den eller det de utgir seg for å være.
  - Brukerautentisering, autentisering av system/organisasjon, autentisering av dataopprinnelse.
- ***Uavviselighet (non-repudiation):*** Hindre mulighet for fornektelse av at en melding er sendt eller mottatt.
  - Kan realiseres ved bruk av digitale signaturer.
- ***Sporbarhet (accountability):*** Å kunne knytte en identitet til en hendelse.
  - Ivaretas gjennom logging av alle hendelser, identifisere alle identiteter, analyse/etterforskning.
- ***Personvern:*** Ikke et sikkerhetsmål, men det er retten til privatliv, til å bli glemt, rett til å bestemme over egne personopplysninger. Et tilleggsmål som bl.a. forutsetter KIT. GDPR (General Data Protection Regulation) definerer krav til personvern.

Alle disse målene har sikkerhetstiltak, som er altså tiltak vi gjør for å oppnå målene

SIKKERHETSTILTAK

- <u>Kan kategoriseres</u>
    - Fysiske tiltak: Dører, gjerder, lås, overvåkning, tilgangskontroll
    - Teknologiske tiltak: Tilgangskontroll, kryptografi, autentiseringsmekanisme, sikkerhetskopiering, sikkerhetsoppdatering av programvare, kryptering (kryptografi)
    - Administrative tiltak: Retningslinjer (policyer), prosedyrer, opplæring, hendelseshåndtering
- <u>For ulike datatilstander</u>
    - Informasjon kan befinne seg i ulike tilstander:
        - Når den lagres, under overføring og når den er i bruk
        - Ulike tilstander krever ulike sikkerhetstiltak.
        - Informasjon **må beskyttes** i alle tilstander.
- <u>I ulike tidsfaser</u>
    - **Forebyggende (preventive) tiltak**: Forhindre og avskrekke angrepsforsøk.
    - **Detekterende (avdekkende) tiltak**: Varsle angrep som forsøkes eller som allerede er skjedd.
    - **Korrigerende tiltak**: Gjenopprette skade på informasjonsressurser etter angrep

  Det er alltid nødvendig å benytte en kombinasjon av tiltak fra alle tre faser for å opprettholde dekkende beskyttelse.


Pause

CASE-OPPGAVE – TWITTER HACK:

- Les artikklen:
  - https://edition.cnn.com/2020/07/17/tech/former-twitter-employees-sleuthing/index.html

  - Social engineering går ut på å skaffe seg tilgang ved å lure noen.

OPPGAVE TIL CASE

1. Hva er det som gikk galt her? Hvilke verdier ble satt på spill?

2. Er det noen flere trusler som kan oppstå som følge av dette annet enn selve bitcoin scammen?

3. Hvilke sikkerhetsmål ble ikke tatt hensyn til? (evt etter rask gjennomgang av sikkerhetsmålene)

4. Hvis dere nå hadde fått i jobb av twitter å unngå at dette kunne skje i fremtiden, hvilke (sikkerhets)tiltak ville dere foretatt?

5. Hvor stor rolle spiller sikkerhet når det kommer til sosiale medier? Hvilke verdier kan bli satt på spill?

6. Hvordan kan man balansere sikkerhet og brukervennlighet i en situasjon som dette? Hva burde prioriteringene være?

UKEOPPGAVE

- https://www.uio.no/studier/emner/matnat/ifi/IN1020/h21/ukeoppgaver/

NESTE UKE

- Datanettverk og litt mer om sikkerhet



SPØRSMÅL

- Email: jehank@uio.no
- eller Mattermost/Teams :)