UKE 12
Krav om informasjonssikkerhet

IN1030 - Gruppe 8

Plan for i dag

- Repetisjon UML modellering
- Introduksjon til informasjonsikkerhet
- K.I.T.
- Tiltak
- Risiko og trusler
- Alias + Ukesoppgaver

Hva er forskjellen på aktører og interessenter?

- Aktører:
  - de som bruker/brukes av systemet
    - individer
    - systemer
- Interessenter:
  - de som påvirker/påvirkes av systemet
    - individer
    - grupper
    - organisasjoner
    - institusjoner

Brukerhistorier → Use-case diagram

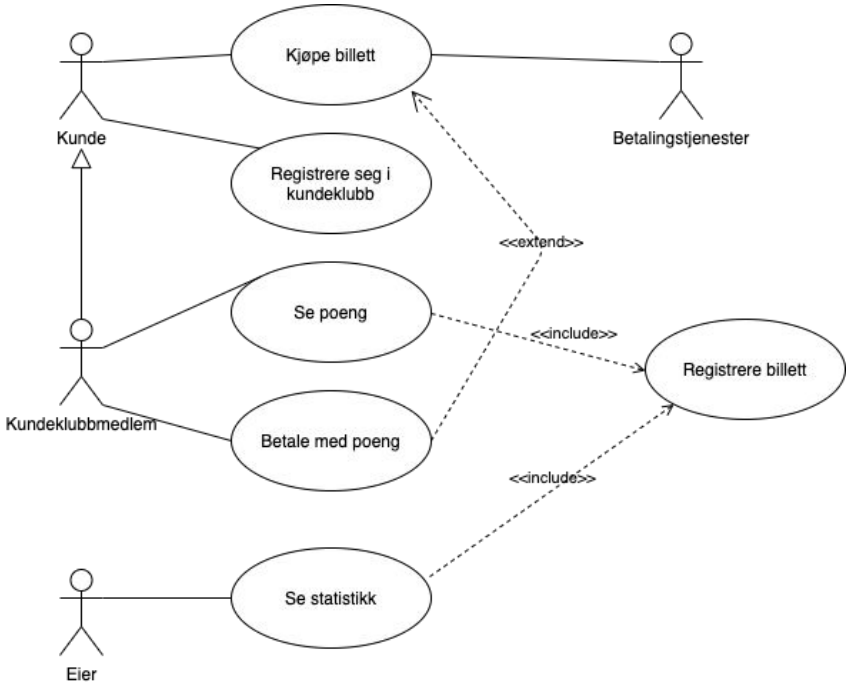
Som kunde ønsker jeg å kjøpe billett slik at jeg kan gå på kino

Som eier ønsker jeg å kunne se statistikk over hvor mange billetter som er solgt slik at jeg kan planlegge visninger fremover

Som kundeklubbmedlem ønsker jeg en oversikt over mine poeng for at jeg kan se om jeg har nok til å kjøpe en kinobillett

Som kundeklubbmedlem ønsker jeg å kunne tjene poeng, slik at jeg kan bruke disse til å betale for billetter

Som kunde ønsker jeg å registrere bruker for å bli medlem av kundeklubben, slik at jeg kan tjene poeng



Tekstlig beskrivelse

Navn: Kjøpe billett
Aktører: Kunde, betalingstjeneste
Prebetingelse: Ingen
Postbetingelse: Billett er kjøpt og PDF genereres

Hovedflyt:
1. Kunde velger en forestilling
2. Systemet viser ledige seter
3. Kunde velger sete blant de ledige
4. Setet holdes av til kunde i 10 minutter
5. Kunde sendes videre til betalingsløsning
6. Kunde velger kort
7. Betaling gjennomføres
8. Bekreftelse på betaling sendes til kunde og registreres i systemet.
9. Billett genereres (PDF)

Alternativ flyt:
4.1 Kunde bruker mer enn 10 minutter på å fullføre kjøp
4.2 Kjøpe avsluttes
4.3 Returnerer til steg 2

