Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver

Del 12: Risikostyring

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
https://www.mn.uio.no/ifi/forskning/grupper/sec/laeringsressurser/uio-risikovurdering-kvalitativ.xlsx

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. Ufør 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)