Uke 12

IN1030 – Gruppe 5 og 6

Dagens plan:

- Repetisjon
  - Introduksjon til informasjonssikkerhet
    - K.I.T
    - Tiltak
    - Risiko og trusler
- Ukesoppgaver
- Obligjobbing?

Mailadressene våre er
tara.soderholm@jus.uio.no og **mysc@uio.no**

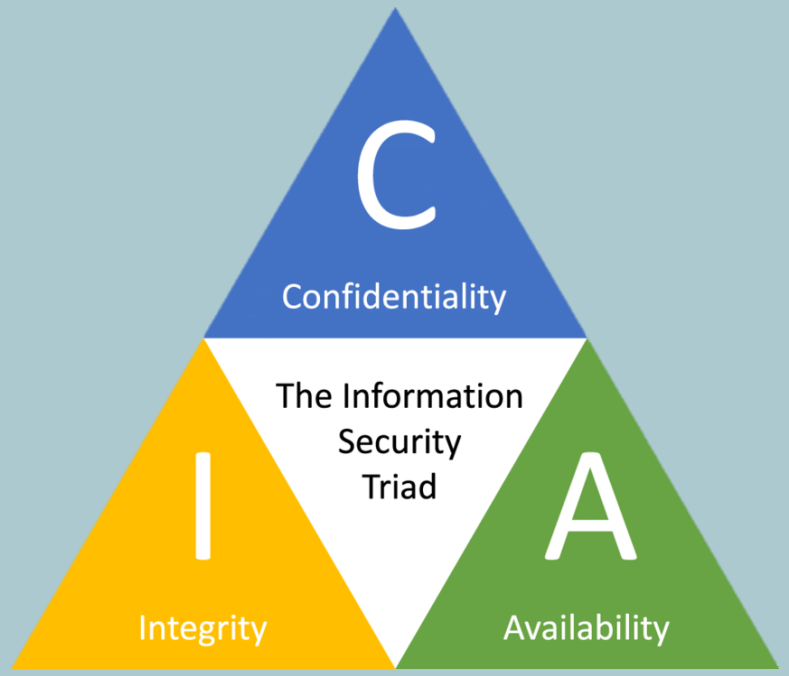
Våre navn (til kontakt gjennom teams etc.) er
Tara Søderholm og My Schultheiss

Informasjonssikkerhet

- Defineres som:

  «Beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet.»
  I tillegg kan andre egenskaper som autentisitet, sporbarhet, uavviselighet og pålitelighet omfattes. (ISO 27000:2016)

- Handler om å beskytte informasjonsressurser mot skade
  - F.eks.: Data, programvare, konfigureringer, utstyr og infrastruktur
- Dekker både tilsiktet og utilsiktet skade;
  - Trusselagenter er som regel mennesker eller naturlige hendelser – mennesker kan gjøre skade både tilsiktet og utilsiktet



Sikkerhetsmålene K.I.T. (C.I.A.)

Konfidensialitet

- Handler om at informasjon ikke skal bli gjort tilgjengelig eller vist til uautoriserte individer, entiteter eller prosesser.
- Typiske trusler:
  - Datatyveri
  - Datalekkasje
- Eksempler på sikkerhetstiltak:
  - Kryptering
  - Autentisering og tilgangskontroll
  - Anonymisering
  - Skallsikring
  - Sikkerhetskultur, bevissthet

Integritet

- Deles i to typer:
  - Dataintegritet:
    - Å sikre at data ikke endres/slettes på uautoriserte måter
  - Systemintegritet:
    - Å opprettholde korrekthet og kompletthet av dataressurser
- Typiske trusler:
  - Ødelagt data
  - Miskonfigurerte systemer
- Eksempler på sikkerhetstiltak:
  - Kryptering
  - Tilgangskontroll
  - Autentisering
  - Sikkerhetskultur, bevissthet

Tilgjengelighet

- Handler om å sikre at data og tjenester er tilgjengelige og brukbare ved forespørsel fra en autorisert entitet/person
- Typiske trusler:
  - Tjenestenekt
  - Hindring av autorisert tilgang til ressurser (løsepengevirus)
  - Forsinkelse av tidskritiske funksjoner
- Eksempler på sikkerhetstiltak:
  - Sikkerhetskopiering (backup)
  - Hendelsesrespons og beredskap
  - Redundans av ressurser

