

Yksinkertainen ohjelmistoriskien arviointimalli

Tässä vaiheessa siirrytään uhkien tunnistamisesta riskien arviointiin. Aiemmin tunnistetut tilanteet, joissa jokin voi mennä pieleen, arvioidaan nyt riskin näkökulmasta. Riski tarkoittaa tässä yhteydessä sitä, kuinka merkittävä uhka on, kun huomioidaan sen vaikutus ja todennäköisyys ohjelmistolle.

Uhat on kirjattu 5. *Uhat ja riskit -taulukko* välilehdelle 1. Uhat (tunnistus). Tässä vaiheessa siirrytään välilehdelle 2. *Riskit* (arviointi), jossa arvioidaan kunkin uhan vaikutus, todennäköisyys sekä määritellään tarvittavat toimenpiteet.

Keskeiset käsitteet

Uhka: Uhka tarkoittaa tilannetta tai tapahtumaa, jossa jokin voi mennä pieleen.

Riski: Riski tarkoittaa uhkan toteutumisen vaikutusta ja todennäköisyyttä. Toisin sanoen: kuinka vakavaa olisi, jos uhka toteutuu, ja kuinka todennäköistä se on.

Riskianalyysi: Riskianalyysissä arvioidaan tunnistetut uhat: kuinka suuri vaikutus niillä on ja kuinka todennäköisesti ne toteutuvat.

Riskimatriisi: Riskimatriisi on työkalu, jolla riskin suuruus määritetään vaikutuksen ja todennäköisyyden perusteella. Sen avulla riskit voidaan luokitella ja asettaa keskinäiseen tärkeysjärjestykseen.

Riskienhallinta: Riskienhallinta tarkoittaa toimenpiteitä, joilla riskejä pienennetään, poistetaan, siirretään tai hyväksytään.

Miten edetään käytännössä

1. Avaa dokumentin 5. *Uhat ja riskit -taulukko* välilehti 2. *Riskit* (arviointi)
2. Arvioi jokaiselle uhkalle vaikutus ja todennäköisyys hyödyntäen tämän dokumentin riskimatriisia ja arviointiohjeita
3. Riskitaso lasketaan automaattisesti
4. Lisää toimenpiteet, vastuuhenkilö ja tila
5. Keskity erityisesti suurimpiin riskeihin

Riskin arvioinnin kriteerit

Seuraavaksi arvioidaan, kuinka vakava ja todennäköinen kukin uhka on.

Vaikutus (1–4)

Vaikutus kuvaa, kuinka vakavat seuraukset uhkan toteutumisella on ohjelmistolle, käyttäjille tai liiketoiminnalle. Arvioi vaikutus sen mukaan, mikä on pahin realistinen seuraus, jos uhka toteutuu.

1 Vähäinen

Yleiskuva:

Ei merkittävää haittaa. Ongelma on rajattu ja helposti korjattavissa.

Käyttäjät:

- Vaikuttaa yksittäiseen käyttäjään tai pieneen rajattuun joukkoon
- Suurin osa käyttäjistä ei huomaa ongelmaa

Yhteiskunnallinen vaikutus:

- Ei käytännössä vaikutusta
- Ei häiriötä palveluiden toimintaan laajemmin

Vaikutus henkeen / terveyteen:

- Ei vaikutusta

Liiketoimintavaikutus:

- Vähäinen haitta
- Pieni kustannus tai hetkellinen häiriö
- Ei vaikutusta maineeseen tai luottamukseen

2 Kohtalainen

Yleiskuva:

Rajattu, mutta selvästi hallittava haitta. Tilanne on hallittavissa ilman merkittävää kriisiä.

Käyttäjät:

- Vaikuttaa useisiin käyttäjiin tai tiettyyn käyttäjäryhmään
- Osa käyttäjistä ei pysty käyttämään palvelua normaalisti

Yhteiskunnallinen vaikutus:

- Rajattu vaikutus (esim. yksittäinen organisaatio tai palvelu)
- Ei laajaa häiriötä yhteiskunnassa

Vaikutus henkeen / terveyteen:

- Epäsuora tai vähäinen vaikutus mahdollinen
- Ei välitöntä vaaraa

Liiketoimintavaikutus:

- Selkeä mutta hallittavissa oleva haitta
- Lisää kustannuksia tai manuaalista työtä
- Mahdollinen lievä mainehaitta

3 Merkittävä

Yleiskuva:

Vakava haitta, joka vaikuttaa selvästi toimintaan tai tietoturvaan, ja vaatii merkittäviä toimenpiteitä.

Käyttäjät:

- Vaikuttaa suureen osaan käyttäjistä
- Palvelu ei toimi normaalisti tai on osittain pois käytöstä

Yhteiskunnallinen vaikutus:

- Vaikuttaa laajemmin (esim. useaan organisaatioon tai kriittiseen palveluun)
- Häiriö näkyy ulospäin

Vaikutus henkeen / terveyteen:

- Mahdollinen epäsuora vaikutus
- Voi vaikeuttaa turvallisuuden liittyviä toimintoja

Liiketoimintavaikutus:

- Merkittävä taloudellinen vaikutus
- Selkeä mainehaitta
- Vaatii johdon reagointia

4 Kriittinen riski

Yleiskuva:

Erittäin vakava vaikutus. Palvelu voi estyä kokonaan tai aiheuttaa laajaa vahinkoa.

