



Digitaalinen turvallisuus vahvistaa luottamusta julkisiin digipalveluihin

Ehdotukset:

- Parannetaan julkisten digipalveluiden informaatioturvallisuutta
- Kehitetään tiedolla johtamisen edellytyksiä julkisten digipalveluiden turvallisuuden hallinnassa
- Uudistetaan digiturvan yhteistoiminnan johtamista ja toimintakulttuuria valtiolla, kunnissa ja hyvinvointialueilla
- Vahvistetaan toimintavarmaa ja häiriösietoista viestintäinfrastruktuuria uudet teknologiset mahdollisuudet huomioiden.

Muutoksilla vahvistamme yhdessä kansalaisten ja yhteisöjen luottamusta julkisiin digipalveluihin. Toteutamme muutokset kansalaisten, viranomaisten, elinkeinoelämä ja järjestöjen yhteistyönä.

Kansalaisten ja yhteisöjen informaatioturvallisuus on muuttuneen turvallisuusympäristön johdosta yhä moninaistuvien tietoihin ja niiden hyödyntämiseen kohdistuvien haasteiden edessä. Julkisten digipalveluiden ja tiedonhallinnan informaatioturvallisuutta tulee parantaa pehmeän infrastruktuurin resilienssiä vahvistamalla. Tulee kuvata ja ottaa käyttöön julkisten digipalveluiden informaatioturvallisuuden yhteiset vastuulliset toimintatavat ja viestintä sekä suunnitella ja toteuttaa asiantuntijaosaamisen kehittäminen.

Julkisten digipalveluiden turvallisuuden tilasta saatavilla olevan tiedon laatu ei ole riittävää, jotta sen perusteella voitaisiin kattavasti ennakoida ja päättää tarvittavista toimenpiteistä. Tarvitsemme julkisten digipalvelujen laajaa ja soveltuvien osin avointa turvallisuuden tilanne- ja ennakkointitiedon systemaattisista tuottamista ja hyödyntämistä. Tulee kehittää strategista digiriskien hallintaa sekä julkisten digipalveluiden turvallisuuden tiedolla johtamisen toimintamalleja: tietojen saatavuutta, eheyttä ja liikkumista eri toimijoiden välillä. Tulee parantaa julkisten digipalveluiden turvallisuuden vaatimustenmukaisuusarviointien ja teknisen valvonnan menettelyjä.

Julkisen hallinnon digiturvan yhteistoiminnalle tuovat nykytilassa haasteita sääntelyn ja toimivallan hajautuminen usealle eri toimijalle sekä yhteistoiminnan useat erilaiset toimintamallit. Digiturvan yhteistoiminnan johtamisen ja toimintakulttuuria tulee uudistaa vahvistamalla kansainvälisiä ja kansallisia valtionhallinnon, aluehallinnon ja paikallishallinnon sekä yhteisöjen digiturvan ekosysteemejä.

Toimintavarma ja häiriösietoinen viestintäinfrastruktuuri on digitalisoituneessa yhteiskunnassa välttämätön. Viranomaisten viestintäratkaisuja tulee vahvistaa ja selvittää 5G:n, pilvipalveluiden ja muiden uusien teknologioiden uhkia ja mahdollisuuksia digiturvan näkökulmasta.

Yksityiskohtaiset perustelut

Johdanto

Kansainvälisen turvallisuustilanteen nopea muuttuminen on entisestään vahvistanut julkisen ja yksityisen sektorin yhteistoiminnan tarvetta digiympäristössä ja yritysten merkitystä kokonaisturvallisuudessa (VN 22:18). Suomi on pärjännyt Euroopan komission vuotuisissa digitaalitalouden ja yhteiskunnan edistymistä

mittaavissa DESI-arvioinneissa erinomaisesti. DESI ei kuitenkaan ota huomioon digiturvan kehitystä. Virolaisen e-Governance Academyn ylläpitämässä kaikkien maailman valtioiden kyberturvallisuuden tilaa arvioivassa NCSI-vertailussa Suomi sijoittuu kymmenenneksi 160 valtion joukossa.