+ Personvern

- Personopplysningsvern (data protection) er et tilleggsmål til K.I.T.-målene som bl.a. forutsetter K.I.T. (Engelsk C.I.A.
- GDPR (General data protection regulation) definerer kravene til personvern

+ Personal data protection

Tiltak

Deles gjerne inn i tre kategorier:

Fysiske tiltak

- Låsing
- Overvåking
- Adgangskontroll

Tekniske tiltak

- Autentisering
- Kryptering
- Autorisering

Administrative tiltak

- Opplæring
- Bakgrunnssjekker
- Internkontroller

Kan gjøres i ulike faser:

Preventivt (forhindring)

Detektivt (funn)

Korrigerende (gjennoppretting)

F.eks:

Preventivt fysisk tiltak: Låse inn

Detektivt administrativt tiltak: Internkontroll

Korrigerende teknisk tiltak: Autentisering

Hva gjør vi?

Vi
- Autentiserer
- Autoriserer
- Krypterer

Autentisering: Å verifisere hvem en entitet er

Autorisering: Å verifisere hva den autentiserte entiteten har tilgang til

Hvordan gjør vi det?

Hva gjør vi?

Vi sørger for

- Konfidensialitet
- Integritet
- Tilgjengelighet

Hvordan gjør vi det?

Tilgangskontroll
Skallsikring
Kryptering

Tilgangskontroll
Endringskontroll
Kryptografiske algoritmer
Skallsikring

Sikkerhetskopier
Redundate systemer
Gode rutiner for hendelseshåndtering og gjennoppretting

Verdier, trusler, sårbarheter og tiltak

Verdier:

- Omhandler ting som er av verdi for organisasjoner:
  - Informasjon,
  - konfidensialitet, integritet og tilgjengelighet for data og systemressurser hos organisasjonene
  - Personopplysningsvern for de involverte/registrerte (privatpersoner)

Trusler:

- Potensielle angrepsscenarioer som styres eller trigges av trusselaktører, og som kan ha negative konsekvenser for verdier

Sårbarheter:

- Fravær av sikkerhetstiltak mot trusler

Sikkerhetstiltak:

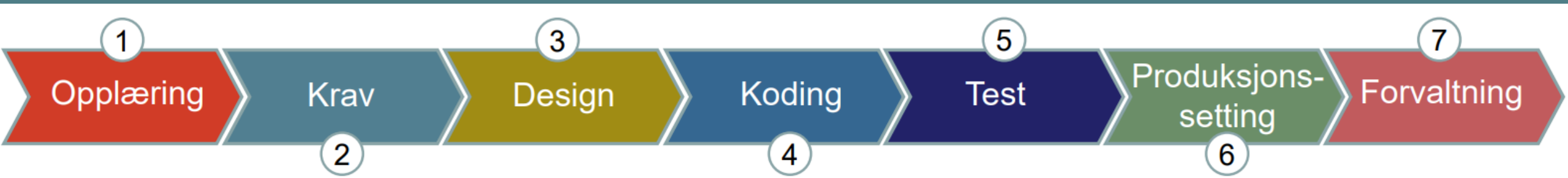
- Metoder for å forhindre trusler og/eller redusere konsekvenser av dem

Person(opplysnings)vern

- Personopplysninger er alle opplysninger og vurderinger som kan knyttes til enkeltpersoner
- «Personopplysning» bruker på lik linje som persondata og personinformasjon
- Personopplysningsvern er å beskytte spesifikke aspekter ved personopplysninger:
  - Å forhindre urettmessig innsamling og oppbevaring av personinformasjon
  - Å forhindre urettmessig bruk av innsamlet personinformasjon
  - Å sørge for at personinformasjon er korrekt
  - Å sørge for åpenhet og innsyn
  - Å sørge for nok informasjonssikkerhet (K.I.T.) rundt personinformasjon
  - Å definere klar ansvarsfordeling

