xxx ministeriön julkaisusarja 2020:xx

Julkri työkalun käyttöohje

Liite 3

Lautakunnat

xxxministeriö Helsinki 2020

Sisältö

1 Työkalun käyttö

Tässä ohjeessa kuvataan, miten Julkri-kriteeristöä käytetään sitä varten kehitetyn Excel-työkalun avulla. Työkalun ideana on, että käyttäjä antaa ensin arviointitilannetta kuvaavat esiehdot, joiden perusteella työkalu valitsee olennaiset, valinnaiset sekä arvioinnin ulkopuolelle jätettävät kriteerit.

1.1 Esiehtojen määrittely

Työkalussa määritellään ensimmäisenä arvioinnin lähtötiedot välilehdellä Esiehdot olevien alasvetovalikoiden avulla. Esiehtoina tulee syöttää seuraavat tiedot:

- arvioitavalta kohteelta vaadittava luottamuksellisuus, eheys ja saatavuus,
- sisältyykö arvioinnin kohteeseen henkilötietoja ja kuuluvatko nämä tiedot erityisiin henkilötietoryhmiin,
- arviointiin sisällytettävät ja arvioinnista poisjätettävät osa-alueet,
- käyttötapaus, jos arviointiin soveltuva käyttötapaus on olemassa.

1.2 Olennaiset kriteerit ja niiden täydentäminen

Työkalu näyttää annettujen esiehtojen perusteella välilehdellä Valitut kriteerit kunkin kriteerin osalta onko se olennainen, valinnainen vai jätetäänkö se arvioinnin ulkopuo-

lelle (Ei sisälly arviointiin). Organisaatio tekee päätöksen kriteerikohtaisesti kunkin kriteerin soveltamisesta. Päätökset kirjataan kriteerikohtaisesti sarakkeeseen Päätös soveltamisesta.

Olennaisia kriteerejä on lähtökohtaisesti sovellettava. Valinnaisten kriteereiden soveltamisesta organisaatio tekee päätöksen riskiarvioinnin ja tapauskohtaisen arvioinnin perusteella. Kriteerejä, jotka eivät sisälly arviointiin, ei lähtökohtaisesti tarvitse soveltaa. Organisaatio voi perustelluista syistä poiketa tästä periaatteesta.

1.3 Kriteerien käyttö arvioinnissa

Edellä kuvattujen vaiheiden perusteella muodostettua kriteeristöä käytetään arvioinnin kohteessa joko tietoturvallisuuden arviointiin tai arviointia edeltäviin tietoturvallisuustoimenpiteiden suunnitteluun.

Työkalun välilehdellä Valitut kriteerit oleva luettelo sovellettavista kriteereistä toimii pohjana, johon voi dokumentoida kriteerikohtaisesti arviointien tulokset sekä toimenpiteet, aikataulut ja vastuut puutteiden korjaamiseksi.

1.4 Työkalun toimintaperiaatteet

Kriteerien valinta perustuu esiehtojen avulla annettavien valintakriteerien yhteisvaikutukseen. Kriteerien valinnassa työkalu noudattaa seuraavaa valintalogiikkaa:

- Turvallisuustasot
    - Kriteeri on olennainen, jos kriteerille määritelty turvallisuustaso on sama tai alempi kuin käyttäjän esiehdoissa määrittelemä tarkastelun kohteen turvallisuustaso. Eli, jos käyttäjä on määritellyt, että arvioinnin kohde sisältää salassa pidettäviä tietoja, niin olennaisia ovat kaikki kriteerit, jotka on luokiteltu koskemaan salassa pidettäviä tai julkisia tietoja.
    - Kun käsitellään henkilötietoja olennaisia kriteereitä ovat ne, jotka on tietosuojan osalta luokiteltu tasolle henkilötieto.
    - Kun käsitellään erityisiin henkilötietoryhmiin kuuluvia tietoja, ovat kaikki tietosuojan osalta luokitellut kriteerit olennaisia.

  - Kriteeri on turvallisuustasojen perusteella olennainen, jos se on yhdenkin turvallisuusnäkökulman (luottamuksellisuus, eheys, saatavuus tai tietosuoja) perusteella olennainen.

