Ukesoppgaver IN1030 2022

Krav on informasjonssikkerhet

Oppgave 1 - Begrep - godt og blandet.

a) Forklar generelt hva informasjonssikkerhet er.
b) Hvilke 3 generelle informasjonssikkerhetsmål har vi? Nevn et eksempel 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 til krav om informasjonssikkerhet?
e) Nevn 3 hovedkategorier av sikkerhetstiltak, med et eksempel fra hver.

Løsningsforslag

a) Generelt kan informasjonssikkerhet tolkes som beskyttelse av informasjonsressurser/verdier mot skade.
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.
c) Tilgangsautorisering er å spesifisere brukeres tilgangsrettigheter til ressurser, mens tilgangskontroll er når systemer håndhever brukeres tilgang til ressureser i henhold til deres tilgangsrettigheter.
d) Hovedkilder for krav til informasjonssikkerhet er:
   - Krav om adekvat sikkerhet i forretningsprosesser i henhold til vanlig praksis.
   - Krav om å begrense sikkerhetsrisiko til et akseptabelt nivå.
   - Juridiske, lovbestemte, regulatoriske og kontraktsmessige krav til informasjonssikkerhet.
e) Hovedkategorier av sikkerhetstiltak:
   - Fysiske sikkerhetstiltak: f.eks. lås på døra
   - Tekniske sikkerhetstiltak: f.eks. kryptering
   - Organisatoriske tiltak: f.eks. bevissthetsopplæring

Oppgave 2 - Risikovurdering

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

b) Definer risikoen for angrepet basert på opplysningene du har fra oppgave 2a.
c) Foreslå 3 sikkerhetstiltak for å redusere nivået på denne risikoen.

Løsningsforslag

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 er blitt utpekt tidligere
   - Motivasjon er f.eks. spionasje
   - Konsekvens er f.eks. svekket demokrati gjennom at vårt demokrtiske system blir skaded
b) Risikoen kan f.eks. beskrives som at en fremmed makt utnytter sårbarhet i Exchange som medfører at stortingsrepresentanters eposter blir stjålet.
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 (Intrusion Detection System).
   - Sterk 2-faktorautentisering av stortingsrepresentantene

Oppgave 3 - Personopplysningsvern.

a) Nevn 5 aktører beskrevet i Personopplysningsloven (GDPR) med kort beskrivelse av rolle/ansvarsområder.
b) Nevn relevante trusselaktører og hvordan de kan skade personopplysningsvern.
c) For DPIA, hvilke trusselaktører er hovedsakelig kilde til personvernkonsekvenser som vurderes?

Løsningsforslag

a) 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 proseserer 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
b) Trusselaktører er f.eks.:
   - Hackere som er utte etter å stjele personopplysninger
   - Den behandingsansvarlige, 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.
c) 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 4 - Innebygd personvern og informasjonssikkerhet

a) 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.
b) 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.

Løsningsforslag

a) 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 trusselmoddelering
   - 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. utarbeid plan for hendelseshåndtering
   - Forvaltning: f.eks. håndtere hendelser og avvik etter planen

b) 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 kodingfasene svært viktig for å utvikle et robust system med god struktur og færrest mulig sårbarheter.