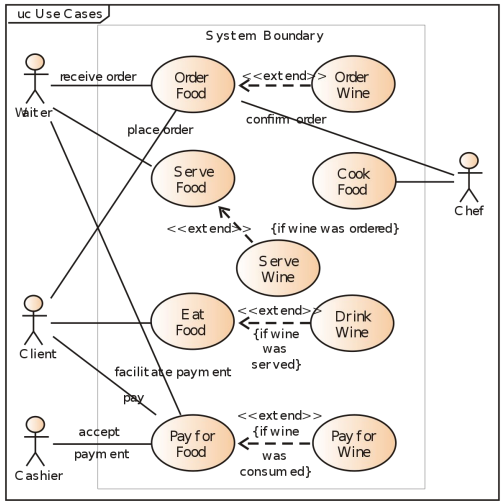
6.1 Kunde velger poeng som betalingsløsning
6.2 Kunde logger inn
6.3 Returnerer til steg 7

7.1 Betaling kan ikke gjennomføres
7.2 Returnerer til steg 2

Diagrammer for dette emnet

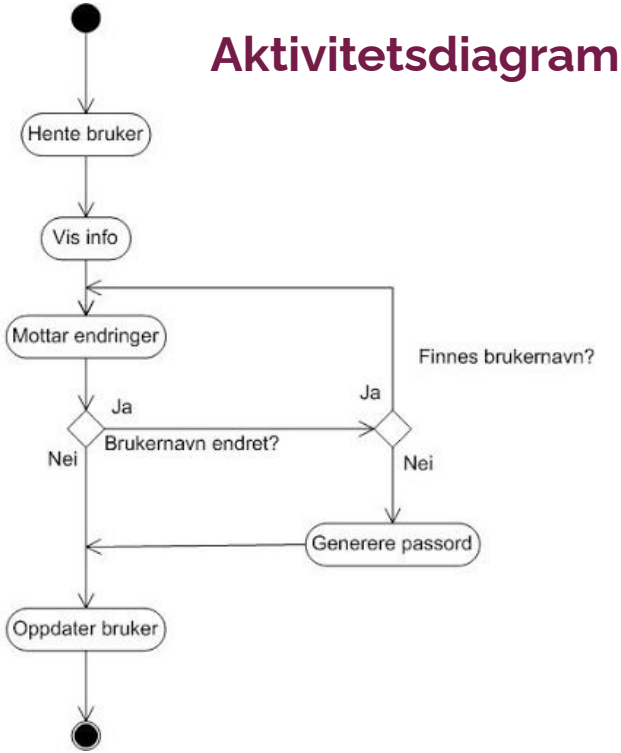
Use Case-diagram:

1.



Aktivitetsdiagram:

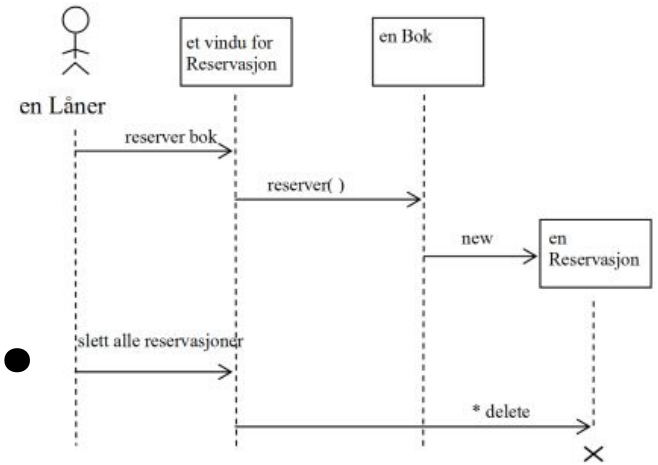
2.



