UKE 12 - Krav om informasjonssikkerhet

IN1030 - Gruppe 2

Hva skal vi i dag?

- Repetisjon UML-diagram
- Introduksjon til informasjonssikkerhet
- K.I.T
- Tiltak
- Risiko og trusler
- Ukesoppgaver

Repetisjon

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

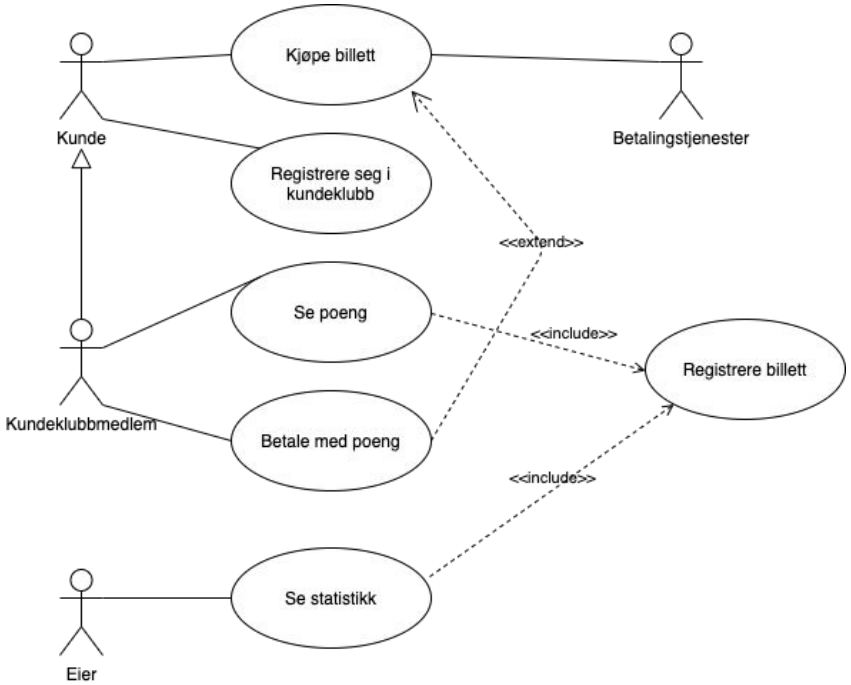
Som kunde ønsker jeg å kjøpe billett slik at jeg kan gå på kino

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

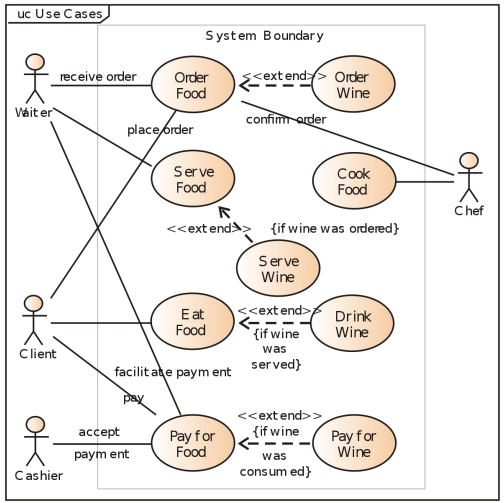
Hovedflyt:
1. Kunde velger en forestilling
2. Systemet viser ledige seter
3. Kunde velger sete blant de ledige
4. Setet holdes av til kunde i 10 minutter
5. Kunde sendes videre til betalingsløsning
6. Kunde velger kort
7. Betaling gjennomføres
8. Bekreftelse på betaling sendes til kunde og registreres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