  - Kriteeri on valinnainen, jos kriteeri ei ole olennainen ja sen turvallisuustaso on yhtä tasoa korkeampi kuin käyttäjän esiehdoissa antama turvallisuustaso. Esimerkiksi jos tarkastelun kohde sisältää salassa pidettäviä tietoja niin TL IV-tasolle luokitellut kriteerit ovat valinnaisia ja käyttäjä päättää riskiarvion perusteella sovelletaanko niitä vai ei. Lisäksi ksiteltäessä luokkaan henkilötieto kuuluvia tietoja, valinnaisia kriteereitä ovat tasolle erityinen henkilötietoryhmä luokitellut kriteerit.

- Osa-alueet

  - Kukin osa-alue voidaan valita mukaan arviointiin (Kyllä) tai jättää pois (Ei).

  - Jos jokin osa-alue on jätetty pois, mikään osa-alueen kriteeri ei sisälly arviointiin. Esimerkiksi jos käsittely ei sisällä henkilötietoja voidaan tietosuojan osa-alue jättää pois tai jos hallinnollisen osa-alueen arviointi jo aiemmin suoritettu, voidaan se jättää pois.

- Käyttötapaukset

  - Kriteeri on olennainen, jos se on määritelty käyttötapauksen perusteella olennaiseksi.

  - Kriteeri voi olla määritelty käyttötapauksessa valinnaiseksi, jolloin organisaatio tekee päätöksen kriteerin soveltamisesta sen perusteella, onko kriteeri tarpeellinen kyseisessä arviointitilanteessa.

- Yhteisvaikutus

  - Kriteeri ei sisälly arviointiin, jos se ei sisälly arviointiin turvallisuustason, osa-alueen tai käyttötapauksen perusteella.

  - Kriteeri on valinnainen, jos se on turvallisuustason tai käyttötapauksen perusteella valinnainen eikä sitä ole rajattu arvioinnin ulkopuolelle turvallisuustason, osa-alueen tai käyttötapauksen perusteella.

  - Muissa tapauksissa kriteeri on olennainen.

2 Käyttötapaukset

Kriteeristöön on ennalta määritelty käyttötapauksia, joihin on poimittu kyseiseen tilanteeseen soveltuvat kriteerit. Organisaatiot voivat myös itse määritellä käyttötapauksia usein toistuviin arviointitilanteisiin. Organisaatiokohtaisten käyttötapausten määrittelyn avulla voidaan tehostaa kriteeristön hyödyntämistä eri tilanteissa, kun käyttötapaukseen voidaan valita ennalta tunnistettujen riskien perusteella sopiva taso ja lisäksi kriteereistä voidaan tiputtaa pois tilanteeseen soveltumattomat kriteerit.

2.1 Ennalta määritellyt käyttötapaukset

2.1.1 Tiedonhallintayksikön hallinnollinen turvallisuusarviointi

Käyttötapaus on tarkoitettu tiedonhallintayksikön tiedonhallintalain mukaisen tietoturvallisuuden vähimmäistason ja tietosuojan arviointiin. Se sisältää arvioinnin hallinnollisen turvallisuuden, tietosuojan sekä varautumisen ja jatkuvuuden hallinnan näkökulmista. Käyttötapausta voi täydentää fyysisen turvallisuuden ja tietojärjestelmäarvioinneilla.

2.1.2 SaaS-pilvipalvelun arviointi

Käyttötapaus on tarkoitettu SaaS-palveluina tuotettujen pilvipalveluiden turvallisuuden arviointiin. Arvioinnissa voidaan käyttää hyväksi pilvipalveluiden tuottajan sertifikaatteja, dokumentaatiota ja muita mahdollisia todisteita turvallisuusvaatimusten toteutumisesta.

2.1.3 Asiantuntijatyön hankinta

Käyttötapaus on tarkoitettu asiantuntijatyön ja konsulttipalveluiden hankinnan turvallisuusvaatimusten toteutumisen arviointiin. Arvioinnin laajuus riippuu toimeksiannon toteutustavasta. Esimerkiksi jos työtä tehdään tilaavan organisaation laitteilla, voidaan tekninen osio jättää soveltamatta, jos vastaava arviointi on tehty

käytettävien laitteiden ja järjestelmien osalta. Jos työ tehdään toimittajan tiloissa, sovelletaan siihen fyysisten turvallisuuden vaatimuksia tai etätyön vaatimuksia.

2.1.4 Tietojärjestelmän palvelutuotannon arviointi

Tietojärjestelmän palvelutuotantoympäristön tai palveluntuottajan arvioinnissa käytettävä kriteeristö. Käyttötapaus huomioi erityisesti palvelutuotannon jatkuvuudenhallintaan ja fyysiseen turvallisuuteen liittyvät kriteerit.

