Tampereen yliopisto

Lausunto

22.12.2020 TAU/4500/011/2020

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Opetus ja tutkimus tulisi saada mukaan yliopistojen ja korkeakoulujen osalta.

Käsittelevät laajasti kriittiseen infrastruktuuriin liittyvää tutkimustietoa ja sitä kautta myös taustatietoa olemassa olevista järjestelmistä ja toimintamalleista sekä organisaatioiden kriittisistä henkilöistä ja näiden yhteystiedoista. Tutkimusaineistot sisältävät usein laajasti henkilötietoja esimerkiksi terveydenhuoltoon liittyen.

Harjoitustoimintaa ja sen roolia tietoturvan kehittämisessä ja varmistamisessa ei ole mainittu. Sertifiointi ei yksin takaa tietoturvaa. Tietoturvatoimintojen kattavuutta jo toimivuutta tulee testata säännöllisin yhteisharjoituksin ja tätä tulee tukea ja ohjata keskitetysti esim. KTK:n kautta.

Sertifioinnin aikataulu on liian tiukka. Voisiko vertaissertifiointi toimia joillain toimialoilla ja toimijoilla ainakin ensimmäisessä vaiheessa. Erimerkiksi hallinnolliseen tietoturvaan tähtäävät sertifikaatit eivät takaa että käytännön prosessit toimivat. Myös itsearviointi lisättynä raportin toimitusvelvoitteella koordinoivalle toimijalle käyttäen esimerkiksi kybermittaria on joillakin toimialoilla riittävä ensimmäinen vaihe kohti laajempaa sertifiointia. Tämä voisi toimia esimerkiksi 3v siirtymäkauden vaatimuksena.

Minimiresursointi suoraan tietoturvaan nimettyjen resurssien osalta olisi syytä määritellä sekä rahallisesti että henkilöresurssien muodossa eri kokoisille organisaatioille. Oman toimen ohella hoidettu tietoturva ei kehity eikä sen toteutumista pystytä riittävästi valvomaan.

Tietoturvarooleille tulee lain kautta turvata toimintaedellytykset.

Julkisen alan toimijoiden tietoturvatilannetiedon jakamiseen kansallisella tasolla olisi syytä laatia prosessit ja tekniset ratkaisut.

Tietoturvatoimien näkyvyyttä organisaation suunnitelmissa tulee vaatia selkeästi. Tietoturvan tulee olla sisäänrakennettu, mutta se tulee olla näkyvä osa organisaation strategista ja toiminnallista suunnittelua ja toteutusta (vrt. tietotilinpäätös).

Tietoturvavastuiden tulee siirtyä politiikoista käytännön vastuun määrittelyyn myös lain tasolla (vrt. työsuojelu). Tällä hetkellä tietoturvasta vastaa titteli, joka laitetaan johonkin kohtaan organisaatiossa sekä yleisellä tasolla johto. Tämä aiheuttaa ongelman ettei tietoturva ole käytännön tasolla kenenkään vastuulla. Yksittäinen nimetty rooli ei riitä mielekkään tietoturvatason aikaansaamiseksi organisaatiossa eikä se hoidu myöskään sisällyttämällä vastuita eri rooleille ilman konkreettisia sanktioita.

On erittäin tärkeää, että tietoturvan resursointi ja investoinnit voidaan kohdistaa käytännöstä hyödyntävään työhön sen sijaan että luodaan sertifiointiorganisaatioille valtion pakottamana lisää liiketoimintaa. Pakotettujen sertifiointien kustannukset tulee järkeistää joko valtion sertifointiorganisaation maksuttomalla palvelulla tai sovittamalla kustannukset organisaation maksukykyyn (kunta vs. etelä-Suomen iso kaupunki)

Väliraportin muut osat, kommentit:

Taustat hyvin selvitetty ja esitetty. Erityisen hyvin tuotu realisoituneiden tietoturvaongelmien kustannukset näkyväksi.

Törmälä Marjut
Tampereen yliopisto