Lausunto

08.08.2024

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Kansaneläkelaitos katsoo, että strategia on kokonaisuutena hyvin valmisteltu ja strategiassa on huomioitu kattavasti eri näkökulmat.

Yksityiskohtaiset huomiot

Johdanto – kyberturvallisuus on osa kokonaisturvallisuutta

Johdannossa todetaan, että "Erityisesti on kasvanut tarve viranomaisten ja elinkeinoelämän väliselle yhteistyölle, ..." Yhteistyö on ollut pitkään jo onnistumisen edellytyksenä ja tässä tulisi korostaa sitä, että tarve kohdistuu erityisesti yhteistyön tiivistämiseen. Kirjaus antaa ymmärtää, ettei yhteistyötä olisi juurikaan ollut.

Tekstissä on maininta siitä, että Suomi käyttää tällä hetkellä vuosittain lähes 300 miljoonaa euroa valtionhallinnon kyberturvallisuuden varmistamiseen. Koska kyseessä on kansallinen strategia, tulisi tässä huomioida myös välillinen julkishallinto, hyvinvointialueet ja kunnat, koska näillä on valtionhallinnon organisaatioiden lisäksi merkittävä rooli kyberturvallisuuden varmistamisessa.

Toimintaympäristön muutos

Sivulla 11 olisi hyvä huomioida myös näkökulma siitä, että Suomessa tapahtuvat häiriöt voivat vaikuttaa rajat ylittävästi. Nyt näkökulma on liian suppea, koska tekstissä ei huomioida tilannetta, jossa Suomi olisi vaikutustoimien kohteena.

Toimitusketjuihin liittyviä riskejä tulisi korostaa teknologista murrosta koskevassa osuudessa enemmän, vaikka asiaa käsitellään myös erillisessä osuudessa.

Lisäksi toimitusketjujen turvallisuutta käsittelevässä osassa tulisi kuvata myös henkilöstöturvallisuuden näkökulmat, jotta kuvaus ei jää liian suppeaksi. Kohdassa viitataan laajasti eri turvallisuusaspekteihin (mm. fyysinen turvallisuus, jne.). Näissä aspekteissa olisi hyvä korostaa sisäpiiriuhkan merkitystä erityisesti tietojenurkinnan ja liikesalaisuuksien urkinnan näkökulmasta.

Nykytila

Julkisen hallinnon toimijoiden resurssit tieto- ja kyberturvallisuudessa tulisi varmistaa. Tuen ja keskitettyjen palveluiden lisäksi tulisi tarkastella myös toimintojen laajempaan keskittämiseen, jolloin eri toimijoiden resursseja voitaisiin kohdistaa esimerkiksi kyberturvallisuustietoisuuden parantamiseen ja varmistamiseen. Näkökulma on riittävällä tavalla huomioitu Pilari II:ssa.

Ministeriöiden ja kyberturvallisuusviranomaisten yhdenmukaisen yleistilannekuvan olemassaolon varmistamisen lisäksi tulisi huolehtia siitä, että yhdenmukainen yleistilannekuva olisi laajasti eri toimijoiden käytössä. Tietojen turvallisen käsittelyn osalta julkisen hallinon toimijoiden toimintaa tulisi ohjata vahvemmin, esimerkiksi turvallisuusluokitusasetuksen soveltamisalaa laajentamalla. Näkökulma on osittain huomioitu Pilari III:ssa.

Tavoitetila ja rakenne

Yleisenä huomiona käytännössä kaikkiin pilareihin liittyy lainsäädännön kehittäminen. Vaikka asiaa sivutaan hyvin erityisesti pilarissa III, tulisi lainsäädännön kehittämistarpeita korostaa laajemmin. Suomen vahvuus suhteellisen pienenä toimijana on dynaamisuudessa, jota tällä hetkellä rajoittaa voimakkaasti epäselvä lainsäädäntö. Tämä korostuu uusien teknologioiden käyttöönotossa (mm. pilviteknologiat), yhteistoiminnassa sekä reagointikyvyssä ja vastatoimissa. Strategiset kehittämisehdotukset kohdassa esitetyn: "Muutetaan säädöspohjaa, normeja ja ohjeita strategian kehittämistoimien edellyttämällä tavalla." -merkitystä ei mahdollisesti ymmärretä lähes kaiken muun kehittämistoiminnan kivijalkana ja mahdollisten ongelmien juurisyynä.

Pilarit ja niiden strategiset tavoitteet

Pilari l: Osaaminen, teknologia ja TKI

Kyberturvallisuusosaamisen kehittämisen osalta tulisi suunnata nykyistä enemmän voimavaroja peruskouluikäisiin lapsiin ja nuoriin alemmilla luokka-asteilla. Kaikille suomalaisille tulisi tarjota

riittävät perustiedot ja mahdollisuus osaamisen kehittämiseen, jotta ajatus kyberturvallisuudesta osana kansalaisvastuuta voisi toteutua.

Pilari ll: Varautuminen

Kansallisen harjoitustoiminnan osalta tulisi kiinnittää huomiota digitaalisen turvallisuuden harjoitustoiminnan kokonaisuuteen. Harjoitustoiminta on jo nyt hyvin aktiivista ja laajaa, mutta haasteeksi muodostuu se, että harjoitusten ajoittuminen tuottaa ajoittain ongelmia. Kyberturvallisuusharjoituksiin sitoutuu usein myös viestinnän, tietosuojan sekä varautumisen asiantuntijoita, jolloin resurssien riittävyys voi tulla haasteeksi.

Pilari lll: Yhteistoiminta

Kyberturvallisuuden toimintakulttuurin uudistamisessa kokonaisturvallisuuden mallin mukaisesti tulee varmistaa, että myös välillisen julkishallinnon toimijat huomioidaan kyberturvallisuuden yhteistoiminnassa. Sama näkemys pätee myös tilannetietojen jakamiseen. On hyvä, että myös itsenäiset julkisoikeudelliset laitokset on huomioitu liitteen 1 kuvassa 3: Yhteiskunnan eri toimijat kansallisen kyberturvallisuuden varmistamisessa.

Pilari lV: Reagointi ja vastatoimet

Resursointi, toimeenpano ja seuranta

Strategisten tavoitteiden ja kehittämistoimien toteuttamiseen on suunnattavien lisäresurssien lisäksi tulisi kiinnittää erityistä huomioita nykyisten suorituskykyjen laajempaan yhteiskäyttöön ja näiden tarjoamiseen esimerkiksi yhteiskunnan muiden toimijoiden käyttöön turvallisuuden ja huoltovarmuuden parantamiseksi. Strategian toimeenpanosuunnitelman valmistelussa olisi hyvä kuulla myös välillisen julkishallinnon toimijoita.

Koskinen Matti
Kansaneläkelaitos