2.2 Organisaatiokohtaiset käyttötapaukset

Käyttötapaukset helpottavat huomattavasti kriteerien valintaa usein toistuvissa tilanteissa. Esimääriteltyjen käyttötapausten lisäksi organisaatio voi määritellä uusia tai muokata valmiita käyttötapauksia. Käyttötapausten määrittelyssä ja käytössä tulee noudattaa erityistä huolellisuutta, jotta ei rajata ulos olennaisia kriteereitä eikä menetetä joustavuutta, joita muut kriteerien valintaan liittyvät ominaisuudet mahdollistavat.

Käyttötapausten määrittelyssä on suositeltavaa noudattaa seuraavia menettelyitä:

Rajaukset: Organisaation tulee määritellä käyttötapauksen rajaukset, joiden perusteella voidaan päättää, onko jokin kriteeri tarpeellinen juuri tässä käyttötapauksessa vai hoidetaanko asia jonkun arvioinnin ulkopuolelle kuuluvan vastuutahon toimesta. Esimerkiksi jos organisaatio lisää uuden palvelun organisaation yhteiseen infrastruktuuriin, voidaan yhteistä infrastruktuuria koskevat kriteerit arvioida kertaalleen ja jättää pois palvelukohtaisista arvioinneista.

Valinnaiset kriteerit: Mikäli on mahdollista, että joissakin tapauksissa kriteeriä sovelletaan ja joissakin ei, kannattaa se määritellä valinnaiseksi. Kriteerien rajaamista kokonaan pois käyttötapauksesta ei tule tehdä, jos on mahdollista, että se on tarpeellinen joissakin käyttötapaukseen sisältyvissä arviointitilanteissa.

Riskiarviot: Samantyyppisissä samalle turvallisuustasolle sisältyvissä käyttötapauksissa voidaan hyödyntää samaa riskiarvio, jolloin samaa riskiperusteista kriteerien arviointia ei tarvitse tarpeettomasti toistaa.

- Tämä voidaan toteuttaa siten, että käyttötapauksesta rajataan kokonaan pois sellaiset kriteerit, joita ei riskiarvion perusteella sovelleta.

- Vastaavasti käyttötapaukseen voidaan etukäteen tehdyn riskiarvion perusteella sisällyttää olennaisena kriteerit, jotka turvallisuustason perusteella luokitellaan valinnaisiksi. Tällöin kaikki valinnaiset kriteerit voidaan arviointitilanteessa merkitä sovellettaviksi ilman uutta riskiarviota.

Dokumentointi: Käyttötapaukset tulee dokumentoida riittävän tarkasti. Erityisesti tulee kuvata rajaukset ja riskiperusteet, joihin kriteerien sisällyttäminen käyttötapaukseen tai poisjättäminen käyttötapauksesta perustuu. Nämä perusteet tulee kuvata niin tarkasti, että myös riippumaton taho voi tarvittaessa arvioida, onko kriteerin poisjättäminen ollut perusteltua

2.3 Käyttötapauksen kuvaaminen työkaluun

Käyttötapauksen nimi sekä lyhyt yleiskuvaus käyttötapauksen sisällöstä kirjataan välilehdelle Käyttötapauskuvaukset. Käyttötapauksen yleiskuvauksessa kuvataan minkälaisiin arviointitilanteisiin käyttötapaus soveltuu.

Koska käyttötapauksen soveltamiseen liittyy useita eri näkökohtia, on suositeltavaa laatia käyttötapauksesta myös erillinen yksityiskohtaisempi kuvaus, jonka perusteella käyttötapauksen hyödyntäjä voi arvioida, soveltuuko käyttötapaus arviointitilanteeseen.

Käyttötapauksessa sovellettavat kriteerit määritellään välilehdellä Käyttötapauskriteerit. Välilehden ylimmälle riville on linkitetty Käyttötapauskuvaukset välilehdellä määriteltyjen käyttötapausten nimet. Käyttötapauksen kriteerien määrittely tehdään kunkin käyttötapauksen sarakkeeseen seuraavasti:

- Käyttötapaukseen sisältyvät olennaiset kriteerit: 1

- Käyttötapaukseen sisältyvät valinnaiset kriteerit: 2

- Käyttötapauksesta poisjätetyt kriteerit: 0