Yhteiskunnan toiminta ja palvelut sekä tiedon yhteiskäyttö perustuvat keskinäiselle luottamukselle turvallisuuden hallinnasta. Turvallisuusongelmat julkisen hallinnon digitaalisissa palveluissa voivat rapauttaa kansalaisten ja yhteisöjen luottamuksen viranomaisiin. Yhteiskunnan on tämän vuoksi panostettava digitalisoitumiseen sekä digitaalisen toiminnan ja palveluiden turvaamiseen tasapainoisesti. Digiturvaan sisältyy kyberturvallisuuden ja kyberpuolustuksen lisäksi riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen sekä tietoturvaluuteen, tietosuojaan ja dis- ja misinformaation hallintaan liittyviä asioita.

Digikompassi antaa suuntaa yhteisten julkisten digipalvelujen turvallisuuden varmistamiseen. Julkisen hallinnon digiturvan kehittämiseksi on myös linjattu kuusi periaatetta (VM 2020:23), jotka ohjaavat ehdotuksia digiturvan kehittämiskohteiksi ja -toimenpiteiksi. Muistiossa ehdotetut kehittämiskohteet, keinot ja toimenpiteet on kuvattu koostetusti taulukossa 1.

Kehittämiskohteet	Julkisten digipalveluiden informaatioturvallisuus	Julkisten digipalveluiden turvallisuuden hallinnan tiedolla johtamisen edellytykset	Digiturvan yhteistoiminta valtiolla, kunnissa sekä hyvinvointialueilla	Toimintavarma ja häiriösietoinen viestintäinfrastruktuuri
Keino	Julkisten digipalveluiden informaatioturvallisuutta vahvistava pehmeän infrastruktuurin resilienssi	Systematisoitu julkisen hallinnon digiturvan tilanne- ja ennakoititietotuotanto ja toimintamallit	Digiturvan kypsyystason kasvattaminen ekosysteemeissä	Turvalliset tietojen vaihdon ratkaisut
Toimenpiteet	- Kuvataan ja otetaan käyttöön julkisten digipalveluiden informaatioturvallisuuden yhteiset vastuulliset toimintatavat ja viestintä. - Suunnitellaan ja toteutetaan informaatioturvallisuuden asiantuntijaosaamisen kehittäminen. - Osallistutaan informaatioturvallisuusstrategian suunnitteluun ja toimeenpanoon. - Arvioidaan avoimen datan uhat ja riskit.	- Kehitetään julkisten digipalveluiden turvallisuuden tiedolla johtamisen toimintamalleja: tietojen saatavuutta, eheyttä ja liikkumista eri toimijoiden välillä johtamisen ja kehittämisen edellytysten parantamiseksi. - Ylläpidetään keskitetysti julkisen hallinnon digiturvan kehittämisen yhteistä resurssisuunnitelmaa. - Parannetaan strategista digiriskien hallintaa sekä julkisten digipalveluiden vaatimustenmukaisuusarviointien ja teknisen valvonnan menettelyjä.	- Uudistetaan digiturvan yhteistoiminnan johtamista ja toimintakulttuuria. - Luodaan toimiva ja vakiintunut digiturvan keskusekosysteemi, jossa ankkureina digitoimisto, DVV ja Traficom/KTK. - Pannaan toimeen NIS2 – ja CER-direktiivit julkishallinnon sektorilla. - Parannetaan julkisen hallinnon ja yhteisöjen yhteistyötä: valkohattuhackerit, kilpailut, bug bounty.	- Toimeenpannaan viranomaisverkkojen kehityksen ja toiminnan varmistaminen (mm. Virve 2.0). - Selvitetään 5G:n, pilvipalveluiden ja uusien teknologioiden uhkia ja mahdollisuuksia digiturvan näkökulmasta.

Taulukko 1. Julkisen hallinnon digiturvan kehittämiskohteet, keinot ja toimenpiteet

Tulevina vuosina arvioidaan erityisesti tiedolla johtamisen ja yhteisen tilanneymmärryksen sekä tähän liittyen informaatiovaikuttamisen ja disinformaation tunnistamisen ja hallinnan merkityksen kasvavan julkisten digipalveluiden tieto- ja kyberturvaloukkausten ja niiden uhkien torjunnassa ja kyberpuolustuksessa. Myös EU, Nato ja muun kansainvälisen digi- ja kyberturvallisuuden yhteistoiminnan sekä viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistoiminnan tarpeiden ennakoidaan lisääntyvän. Jatkossakin teknologioilta ja palvelutuotannolta edellytetään turvallisuutta, mikä vaatii digiturvallisuuden toteutumisen jatkuvaa arviointia ja valvontaa. Muistion ehdotukset rakentavat erityisesti yhteistyön edellytyksenä olevaa luottamusta sekä osaltaan vähentävät riskien vaikutuksia yhteisiin digipalveluihin. Ehdotetut toimenpiteet perustellaan tarkemmin seuraavissa luvuissa.

