

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Kiitämme lausuntopyynnöstä ja mahdollisuudesta lausua Suomen uudesta kyberturvallisuusstrategiasta. Strategia vaikuttaa hyvin valmistellulle ja se ottaa kantaa selkeisiin kehityskohteisiin kansallisesti ja julkishallinnossa.

Haluamme erityisesti kiinnittää huomioita siihen, että esimerkiksi hyvinvointialueiden kyberturvallisuuden ja tietosuojan liittyen säädetään useissa eri laeissa, asetuksissa ja määräyksissä. Nämä ovat EU tason regulaatiota, kuten yleinen tietosuoja-asetus (GDPR). Kansallista lainsäädäntöä kuten tiedonhallintalaki ja syksyllä 2024 voimaan tuleva kyberturvallisuuslaki. Erityislakeja mm. asiakastietolaki ja sen toimeenpanoa tukevat THL:n määräykset. Eri ministeriöiden, virastojen, lautakuntien ym. tuottamana on lukuisia suosituksen taseisia ohjeistuksia ja kriteeristöjä. Lisäksi kansainvälisiä standardeja kuten ISO 27001 sarja ja kansallisia kriteeristöjä kuten PiTuKri vaaditaan ja sovelletaan vaihtelevasti. Näiden lisäksi valvovien viranomaisten tulkinnat ja oikeuskäytännöt vaikuttavat sovellettaviin vaatimuksiin.

Luonnoksen kohdassa ”Julkiset palvelut ovat turvallisia” mainitaan seuraavasti:

”Julkisten palveluiden vaatimustenmukaisuuden arviointia ja hyväksyntää sekä arviointikriteeristöjä on kehitettävä ja selkeytettävä ja siihen veloitettava entistä paremmin.”

Pidämme tätä tervetulleena kirjauksena. Toivomme nykyisen regulaation ja suositusten voimakasta selkeyttämistä ja yksinkertaistamista. Nykyinen tilanne kuluttaa organisaatioiden tietosuoja-asiantuntijoiden ja kyberturvallisuuden asiantuntijoiden resursseja näiden vaatimusten tulkintaan. Tämä on pois varsinaisesta kyberturvallisuuden ja tietosuojan tehokkaasta toimeenpanosta. Parhaita käytäntöjä ja ohjeita on runsaasti käytettävissä. On hyvä aika keskittyä näiden toimeenpanoon organisaatioissa.

Edelleen luonnoksen kohdassa ”Julkiset palvelut ovat turvallisia” mainitaan seuraavasti:

”Lisäksi automaattista teknistä seuranta ja valvontaa on tärkeää kehittää ja siihen velvoittaa. On varmistettava, että palvelut priorisoidaan turvallisuustilanteen mukaisesti, potentiaalsiin häiriötilanteisiin varaudutaan ja häiriöiden vaikutukset viranomaisten ja yhteiskunnan toimintaan kyetään minimoimaan.”

Toivomme selkää kansallista ohjeistusta ja yhteismitallisia arviointikriteeristöä. Lisäksi pyydetään huomioimaan, että esimerkiksi hyvinvointialueilla ja kunnissa talous monessa tapauksessa hyvin kireällä. Kyberturvallisuuteen korvamerkityt rahat ja selkeät vaatimukset sen käytölle auttaisivat esimerkiksi hyvinvointialueita toteuttamaan Kyberturvallisuuden minimitasoa yhteismitallisesti valtakunnallisesti.

Luonnoksen kohdassa ”yhteinen tilanneymmärrys toiminnan perustana” mainitaan, että:

”Kyberturvallisuuden yhteistoiminnalle tuovat haasteita sääntelyn ja tehtävien hajautuminen usealle eri toimijalle sekä yhteistoiminnan erilaiset toimintamallit ja soveltuvien yhteisten tietojärjestelmien puute”.