Diagrammer for dette emnet

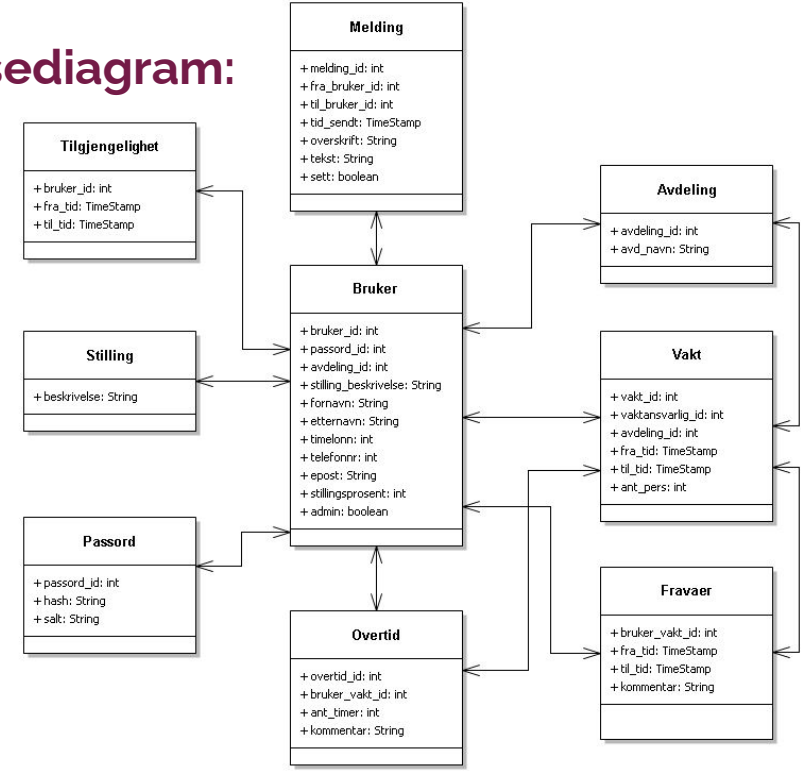
Sekvensdiagram:

3.

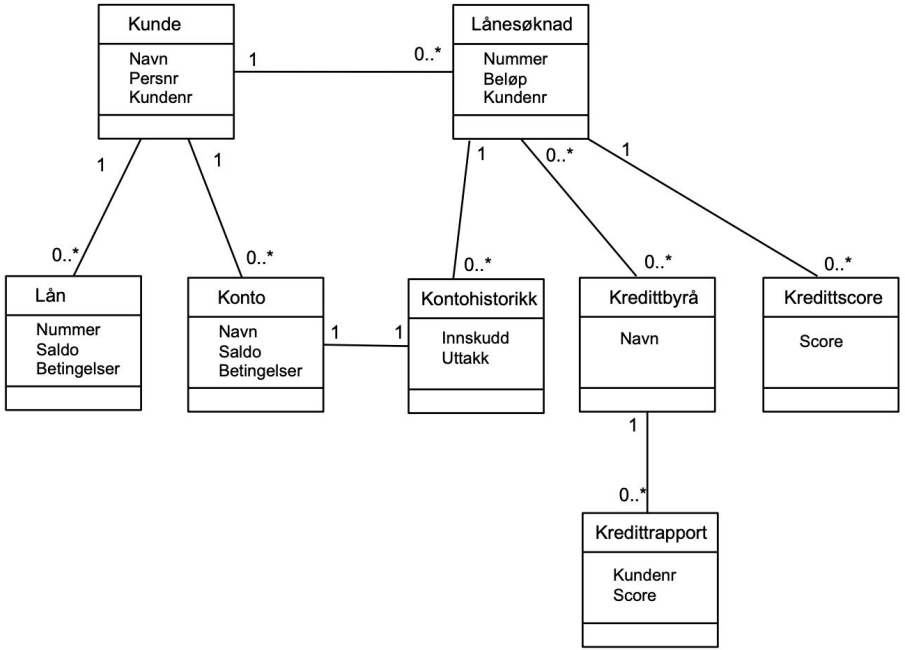


Klassediagram:

4.



