Universitetet i Oslo
IN2120 Informasjonssikkerhet, høst 2025
T07 Risikostyring
Teoretiske oppgaver med løsningsforslag

Oppgave 1: Risikofaktorer

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

Løsningsforslag

a. «Risiko» er en relevant kombinasjon av en gitt trussel, en eller flere sårbarhet(er) som kan bli utnyttet av trusselen og forårsake en hendelse, og verdier som kan skades gjennom hendelsen. «Risikonivå» er størrelsen på en gitt risiko, som beregnes som funksjon av sannsynlighet for hendelsen og alvorlighet av konsekvensene som følge av hendelsen.
b. Faktorer som bidrar til økt sannsynlighet for en sikkerhetshendelse er f.eks. 1) at det fins en eller flere trusselaktører med motivasjon og kapasitet til å utføre trusselscenarioet som fører til hendelsen, og 2) at verdiene og omgivelsen rundt verdiene er sårbare for trusselscenarioet, dvs at det ikke lett lar seg stoppe.
c. Å redusere sannsynlighet for sikkerhetshendelser er meningsfullt, og kan gjøres ved å redusere relevante trusselaktørers styrke (motivasjon og kapasitet) eller å redusere sårbarheter for trusselscenarioer som trusselaktørene kan utføre.
   - Det er relativt lett å redusere eller fjerne sårbarheter, som gjøres ved å implementere sikkerhetstiltak.
   - Det er relativt vanskelig å redusere styrken (motivasjon/kapasitet) til trusselaktører. Nedenfor er noen eksempler på at det kan være mulig.
     - For interne ansatte er det viktig å unngå scenarioer eller situasjoner som kan motivere til å bli en innsidetrussel. F.eks. ved nedbemanning må prosessen med å si opp ansatte være 100% rettferdig. Det betyr naturligvis ikke at urettferdig behandling gir en saklig grunn til å bli en innsidetrussel. Det betyr bare at urettferdig behandling kan medføre at en ansatt mister dømmekraft og derfor blir en innsidetrussel, som man bør forsøke å unngå.
     - Eksterne hacktivister kan bli motivert til å utføre cyberangrep mot en virksomhet hvis dens aktiviteter bryter med hacktivistenes politiske overbevisning. Virksomheter bør være oppmerksomme på denne dynamikken, uten at de dermed skal la seg presse av hacktivister.
     - Avskrekking kan ha en effekt, der statlige aktører kan demonstrere vilje og evne til å gjengjelde cyberangrep. En virksomhet som demonstrerer høy modenhet av sikkerhetsstyring vil primært være godt beskyttet mot cyberangrep fordi den er flink til å tette sårbarheter, og samtidig kan dette kan demotivere trusselaktører fra å angripe virksomheten.
     - Å forhindre tilgang til exploits og informasjon om åpne sårbarheter er med på å begrense trusselaktørenes kapasitet.

d. Hvis en sikkerhetshendelse inntreffer vil konsekvensene være desto mer alvorlig jo dårligere beredskap virksomheten har (dvs. jo mindre forberedt den er), f.eks. ved manglende sikkerhetskopiering og manglende hendelseshåndtering.
e. Ved å anta at en sikkerhetshendelse vil inntreffe fins det en rekke tiltak som kan redusere konsekvensene. Det er viktig å ha 1) gode rutiner for sikkerhetskopiering, 2) gode rutiner for hendelseshåndtering, og kanskje nyttig å ha 3) cyberforsikring. Det er relativt vanskelig å redusere størrelsen og sensitiviteten på selve verdiene, men outsourcing av funksjoner kan redusere mengde og størrelse på verdier som virksomheten har ansvar for (har som oppgave å forvalte). Virksomheten er likefult ansvarlig i betydning regnskapelig (eng. accountable) overfor sluttbruker selv om visse funksjoner er outsourcet.

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?

Løsningsforslag

a. Generelt betyr sikkerhetsbrudd at det oppstår et brudd på ett eller flere av KIT-sikkerhetsmålene (konfidensialitet, integritet og tilgjengelighet) for verdier. Mer spesifikt betyr sikkerhetsbrudd f.eks. informasjonstyveri eller at det skjer annen skade på data, programvare eller maskinvare, eller at det oppstår forstyrrelser i digitale prosesser som følge av cyberangrep. Indirekte betyr sikkerhetsbrudd også at det oppstår forstyrrelse av tjenester og fysiske prosesser i den grad disse påvirkes av angrep mot underliggende digitale systemer.
b. Konsekvensaspekter er f.eks.
   - redusert omsetning/profitt, økonomisk tap
   - svekket ytelse av tjeneste
   - brudd på juridisk etterlevelse
   - erstatning, bøter og juridiske kostnader
   - skadet omdømme
   - kostnader ved håndtering og gjenoppretting
   - belastning for ansatte og brukere, mulig traumatisering av offer for sosial manipulering
c. Ulike konsekvensaspekter ved en type hendelse bør inkluderes som en helhetlig konsekvens.
   - Ved kvalitativ vurdering av konsekvens kan helhetlig konsekvens estimeres som den største konsekvens for de ulike aspektene.
   - Ved kvantitativ vurdering kan helhetlig konsekvens beregnes som sum av kvantitativ konsekvens for de ulike aspektene.