Käyttäjät:

- Vaikuttaa lähes kaikkiin käyttäjiin
- Palvelu ei ole käytettävissä tai toimii täysin virheellisesti

Yhteiskunnallinen vaikutus:

- Laaja vaikutus yhteiskuntaan tai kriittiseen infrastruktuuriin
- Häiriö voi ketjuuntua muihin palveluihin

Vaikutus henkeen / terveyteen:

- Mahdollinen suora tai epäsuora vakava vaikutus
- Voi vaarantaa turvallisuuden

Liiketoimintavaikutus:

- Vakava taloudellinen tappio
- Merkittävä maineen menetys
- Mahdollisesti toiminnan keskeytyminen

Todennäköisyys (1–4)

Todennäköisyys kuvaa, kuinka helposti tai usein uhka voi toteutua käytännössä. Arvioi todennäköisyys sen mukaan, kuinka helppoa tilanteen toteutuminen on käytännössä, ei sen mukaan, kuinka vakava se on. Jos olet epävarma, arvioi mieluummin hieman suurempi todennäköisyys kuin liian pieni.

Arvioinnissa kannattaa huomioida:

- voiko tilanne syntyä normaalissa käytössä
- kuinka usein vastaava tilanne voisi tapahtua
- vaatiiko toteutuminen erityisiä olosuhteita

Todennäköisyys	4				
	3				
	2				
	1				
		1	2	3	4
		Vaikutus			

1 Epätodennäköinen

Toteutuminen on hyvin harvinaista. Teoriassa mahdollinen, ei tiedetä käytännössä tapahtuneen tai tapahtuu erittäin harvoin.

2 Mahdollinen

Tiedetään yksittäisiä tapauksia (omassa tai muissa organisaatioissa), mutta ei tapahdu säännöllisesti.

3 Todennäköinen

Toteutuminen on realistista ja tapahtuu aika ajoin. Tiedetään tapahtuneen useammin tai säännöllisesti jossain.

4 Erittäin todennäköinen

Tapahtuu usein tai on jo tapahtunut / lähellä tapahtua omassa toiminnassa.

1–3 → Vähäinen riski

Mitä tarkoittaa:

- Riski on pieni tai epätodennäköinen
- Vaikutus on rajattu eikä häiritse toimintaa merkittävästi

Toimenpiteet:

- Ei välttämättä vaadi aktiivisia toimenpiteitä
- Kirjataan ylös
- Seurataan tilannetta

4–6 → Kohtalainen riski

Mitä tarkoittaa:

- Riski on realistinen ja voi toteutua
- Vaikutus on rajattu mutta selvästi haitallinen

Toimenpiteet:

- Suunnitellaan toimenpiteet
- Toteutetaan, jos kustannus-hyöty on järkevä
- Aikataulutetaan (ei välttämättä kiireellinen)

8–9 → Merkittävä riski

Mitä tarkoittaa:

- Riski on todennäköinen tai vaikutus suuri
- Vaikuttaa selvästi toimintaan tai tietoturvaan

Toimenpiteet:

- Vaatii toimenpiteitä
- Priorisoidaan kehitykseen
- Vastuutetaan selkeästi

12–16 → Kriittinen riski

Mitä tarkoittaa:

- Erittäin todennäköinen tai erittäin vakava vaikutus

Riskitason määrittäminen

Vaikutuksen ja todennäköisyyden perusteella muodostetaan riskitaso.

Riskitaso

Riskitaso = vaikutus × todennäköisyys

1–3: Vähäinen

4–6: Kohtalainen

8–9: Merkittävä

12–16: Kriittinen

- Vakava uhka liiketoiminnalle tai turvallisuudelle

Toimenpiteet:

- Korjattava välittömästi
- Vaatii johdon näkyvyyden / päätöksen / hyväksynnän

Valmis: Toimenpiteet on tehty ja riski pienennetty, arvioidaan uudestaan.

Hyväksytty: Riski on päätetty hyväksyä, ei tehdä lisätoimenpiteitä.

Riskin käsittely

Riskin käsittelyssä sovitaan, mitä riskille tehdään, kuka siitä vastaa ja millä aikataululla.

Toimenpiteet

Kirjaa konkreettiset toimenpiteet, joilla tunnistettua riskiä voidaan pienentää tai hallita. Tavoitteena on vähentää riskiä joko estämällä uhkan toteutuminen tai pienentämällä sen vaikutusta. Toimenpiteet voivat liittyä esimerkiksi käyttöoikeuksien rajaamiseen, syötteiden validointiin, rajapintojen suojaamiseen tai tiedon salaamiseen.

Riskin omistaja

Riskin omistaja vastaa siitä, että riskille sovitut toimenpiteet etenevät ja tulevat toteutetuiksi. Omistaja ei välttämättä toteuta toimenpiteitä itse, mutta huolehtii, että asia ei jää käsittelemättä. Omistajan tulee olla roolissa, jossa hänellä on riittävä vastuu ja päätösvalta, jotta riskille sovitut toimenpiteet voidaan toteuttaa.

Määräaika

Päivä, jolloin toimenpide tai osatoimenpide tulee olla tehtynä tai tehdään riskin uudelleen arviointi.

Riskin tila

Avoin: Riski on tunnistettu, ei vielä päätetty mitä tehdään.

Käsittelyssä: Toimenpiteet on sovittu ja niitä toteutetaan.