Domenemodell - klassediagram uten metoder



IN1020

VERDIER → TRUSSELAKTØRER

Sikkerhetstiltak → K.I.T (konfidensialitet, integritet, tilgjengelighet)

Sporbarhet og autentisering

Private policy - policy for autorisasjon (tilgang)

Informasjonssikkerhet

Informasjonssikkerhet

- Informasjonssikkerhet = beskytte informasjonsressurser mot skade.
- Eksempel på informasjonsressurser som skal ***beskyttes***:
  - Data, programvare, konfigureringer, utstyr og infrastruktur
  - Mot: eks. brut på KIT
- Dekker tilsiktet og utilstiktet skade
  - Trusselagenter → mennesker eller naturlige hendelser
  - Mennesker kan gjøre skade tilsiktet/utilsiktet

- **Definisjon av informasjonssikkerhet:**
  - *Beskyttelse av informasjonens* ***konfidensialitet***, ***integritet*** *og* ***tilgjengelighet****. I tillegg kan andre egenskaper, f.eks. autensitet, sporbarhet, uavviselighet og pålitelighet omfattes* (ISO 27000:2016)

Kilder til krav om informasjonssikkerhet

- Krav om adekvat sikkerhet i forretningsprosesser i henhold til vanlig praksis.
    - *Vanlig praksis setter f.eks. krav om brukerautentisering og tilgangskontroll*
- Krav om å begrense sikkerhetsrisiko i et foretak til et akseptabelt nivå.
    - *Risikovurdering kan f.eks. sette krav om 2-faktorautentisering*
- Juridiske, lovbestemte, regulatoriske og kontraktsmessige krav til informasjonssikkerhet.
    - *Sikkerhetsloven setter en rekke krav om sikkerhetstiltak for de som er underlagt loven. – GDPR setter krav om beskyttelse av persondata.*

Sikkerhetsmål K.I.T. *(+Personvern)*

Konfidensialitet

At informasjon ikke blir gjort tilgjengelig eller vist til uautoriserte individer, entiteter eller prosesser.

Trusler:

- Datatyveri
- Datalekkasje

Eksempler på sikkerhetstiltak:

- Kryptering
- Autentisering og tilgangskontroll
- Anonymisering
- Skallsikring
- Bevissthet

Integritet

- *Dataintegritet: å sikre at data ikke blir endret/slettet på en uautorisert måte*
- *Systemintegritet: å opprettholde korrekthet og kompletthet av dataressurser*

Trusler:

- Ødelagte data og miskonfigurerte systemer

Eksempler på sikkerhetstiltak:

- Kryptografisk integritetssjekk
- Konfigurasjonsstyring
- Endringsledelse
- Tilgangskontroll
- Skallsikring
- Sertifisert programvare
- Bevissthet

Tilgjengelighet

Å sikre at data og tjenester er tilgjengelige og anvendbare ved forespørsel fra en autorisert entitet

Trusler:

- Tjenestenekt
- Hindring av autorisert tilgang til ressurser
- Forsinkelse av tidskritiske funksjoner

Eksempler på sikkerhetstiltak::

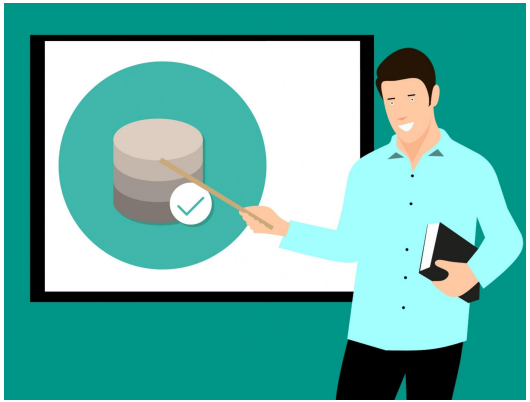
- Redundans av ressurser
- Backup
- Hendelsesrespons og beredskap
- Failover-konfigurasjon

Sikkerhetsmål: K. I. T.

Konfidensialitet: jeg skal **ikke se** data jeg ikke skal kunne se.

Integritet: jeg skal **ikke endre** data jeg ikke skal kunne endre.

Tilgjengelighet: jeg **skal kunne gjøre det jeg vil** med data jeg er skal kunne gjøre det jeg vil med.



Hva gjør vi da?