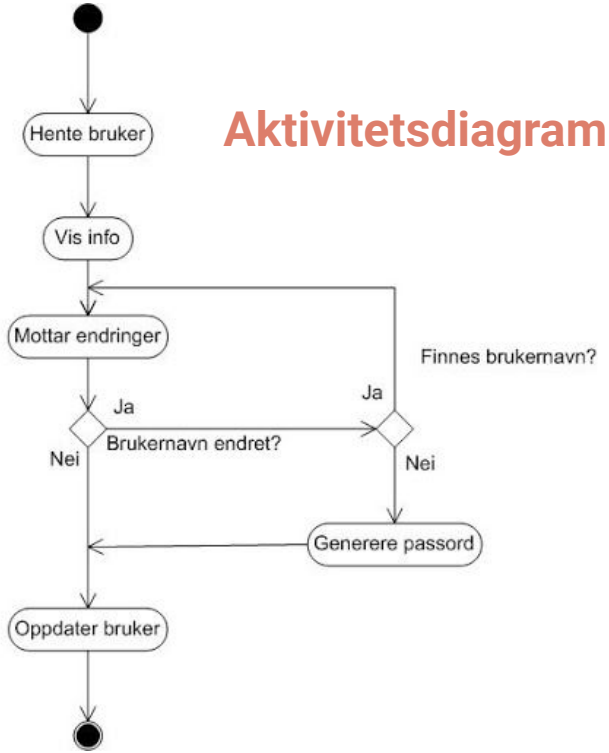
6.1 Kunde velger poeng som betalingsløsning
6.2 Kunde logger inn
6.3 Returnerer til steg 7

7.1 Betaling kan ikke gjennomføres
7.2 Returnerer til steg 2

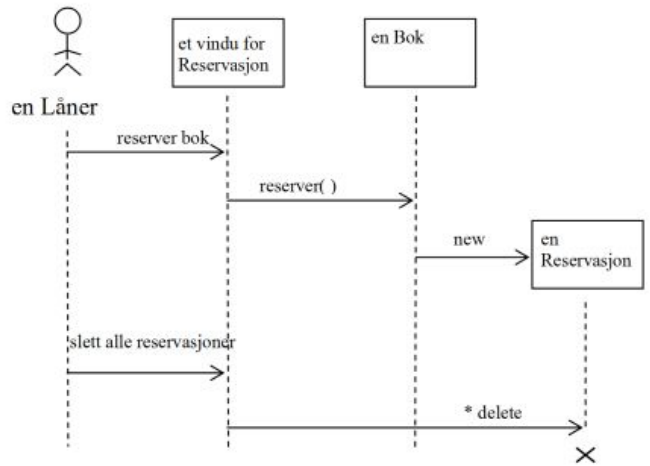
Use Case-diagram:



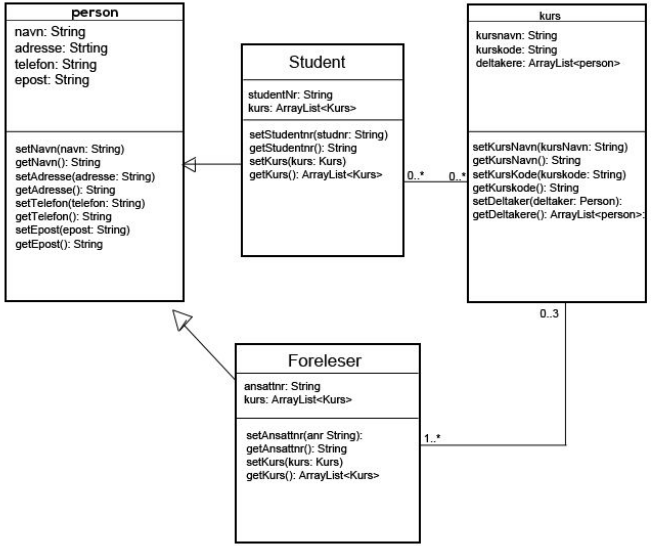
Aktivitetsdiagram:



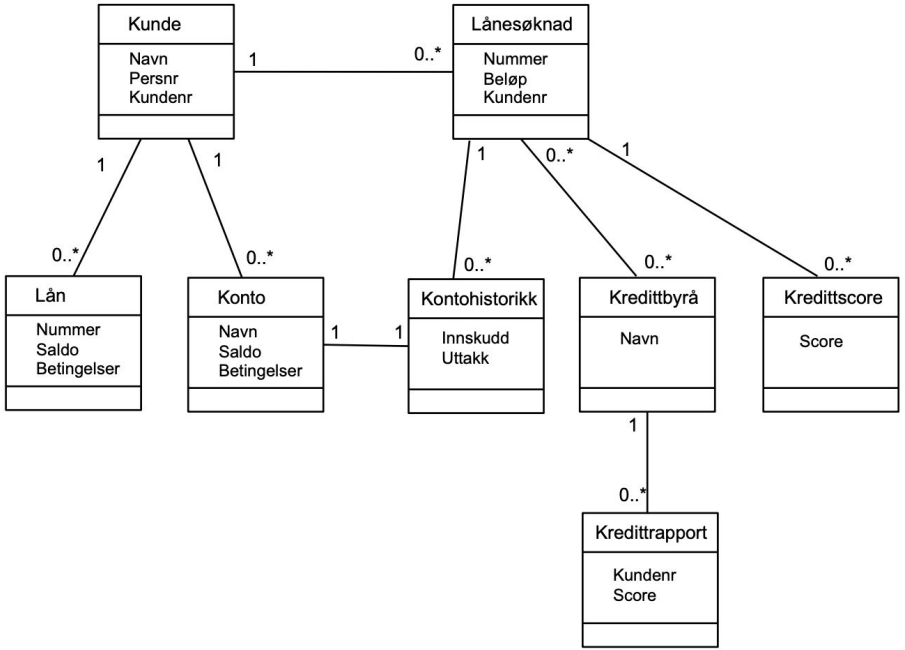
Sekvensdiagram:



Klassediagram:



Domenemodell - klassediagram uten metoder



Spørsmål?

Oblig 5

Risikohåndtering

Knagger å henge risiko på (Hovedtyper):

- **Prosjektrisiko**
  - tidsplan og/eller ressurser
- **Produktrisiko**
  - kvaliteten eller programvaren som utvikles
- **Forretningsrisiko**
  - organisasjonen som utvikler/eier programvaren

Vurderinger for risikoanalyse:
Sannsynlighet: *svært lav - lav - moderat - høy - svært høy*
Konsekvens: *ubetydelig - mindre alvorlig - alvorlig - katastrofal*

Relevant til oblig 5, oppg. 5

Risiko	Sannsynlighet	Konsekvens	Tiltak
Ansatte blir syke	Høy	Alvorlig	Ha tilgang til vikarbyrå
Intern konflikt	Svært høy	Katastrofal	Teambuilding HMS-oppfølging

Relevant til oblig 5, oppg. 5

Informasjonssikkerhet

Verdier, trusler, sårbarheter og tiltak

- Verdier
  - Informasjon av verdi
  - 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

IM

ifi.uio.no Administrativ melding

Lønnsoppdatering 2022

To: Emma Tvinnereim

15 April 2022 at 18:39

UiO : Universitetet i Oslo

Mottaker: < emmatv@ifi.uio.no >

1 ny melding angående lønnslisten din for 2022

https://uio.no/NO/Payr0ll/2022/f0rm.pdf

Informasjonssikkerhet

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

Informasjonssikkerhet

- Informasjonssikkerhet = beskytte **informasjonsressurser** mot skade.
- Informasjonsressurser:
    - Data, programvare, konfigureringer, utstyr og infrastruktur
- Dekker tilsiktet og utilstiktet skade
    - Trusselagenter → mennesker eller naturlige hendelser
    - Mennesker kan gjøre skade tilsiktet/utilsiktet

Hvorfor?

- Som vi allerede har snakket om…
    - juridiske/lovbestemte krav
        - GDPR
            - Beskyttelse av persondata
            - innebygd personvern

Personopplysningsloven: (og GDPR)

- I 2018: så kom «General Data Protection Regulation» (GDPR), som ble tatt inn i Personopplysningsloven.
  - det legges større ansvar på at virksomhetene selv ivaretar personvernet når de behandler personopplysninger, mindre ansvar til Datatilsynet
  - Kravene til utvikling og vedlikehold av internkontroll skjerpes.
  - Forordningen har større fokus på informasjonssikkerhet og avvikshåndtering.
  - Nytt i forordningen er kravet om at informasjonssystemer skal designes med «innebygd personvern».

Sikkerhetsmål K.I.T.

Konfidensialitet

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

Trusler:

- Datatyveri
- Datalekkasje
- Have I been pwnd ?

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

- Hydro & Løsepengeviruset

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:

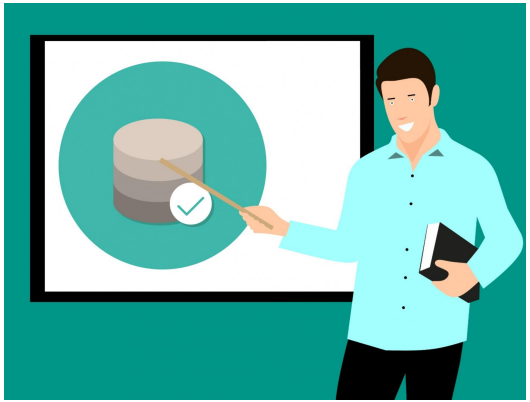
- Redundans av ressurser
- Backup
- Hendelsesrespons og beredskap
- Failover-konfigurasjon

Sikkerhetsmål - opprettholde:

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 skal kunne gjøre det jeg vil med.



