|  |
| --- |
| [Täytä tekijä]  [Täytä organisaatio]  [Täytä päivämäärä] |

|  |
| --- |
| [Täytä hankkeen nimi] |
| Tietoturvan ja tietosuojan riskianalyysi |
| Versio: [Täytä versionumero] |

**Sisällysluettelo**

[Versiohistoria 2](#_Toc499898561)

[1 Otsikko 3](#_Toc499898562)

[1.1 Otsikko 3](#_Toc499898563)

[1.1.1 Otsikko 3](#_Toc499898564)

Versiohistoria

|  |  |  |  |
| --- | --- | --- | --- |
| **Päivä** | **Versio** | **Kuvaus** | **Tekijä** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Analysoidun kokonaisuuden kuvaus

[Mistä kokonaisuudesta on kyse, mitkä sen rajat ja rajapinnat. Millaiseen ympäristöön palvelu tulee? Minkä järjestelmien kanssa tulevan palvelun pitää kommunikoida ja miten? Mitä osia ja alikokonaisuuksia on. Keitä ovat käyttäjät: kaupungin henkilökuntaa, kuntalaisia vai ulkopuolisia? Mitä tietoa siirtyy järjestelmään päin ja mitä siitä ulos?]

Haluttu tietoturvallisuuden ja tietosuojan taso

[Mitkä ovat lainsäädännön vaatimukset? Mitä on ohjausryhmä päättänyt tietoturvan ja tietoturvallisuuden tasosta?]

Käytetty menetelmä

[Montako työpajaa käytettiin, ketkä olivat läsnä analyysiä tehdessä ja missä rooleissa? Käytettiinkö jotain erityistä menetelmää? Mitkä olivat todennäköisyyden ja vakavuuden arvioinnissa käytettävät kriteerit?]

Löydetyt riskit

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Uhan tunnus | Uhan kuvaus | Nykyiset hallintakeinot | Todennäköisyys  (TN) | Vaikutus  (V) | Riskiluku  (TN x V) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

[Uhan tunnus on yksikäsitteinen tunnus, esimerkiksi pelkkä juokseva numero tai kategoriaan liittyvä (vaikka DB-6 tietokantaan liittyvälle uhalle numero 6).

Uhan kuvauksessa on hyvä kertoa aktiivimuodossa, kuka tekee mitä saadakseen aikaan minkä ongelman. Esimerkiksi ”kaupunkilainen antaa järjestelmään väärän sähköpostiosoitteen ja tieto muuttuneesta tapaamisajasta ei mene perille” tai ”virkailija poistaa vahingossa kaikki asiakastiedot”.

Nykyiset hallintakeinot -sarakkeeseen kirjoitetaan olemassa olevat tietoturvapiirteet, esimerkiksi valmis tunnistuspalvelu tai käsittelyprosessin tarkistuspisteet yms. Aivan uudessa järjestelmässä sarake voi olla varsin tyhjä.

Todennäköisyys-sarakkeessa on numeroarvio uhan toteutumisen todennäköisyydestä nykyiset hallintakeinot huomioon ottaen kappaleen 3 mukaisella luokittelulla.

Vaikutus-sarakkeessa on numeroarvio uhan toteutumisen vaikutuksesta nykyiset hallinta-keinot huomioon ottaen kappaleen 3 mukaisella luokittelulla.

Riskiluku saadaan kertolaskulla todennäköisyys- ja vaikutus-sarakkeiden luvuista.]

Riskienhallintasuunnitelma

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Uhan tunnus | Uhan kuvaus | Riskiluku nyt | Uudet hallintakeinot | Riskiluku tämän jälkeen |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

[Tähän taulukkoon poimitaan ne riskit, joiden riskiluku on yli ohjausryhmän päättämän hyväksytyn riskitason. Uhan tunnus, uhan kuvaus ja riskiluku saadaan edellisen kappaleen taulukosta.

Uudet hallintakeinot -sarakkeeseen tulee kirjata millä toimenpiteillä riskitaso saadaan madallettua hyväksyttäväksi. Nämä toimenpiteet tulee siirtää hankkeen tehtäviksi tai delegoida hankkeesta ulos, kun analyysin tulos hyväksytään.

Riskiluku tämän jälkeen on arvio siitä, mille tasolle riski pystytään uusin hallintakeinoin pienentämään.]