Øvelse 16 - Virksomhedscase: Risikovurdering

Identifikation af informations sikkerhedsrisici (Risikoidentifikation):

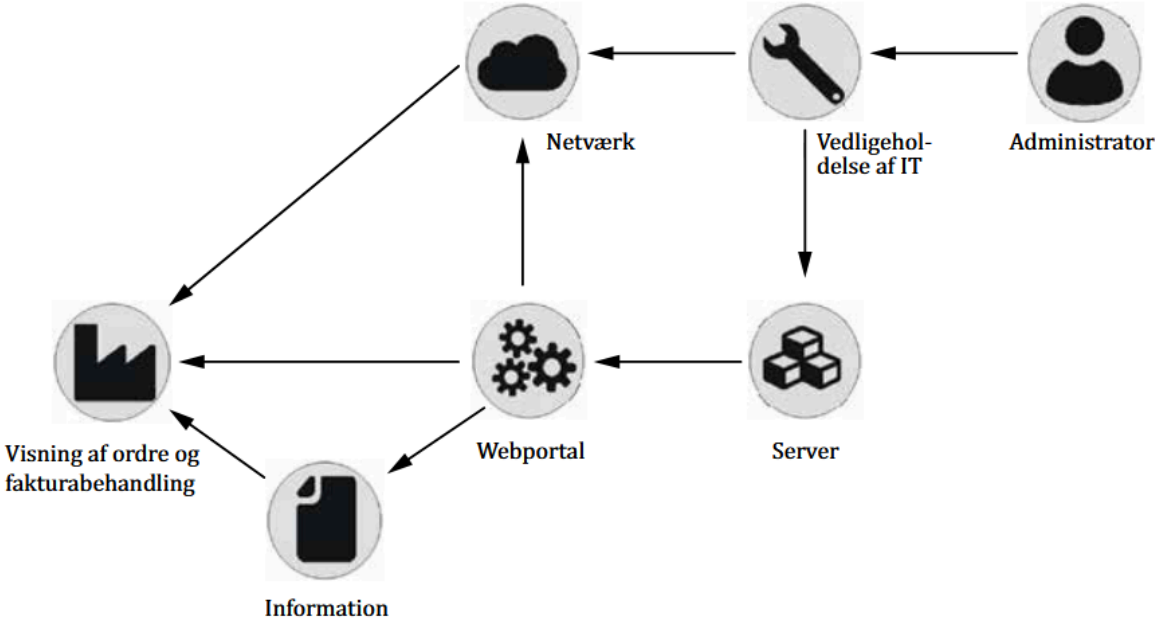
1. Læs om risikoidentifikation i ISO/IEC 27005:2024 afsnit 7.2 (side 17 - 19), følg vejledningen når i arbejder.
2. Vælg en hændelse ovenfor.
    a. En trussel aktør der udsætter LiveFeed-websiden som kunderne bruger, via over for overbelastning angreb (DDoS). Trussel aktøren har købt adgang til LiveFeed dashboard, og er i stand til at tilgå endpoints for kamera-historik, live-feed og kundesupport.
3. Undersøg Sentinel Surveillance Systems informationssikkerheds politik og identificer hvilke dele af politikken der relaterer sig til den valgte hændelse.
    a. 1.3 Mål: DDOS-angreb ville have direkte indflydelse på Tilgængeligheden af IoT-enhedernes tilgængelighed. Disse enheder kan også kompromitteres og udnyttes til et botnet.
    b. 1.5 Opfølgning: SSS påstår at de løbende holder øje på sikkerhedshændelser, dette kunne være en hændelse som vores DDOS-angreb.
4. Identificer så mange risici som muligt ved hændelsen. I skal være opsøgende og meget gerne tage udgangspunkt i kendte trusler (i kender kilder til trusselsidentifikation) og underbygge jeres identifikation med kilder fra internettet og/eller de ressourcer jeg angiver herunder.
    a. "I 3. kvartal 2024 rapporterede gennemsnitligt 7% af brugerne at være udsat for et Ransom DDoS-angreb, men i august 2024 steg dette tal til 10% - altså én ud af ti " (https://learn.g2.com/ddos-attack-statistics)

       De mest almindelige operationelle påvirkninger er betydelig stigning i responstider (52%), lette stigninger i responstider (33%), transaktionsfejl (29%) og komplet nedlukning af tjenester (13%)" (https://www.akamai.com/blog/security/ddos-attack-trends-2024-signify-sophistication-overshadows-size)

       "Den gennemsnitlige varighed af DDoS-angreb var 68 minutter på tværs af industrier i 2024 " (https://learn.g2.com/ddos-attack-statistics)