Julkisten digipalveluiden informaatioturvallisuus

Keino: Julkisten digipalveluiden informaatioturvallisuutta vahvistava pehmeän infrastruktuurin resilienssi

Muuttuneessa turvallisuusympäristössä uhkat kansalaisten ja yhteiskunnan tietoihin kohdistuvista tietoturvaloukkauksista sekä disinformaation leviämisestä, ja tietojen hyödyntämisestä vihamielisiin käyttötarkoituksiin ovat lisääntyneet. Julkisten digipalvelujen turvallisuuden tilasta ei kuitenkaan kattavasti viestitä palvelujen käyttäjille. Disinformaation leviämistä sekä tietojen oikeudetonta muuttamista ja vihamielistä käyttöä on torjuttava parantamalla informaatioturvallisuutta vahvistavaa pehmeän infrastruktuurin resilienssiä. Pehmeällä infrastruktuurilla tarkoitetaan yhteisiä toimintatapoja, osaamista, luottamusta ja näihin liittyviä mekanismeja, käytänteitä ja vastuullisuutta.

Huoltovarmuuskeskus (2021) on ehdottanut kansallisen informaatioturvallisuusstrategian luomista tiiviissä yhteydessä kyberturvallisuusstrategian kanssa. Valtiovarainministeriö osallistuu informaatioturvallisuusstrategian ja sen toimeenpano-ohjelman valmisteluun ja toteutukseen. Siihen liittyen valtiovarainministeriö johdolla yhdessä muiden viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä kuvataan ja otetaan käyttöön julkisten digipalveluiden informaatioturvallisuuden yhteiset vastuulliset toimintatavat. Lisäksi suunnitellaan viestintä ja toteutetaan asiantuntijaosaamisen kehittäminen. Tavoitteena on turvata kansalaisten ja yhteiskunnan tietojen ja julkisten digipalveluiden eheyttä, saatavuutta, ja luottamuksellisuutta. Resilienssi vääristellyille ja valheellisille tiedoille sekä tietojen vihamieliselle käytölle kasvaa, kun julkiset digipalvelut sekä yhteiskunnan ja kansalaisten merkittävät tiedot ovat turvatut sekä tarpeellisin osin saatavilla ja myös saavuttavat kansalaiset, yhteisöt ja viranomaiset.

Edistetään kansalaisten ja julkisen hallinnon henkilöiden osaamista informaatiovaikuttamisen ja disinformaation hallinnassa sekä digiturvataidoissa. Lisätään kansalaisten, yhteisöjen ja henkilöstön ymmärrystä ja osaamista digitaalisista perusoikeuksista ja -velvollisuuksista. Selvitetään kansalaisille suunnattuun ennakoivaan digiturvaviestintään liittyvät toimenpiteet ja toimivaltuudet viranomaisten kesken. Osallistutaan kansallisiin ja kansainvälisiin harjoituksiin. Osaamisen kehittämisessä huomioidaan erityisryhmät. Eri viranomaislähteistä saatavilla olevaan avoimeen dataan ja erityisesti tietojen yhdistämismahdollisuuksiin liittyvät uhat ja riskit arvioidaan ja toteutetaan riskejä vähentävät toimenpiteet.

