AY

29.4.2022

Digi- ja väestötietovirasto
Lausunto on valmisteltu lausuntopalvelu.fi:ssä

Viite: DVV/3686/2022

Lausunto Julkisen hallinnon digitaalisen turvallisuuden arkkitehtuurin viitekehys

THL kiittää mahdollisuudesta kommentoida JUDO-hankkeessa laadittua digitaalisen turvallisuuden arkkitehtuurin viitekehystä

1. Kommentit dokumentaation ja verkkosivun rakenteesta ja käytettävyydestä

Kokonaisuus on erittäin hyvin jäsennelty ja selkeä. Se tarjoaa hyödyllisen työkalupakin, jota on mahdollista soveltaa monipuolisesti organisaation omista tarpeista lähtien. Viitearkkitehtuuri koostaa hyvin ohjeita, määräyksiä ja standardeja sekä nostaa niiden väliset yhteydet ja päällekkäisyydet esille.

Sivustomuotoinen toteutus on erittäin toimiva ja ylläpidon sekä täydennysten kannalta perusteltu. Sivuston käytettävyys on hyvä ja ulkoasu hyvin selkeä. Sivuston suunnittelussa on onnistuneesti luotu aineiston kohderyhmän näkökulmasta lukijaystävällinen kokonaisuus laajasta ja monitahoisesta aiheesta. Vaikka materiaali kokonaisuudessaan on laaja, yksittäiset osiot on onnistuttu pitämään tiiviinä ja sisältävät olennaisen, ilman mittavia ja raskaita ”selitys- ja perustelutekstimassoja”.

On hyvä, että materiaalissa on runsaasti linkityksiä esimerkkeihin ja lisämateriaaleihin, sivustototeutus tukee hyvin lisätietojen ja mallien löytämistä materiaalin hyödyntäjille.

Sanasto ja termit on hyvä kokonaisuus. Sanaston käytettävyyttä parantaisi, jos termit olisivat aakkosjärjestyksessä ja/tai ryhmiteltyinä mahdollisen lähteen, merkintä esim. uuteen, 5:en sarakkeeseen mukaan. Myös ruotsin- ja englanninkieliset termit käsitteistä olisivat usein tarpeen. Sanasto-osiossa voisi mahdollisesti olla myös viittauksia joihinkin toimialakohtaisiin sanastoihin; esimerkiksi sosiaali- ja terveydenhuollon tiedonhallinnan sanastot sisältää käytönhallinnan sanaston, joka linkittyy joihinkin erityisesti sote-aihepiirissä tietoturvallisuuteen ja tietojärjestelmien käyttäjä- ja käyttöoikeushallintaan liittyviin käsitteisiin, https://sotesanastot.thl.fi/termed-publish-server?lang=fi

Eri osa-alueissa esitetyissä välineissä / malleissa voisi olla versiotietoja. Esimerkiksi työkaluihin liittyen kokonaisuutta hahmottaisi paremmin, jos näkisi jonkinlaisen statustiedon esimerkiksi kriittisten kohteiden luokittelutyökalun versiotiedon. Näin lukijat pystyisivät myös arvioimaan ja hahmottamaan uudet ja päivitetyt työkalut aiemmin jo tarjolla olleista.

Viitekehyksen ylläpidon ja käytön näkökulmasta etusivulla tai johdantosivulla voisi olla ”Viimeisimmät päivitykset” -osio, vrt. viitattu NIST-kehikko.

2. Kommentit viitekehyksessä kuvatuista toiminnoista (tunnistaminen, suojautuminen, havainnointi, reagointi ja palautuminen)

Viitekehyksen jäsennys on toimiva, toimintalähtöinen ja erittäin havainnollinen. Erityisen hyvä käytäntö on ”Miksi tarvitsette tätä” perusteluosiot eri osa-alueissa.