       Sandsynligheden er ret høj, konsekvens er dårlige responstider, fejl og værste tilfælde nedetid i muligvis en time eller flere timer.
    b. Da deres kameraer er IoT-enheder er der en risiko for at enkelte eller masser af kamera enheder kan angribes direkte med et DDOS angreb
    c. Nedetid på LiveFeed

5. Hvilke primære aktiver er involveret i de enkelte risici? (Hvilke informationer eller processer der har værdi for virksomheden kan blive påvirket af hændelsen?)
    a. Klient-webportal, kundedata.
6. Hvilke understøttende aktiver er involveret i de enkelte risici? (hardware, software, netværk, mennesker, bygninger osv.)
    a. Databaser
    b. Servere
    c. Source Code
    d. Strømforsyning
    e. Aircondition til serverrum
    f. Routere og Switches
7. Hvilken relation er der mellem primære og understøttende aktiver? (se evt. figur A.2 i ISO/IEC 27005:2024 side 49)



Figur A.2 — Eksempel på et diagram over aktivers indbyrdes afhængighed

    a. Klient-webportalen kommunikerer med servere via routere og switches.
    b. Klient-webportalen kommunikerer med servere som har brug for aircondition og strøm
    c. Klient-webportalen fetcher data fra databaser
    d. Klient-webportalen håndtere business logik ud fra sourcecode
    e. Kundedata opholdes i database(r)
    f. Kundedata sendes in-transit til servere og database(r) via switches og routere

8. Beskriv hvem der er risikoejer for de enkelte risici, brug evt. de ledelses titler i arbejdede med i øvelse 2

    Vi har lavet en lille rangering af 3 titler. Primært vil det være CTO der er risikoejer i vores tilfælde, da et DDOS angreb vil ramme hans afdeling. Netværksadministrator vil bare være med til at fixe problemet. Ledelsen skal selvfølgelig have besked, men ikke direkte risikoejer og ansvarlig i første omgang.

a. Ledelsen
    i. CTO
        1. Netværksadministrator

9. Lav en samlet liste over identificerede risici, deres aktiver (primære og understøttende) og relation samt angivelse af risikoejere.

Risiko	**Primære Aktiver**	**Understøttende aktiver**	**Relation mellem primære og understøttende**	**Risikoejere**
Nedetid på LiveFeed	Klient-webportal	Routere, switches, aircon, strøm, databaser,	Webportalen kræver databasen er tilgængelig, og at kommunikationen mellem dem er oppe	CTO
Nedetid på video playback	Klient-webportal	Routere, switches, aircon, strøm, databaser,	Klient-webportal skal kommunikere med databaser	CTO
Autentificering er utilgængeligt	Klient-webportal	Routere, switches, databaser	Klienter skal kunne autentificere sig selv for at kunne tilgå dashboardet	CTO

Analyse af informationssikkerhedsrisici (Riskoanalyse):

1. Læs om risikoanalyse i ISO/IEC 27005:2024 afsnit 7.3 (side 19 - 22), følg vejledningen når i arbejder.
    a. Tjek
2. Vurder potentielle konsekvenser for hver risiko. Brug Risikomatrixen og skalaen for konsekvens fra Case sentinel surveillance systems.pdf

Risko	Konsekvens	Sandsynlighed	Risiko score
Nedetid på LiveFeed	2	5	10
Nedetid på video playback	2	5	10
Nedetid på kameradata-database	4	5	20

3. Lav en liste over potentielle konsekvenser for hver risiko, begrund jeres vurdering.
    a. Nedetid på LiveFeed:
        i. Kunder vil ikke kunne se et live feed fra deres kameraer.
    b. Nedetid på video playback:
        i. Kunder vil ikke kunne tilgå gemt video matriale.
    c. Nedetid på kameradata-database:
        i. Video matriale vil ikke kunne blive gemt i databasen, og vil gå tabt i nedtids perioden.
4. Vurder sandsynligheden for hver risiko. Brug Risikomatrixen og skalaen for sandsynlighed fra Case sentinel surveillance systems.pdf
    a. *"I 3. kvartal 2024 rapporterede gennemsnitligt 7% af brugerne at være udsat for et Ransom DDoS-angreb, men i august 2024 steg dette tal til 10% - altså én ud af ti " (https://learn.g2.com/ddos-attack-statistics)*

        De mest almindelige operationelle påvirkninger er betydelig stigning i responstider (52%), lette stigninger i responstider (33%), transaktionsfejl (29%) og komplet nedlukning af tjenester (13%)" (https://www.akamai.com/blog/security/ddos-attack-trends-2024-signify-sophistication-overshadows-size)

5. Lav en liste over sandsynlighed for hver risiko, begrund jeres vurdering.

Evaluering af informationssikkerhedsrisici (Risikoevaluering):

1. Læs om risikoevaluering i ISO/IEC 27005:2024 afsnit 7.4 (side 22 - 23), følg vejledningen når i arbejder.
2. Brug risikomatrix fra Case sentinel surveillance systems.pdf til at vurdere det samlede risikoniveau for hver risiko.
3. Prioritér listen med risici i forhold til risiko villighed beskrevet i Case sentinel surveillance systems.pdf. Opdel listen i de risici der kan accepteres (grøn) og de risici der bør nedbringes (gul og rød).