Julkisen hallinnon on jatkossa otettava aiempaa vahvempi ote julkisten digipalvelujen ja tietojen turvallisuudesta viestimisestä kansalaisille, jolloin informaatiovaikuttamiselle jää vähemmän tilaa. Tätä toteutetaan tuottamalla kehittämistoimenpiteinä disinformaatioresilienssiä vahvistavaa tietoa, koulutuksia ja harjoituksia. Kansalaisten voi olla vaikea tunnistaa, miten hänen elämäntapahtumansa linkittyvät digitaalisuuteen ja miten hänen tietojensa turvataan julkisissa palveluissa. Avoin viestintä ja vuorovaikutus vahvistaa kansalaisten luottamusta viranomaisten kyvystä hoitaa tehtäviään. Vaikka viranomaisen toimisi parhaalla mahdollisella tavalla, erilaiset riskit saattavat realisoitua täysin julkisesta hallinnosta riippumattomista syistä. Silloin tarvitaan oikea-aikaista viestintää luottamuksen palauttamiseksi.

Julkisten digipalveluiden turvallisuuden hallinnan tiedolla johtamisen edellytykset

Keino: Systematisoitu julkisen hallinnon digiturvan tilanne- ja ennakointitietotuotanto ja toimintamallit

Julkisten digipalveluiden turvallisuuden tilasta saatavilla olevan tiedon laatu ei ole riittävää, jotta sen perusteella voitaisiin kattavasti ennakoida ja päättää tarvittavista toimenpiteistä. Digiturvatilanne ja -ennakointitiedot eivät nykytilassa myöskään liiku julkisen hallinnon johtamisen sekä strategia-, normi-,

resurssi- ja informaatio-ohjauksen ja digiturvan asiantuntijatehtävien näkökulmista riittävästi kaikkien eri julkisen hallinnon toimijoiden välillä. Digiturvan kehittäminen ei ole perustunut kattavaan yhteisesti jaettuun digiturvan nykytilaymmärrykseen ja strategiseen tulevaisuusnäkökymään.

Hyvinvointialueiden tai kuntien kokonaisuudesta ei ole saatavilla digiturvatilannekuvaa. Valtioneuvoston tilannekuvatiedon jakamisen periaatteet ovat osin epäselvät ja osa toimijoista kokee, etteivät ne saa kattavasti tilannekuvatietoja. Tähän vaikuttaa osittain se, että osa tilannekuvatiedosta on turvaluokiteltua tai salassa pidettävää, mikä rajoittaa tiedon jakamista organisaatioiden välillä ja jopa organisaatioiden sisällä. Erityisesti turvaluokitellun tiedon jakamiseen liittyvät rajoitukset voivat kuitenkin olla monelta osin perusteltuja. (VM 2022)

Edistetään julkisten digipalvelujen laajaa ja soveltuvin osin avointa turvallisuuden tilanne- ja ennakointitiedon systemaattisista tuottamista ja hyödyntämistä. Kehitetään julkisten digipalveluiden turvallisuuden tiedolla johtamisen toimintamalleja. Tavoitetilassa laaja ja soveltuvin osin avoimesti saatavilla oleva digiturvan tilanneymmärrys ja strateginen digiturvaennakointi vahvistavat digiturvan tiedolla johtamista.

Digiturvaennakointi vastaisi mm. seuraaviin kysymyksiin: Millaiseen toimintaympäristöön tulevana vuosina varaudumme nykyisillä kehittämistoimenpiteillä? Mitä mahdollisuuksia ja uhkia on edessä? Miten digiturvan toimintaympäristön tulevaisuus muuttuu kansallisen ja kansainvälisen turvallisuustilanteen muuttuessa?

Digiturvaennakointi olisi julkisen hallinnon yhteinen ja jatkuvaluonteisesti päivitettävä näkymä digiturvallisuuden tulevaisuuteen. Digiturvaennakointi yhdistäisi erilaiset keskipitkän ja pitkän tähtäimen strategisten ennakointitöiden tulokset ja ohjauksen asiakirjat. Se loisi julkiselle hallinnolle yhteisen kuvan siitä, mihin suuntaan digitaalinen toimintaympäristö ja sen turvallisuus osana kokonaisturvallisuutta on todennäköisesti kehittymässä tulevana vuosina. Digiturvaennakointi auttaisi arvioimaan tehdäänkö nyt niitä asioita, jotka vastaavat tavoitellulla tavalla digiturvallisuuden kehityskulkuun. Digiturvaennakointi voisi myös kertoa ennakoiden, mitä sääntelyä, vaatimuksia, ohjeistusta on julkisessa hallinnossa valmistelussa, jotta niiden valmisteluun voisi osallistua ja julkaisuun varautua. Digiturvaennakointia hyödynnettäisiin myös keskitetysti ylläpidetyn julkisen hallinnon digiturvan kehittämisen yhteisen resurssisuunnitelman hallinnassa.