Tiltak

Tiltakskategorier

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

PREVENTIVE	DETEKTIVE	KORRIGERENDE

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

Tekniske tiltak

Autentiserer: er bruker bruker?

Autoriserer: utdeling av rettigheter

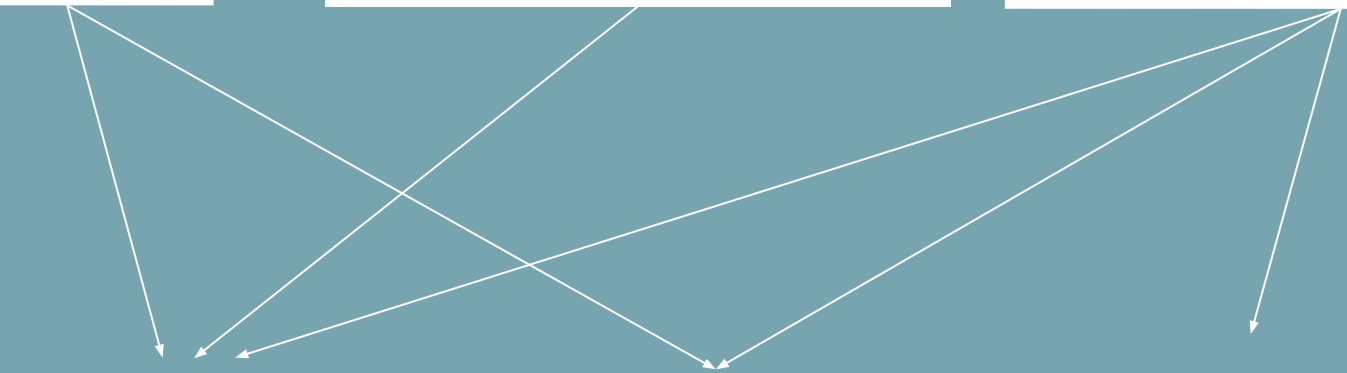
Krypterer: hold data hemmelig

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

Flere begrep og hvordan vi kan sikre det

Sporbarhet	Uavviselighet	Personvern
Knytte en identitet til en hendelse	Hindre mulighet for fornektelse av at en melding/data er sendt eller mottatt	- Retten til privatliv - Retten til å bli glemt - Retten til innsyn



Autentisering **Autorisasjon** **Kryptering**

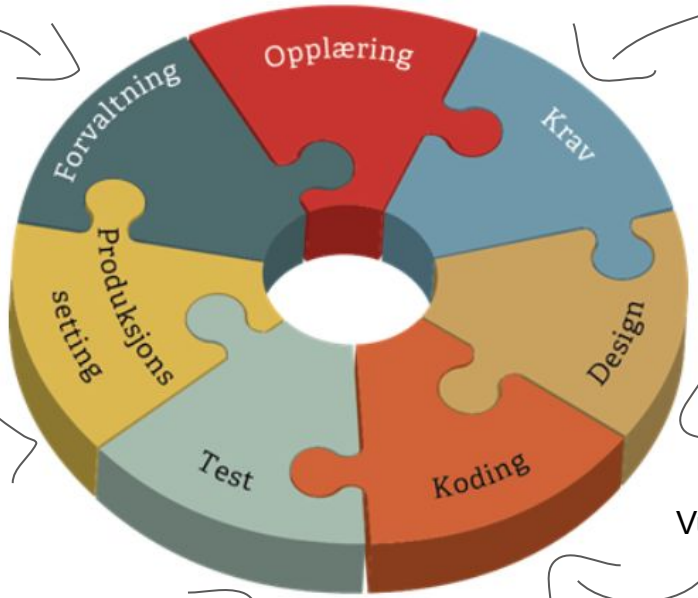
Datatilsynet: Guide

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?