Øvelse 17 - Virksomhedscase: Risikohåndtering

Valg af passende muligheder for håndtering af information sikkerhedsrisici (Risikohåndtering - beslutning om hvordan risikoen skal håndteres):

1. Læs om risikohåndtering i ISO/IEC 27005:2024 afsnit 8.2 (side 24), følg vejledningen når i arbejder.
2. Beslut hvordan hver risiko skal håndteres? Undgå, flytte/dele eller forøge/minimere.
3. Tilføj til risikolisten for hver risiko, en kort beskrivelse af hvordan i vil håndtere risikoen.

Risko	**Håndtering**	**Beskrivelse**
Nedetid på LiveFeed	Risiko Fastholdelse	Det er en accepteret risiko fordi sandsynligheden ikke kan reduceres
Nedetid på video playback	Risiko Fastholdelse	Det er en accepteret risiko fordi sandsynligheden ikke kan reduceres
Nedetid på kameradata-database	Modificering	Alvoren kan reduceres ved at have flere backups

Fastlæggelse af alle de foranstaltninger der er nødvendige for at håndtere informationssikkerhedsrisici (Risikohåndtering - valg af foranstaltninger):

1. Læs om risikohåndtering i ISO/IEC 27005:2024 afsnit 8.3 (side 25 - 27), følg vejledningen når i arbejder.
2. For hver risiko udvælges en eller flere foranstaltninger i ISO/IEC 27002:2022 som kan nedbringe risikoen til et acceptabelt niveau. I jeres gruppe skal i sammen begrunde hvordan foranstaltningen nedbringer risikoen. I må gerne bruge andre kilder end ISO/IEC 27002 men vær opmærksom på at der stilles krav til beskrivelsen af "skræddersyede foranstaltninger".

Risko	**ISO foranstaltning**	**Begrundelse**
Nedetid på LiveFeed	8.16 Overvågning af aktiviteter 8.6 Kapacitetsstyring	8.6: Til alle risici så kan man afvise båndbredde så der ikke er mulighed for et DDOS angreb

		8.16: Da den vil hjælpe SSS med at opdage unormal adfærd. Så som DDOS angreb
Nedetid på video playback	8.16 Overvågning af aktiviteter 8.6 Kapacitetsstyring	8.16: Da den vil hjælpe SSS med at opdage unormal adfærd. Så som DDOS angreb 8.6: Til alle risici så kan man afvise båndbredde så der ikke er mulighed for et DDOS angreb
Nedetid på kameradata-database	8.14 Redundans i faciliteter til informationsbehandling 8.16 Overvågning af aktiviteter 8.6 Kapacitetsstyring	8.14: Der kan anvendes redundante netværk og parallelle instanser af software til at imødekomme belastninger. 8.16: Da den vil hjælpe SSS med at opdage unormal adfærd. Så som DDOS angreb 8.6: Til alle risici så kan man afvise båndbredde så der ikke er mulighed for et DDOS angreb

3. Beskriv hvilket niveau risikoen nedbringes til. Hvis det ikke er muligt at nedbringe risikoen til et acceptabelt niveau så snak om hvordan i vil kommunikere risikoen til risikoejer og eller direktionen (så de forstår det).
    a. Nedetid på LiveFeed: Beskriver risikoen på et højt niveau så vidt at aktiv ejerne kan forstå begrundelsen konceptuelt.
        i. Vi mister penge på kunder, der mister tillid til vores produkt. Dog er det en risiko som ikke kan nedbringes pga naturen for en service som skal række kunden via en webportal.
    b. Nedetid på video playback: Beskriver risikoen på et højt niveau
        i. Hr. Fru. Mester direktør. Hvis video playback ikke er tilgængeligt for vores brugere, vil det betyde at vi mister penge :)
    c. Nedetid på kameradata-database: Beskriver risikoen på et højt niveau
        i. Hr. Fru. Mester direktør. Hvis databasen er nede og ikke er tilgængeligt, vil det betyde at der ikke vil kunne blive gemt nogen video, for vores kunder og vi mister mange penge :)

4. Del jeres output fra øvelse 16 og 17 med mig i afleveringsopgaven på itslearning (husk at aflevere som gruppe!)- den er på dagens plan og hedder **"Afleveringsopgave: Risikostyring - Sentinel Surveillance Systems"**