Osa-alueiden kautta rakentuu erittäin kattava kokonaispaketti, jota voisi ylläpitää ja kehittää siihen suuntaan, että eri aiheista löytyy erityyppisiä laadukkaita esimerkkejä. On hyvä, että esimerkkejä on jo koottu myös eri toimialoilta.

3. Kommentit sisällöstä ja toimeenpano-ohjeista

On hyvä, että työkalut on koottu ”Työkalut ja materiaali sivulle”. Eri osioissa on kuitenkin myös monia linkkejä lisätietoihin ja suosituksiin sekä viitekehyksiin, tätä asiaa voisi nostaa esiin myös työkalut ja materiaali-osiossa.

Viitekehyksen esittelyssä toimenpiteiden jaottelua kuvataan kahdelle tasolle, mutta yksityiskohtaisessa materiaalissa näkyy myös ”Taso 3”. Tasomallin kokoaminen ja selittäminen johdanto- tai viitekehysmateriaalissa voisi helpottaa lukijoita.

Eri osioiden ”puolirakenteinen” jäsentely, jossa on monia luetteloita ja osa-alueita sekä eri kohdille selkeät tunnisteet on erittäin havainnollinen ja selkeä. Väreillä tehdyt jäsennykset helpottavat hahmottamista ja soveltamista.

Yleisesti käytettyjen mallien ja menetelmien, kuten RACI, ISO 31000, VAHTI-suositukset, hyödyntäminen on kannatettavaa.

On hyvä, että IT-ympäristön lisäksi myös OT-ratkaisut on huomioitu (ja myös määritelty siinä yhteydessä, jossa asia nostetaan esiin).

Jatkuvuus- ja varautuminen -osiossa oleva esimerkki THL:n Tietoturvasuunnitelman määräyksestä sopii erinomaisesti viitekehyksen kyseiseen kohtaan ja havainnollistaa hyvin lukijakunnalle eri toimialoilla saatavilla olevien ja noudatettavien mallien tärkeyttä.

Viestintäseikkojen huomiointi viitekehyksessä on tärkeää ja kannatettavaa. Esimerkkinä käytetty viestintäsuunnitelma tietoturvapoikkeaman rungosta (viite hieman epäselvä) on havainnollinen ja mallina hyödyllinen.

Viitekehys ja siinä viitatut mallit soveltuvat pääosin erittäin hyvin myös sote-organisaatioissa sovellettavaksi, ja viitekehyksen mukaisia sisältöjä ja jäsennyksiä tullaan huomioimaan ja hyödyntämään mm. THL:n tulevissa määräyksissä sote-tiedonhallinnan ohjaukseen.

Pääjohtaja Markku Tervahauta

Tiedonhallintajohtaja Aleksi Yrttiaho

SIGNATURES **ALLEKIRJOITUKSET** **UNDERSKRIFTER** **SIGNATURER** **UNDERSKRIFTER**

This documents contains 2 pages before this page
Tämä asiakirja sisältää 2 sivua ennen tätä sivua
Detta dokument innehåller 2 sidor före denna sida
Dokumentet inneholder 2 sider før denne siden
Dette dokument indeholder 2 sider før denne side

Aleksi Yrttiaho
002c4ac0-f5b4-4e32-a237-60bab84a15fd - 2022-05-02 15:48:22 UTC +03:00
BankID / MobileID - 0ecbfd0d-0d5f-40bf-9051-d2b567858e79 - FI

Markku Petteri Tervahauta
f73381db-9844-40cc-aaca-e90a405d1d9f - 2022-05-02 15:53:44 UTC +03:00
BankID / MobileID - b726ab87-5239-4c91-b796-a60c85c7aac4 - FI

authority to sign	asemavaltuutus	ställningsfullmakt	autoritet til å signere	myndighed til at underskrive
representative	nimenkirjoitusoikeus	firmateckningsrätt	representant	repræsentant
custodial	huoltaja/edunvalvoja	förvaltare	foresatte/verge	frihedsberøvende