Konfidensialitet	Integritet	Tilgjengelighet
Tilgangskontroll Skallsikring Kryptering	Tilgangskontroll Endringskontroll Kryptografiske algoritmer Skallsikring	Sikkerhetskopier Redundante system (flere enheter) Gode rutiner for hendelseshåndtering og gjenoppretting

Personvern

Person(opplysnings)vern (data protection) er et tilleggsmål som bl.a. forutsetter KIT. GDPR (General Data Protection Regulation) definerer krav til personvern.

Personopplysninger *er alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson*

Person(opplysnings)vern er å beskytte spesifikke aspekter ved personopplysninger:

- Forhindre urettmessig innsamling og oppbevaring av personinformasjon
- Forhindre urettmessig bruk av innsamlet personinformasjon
- Sørge for at personinformasjon er korrekt
- Sørge for åpenhet og innsyn
- Sørge for adekvat informasjonssikkerhet (KIT) rundt personinformasjon
- Definere klar ansvarsfordeling

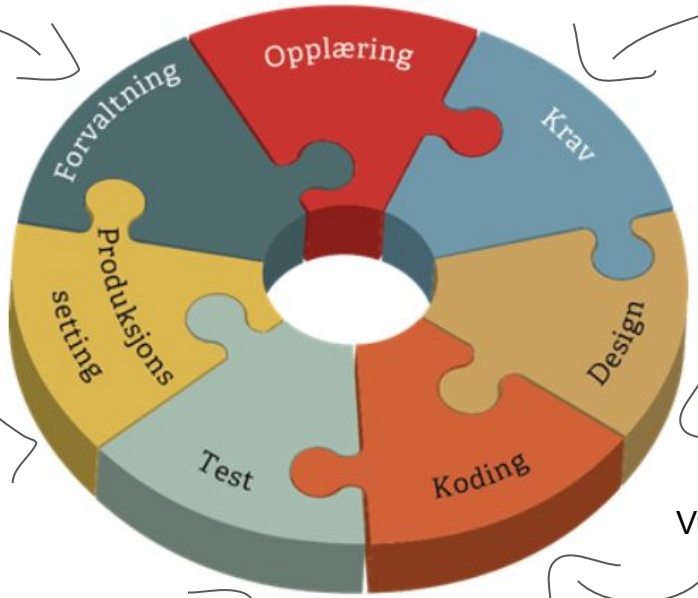
Fra forelesning, 19/4 2022

Innebygd personvern og informasjonssikkerhet:

De som bygger IT systemer må ha kompetanse

Forvalte systemet: skjer det noe - hold seg til planen

Må definere personopplysninger som skal lagres



Har vi en plan for å fjerne sårbarheten?
Hvis det skjer har vi en plan for varsling?

- Plikt til å varsle datatilsynet
- Gi beskjed til pressen à økt tillit

Personvernkrav og sikkerhetskrav gjenspeiles i designet

Vurdere sårbarheter i biblioteker/verktøy

Er krav implementert?
Er kravene riktig implementer?

Tiltak

Tiltakskategorier

Fysiske tiltak	Tekniske tiltak	Administrative tiltak
Låse Overvåke Adgangskontroll Strømførsel	Autentisering Kryptering Autorisering	Opplæring Bakgrunnssjekk Internkontroll

Tiltak kan gjøres i ulike faser:

PREVENTIVE

DETEKTIVE

KORRIGERENDE

Tekniske tiltak

Autentiserer: *er bruker, bruker?*

Autoriserer: *Utdeling av rettigheter*

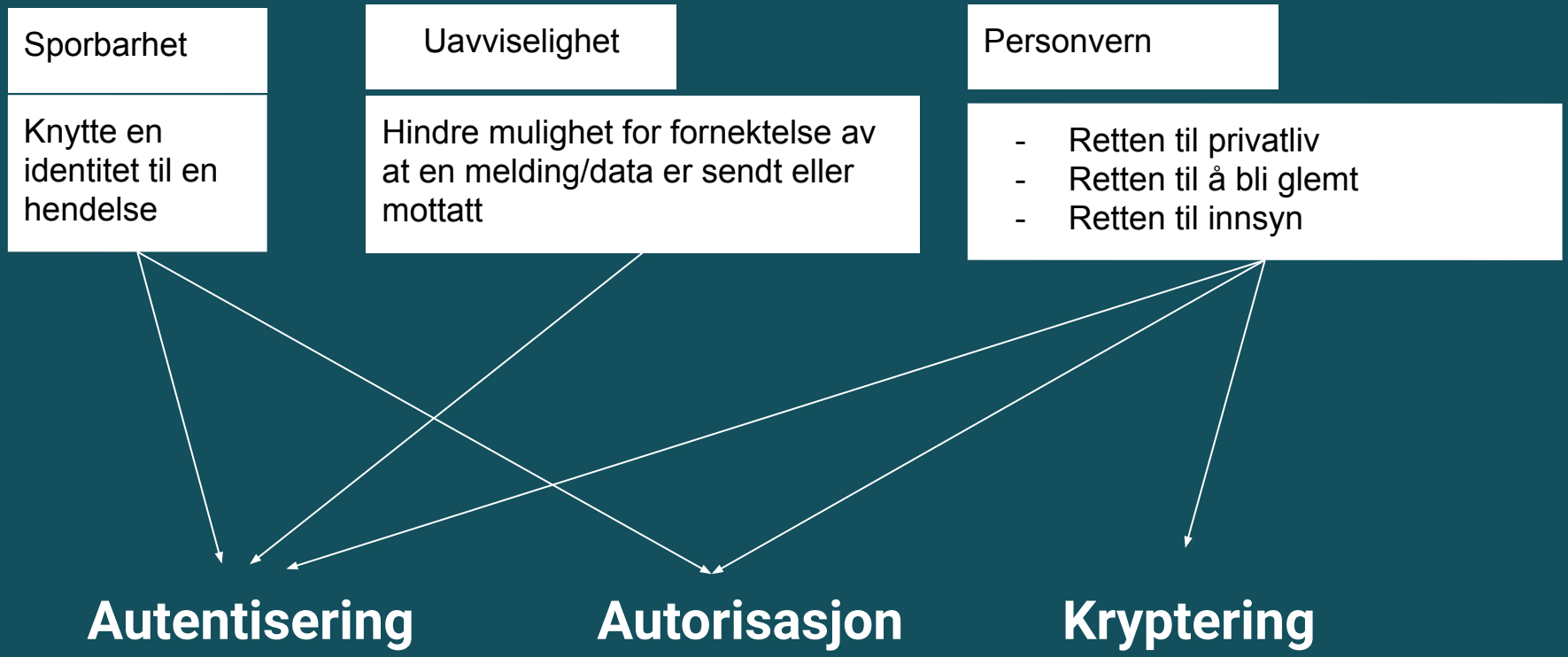
Krypterer: *hold data hemmelig*

Hva kan være eksempler på disse tiltak?

Sikkerhetstiltak - de ulike fasene

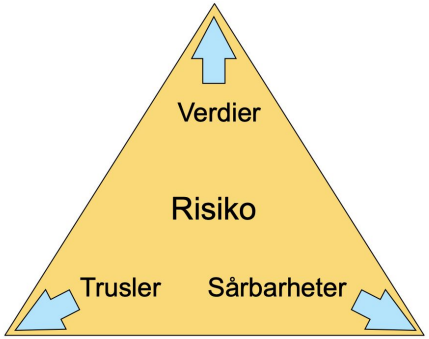
- **Preventive**
  - Forhindre og avskrekke angrep/forsøk
  - Teknisk tiltak: Kryptere filer
  - Fysiske tiltak: låse inn
  - Administrativt: bakgrunnssjekk
- **Detektive**
  - Varsler angrep som blir forsøkt gjort eller som allerede har skjedd
  - Inntreningsdeteksjon
  - Administrerende tiltak: internkontroll
- **Korrigerende**
  - Gjenopprette skader på dataressurser etter angrep
  - Hente backup av data