Trussel
Trusselaktør
Sårbarhet

Trusselscenario
Trusselmodellering

Sporbarhet
Uavviselighet
Internkontroll
Styring

Risikovurdering
Risiko
Verdi
Konsekvens

Personvern

Konfidensialitet
Integritet
Tilgjengelighet

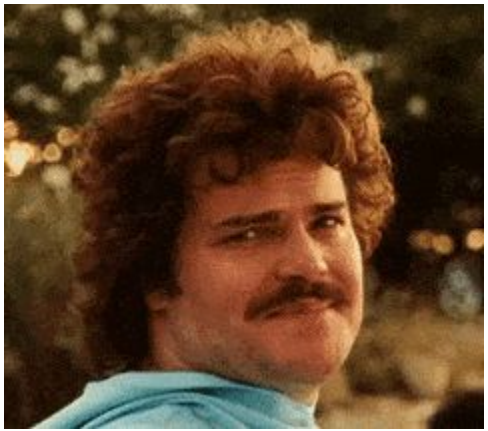
Fysiske tiltak
Administrative tiltak
Tekniske tiltak
Preventive tiltak
Detektive tiltak
Korrigerende tiltak

Autentisering
Autorisering
Kryptering
Skallsikring
Tilgangskontroll
Sikkerhetskopier

Spørsmål?

Ukesoppgaver

Talk but write



UKESOPPGAVER

Fasit

Oppgave 1

Spørsmål A: Forklar generelt hva informasjonssikkerhet er.

Svar A: Generelt kan informasjonssikkerhet tolkes som beskyttelse av informasjonsressurser/verdier mot skade.

Spørsmål B: Hvilke 3 generelle informasjonssikkerhetsmål har vi? Nevn et eksempler på trusler mot hvert sikkerhetsmål, samt hvordan trusselen kan forhindres med sikkerhetstiltak.

Svar B: Spesifikt betyr informasjonssikkerhet å opprettholde sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet (KIT) av informasjonsressurser.

- Konfidensialitet: Trussel er f.eks. tyveri av data. Tiltak er f.eks. tilgangskontroll
- Integritet: Trussel er f.eks. korrupte data. Tiltak er f.eks. data-autentisering
- Tilgjengelighet: Trussel er f.eks. kryptovirus. Tiltak er f.eks. back-up.

Oppgave 1

Spørsmål C: Hva er forskjellen mellom tilgangsautorisering og tilgangskontroll?

Svar C: Tilgangsautorisering er å spesifisere brukeres tilgangsrettigheter til ressurser, mens tilgangskontroll er når systemer håndhever brukeres tilgang til ressurser i henhold til deres tilgangsrettigheter.

Spørsmål D: Hva er 3 hovedkilder for krav til informasjonssikkerhet?

Svar D:
Hovedkilder for krav til informasjonssikkerhet er:

- Krav om adekvat sikkerhet i forretningsprosesser i henhold til vanlig praksis.
- Krav om å begrense sikkerhetsrisiko i et foretak til et akseptabelt nivå.
- Juridiske, lovbestemte, regulatoriske og kontraktsmessige krav til informasjonssikkerhet.

Oppgave 1

Spørsmål: Nevn 3 hovedkategorier av sikkerhetstiltak, med et eksempel fra hver.

Svar:
Hovedkategorier av sikkerhetstiltak:

- Fysiske sikkerhetstiltak: f.eks. lås på døra
- Tekniske sikkerhetstiltak: f.eks. kryptering
- Organisatoriske/Administrative tiltak: f.eks. bevissthetsopplæring

Oppgave 2

Spørsmål:
Stortinget ble utsatt for dataangrep 5.mars 2021.
Les om dataangrepet i artikkelen på NRK som du finner i denne linken.

a) I angrepet på Stortinget, definer følgende:
   - Verdier
   - Sårbarhet(er)
   - Trusselaktør
   - Trusselmotivasjon
   - Sannsynlighet
   - Konsekvens

Svar A: Angrepet på Stortinget kan beskrives med følgende eksempler av karakteristika

- Verdier er f.eks. eposter til stortingsrepresentantene
- Sårbarheten lå visstnok i Microsoft Exchange-serveren
- Trusselaktøren er ikke attribuert, men Russland og Kina er blitt utpekt tidligere.
- Motivasjon er f.eks. spionasje
- Konsekvens er f.eks. svekket demokrati gjennom at vårt demokratiske system blir skadet

Oppgave 2

Spørsmål B: Definer risikoen for angrepet basert på opplysningene du har fra oppgave 2a.

