Informasjonssikkerhet: Teori og praksis

Audun Jøsang
2. utgave 2023
Universitetsforlaget

Oppgaver

Kapittel 14: Risikostyring

Oppgave 1: Risikofaktorer

a. Hva er forskjellen på «risiko» og «risikonivå» i kontekst av informasjonssikkerhet?
b. Nevn faktorer/elementer som kan påvirke sannsynligheten for en sikkerhetshendelse (at hendelsen inntreffer).
c. Forklar om det er lett/meningsfullt å redusere sannsynligheten for en hendelse.
d. Nevn faktorer/elementer som kan påvirke konsekvensen av en sikkerhetshendelse (hvor alvorlig en hendelse er).
e. Forklar om det er lett/meningsfullt å redusere konsekvensen av en sikkerhetshendelse.

Oppgave 2: Risikoaspekter

a. Hva menes med at en hendelse medfører et sikkerhetsbrudd?
b. Nevn relevante konsekvensaspekter av en sikkerhetshendelse.
c. I tilfelle en sikkerhetshendelse har ulike konsekvensaspekter – hvordan bør disse inkluderes i analysen av hendelsens risiko?

Oppgave 3: Risikokommunisering

a. Hvorfor er det viktig å kommunisere trussel-/risikovurderinger?
b. Hvem skal trussel-/risikovurderinger kommuniseres til?
c. Nevn faktorer for å kunne kommunisere trussel-/risikovurderinger på en god måte?

Oppgave 4: Tolkning av risiko

Ordet «risiko» har mange ulike meninger. I setningene nedenfor, gi en tolkning av «risiko», og omskriv setningen ved å bruke andre ord enn «risiko».

a. «Det er risiko for regnvær når vi skal ha hageselskap på lørdag.»
b. «Det er forbundet med stor risiko å kjøpe aksjer i Norwegian nå.»
c. «Det er liten risiko å sette pengene i banken.»
d. «Kryptovirus utgjør en betydelig risiko.»

Oppgave 5: Operasjonell risiko

a. Hva menes med at informasjonssikkerhetsrisiko er en form for operasjonell risiko?
b. Hva er potensialet for å styre operasjonell risiko i forhold til å styre markedsrisiko?

Oppgave 6: Beslutningspunkter i forbindelse med risikostyring

Risikostyringsprosessen beskrevet i ISO 27005 inneholder 2 beslutningspunkter.

a. Beskriv en situasjon hvor svaret på beslutningspunkt 1 (etter risikovurdering) er NEI, som dermed medfører en ny gjennomgang av kontekst eller trinnene i selve risikovurderingen.
b. Beskriv en situasjon hvor svaret på beslutningspunkt 2 (etter planen for risikohåndtering) er NEI, som dermed medfører en ny gjennomgang av alle tidligere faser i risikostyringen.

Case om risikostyring for advokatfirma

Aker Advokater er et (fiktivt) advokatfirma i Oslo som tar på seg oppdrag for juridisk rådgivning og for å representere personer og organisasjoner i rettsaker. En heltidsansatt kontorsjef bistår advokatene med kontorstøtte og i saksbehandling. Regnskap gjøres av et eksternt regnskapsbyrå.

Oppgavene går ut på å gjøre en risikovurdering.

Mal for risikovurdering ligger på http://www.nettressurser.no/informasjonssikkerhet

Situasjon for oppgave: Egen server

Advokatfirmaet har en egen filserver stående i firmaets lokaler, driftet av kontorsjefen med støtte fra et eksternt IT-firma. Serveren benyttes for lagring av saksdokumenter, for kontorfunksjoner og som epost-server. Alle advokatene har også personlige enheter som laptopp og smarttelefon. Saksdokumenter kopieres manuelt fra personlige enheter (laptopp og smarttelefon) via VPN til serveren. Til nå er det ikke inntruffet noen sikkerhetshendelser.

Antagelser:

- Innlogging til serveren skjer med vanlig passord
- Det fins ingen policy for passord, alle velger passord som de vil og endrer når de vil.
- De ansatte har en ad-hoc bevissthet og kultur rundt informasjonssikkerhet.
- Det eksterne IT-firmaet gjør følgende:
    - Backup av datafiler og epost hver natt,
    - Konfigurerer det lokale nettverket med brannmur
    - Oppdatering og konfigurering av programvare ca. en gang per år.
    - Logging av nettverkstrafikk og aktiviteter på serveren
    - Monitorering av logger med Snort IDS, men ingen hendelsesrespons.

Oppgave

a. Identifiser viktige verdier (informasjon, IT-infrastruktur, tjenester), og relevante sikkerhetsmål (konfidensialitet, integritet, tilgjengelighet), som trenger beskyttelse.
b. Utfør en enkel risikovurdering, ved å beskrive en eller flere risikoer og relevante sikkerhetstiltak. Bruke mal for kvalitativ eller relativ risikovurdering (og eventuelt også mal for relativ konsekvensberegning), som ligger på Canvas for ITLED4230 2022. Hver risiko og foreslåtte sikkerhetstiltak beskrives ved å:

    - beskrive trussel, sårbarhet(er) og hendelse (brudd på sikkerhetsmål).
    - beskrive konsekvensaspekter ved hendelsen
    - estimere sannsynlighet og konsekvensnivå
    - beregne risikonivå før nye sikkerhetstiltak.
    - foreslå sikkerhetstiltak for å redusere risikoen
    - revurdere risikonivået etter innføring av sikkerhetstiltak(ene)