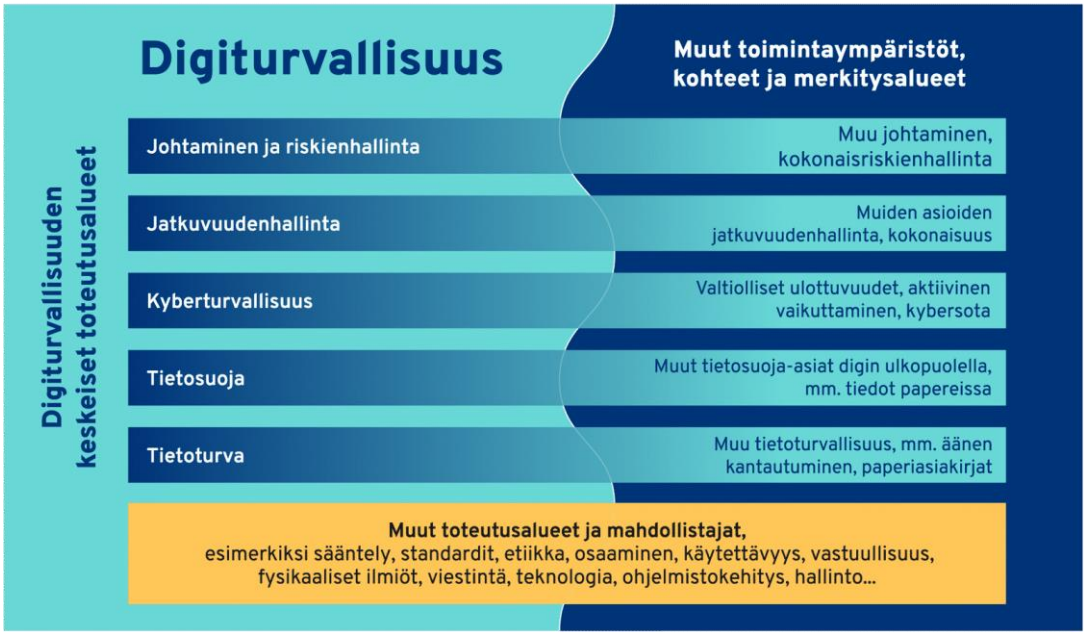
Digitaalinen turvallisuus

1 Mitä on digiturva?

Digitaalisella turvallisuudella eli digiturvalla pyritään varmistamaan, että digitaalinen toimintaympäristö on luotettava, turvallinen ja saatavilla. Tämä edellyttää, että eri toimijat osaavat varautua digitaaliseen toimintaympäristöön kohdistuviin uhkiin, kestävät häiriötilanteita ja pystyvät palautumaan niistä mahdollisimman hyvin ja nopeasti. Arkistenkin toimintojen turvaaminen vaatii laaja-alaista yhteistyötä, jaettuja toimintamalleja sekä halua kehittää niitä.

Digitaalisen turvallisuuden toteutusalueet ulottuvat myös digitaalisen maailman ulkopuolelle. Digitaalinen turvallisuus ei siis ole organisaation tai yhteiskunnan muusta toiminnasta erillinen kokonaisuus vaan olennainen osa niiden kaikkea toimintaa.

Julkisen hallinnon digitaalisella turvallisuudella on viisi painopistettä, jotka ovat kaikille toimijoille yhteisiä ja välttämättömiä hallitun digitaalisen turvallisuuden tuottamiseksi. Nämä painopisteet ovat johtaminen ja riskienhallinta, jatkuvuudenhallinta, tietoturva, tietosuoja ja kyberturvallisuus.[1]



2 Digitaalisen turvallisuuden arkkitehtuuri

Digitaalisen turvallisuuden arkkitehtuuri on ensisijaisesti digiturvan hallintaa tukeva työväline, jonka avulla voidaan muodostaa käsitys organisaatioon kohdistuvista vaatimuksista ja strategisista linjauksista sekä niitä toteuttavista digitaalisen turvallisuuden rakennusosista. Digitaalisen turvallisuuden rakennusosat voivat olla infrastruktuuriin liittyviä teknisiä