Parannetaan tietojen saatavuutta, eheyttä ja liikkumista eri toimijoiden välillä johtamisen ja kehittämisen edellytysten parantamiseksi sekä julkisten digipalvelujen tieto- ja kyberturvaloukkausten ja niiden uhkien torjumiseksi ja kyberpuolustuksen toteuttamiseksi. Varmistetaan yhteisen tilannetiedon hallinta ja toimintamallit normaalioloissa sekä laaja-alaisissa tietoturvaloukkaus- ja uhkatilanteissa ja poikkeusoloissa. Arvioidaan ja toteutetaan säädösten muutostarpeet tilannetietojen jakamisen edellytysten parantamiseksi. Arvioidaan viranomaisille asetettavia velvoitteita kerätä ja jakaa tietoja nykytilasta ja häiriötilanteista ohjaaville sekä koordinoiville toimijoille. Hallitaan kuntien ja hyvinvointialueiden tilannetietoja osana kokonaisuutta. Strategisten digiriskien hallinnan palveluiden kehittämistä jatketaan ja tuotetut prosessit ja työvälineet otetaan laajasti käyttöön koko julkisessa hallinnossa.

Vahvistetaan strategista digiriskien hallintaa sekä julkisten digipalveluiden turvallisuuden vaatimustenmukaisuusarvointien ja teknisen valvonnan menettelyjä. Julkisten digipalvelujen ja tietojärjestelmien digiturvallisuutta tulisi arvioida jo kehitysvaiheessa. Tämän arvioidaan pienentävän koko elinkaaren aikaisia kustannuksia vähentämällä korjaustarpeita ja käytön aikaisia häiriöitä. Myös digipalvelujen ja tietojärjestelmien käytön aikaisen teknisen valvonnan niin ikään arvioidaan vähentävän häiriöiden sekä tietoturva- ja tietosuojaloukkausten määrää, ja siten pienentävän kokonaiskustannuksia.

Lain viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista painopisteenä on teknisen tietoturvallisuuden arviointi. Julkisen hallinnon digipalvelujen turvallisuus edellyttää kuitenkin tätä kattavampaa turvallisuusajattelua. Tavoitteena tulisi olla myös palvelujen toiminnan jatkuvuuden varmistaminen. Tavoitetilassa julkisten digipalveluiden ja tietojärjestelmien tietoturvallisuuden ja varautumisen arvioinnin velvoittavuudesta on säädetty sekä sääntelyä mm. arviointilaitosten hyväksymisestä sekä yhteishankintayksiköiden ja yhteisten palvelujen arvioinnista on selkiytetty (VM 2021b). Tiedonhallintalautakunnan antaman *Julkisen hallinnon tietoturvallisuuden arviointikriteeristön (Julkri)* käyttö julkisen hallinnon digipalvelujen ja tietojärjestelmien arvioinnissa on velvoitettu.

Koska sekä digitaalisen toimintaympäristön että sitä uhkaavien kyberuhkien kehittyminen on nopeaa, on syytä arvioida, kuinka tehokasta perinteinen ajoittain tehtävä tietoturvallisuuden arviointi on. Tulisikin kehittää ja velvoittaa automaattista ja jatkuvasti kehittyvää arviointitoimintoa sekä teknistä valvontaa, joiden avulla tietojärjestelmien tietoturvallisuuden tasoa on mahdollista seurata jatkuvasti. Niiden toteuttamisessa keskeistä on julkisten digipalvelujen ja tietojärjestelmien kuvailutietovarannon muodostaminen. Se tukee häiriötilanteiden selvittämistä mahdollistamalla palveluiden riippuvuuksien ja yhteisten haavoittuvuuksien tunnistamista. Kuvailutietovarannon ylläpito ja tietojenvaihto on velvoitettava.