Svar B: Risikoen kan f.eks. beskrives som at en fremmed makt utnytter sårbarhet i Exchange som medfører at stortingsrepresentanters eposter blir stjålet.

Spørsmål C: Foreslå 3 sikkerhetstiltak for å redusere nivået på denne risikoen.

Svar C: Eksempler på sannsynlighetsreduserende sikkerhetstiltak er.

- Lagre eposter kryptert på serveren
- Flytte epost-tjeneren til skyen
- Sterkere beskyttelse av epost-tjeneren med mer avanserte brannmurer og IDS(IntrusionDetectionSystem).
- Sterk 2-faktorautentisering av stortingsrepresentantene

Oppgave 3A

Spørsmål : Nevn 5 aktører beskrevet i Personopplysningsloven (GDPR) med kort beskrivelse av rolle/ansvarsområder.

Svar:
Personopplysningsloven beskriver bl.a. følgende aktører:

- **Den registrerte:** Fysiske personer som på en eller annen måte kan spores fra informasjon lagret om dem (personopplysninger)
- **Den behandlingsansvarlige:** Entitet med overordnet ansvar for at behandling av personopplysninger foregår lovmessig.
- **Databehandleren:** Entitet som prosesserer data på vegne av den behandlingsansvarlige.
- **Datatilsynet:** Direktorat med oppgave å håndheve Personopplysningsloven
- **Personvernombud:** En ansatt utnevnt av behandlingsansvarlige eller av databehandleren til rollen som personvernombud for å gi råd om forpliktelser i henhold til Personopplysningsloven

Oppgave 3B & C

Spørsmål B: Nevn relevante trusselaktører og hvordan de kan skade personopplysningsvern.

Svar: Trusselaktører er f.eks.:

- Hackere som er ute etter å stjele personopplysninger
- Den behandlingsansvarlige, som samler inn, lagrer og behandler sensitive personopplysninger på ulovlig vis, f.eks. uten samtykke, på usaklig grunnlag eller ved å ikke slette data som ikke lenger trengs
- Databehandleren som f.eks. bryter databehandleravtalen og selger eller videresender personopplysninger til tredjeparter.

Spørsmål C: For DPIA (Data Protection Impact Assessment), hvilke trusselaktører er hovedsakelig kilde til personvernkonsekvenser som vurderes?

Svar: For DPIA er det særlig den behandlingsansvarlige og databehandleren som er kilder til personvernkonsekvens, ved at de samler inn, lagrer og behandler personopplysninger på urettmessig måte.

Oppgave 4A

Spørsmål: Nevn hvilke 7 faser Datatilsynet definerer for å oppnå innebygd personvern og informasjonssikkerhet, med eksempler på hva man gjøre for å støtte personvern og/eller informasjonssikkerhet i hver fase.

Svar:
Datatilsynets veileder spesifiserer følgende 7 faser:

- Opplæring: de involverte må ha basiskunnskap om personvern og informasjonssikkerhet
- Krav: f.eks. definere type personopplysninger som skal samles inn og behandles, og hvor lenge det skal lagres
- Design: f.eks. gjøre trusselmodellering
- Koding: f.eks. sørge for at sårbarheter er fjernet eller tilstrekkelig redusert
- Test: f.eks. verifisere at trusselscenarier som ble avdekket i designfasen er håndtert
- Produksjonssetting: f.eks. utarbeide plan for hendelseshåndtering
- Forvaltning: f.eks. håndtere hendelser og avvik etter planen

Oppgave 4B

Spørsmål: Teamet du er en del av skal utvikle et system for oppmøteregistrering av leirdeltakere. Deltakerne må registreres med fullt navn, fødselsdato, allergier, pårørendes tlfnr og betalingsinformasjon. Det er 4 leirledere som registrerer deltakerne. Ranger de 7 fasene etter muligheten for å oppnå adekvat personvern og informasjonssikkerhet. Gi eksempler.

Svar: Alle de 7 fasene er opplagt viktige. Det er kanskje spesielt viktig å vurdere krav og spesifikasjoner, og vurdere om disse er adekvate i henhold til Personopplysningsloven. Dernest er design- og koding-fasene svært viktig for å utvikle et robust system med god struktur og færrest mulig sårbarheter.

Official website of the Department of Homeland Security

emmatv@uio.no