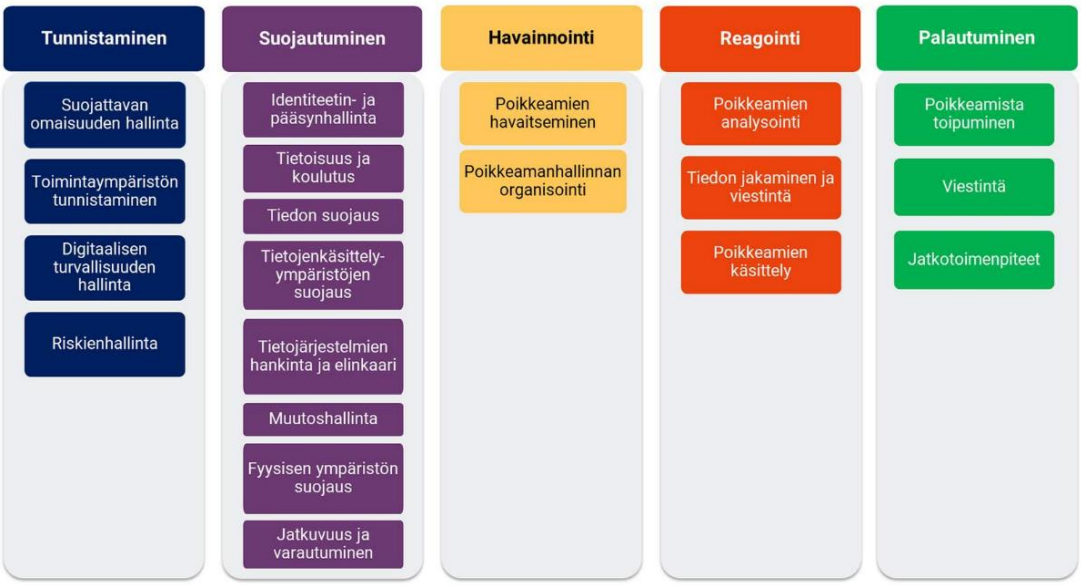
[1] Mitä on digiturva? | Digi- ja väestötietovirasto (dvv.fi)

komponentteja, mutta myös esimerkiksi henkilöstön osaamiseen liittyviä organisatorisia toimintatapoja.

Digi- ja väestötietoviraston julkaisema digiturva-arkkitehtuurin viitekehys[2] auttaa jäsentämään organisaation kyvykkyyksiä viiden toiminnon kautta, joiden avulla organisaatio pystyy suunnittelemaan digitaalisen turvallisuuden rakenteen niin, että se muodostaa kattavan kokonaisuuden. Ohessa esitettyä viitekehystä voidaan hyödyntää digitaalisen turvallisuuden kehittämisen työkaluna varmistamaan, että digiturvan kokonaisuus palvelee muun muassa lainsäädännön asettamia vaatimuksia ja kaikki näkökulmat on huomioitu riittävän kattavasti.

Digiturva-arkkitehtuurin viitekehys kokoaa käytäntöjä useasta eri standardista ja se koostuu viidestä **avaintoiminnoista**: tunnistamisesta, suojautumisesta, havainnoinnista, reagoinnista, palautumisesta.

Toiminnot jakautuvat viitekehyksessä useampaan alakategoriaan sekä niiden muodostamiin digitaalisen turvallisuuden rakennusosiin. Digiturva-arkkitehtuuria ja siihen liittyvää dokumentaatiota voi hyödyntää yhtenä työkaluna tietoturva- ja tietosuojavaatimustenmukaisuuden osoittamiseksi.



2.1 Avaintoiminnot pähkinänkuoressa:

2.1.1 Tunnistaminen (”Mitä suojattavaa meillä on?”)

Tunnistamisen tavoitteena on, että organisaatio on tunnistanut oman toimintaympäristönsä sekä toiminnan mahdollistavat ja toiminnan jatkuvuuteen liittyvät kriittiset suojattavat kohteet ja omaisuuden. Lisäksi organisaatio tunnistanut näihin kohdistuvat uhat ja riskit sekä niiden mahdollisen vaikutuksen toimintaansa.

[2] Digitaalisen turvallisuuden arkkitehtuuri - Digitaalisen turvallisuuden arkkitehtuurin julkinen dokumentaatio - DVV external Confluence

Oman toimintaympäristön ja suojattavien kohteiden tunnistaminen on ensimmäinen askel kohti kattavan digitaalisen turvallisuuden arkkitehtuurin muodostamista. Toimenpiteet, kuten kohteiden suojaus tai poikkeamien havainnointi voidaan tehdä vain, mikäli oma ympäristö tunnetaan riittävän hyvin.