Tämä on valitettava epäkohta, joka vie turhaan organisaatioiden vähäisten tietosuojaan ja kyberturvallisuuteen keskittyvien asiantuntijoiden resursseja varsinaiselta näitä asioita edistävältä työltä. Koska toimivaltaisista viranomaisista on lukuisia, näiden asettamat vaatimukset ja suositukset ovat voivat olla osin jopa ristiriitaisia tai tulkinnanvaraisia. Lisäksi vaaditaan erilaisia ilmoituksia ja raportointeja esimerkiksi kyberturvallisuuden poikkeamatilanteessa, joka voi samalla aiheuttaa myös henkilötietojen tietoturvaloukkauksen. Tällaisessa tapauksessa tulee esimerkiksi hyvinvointialueiden tehdä ilmoituksia monen eri toimivaltaisen viranomaisen suuntaan erikseen ja eri tavoilla. Tämä vie poikkeamatilanteessa asiantuntijoiden resursseja varsinaiselta tilanteen hallinnalta ja voi johtaa tilanteen pahenemiseen. Toivomme että Kyberturvallisuuteen liittyen perustettaisiin oma operatiivisempaan toimintaan osallistuva tai koordinoiva ”112 palvelu” johon yhteyttä ottamalla tieto tilanteesta menisi kaikille toimivaltaisille viranomaisille ja lisäksi palvelusta saisi välittömästi apua ja resursseja tilanteen selvittämiseen ja korjaustoimiin. Analogiana siis yleinen hätänumero 112, jonka kautta avuntarvitsija saa paikalle esimerkiksi poliisin ja pelastusviranomaiset. Nykyisellään Kyberturvallisuuskeskus on lähes ainoa sellainen taho, joka voi avustaa organisaatiota rajallisilla resursseillaan. Muu raportointi vaikuttaa lähinnä perustuvan siihen, että valvova viranomainen haluaa tiedon siitä, onko regulaatiota ja ohjeita noudatettu ja mikä organisaation palveluiden tilannekuva on.

Luonnoksen kohdassa ”yhteinen tilanneymmärrys toiminnan perustana” mainitaan myös, että:

”Tiivis viranomaisyhteistyö, tilannekuvan ja -ymmärryksen muodostaminen sekä tiedonhankinnan edellytysten varmistaminen ovat keskeisiä tavoitetilan saavuttamiseksi. Esimerkiksi julkisten palvelujen osalta tarvitaan nykyistä parempia keinoja ja edellytyksiä kerätä, analysoida ja jakaa tietoa kyberturvallisuuden ja kyberresilienssin tasosta.”

Kannatamme kirjausta ja kansallisen tilannekuvan merkittävää kehittämistä. Toteamme tämän olevan organisaatioiden omaa tilannekuvaa merkittävästi täydentävää palvelua, ei sitä ohjaavaa.

Luonnoksen kohdassa ”Viranomaisten yhteistoiminta on sujuvaa ja saumatonta” todetaan, että:

”Uusina toimijoina hyvinvointialueiden on tärkeää edistää kyberturvallisuuskulttuuria ja -osaamista yhteistyössä muiden toimijoiden kanssa.”

Kannatamme kirjausta ja toivomme hyvinvointialueiden verkostomaisen tiedonvaihtotoiminnan kehittämistä edelleen. Lisäksi pyydämme myös huomioimaan ja hyödyntämään hyvinvointialueilla olevan kyberturvallisuuden osaamisen sekä toiminnan realiteetit tuntevan toimialatuntemuksen, kansallisia ja toimialakohtaisia toimenpiteitä suunniteltaessa.

Yleisesti toteamme vielä lopuksi, että Suomessa julkisen, yksityisen ja kolmannen sektorin tulee tehdä tiiviistä yhteistyötä kyberturvallisuudessa. Toivomme että kaikki sektorit ohjaavat ja neuvovat kyberturvallisiin valintoihin kansalaisten hankkiessa ja käyttäessä erilaisia digitaalisia palveluja olivatpa ne minkä sektorin palveluita tahansa.

Ruotsala Marko
Pohjois-Savon hyvinvointialue