Flere begrep og hvordan vi kan sikre det



Verdier, trusler, sårbarheter og tiltak

- **Verdier**
  - Informasjon av verdi
  - Konfidensialitet, integritet og tilgjengelighet for data og systemressurser tilhørende organisasjoner
  - Personopplysningsvern for de registrerte (privatpersoner)
- **Trussel**
  - Et potensielt angrepsscenario som styres eller trigges av en trusselaktør, og som kan ha negative konsekvenser for verdier (brudd på sikkerhet/personvern).
- **Sårbarhet**
  - Fravær av sikkerhetstiltak mot trusler
- **Sikkerhetstiltak**
  - Metode for å forhindre trusler eller redusere konsekvenser

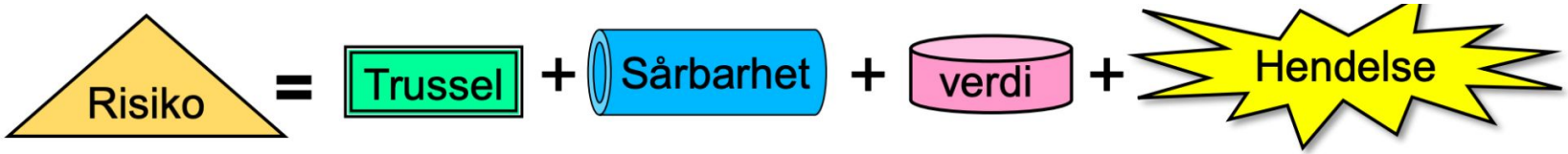


Generell model for risiko.
Figur fra forelesing, 19/4 2022 slide 23

Risiko og Risikonivå

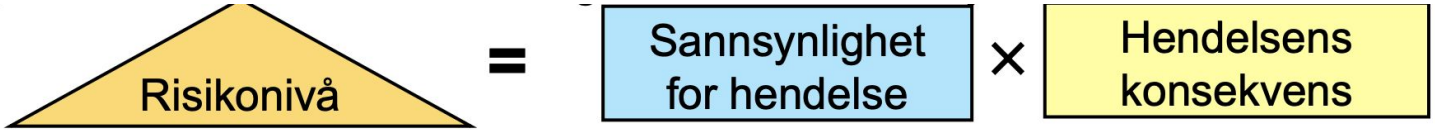
Risiko

Risiko er en relevant kombinasjon av trussel / sårbarhet / hendelse som utgjør et brudd på KIT + P for en verdi. Risikoidentifisering er å kartlegge slike relevante kombinasjoner.



Risikonivå

Risikonivå (også kalt risikoeksponering) er kombinasjonen av hendelsens sannsynlighet og konsekvens. Risikonivå beregnes med risikoanalyse.



Fra forelesning, 19/4 2022

Typer av risiko

Tre hovedtyper av risiko:

- Prosjekt-risikoer vil ha effekt på tidsplanen og/eller ressurser
- Produkt-risikoer vil ha effekt på kvaliteten eller av programvaren som utvikles
- Forretnings (Business)-risikoer vil ha effekt på organisasjonen som utvikler eller eier programvaren

Risiko type	Mulige risikoer
Teknologi	Databasen som brukes i systemet klarer ikke å prosessere så mange transaksjoner per sekund som forventet
Mennesker	Umulig å rekruttere mennesker med den kompetanse som kreves Nøkkel personell ikke tilgjengelig i kritiske faser
Organisasjon	Organisasjonen blir restrukturert slik at ulik ledelse er ansvarlig for prosjektet
Verktøy	Ulike programvareverktøy lar seg ikke integrere
Krav	Endringer av krav krever omfattende "redesign"
Estimering	Underestimering (i tid) av programvareutviklingen Tiden det tar å rette feil er underestimert

Typer av risiko. Matrice fra pensumboken (kap. 22.1.1), gjengitt fra forelesing 22/3 2022

Risiko(nivå)analyse

- Vurder sannsynlighet og mulig konsekvens for hver risiko
- Sannsynlighet kan være svært lav, lav, moderat, høy eller svært høy
- Konsekvensen kan være katastrofal, alvorlig, mindre alvorlig eller ubetydelig

