Dilemmatrening — Informasjonssikkerhet

Hjelp til diskusjon

Dilemma A og B

TEMA: Sende opplysninger i e-post

- Alle sider av informasjonssikkerhet (konfidensialitet, integritet og tilgjengelighet) må vurderes.
- Deltagerne må vurdere hensynene bak kravene.
- Hvordan kan du være sikker på hvem som er avsender og mottaker?
- Hvorfor er det eventuelt viktig å vite hvem som er avsender/mottaker?
- E-post er ikke en like sikker kommunikasjonskanal som en del andre kanaler.
  → Er det viktig at informasjonen ikke kommer på avveie?
  → Hvor sikker er du på at informasjonen er riktig når den blir sendt per e-post?
- E-post er i mange sammenhenger et veldig praktisk arbeidsverktøy. Er det viktig at det går raskere og enklere å sende informasjonen på e-post?

Dilemma C

TEMA: Sosial manipulasjon

- Alle sider av informasjonssikkerhet (konfidensialitet, integritet og tilgjengelighet) må vurderes.
- Hvordan kan du vite at det er riktig person du forholder deg til, og er det viktig?
- Hva er konsekvensen dersom opplysningene kommer på avveie?
- Hvordan kan man ivareta en effektiv håndtering av slike forespørsler, og samtidig ivareta konfidensialitetsbehov?
- Kunne Storskolen hatt andre systemer/rutiner som hadde gjort at situasjonen aldri oppstod?
- Bør det innføres retningslinjer for håndtering av slike henvendelser, og i så fall hvilke?

Dilemma D

TEMA: Beredskap og øvelser

- Alle sider av informasjonssikkerhet (konfidensialitet, integritet og tilgjengelighet) må vurderes.
- Det kan være nyttig å diskutere hvor store hendelser de som er på jobb klarer å håndtere:
  → Er det troverdig å tenke seg at hendelser som kan skape mer omfattende utfordringer oppstår?
  → Forekommer det situasjoner hvor det er færre til stede på jobb enn normalt?
  → Kan det tenkes at det kan være situasjoner hvor det er ønskelig eller påkrevet at feil rettes eller henvendelser besvares raskere enn normalt?
- Øvelser er viktig for å:
  → Se at beredskapsplaner med prosedyrer lar seg gjennomføre og fungerer i organisasjonen
  → At de ansatte vet hva de skal gjøre hvis hendelser oppstår.
  → Gjøre det mindre sannsynlig at en uønsket hendelse eller situasjon utvikler seg til en krise.

Dilemma E

TEMA: Tilgangsstyring

- Alle sider av informasjonssikkerhet (konfidensialitet, integritet og tilgjengelighet) må vurderes.
- Deltagerne må vurdere hensynene bak kravene.
- For å få de ansatte til å følge kravene er det viktig at de forstår hvorfor kravene er innført.
- Tilgangsstyring handler ikke kun om å begrense tilgang, men også ivareta behov for tilgang til informasjon og systemer.
- Det kan ikke stilles krav som er så strenge at de gjør arbeidshverdagen unødvendig vanskelig.

Dilemma F

TEMA: Bring your own device

- Alle sider av informasjonssikkerhet (konfidensialitet, integritet og tilgjengelighet) må vurderes.
- Deltagerne må vurdere hensynene bak kravene.
- For å få de ansatte til å følge kravene er det viktig at de forstår hvorfor kravene er innført.
- Viktig å avveie muligheten for kontroll med informasjon og effektivitet i arbeidshverdagen.
- Påvirkes sikkerheten av eierskap til nettbrettet/pc-en/mobiltelefonen?
- Er det andre tiltak som ville ivaretatt sikkerheten bedre?

Dilemma G og H

TEMA: Adgangskontroll

- Alle sider av informasjonssikkerhet (konfidensialitet, integritet og tilgjengelighet) må vurderes.
- Deltagerne må vurdere hensynene bak kravene.
- For å få de ansatte til å følge kravene er det viktig at de forstår hvorfor kravene er innført.
- Det er viktig å huske på at fysisk sikkerhet og adgangskontroll påvirker informasjonssikkerheten.
- Krav til adgangskontroll må være praktiske i arbeidshverdagen. For mange eller for strenge sikkerhetstiltak kan føre til at de ansatte omgår kravene.
- Det kan være hensiktsmessig å differensiere mellom hvem som får tilgang til hvilke deler av lokalet.

Dilemma I

TEMA: Låse pc

- Alle sider av informasjonssikkerhet (konfidensialitet, integritet og tilgjengelighet) må vurderes.
- Skal alle alltid ha tilgang til all informasjon selv om man jobber på samme prosjekt?
- Hvis alle kan bruke en ulåst pc, vet man ikke hvem som har endret/lagt til/slettet informasjon. Hvilke konsekvenser vil dette få, og for hvem? (Arbeidsplassen, deg selv, andre brukere)
- Kan du få problemer dersom en kollega bruker din pc til å utføre handlinger som ikke er tillatt? F.eks. laste ned filer ulovlig eller utført andre handlinger i strid med intern sikkerhetsinstruks.

→ Du finner mer informasjon på digdir.no