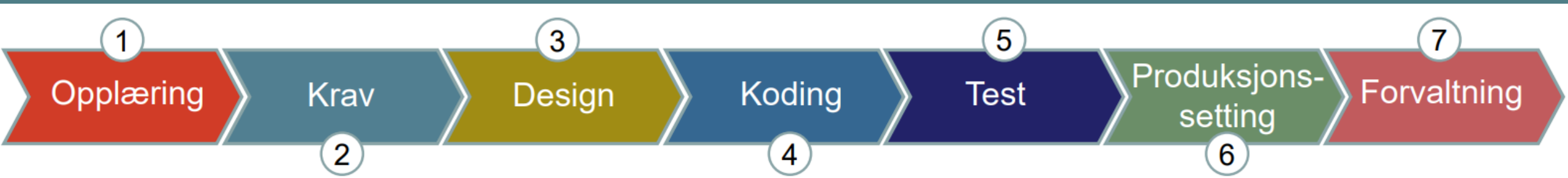
Innebygd IS og personvern

- At IS og personvern er innebygd betyr at en tar hensyn til akkurat disse tingene under hele livssyklusen til programvare og applikasjoner
- Et viktig mål er å finne og redusere sårbarheter tidlig i utviklingsprosessen slik at det blir færre hendelser og sårbarheter å håndtere under drift
- Livssyklusen kan deles inn i 7 faser av en prosess:



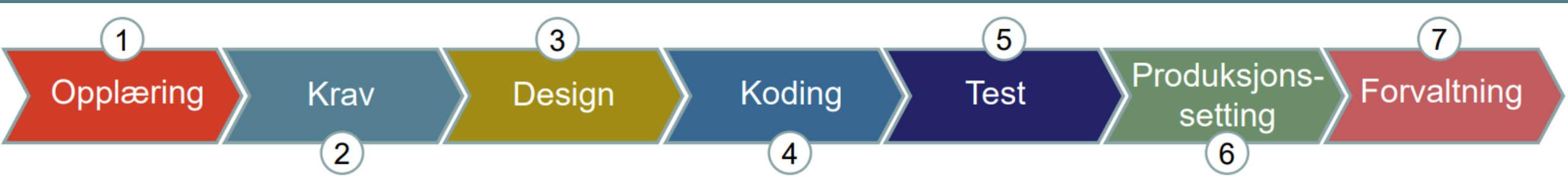
1. Opplæring

- Alle som deltar i utvikling og drift av digitale tjenester og applikasjoner skal ha basiskunnskap og forståelse for
  - Informasjonssikkerhet og personvern
  - Risikovurderinger
  - Trusselmodellering



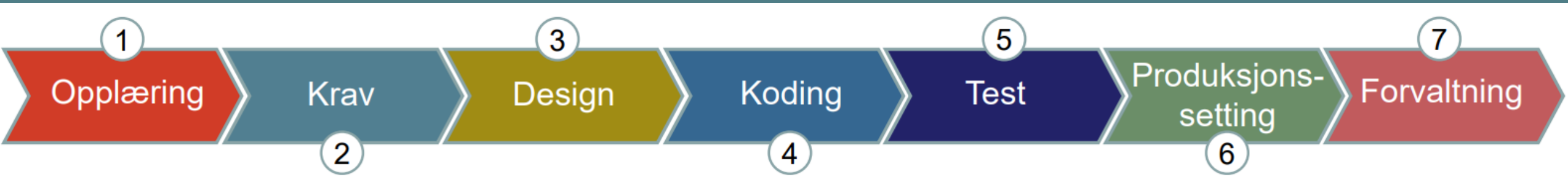
2. Krav

- Krav om informasjonssikkerhet og personvern deles inn i
  - God praksis for sikkerhet i applikasjoner og forretningsprosesser
  - Begrensning av sikkerhetsrisiko til et akseptabelt nivå
  - Juridiske lovbestemte, regulatoriske og kontraktsmessige krav til IS og personvern