Digiturvan yhteistoiminta valtiolla, kunnissa sekä hyvinvointialueilla

Keino: Digiturvan kypsyystason kasvattaminen ekosysteemeissä

Nykytilassa julkisen hallinnon digiturvan yhteistoiminnan kehittämiseksi tuovat haasteita niin sääntelyn ja toimivallan hajautuminen usealle eri toimijalle kuin digiturvan yhteistoiminnan erilaiset toimintamallit. Digiturvan yhteistoimintaryhmiä on lukuisia, ja eri tarkoituksiin on rakentunut lukuisia erilaisia yhteistoiminnan muotoja. Yhteistoiminta eri toimijoiden välillä toteutuu vain osittaisena. Toimintaa rajoittavat yhteistoimintakulttuuri, rajalliset resurssit ja osaaminen, turvallisten palvelujen saatavuus, käyttöönottettavuus ja käytettävyyys sekä tietojen luokitteluun, jakamiseen ja käyttöön liittyvät lainsäädännölliset ja tekniset rajoitukset. (VM 2022)

Tavoitetilassa toimintakulttuuria ja johtamista on uudistettu. Digiturvan yhteistoiminnan keskeiset vastuut ja yhteiset toimintamallit ovat velvoittavia, ja yhteistoiminnan vahva ohjaus perustuu jaettuun ja analysoituun tilanneymmärrykseen (VM 2022). Vahvistetaan kansainvälisten ja kansallisten valtionhallinnon, aluehallinnon ja paikallishallinnon sekä yhteisöjen digiturvan ekosysteemejä. Parannetaan julkisten digipalvelujen tuotanto-, käyttäjä- ja sidosryhmäverkostojen hallintaa. Kehitetään julkisen hallinnon ja yhteisöjen yhteistyötä, esimerkiksi valkohattuhakkerit, kybertaitokilpailut, bug bounty. Tällä tavoitellaan digiturvan kypsyystasojen nostamista ja yhteistoiminnan keskeisten toimintamallien parantamista.

Luodaan digiturvan kehittämisen ja hallinnan osin keskitetty ja laaja verkostomainen malli. Tavoitteena toimiva ja vakiintunut digiturvan ekosysteemi, jossa ankkureina ovat digitoimisto, Digi- ja väestötietovirasto (DVV) sekä Liikenne- ja viestintävirasto Traficom ja erityisesti sen Kyberturvallisuuskeskus. Digi- ja väestötietoviraston digiturvatehtäviä ja yhteistoimintaa tarkennetaan osana muiden keskeisten digiturvatoimijoiden tehtävien selkeyttämistä.

Valtiovarainministeriön johdolla toimeenpannaan ns. NIS2.0 direktiivi ja CER-direktiiviehdotus kansallisesti julkisessa hallinnossa. Selvitetään ja toteutetaan Suomen Nato-jäsenyyden vaikutukset julkisen hallinnon digiturvan kansainväliseen yhteistyöhön. Hyvinvointialueiden perustamisen ja työn käynnistymisen

yhteydessä edistetään koordinaatiota julkisen hallinnon digiturvan yhteisten palveluiden ja muiden hyvinvointialueille suunnattujen digiturvapalveluiden välillä.

Kuntien merkittävimmät digiturvariskit ovat valtiovarainministeriön syksyllä 2021 tekemän riskikyselyn (VM 2021a) perusteella: viranomaisten toimintaan ja palveluihin kohdistuvat vakavat tietoturvahyökkäykset, digiturvaosaamisen tai vähäisen arvostuksen vuoksi puutteelliset toimenpiteet sekä kriittiseen infrastruktuuriin kohdistuvat hyökkäykset, haitanteot ja sabotaasi. Vaikutuksiltaan suurimmiksi riskeiksi arvioitiin toipuminen laajoista häiriöistä sekä häiriön johdosta menetettyjen tietojen palauttaminen.

Kaikilla kunnilla on samat tehtävät ja samankaltaiset riskit, mutta erilaiset resurssit niiden hallitsemiseksi. Kuntien toimialajohdon ja palveluita hankkivien henkilöiden digiturvaosaamista tulee kehittää jatkossakin. Häiriötilanteista toipumiseen tähdäten tulee kehittää yleistä teknisen digiturvan osaamista ja pitää erityisesti huolta tietojen varmuuskopiointiin ja palauttamiseen. Kunnille suunnattua harjoitustoimintaa tulee myös kehittää ja laajentaa niin, että entistä useampi kunta voi harjoituksiin osallistua. Kunnille suunnattuja digiturvapalveluita tulee kehittää edelleen. Valtiolle, kunnille ja hyvinvointialueille on velvoitettava tietoturvavastaavan rooli.

