Digiturvallisuuden mittarit

Kunnanhallitus 13.11.2023 § 299
409/07.00.00.01/2020 Tietosuoja-asiat 2020-

Yhteiskunnallisen tilanteen muutos vaatii digiturvallisuuden mittareiden määrittelyä. Organisaation tulee olla selvillä tietoturvallisuutensa tasosta. Kyberturvallisuudesta on tullut entistä tärkeämpää. Nykyään on entistä enemmän digitaalista tietoa ja asiakirjallista aineistoa. Digiturvallisuusympäristö on muuttunut edellisestä tietotilinpäätöksestä esimerkiksi ohjelmistojen uusien versioiden, uusien ohjelmistojen, lainsäädännön ja tiedonhallintaan vaikuttavien uusien normien sekä uusien globaalienkin uhkien myötä. Yhteiskunta ja maailma ovat muuttuneet, kansainvälistyneet ja moninaistuneet viime vuosina vauhdilla. Tietoturvallisuuteen keskittymisen sijasta nykyään painotetaan erityisesti tietojen ja palveluiden saatavuutta. Lisäksi on omaan organisaatioon vaikuttavia yhteiskunnallisia muutoksia, kuten hyvinvointialueeseen ja te-palveluihin liittyviä. Digitaalinen turvallisuus tukee organisaation tehtävän ja tavoitteen mahdollisimman häiriötöntä hoitamista. Digi- ja kyberturvallisuutta uhkaaviin tekijöihin kuuluvat myös luonnonilmiöt, koska koko digitaalinen yhteiskunta on pitkälti riippuvainen toimivasta tietoliikenneinfraktuurista.

Tieto- ja kyberturvallisuus kuuluvat digitaalisen turvallisuuden viitekehykseen, mikä koostuu riskienhallinnasta, toiminnan jatkuvuudesta ja varautumisesta, tietoturvallisuudesta, tietosuojasta ja kyberturvallisuudesta. Näitä termejä käytetään joskus toistensa synonyymeinä, vaikka niiden määritelmät ovatkin erilaiset. Organisaation digitaalisen turvallisuuden kannalta ei ole olennaista, tuleeko jokin asia käsitellyksi tietoturva- vai kyberturva-asiana. Tärkeintä on, että kaikki digitaaliseen turvallisuuteen liittyvät asiat huomioidaan ja kaikilla toimenpiteillä edistetään kyseisen osa-alueen ja samalla kyberturvallisuuden toteutumista.

Rekisterinpitäjän on noudatettava tietosuoja-asetuksen säännöksiä ja pystyttävä osoittamaan se erilaisilla dokumenteilla ja toimintatavoilla. Rekisterinpitäjän on osoitettava, että se käsittelee henkilötietoja lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Organisaation koko, henkilötietojen määrä ja luonne vaikuttavat osoitusvelvollisuuden laajuuteen.

Rekisterinpitäjän on arvioitava, miten vaatimukset toteutuvat. Apukeinoina ovat erilaiset käytännesäännöt, sertifikaatit, tietoturvan ja tietosuojan omavalvontasuunnitelma ja säännöllinen raportointi. Organisaation tietosuojavastaavalla on myös tärkeä tehtävä tietojen annon ja neuvonnan lisäksi seurata, että organisaatiossa noudatetaan tietosuojasääntelyä.

Hyvin valituilla mittareilla saadaan tietoa tietojenkäsittelyn tilasta ja tietosuojasääntelyn noudattamisesta ja organisaation tietoturvallisuuden tasosta. Hyviä laadullisia tai numeerisia mittareita kuten numeerisia raja-arvoja tai vaatimustenmukaisuuden todentamista ovat esimerkiksi henkilöstön suorittamat tietoturva- ja tietosuojakoulutuksen määrä (montako prosenttia henkilöstöstä suorittanut), henkilötietojen tarkastus-, muutos ja poistopyyntöjen lukumäärä, henkilötietojen tietoturvaloukkausten määrä, Taisto-harjoitukseen osallistuminen ja tietoturvaa koskevien koulutusten lukumäärät.

Nyt asetettavien mittareiden lisäksi tulee laatia vuosittain tietotilinpäätös. (Viimeisin ollut Tohmajärven kunnan tietotilinpäätös 2019, 21.2.2020, Khall 1.6.2020).

Tietotilinpäätöksen sisällysluettelo voi olla seuraavanlainen: Julkinen tiivistelmä Johdon tiivistelmä 1. Johdanto 2. Tietosuojan ja tietoturvallisuuden toteuttaminen 3. Tiedonhallinta, tietovarannot ja tietovirrat 4. Lainsäädäntö ja muu ohjeistus 5. Rekisteröidyn oikeuksien toteutuminen 6. Arviointi, kehittäminen ja tiedon hyödyntäminen 7. Seuranta ja mittarit.

Sen lisäksi kehitetään toimintatapoja sekä tehdään tietotilinpäätös ja tietosuojan vuosikello. Toimintatapoja kehitetään havaittujen ja raportoitujen poikkeamien pohjalta. Vuosikellon toteutumista seuraamalla voidaan todentaa vaatimusten mukaisuus. Tietotilinpäätös on yksi sisäisen ja ulkoisen valvonnan keinoista.

Tohmajärven kunnan toimintamalli on DVV:n VAHTI hyvät käytännöt tukimateriaalin mukainen.

Hallintosäännön 52 a §:n mukaan kunnanhallituksella on vastuu tietoturvajärjestelyistä.

Asian valmistelija

tiedonhallinnan asiantuntija Saara Leinonen, saara.leinonen@tohmajarvi.fi, puh. 040 105 4012

Esittelijä

kunnanjohtaja Mikko Löppönen, mikko.lopponen@tohmajarvi.fi, puh. 040 105 4001

Päätösehdotus

Kunnanhallitus vahvistaa tietotilinpäätöksessä seurattaviksi digiturvan mittareiksi:
1 henkilöstön suorittamat tietoturva- ja tietosuojakoulutuksen lukumäärät (montako prosenttia henkilöstöstä suorittanut)
2 henkilötietojen tarkastus-, muutos- ja poistopyyntöjen lukumäärä
3 henkilötietojen tietoturvaloukkausten määrä
4 Taisto-harjoitukseen osallistuminen
5 tietoturvaa koskevien koulutusten lukumäärät.

Päätös

Hyväksyttiin päätösehdotuksen mukaisesti.

_____