Tunnistamisen lopputuloksena muodostuu kuvaus oman organisaation digitaalisesta ympäristöstä, kuten

- Järjestelmistä, tietovarannoista, laitteista ja niiden sisältämästä tiedosta
- Toimintaympäristöstä ja toimintaa ohjaavista tekijöistä kuten lainsäädännöstä
- Digitaalisen turvallisuuden hallintamallista, kuten käytännöistä ja suunnitelmista
- Digitaalisen ympäristön uhkista, riskeistä ja niiden hallintakeinoista

2.1.2 Suojautuminen (”Miten suojaudumme uhilta?”)

Suojautumisen tavoitteena on, että organisaatio suojaa tunnistetut kohteet, kuten tietojärjestelmät, tietovarannot ja tiedot riskienhallinnan keinoin tunnistetuilta uhilta ja riskeiltä. Käytännössä tämä tarkoittaa muun muassa identiteetin- ja pääsynhallinnan, tietoverkkojen turvallisuuden, tietoturvallisuuden ja turvallisuusteknologian suunnittelua ja toteuttamista suhteessa tunnistettuihin riskeihin sekä näiden toimenpiteiden dokumentointia ja kuvaamista.

2.1.3 Havainnointi (”Miten havaitsemme poikkeamat?”)

Havainnoinnin tavoitteena on, että organisaatio kykenee seuraamaan oman ympäristönsä tilaa ja tunnistamaan digitaaliseen turvallisuuteen vaikuttavia häiriöitä ja poikkeamia.

Havainnointikyvyn toteuttamiseksi on olemassa useita erilaisia teknisiä ratkaisuja, mutta pelkästään teknisiin ratkaisuihin tukeutuminen ei riitä, vaan prosessit ja toimintamallit havaittujen poikkeamien hallintaan, käsittelyyn ja korjaamiseen on oltava olemassa. Havainnoinnin tukena toimii myös käyttäjien tekemät ilmoitukset.

2.1.4 Reagointi (”Kuinka hallitsemme poikkeamia?”)

Reagoinnin tavoitteena on, että organisaatiolla on kyvykkyys reagoida havaittuihin digitaalisen turvallisuuden poikkeamiin mahdollisimman nopeasti. Käytännössä tämä tarkoittaa poikkeamahallintaprosessin toteuttamista siten, että henkilökunta ja sidosryhmät tietävät tehtävänsä ja roolinsa reagointitoimenpiteissä.

Keskeisenä osana poikkeamatilanteisiin reagointia on tilanteen analysointi ja poikkeamaan johtaneiden syiden selvittäminen sekä tarvittavien korjaustoimenpiteiden tekeminen. Lisäksi tilanteen koordinointiin, viestintään ja raportointiin liittyvät käytännöt tulee olla ennalta määritelty.

Reagointi digitaalisen turvallisuuden poikkeamatilanteisiin tapahtuu useimmiten joko teknisin valvontavälinein havaitun tai käyttäjien ilmoittamien poikkeamien seurauksena. Reagoinnin osalta on tärkeää, että mahdollisia poikkeamatilanteita on pohdittu jo etukäteen ja niihin liittyvät suunnitelmat viestinnästä, palautumisesta ja jatkuvuudesta on ajan tasalla sekä tarpeellisten henkilöiden tiedossa. Poikkeamatilanteisiin reagointia onkin suositeltavaa harjoitella säännöllisin väliajoin joko järjestämällä sisäisiä ja kohdennettuja harjoituksia tai osallistumalla ulkopuolisen tahon järjestämään harjoitukseen.

2.1.5 Palautuminen ("kuinka pystymme jatkamaan toimintaamme?")

Palautumisen tavoitteena on, että organisaatiolla on kyky toipua häiriön aiheuttamasta organisaation toimintaan vaikuttavasta ilmiöstä (poikkeama, hyökkäys, katkos toiminnassa, muu virheellinen toiminta) takaisin normaaliin toimintatilaan.

Käytännössä tämä tarkoittaa toipumissuunnitelmien laatimista ja esimerkiksi suojattavien järjestelmien varmuuskopiointia sekä mahdollisia kahdennuksia. Toipumissuunnitelmia ja niihin liittyviä menetelmiä tulisi kehittää häiriötilanteista saatujen kokemusten perusteella.

2.2 Lisätietoja

Mikäli haluat tutustua tarkemmin digitaalisen turvallisuuden arkkitehtuurin viitekehykseen, tutustuthan Digi- ja väestötietoviraston ja eOppivan laatimaan kurssiin digitaalisen turvallisuuden arkkitehtuurista ja sen hyödyntämisestä organisaatiossa.

Löydät kurssiin eOppivasta: Mitä on digitaalisen turvallisuuden arkkitehtuuri? - Digitaalinen turvallisuus järjestykseen arkkitehtuurin avulla (eoppiva.fi)