Toimintavarma ja häiriösietoinen viestintäinfrastruktuuri

Keino: Turvalliset tietojen vaihdon ratkaisut

Digitalisoitunut yhteiskuntamme vaatii viestintäinfrastruktuurilta aiempaa enemmän kykyä välittää tietoa kaikissa olosuhteissa. Riippumatta kansallisesta tai kansainvälisestä turvallisuustilanteesta, infrastruktuurimme on kyettävä tuottamaan ja välittämään tietoa kaikissa olosuhteissa turvallisesti. Tämä vaatii uudenlaisia teknisiä kyvykkyyksiä. Venäjän hyökkäyssodassa Ukrainaan on käynyt ilmi uusia tapoja vahingoittaa ja toisaalta rakentaa tietoverkkoja ja tietojärjestelmiä. Siksi tulee selvittää yhteistyössä toimialaviranomaisten kanssa tällaisten toimien vaikutukset julkiselle hallinnolle ja tunnistaa mahdolliset tarpeet jatkuvuudenhallinnan ja varautumisen kehittämiseksi.

Julkisen hallinnon toimijoiden välisen sujuvan ja turvallisen työskentelyn varmistamiseksi tarvitaan luotettavia tietojärjestelmiä ja viestintävälineitä. Viranomaistoiminnassa on huomioitava salassa pidettävien ja turvallisuusluokiteltujen tietojen erityisvaatimukset. Valtiovarainministeriön johdolla varmistetaan viranomaisten ja muiden turvallisuustoimijoiden käyttämien kriittisten viestintäverkkojen (Virve ja Virve 2) kehitys, käyttöönotto ja toiminta. Nostetaan esille 5G-verkkojen turvallisuuden ja varautumisen vaatimukset osana yhteiskunnan kriittistä infrastruktuuria. Varmistetaan turvallisten satelliittiyhteyksien kehitys kansallisia tarpeita varten. Edistetään mobiililaitteiden digiturvan kehittymistä. Valtiovarainministeriön johdolla selvitetään lisäksi kvanttilalauksen, kvanttiteknologialle resistentin salauksen, automatisoitujen ja oppivien teknologioiden, EU-tiedon turvasataman sekä globaalien pilvipalveluiden mahdollisuudet ja uhat digiturvan näkökulmasta.

Toimintaympäristön turvallisuuden tila Suomessa on aiempaa suuremman kiinnostuksen kohteena myös kansainvälisten yritysten näkökulmasta. Digiturva on olennainen osa liiketoimintaympäristön kokonaisturvallisuutta. Selvitetään julkisten digipalvelujen turvallisuuden ja resilienssin vaikutus yritysten kokonaisturvallisuusarvioihin ja mahdolliset digipalvelujen turvallisuuden ja resilienssin kehitystarpeet. Toteutetaan tarvittavat toimenpiteet selvityksen perusteella.

Lähteet

EU. (2020): The Digital Economy and Society Index (DESI). <https://digital-strategy.ec.europa.eu/en/policies/desi>, vierailtu 6.6.2022

e-Governance Academy. (2020). National Cyber Security Index (NCSI). Viro. <https://ncsi.ega.ee/ncsi-index/>, vierailtu 6.6.2022.

Huoltovarmuuskeskus. (2021): [Informaatiovaikuttamisen torjunta -esiselvitys](#).

Valtioneuvosto. (2022): [Ajankohtaisselonteko turvallisuusympäristön muutoksesta](#). Valtioneuvoston julkaisuja 22:18. 13.4.2022.

Valtiovarainministeriö (VM). (2020): [Julkisen hallinnon digitaalinen turvallisuus](#). Valtiovarainministeriön julkaisuja 2020:23. 8.4.2020.

Valtiovarainministeriö (VM). (2021a): [Kuntien digitaalisen turvallisuuden riskikyselyn tulokset](#). 8.2.2021.

Valtiovarainministeriö (VM). (2021b): [Selvitys digitaalisen turvallisuuden arvioinnin kehitystarpeista](#). 10.5.2021

Valtiovarainministeriö (VM). (2022): [Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvitys](#). Luonnos. 3.5.2022