Suomen Erillisverkot Oy

Lausunto

30.12.2020

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla on erittäin tärkeä asia ja sitä tulee kehittää yhteiskunnassa laaja-alaisesti. Viranomaisista tulisi tunnistaa turvallisuusviranomaisten lisäksi kaikki muut viranomaiset, jotka merkittävässä määrin käsittelevät kansalaisten tietoja sekä tarjoavat käyttöön tietoturvallisia kansalaispalveluja (esim. Kela, Digi- ja väestötietovirasto).

Viranomaisten välisen yhteistyön lisäksi yhteistyötä pitää lisätä tai ainakin se pitää mahdollistaa viranomaisten ja yksityisten toimijoiden välillä (ns. public-private -yhteistyö). Yksinomaan teknologioiden hyödyntämisessä viranomaiset eivät ole omavaraisia, vaan ne tukeutuvat kaupallisiin teknologisiin tuotteisiin ja palveluihin.

Linjaus 1: Linjauksessa tuodaan esille tarve säätää viranomaisten väliseen yhteistyöhön yhteneväinen säädöspohja.

- Asiassa on hyvä huomioida, että toimintaa osallistuu myös muita toimijoita kuin varsinaisia viranomaisia. Viranomaisen tehtäviä (ns. julkisia hallintotehtäviä) hoidetaan lain nojalla myös esimerkiksi osakeyhtiömuotoisissa toimijoissa. Tästä esimerkkinä voidaan mainita Erillisverkkojen julkisen hallinnon turvallisuusverkkotoiminta. Linjauksissa olisi siten viranomaisten lisäksi hyvä huomioida keskeiset kriittisen infrastruktuurin ylläpitoon ja tuottamiseen osallistuvat tahot.

- Viranomaisten välisessä sekä myös viranomaisten ja muiden tahojen välisessä yhteistyössä tulee huomioida erilaisten tietoturvaloukkaustilanteiden luonteet sekä erityisesti se, että ne tyypillisesti edellyttävät erittäin nopeaa reagointia. Yhteistyörakenteiden tulisi mahdollistaa nopea toiminta.

Linjaus 5: Linjauksessa todetaan tarve selvittää viranomaisten tarpeet teknologisille ratkaisuille salassa pidettävän ja turvaluokitellut tiedon vaihtamiseen.

- Viranomaisten lisäksi on syytä huomioida keskeiset kriittisen infrastruktuurin ylläpitoon ja tuottamiseen osallistuvat tahot. Lisäksi on huomioitava, että vastaavaa tietojen vaihtotarvetta on

lisäksi viranomaisen ja siitä ulkopuolisen tahon kanssa. Tällainen tarve voi syntyä esimerkiksi tietoturvaloukkauksen tutkinnan yhteydessä, jossa hyödynnetään yksityisen toimijan osaamista.

Linjaus 11: Linjauksessa edellytetään kriittisille toimialoille velvoitetta säännöllisiin auditointeihin.

- Esimerkiksi tietojenkäsittely-ympäristöjen auditoinnit kuormittavat merkittävästi Traficomin toimintaa. Toisaalta laki arviointilaitoksista mahdollistaa myös muiden tahojen auditoinnit, mutta lainmukaisia virallisia arviointilaitoksia on toistaiseksi vähän. Tämän johdosta poliittinen linjaus 13 (arviointilaitosten määrän lisääminen) on erittäin kannatettava.

Linjaus 12: Linjauksen mukaan kriittisten toimialojen merkittävimpien toimijoiden tulee osoittaa käyttävänsä tietoturvallisuuden hallintajärjestelmää ISO 27001 -sertifioinnilla vuoden 2024 loppuun mennessä.

- Linjauksessa 11 määriteltiin velvoite kriittisten toimialojen säännöllisille auditoinneille. Myös ISO 27001 -sertifiointiin sisältyy säännölliset auditoinnit. Ovatko linjaukset tarkoitettu erillisiksi, vai täyttääkö ISO 27001 -sertifikaatti kohdan 11 vaatimuksen säännöllisistä auditoinneista?

Linjaus 13: Linjauksen mukaan tietoturvallisuuden arviointilaitosten määrää lisätään tehostamalla arviointilaitosten hyväksymismenettelyä ja valmistelemalla tämän mahdollistavat lakimuutokset.

- Edellä todetun mukaisesti tämä on erittäin kannatettava tavoite. Arviointilaitosten lisääminen pienentää viranomaisten auditoinneista aiheutuvaa kuormaa ja vaikuttaa kilpailun lisääntymisen kautta myös auditointikustannuksiin.

Linjaus 25: Linjauksen mukaan julkisen sektorin toimijat hyödyntävät Kyberturvallisuuskeskuksen laatimaa pilvipalveluiden turvallisuuden arviointikriteeristöä (PiTuKri) pilvipalveluiden tietoturvallisuusvaatimusten määrittämisessä sekä pilvipalveluntarjoajien ja pilvipalveluihin perustuvien valmistuotteiden tietoturvallisuuden tason arvioimisessa hankintoja tehdessään.

- Mitä enemmän erilaisia vaatimuskriteeristöjä on, sitä työläämpää auditointien tekeminen on. Vaatimuskriteeristöjä tulisi pyrkiä yhtenäistämään ja yhdistämään – esimerkiksi PiTuKri:n vaatimukset voisivat sisältyä Katakrin vaatimuksiin.

Linjaus 31: Linjauksen mukaan arvioidaan mahdollisuudet hyväksyä kriittisiä toimialoja valvovien viranomaisten tietoturvamääräykset tai olemassa olevat tietoturvan arviointikriteerit yleisen tietosuoja-asetuksen mukaisiksi sertifiointikriteereiksi.

- Tämä on kannatettavaa päällekkäisyyksien välttämiseksi. Tietoturvan arviointikriteerien tulee myös kattaa tietosuojan vaatimukset.

Väliraportin muut osat, kommentit:

-

Lehtimäki Timo
Suomen Erillisverkot Oy

Haikarainen Ara
Suomen Erillisverkot Oy