*I **oblig 5** må dere ta med følgende i matricen (min 6 risikoer):*

- *Definert risiko*
- *Sannsynlighet for risiko*
- *Konsekvens av risiko*
- *Hvilke tiltak som må iverksettes for å unngå/minimere risikoen.*
- *Hvem som er ansvarlig for hvert risikomoment.*

Eksempel på risikoanalyse-matrice. Matrice fra pensumboken (kap. 22.1.1), gjengitt fra forelesing 22/3 2022

Risiko	Sannsynlighet	Konsekvens
Det er umulig å rekruttere medarbeidere med kompetansen som er nødvendig	Høy	Katastrofal
Nøkkel personell er syke eller fraværende i kritiske faser av prosjektet	Moderat	Alvorlig
Det er foreslått endringer i kravspesifikasjonen som vil kreve store endringer i design av systemet	Moderat	Alvorlig
Organisasjonen restruktureres slik at ulik ledelse har ansvar for prosjektet	Høy	Alvorlig
Databasesystemet kan ikke prosessere antall transaksjoner per sekund som forventet	Moderat	Alvorlig

Alias-Oppgave

Trussel
Trusselaktør
Sårbarhet

Trusselscenario
Trusselmodellering

Sporbarhet
Uavviselighet
Internkontroll
Styring

Risikovurdering
Risiko
Verdi
Konsekvens

Personvern

Konfidensialitet
Integritet
Tilgjengelighet

Fysiske tiltak
Administrative tiltak
Tekniske tiltak
Preventive tiltak
Detektive tiltak
Korrigerende tiltak

Autentisering
Autorisering
Kryptering
Skallsikring
Tilgangskontroll
Sikkerhetskopier

Ukesoppgaver

Ukesoppgaver - Oppgave 1 og 2

Oppgave 1 - Begreper

a) Forklar generelt hva informasjonssikkerhet er.
b) Hvilke 3 generelle informasjonssikkerhetsmål har vi? Nevn et eksempler på trusler mot hvert sikkerhetsmål, samt hvordan trusselen kan forhindres med sikkerhetstiltak.
c) Hva er forskjellen mellom tilgangsautorisering og tilgangskontroll?
d) Hva er 3 hovedkilder for krav til informasjonssikkerhet?
e) Nevn 3 hovedkategorier av sikkerhetstiltak, med et eksempel fra hver.

Oppgave 2 - Trusselscenario

Stortinget ble utsatt for dataangrep 5.mars 2021.
Les om dataangrepet i artikkelen på NRK som du finner i denne linken.
(*Les evt. om saken på NRK Beta her eller på:*
*"**Seks hackergrupper utnyttet Microsoft-sårbarhetene før de ble kjent**"*)


Stortinget er utsett for dataangrep – data skal vere henta ut

Stortinget er ramma av eit dataangrep, opplyser dei i ei pressemelding. Stortinget stadfestar at data er henta ut, men veit enno ikkje omfanget av angrepet. Stortingspresidenten seier dette angrepet verkar både meir avansert og omfattande enn angrepet i haust.

Espen Alnes
Journalist
Kristian Skårdalsmo
Journalist
Martin Gundersen
Journalist
Line Tomter
Journalist
Julia Kirsebom Thommessen
Journalist

Vi rapporterer frå Oslo

Publisert 10. mars kl. 15:23
Oppdatert 10. mars kl. 20:42

a) I angrepet på Stortinget, definer følgende:
   - Verdier
   - Sårbarhet(er)
   - Trusselaktør
   - Trusselmotivasjon
   - Sannsynlighet
   - Konsekvens
b) Definer risikoen for angrepet basert på opplysningene du har fra oppgave 2a.
c) Foreslå 3 sikkerhetstiltak for å redusere nivået på denne risikoen.

Pensum for denne uken

Foilere fra forelesing

Neste uke: DevOps og håndtering av kode

Foilere

Kapitel 10 i Sommerville: link (merk at password fremgår av filnavn)

Oblig 5 frist: fredag, 6.mai, kl. 23:59.

Takk for i dag!

Har du spørsmål, så send endelig en mail på: nhmoller@uio.no