Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2018
Workshop-spørsmål

Forelesning 8: Risikostyring, Beredskap og Kontinuitetsstyring

Spørsmål 1: Risikofaktorer

En mulig definisjon på IT-sikkerhetsrisiko er: *Risiko = Sannsynlighet × Konsekvens*

a. Forklare hva som menes med *Sannsynlighet* og *Konsekvens* i denne definisjonen.
b. Diskutere, f.eks med et relevant eksempel, om dette er en rimelig definisjon.
c. Nevn faktorer for *Sannsynlighet* av en sikkerhetshendelse (at trusselen inntreffer).
d. Diskuter om det er meningsfullt å analysere risiko basert på detaljerte faktorer (som trusselaktørens *motivasjon* og *kapasitet*) i en praktisk risikoanalyse.

Spørsmål 2: 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.

Spørsmål 3: Risikobeskrivelse

Hvordan bør hver risiko beskrives?

Spørsmål 4: Kvalitativ risiko

a. Anta at en risikovurdering bruker tre nivåer av sannsynlighet (lav, middels, høy) og tre nivåer av konsekvens (liten, moderat, stor). Lag en passende tabell over kvalitative risikoer med 5 kvalitative risikonivåer.
b. Hva er grunnlaget for spesifisering av kvalitative risikonivåer i tabellen?
c. Hvordan brukes tabellen/matrisen til å estimere risikonivåer?

Spørsmål 5: Relativ / Semi-kvantitativ risiko

a. Anta at en risikovurdering bruker fire relative nivåer av sannsynlighet: 0 (ekstremt sjelden), 1 (sjelden), 5 (sannsynlig), 10 (svært sannsynlig), og fire relative nivåer av konsekvens: 0 (ubetydelig), 1 (liten), 5 (moderat), 10 (stor). Lag en passende tabell med relativ / semi-kvantitativ risiko som inneholder 7 numeriske relative risikonivåer.
b. Hva er grunnlaget for å angi de relative risikonivåene i tabellen?
c. Hvordan brukes tabellen/matrisen til å estimere risikonivåer?

Spørsmål 6: Kvantitativ risiko

Anta at du skal foreta en kvantitativ risikoanalyse for en bedrift. En bestemt trussel forventes å resultere i en sikkerhetshendelse annenhver måned med en kostnad på $3 000 per hendelse.

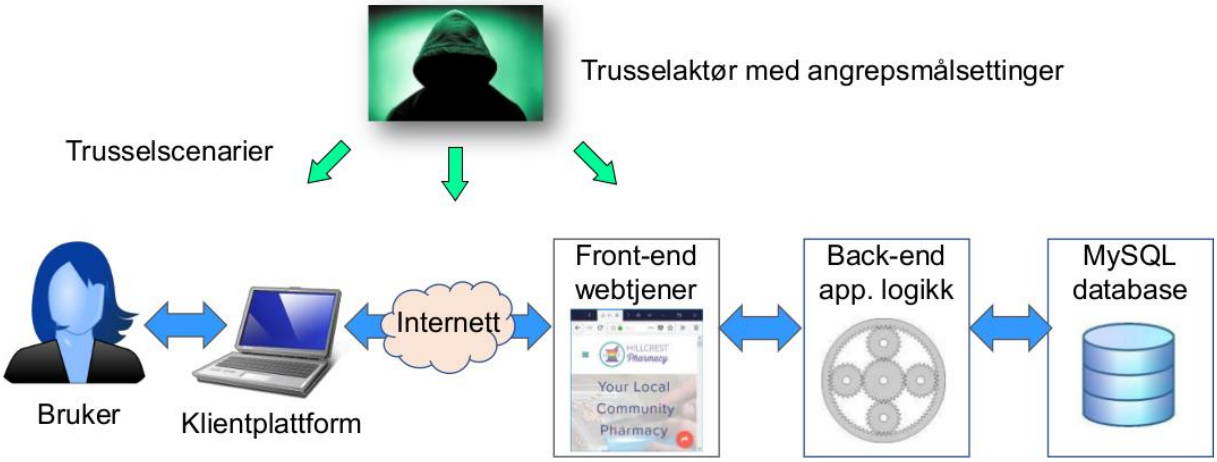
a. Hva er forventet tap for hver enkelthendelse (SLE) (Single Loss Expectancy) og forventet tap per år (ALE) (Annualised Loss Expectancy) ?
b. Hvordan bør ALE brukes for å bestemme håndteringen av denne risikoen?
c. Når et sikkerhetstiltak innføres, hvordan vil dette endre en senere risikoanalyse?
d. I stedet for å redusere risikoen, nevn to alternative måter å håndtere en risiko.

Spørsmål 7: Kvalitativ vs. kvantitativ risiko

På hvilken måte er kvalitativ og kvantitativ risikoanalyse forskjellig? Forklar en betydelig ulempe ved hver type.

Spørsmål 8: Trusselmodellering

Anta at du skal gjøre risikovurdering for et online-apotek, der diagrammet under illustrerer hovedelementer i arkitekturen, i tillegg til abstrakte trusler.



Det kan f.eks. antas at angriperen (trusselaktøren) har som målsetting å 1) ta over brukerkontoer og deres innkjøpshistorie, 2) stjele brukerdatabasen (og passord), 3) sabotering, DDoS eller tilgrising av nettsiden, eller 4) lagre skadevare (XSS, trojanere, exploits) på nettsiden. Du kan også vurdere andre angrepsmålsettinger.

a. Beskriv relevante trusselscenarier for hver angrepsmålsetting du vil vurdere. Ikke bli stående fast pga. mangel på detaljer i denne case-beskrivelsen, du kan gjøre antagelser du syns passer. Det viktige er å kunne identifisere og artikulere relevante trusselscenarier, dvs. trinn angriperen må ta for å oppnå en bestemt angrepsmålsetting.
b. For hvert trusselscenario, foreslå sikkerhetstiltak som kan blokkere eller redusere trusselen.

Spørsmål 9: Feilbetegnelsen «ROS-analyse»

a. Hva er problemet med begrepet «ROS-analyse» (risiko- og sårbarhetsanalyse) som ofte brukes på norsk i sammenheng med risikostyring?
b. Hvorfor er TOR-analyse (trussel og risikoanalyse) en bedre betegnelse ?

Spørsmål 10: Konsekvensanalyse

a. Hva er spesielt med risiko relatert til katastrofer, i form av sannsynlighet og konsekvens?
b. Som en del av virksomheten kontinuitetsplanlegging gjøres ofte en konsekvensanalyse (BIA -Business Impact Analysis). Forklare kort hensikten med en konsekvensanalyse.
c. Hvorfor er en konsekvensanalyse ofte mer meningsfylt enn en tradisjonell risikovurdering i tilfelle beredskap og kontinuitetsstyring.

Spørsmål 11: Lengste akseptable nedetid

a. Hva er typisk *lengste akseptable nedetid* (MTD – Maximum Tolerable Dowtime) for en forretningsprosess definert henholdsvis som: (i) kritisk og (ii) ikke-essensiell ?
b. Anta at IT-systemene til en organisasjon har fått så store skader at det alvorlig påvirker forretningsprosessene. Hvordan tas MTD i betraktning for å beslutte vedrørende aktivering av beredskapsplaner for flytting av forretningsprosesser?