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?

Løsningsforslag

a. Kunnskap om virksomhetens eksponering overfor trusler og risikoer er essensielt for at virksomheten skal kunne beskutte seg mot disse. Det er utilstrekkelig at bare teamet for trussel-/risikovurdering har kunnskapen, den må kommuniseres.
b. De som trenger kunnskap om trussel-/risikovurderinger er f.eks.
   - Ledelsen og styret for virksomheten. Disse enhetene gjør strategiske valg og gir budsjett til sikkerhetsarbeidet.
   - Enheter som forvalter infrastruktur og som innfører/drifter sikkerhetstiltak.
   - Responsmiljøer.
c. Faktorer for god kommunikasjon av trussel-/risikovurderinger er f.eks.
   - avsender og mottager har felles forståelse av begreper
   - mottager forstår betydningen av trusler og risikoer
   - mottager har tillitt til kvaliteten av vurderingene
   - god fremleggelse og visualisering av trusler og risikoer

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.»

Løsningsforslag

Eksempler på omskriving av setningene er:

d. «Risiko» betyr «sannsynlighet». Omskrevet: *«Det er en mulighet for regn når vi skal ha hageselskap på lørdag.»*
e. «Stor risiko» betyr «stor variasjon i mulig fortjeneste eller tap. Omskrevet: *«Det er helt uforutsigbart om man vil tjene eller tape på å kjøpe aksjer i Norwegian nå.»*
f. «Liten risiko» betyr liten variasjon i mulig fortjeneste eller tap, for innskuddsrenten er stabil. Omskrevet: *«Det er helt forutsigbart hva man får igjen ved å sette penger i banken.»*
g. «Betydelig risiko» betyr «stor sikkerhetsrisiko». Omskrevet: *«Infeksjon av kryptovirus er relativt sannsynlig og vil ha en alvorlig konsekvens.»*

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?

Løsningsforslag

a. Operasjonell risiko betyr at det fins en mulighet for tap eller skade som følge av uønskede hendelser forbundet med drift av systemer og prosesser. Informasjonssikkerhetsrisiko betyr nettopp at det fins en mulighet for tap eller skade søm følge av sikkerhetshendelser, dvs. brudd på sikkerhet.
b. Uønskede hendelser skyldes typisk svakheter i egen drift, slik at operasjonell risiko kan styres/reduseres ved å fjerne slike svakheter. Til sammenligning er markedsrisiko noe som er utenfor egen kontroll, slik at det er vanskeligere å styre.

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. Foreslå hva som kan gjøres for å forbedre og gjøre risikovurderingen akseptabel.
b. Beskriv en situasjon hvor svaret på beslutningspunkt 2 (etter planen for risikohåndtering) er NEI, som dermed kan medføre en ny gjennomgang av tidligere trinn i risikostyringen. Foreslå hva som kan gjøres for å forbedre og gjøre risikohåndteringsplanen akseptabel.

Løsningsforslag

a. Det er mulig at risikovurderingen er uakseptabel, f.eks. i følgende situasjoner:
    i. Det er mulig at de estimerte risikonivåene har en svært skjev fordeling, f.eks. hvis flesteparten av risikoer har samme nivå (f.eks. bare svært lave risikoer eller bare svært høye risikoer), noe som gjør det nokså meningsløst å rangere risikoene. Da kan re-kalibrering av estimering av sannsynlighet og konsekvens bidra til bedre fordeling av risikoer.
    ii. Det er mulig at det hersker svært stor uvisshet rundt estimering av sannsynlighet og konsekvens for noen (høye) risikoer. Da kan det være bra å skaffe mer informasjon eller ekspertvurderinger for å bestemme disse estimatene med større visshet.
b. Det er mulig at den foreslåtte planen for håndtering av risikoene er uakseptabel for ledelsen, f.eks. i følgende situasjoner:
    iii. Fordi planen for risikohåndtering er for dyr eller for ambisiøs, f.eks. hvis nivået for akseptabel risiko er satt veldig lavt. Ledelsen kan da vurdere å høyne nivået for akseptabel risiko, slik at færre og mindre ambisiøse sikkerhetstiltak vil være tilstrekkelig får å oppnå akseptabel risiko.
    iv. Fordi risikonivået av planlagte beholdte risikoer (risikoer man ikke gjør noe med) ansees å være for høyt. Med andre ord, det er for mange aksepterte risikoer, som kan være et resultat av at nivået for akseptable risikoer er satt for høyt. Ledelsen kan vurderer å senke nivået for akseptabel risiko. Det betyr at flere risikoer må reduseres, som videre betyr det at flere sikkerhetstiltak må innføres, som til slutt vil kreve et høyere budsjett.
    v. Fordi den estimerte kostnaden for risikohåndteringsplanen anses til å være misvisende på grunn av feilvurdering av kostnad med risikohåndtering. Det betyr at mer nøyaktigkostnader må revurderes.