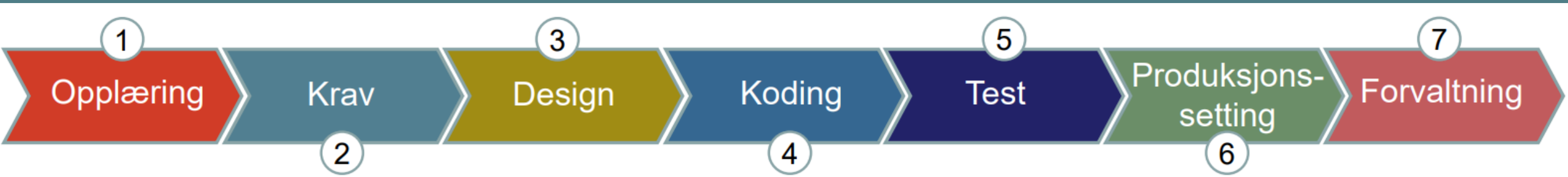
3. Sikkert design, 4. Sikker koding

- Sikkert design
  - En ønsker å spesifisere «sikre funksjoner» som er godt designet med hensyn til nettopp sikkerhet
  - Områder som kryptering, autentisering, logging osv er viktig
- Sikker koding
  - En ønsker å unngå at sårbarheter bygges inn i systemet under koding, og at sikkerhetsfunksjoner fungerer i henhold til krav og design
  - F.eks. statisk analyse, gjennomgang av kode, bruk av «sikre» programmeringsspråk er viktig



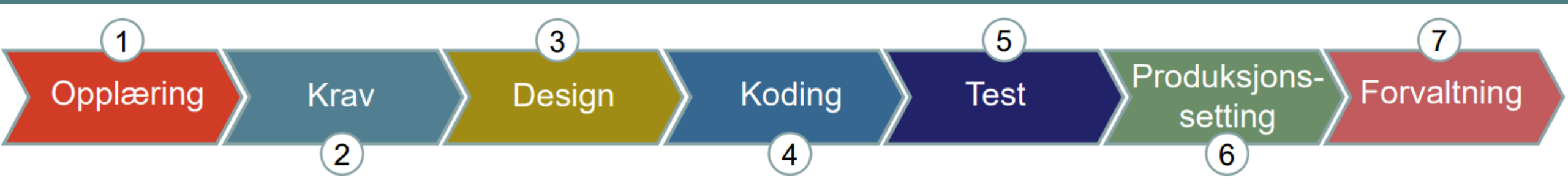
5. Sikkerhetstesting

- En ønsker å avdekke sårbarheter som ikke ble oppdaget i design- eller kodefasene
- En kan f.eks. utføre:
  - Dynamisk testing/ sårbarhetsanalyse – hvor en bl.a. sjekker at brukere får tilgang til informasjon/funksjonalitetene de skal (og ikke de de ikke skal)
  - Penetrasjonstesting – simulerte angrep for å evaluere sikkerheten
  - Fuzztesting – en forsøker å fremprovosere feil i systemet ved å gi korrupte inputverdier



6. Produksjonssetting, 7. Forvaltning

- Produksjonssetting
  - En lager planer for drift, vedlikehold og hendelseshåndtering, med definerte prosedyrer for drift, avviksrapportering og hendelseshåndtering
  - En lager formelle godkjenninger av produksjonssetting hvor en krever verifisering og dokumentasjon på at alle krav til sikkerhet er oppfylt og identifiserte sårbarheter er tilstrekkelig fjernet
- Forvaltning
  - En kjører drift og vedlikehold hvor prosedyrer og rutiner skal følges
  - En fører avviks- og hendelseshåndtering hvor en rapporterer avvik og hendelser og hvordan en skal håndtere disse



PAUSE

Ukesoppgaver

1. Begreper:
   A. Forklar generelt hva informasjonssikkerhet er
   B. Hvilke tre generelle IS-mål har vi? Nevn eksempler på trusler mot hvert sikkerhetsmål, samt hvordan trusselen kan forhindres med sikkerhetstiltak
   C. Hva er forskjellen mellom tilgangsautorisering og tilgangskontroll?
   D. Hva er tre av hovedkildene for krav til IS?
   E. Nevn tre hovedkategorier av sikkerhetstiltak – med ett eksempel fra hvert

Ukesoppgaver

2. Trusselscenario

Stortinget ble utsatt for dataangrep 5. mars 2021. Les om angrepet i artikkelen på NRK: https://www.nrk.no/norge/stortinget-utsett-for-nytt-dataangrep-1.15411279

A. Fra angrepet, definer disse aspektene:
   - Verdier
   - Sårbarhet(er)
   - Trusselaktør
   - Trusselmotivasjon
   - Sannsynlighet
   - Konsekvens

B. Definer risikoen for angrepet basert på opplysningene fra oppg. A.

C. Foreslå tre sikkerhetstiltak for å redusere nivået på denne risikoen

OBLIGJOBBING