Helen Oy/Digitaaliset ratkaisut

Lausunto

04.01.2021

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Linjaus 1.

Viranomaisten välisessä sekä myös viranomaisten ja muiden tahojen välisessä yhteistyössä tulee huomioida erilaisten tietoturvaloukkaustilanteiden muodot ja tilanteet. Yhteistyössä vaaditaan monitoimijayhteistyötä nopeassa aikataulussa reagointia. Yhteistyörakenteiden tulisi mahdollistaa nopea toiminta.

Yhden viranomaisen kontaktointimalli helppottaisi toimintaa(Traficom, Poliisi, Tietosuojavaltuutetun toimisto).

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

On tärkeätä huomioida tietoturvaloukkaustilanteiden selvityksessä myös kolmansien osapuolien kanssa kommunikointi(SOC ja muut tietoturvatoimijat) ja näin ratkaisusta voi tulla kapealla käyttäjäryhmäkohdennuksella epäkelpo.

Linjaus 12. Kriittisten toimialojen merkittävimpien toimijoiden tulee osoittaa käyttävänsä tietoturvallisuuden hallintajärjestelmää ISO 27001 -sertifioinnilla vuoden 2024 loppuun mennessä.

Jatkotyössä on selvitettävä, millaisia toiminnanmuutoksia ja lisäresursointia tietoturvasertifikaatin hankkiminen kriittisiltä toimialoilta vaatii ja mitkä sen todelliset kokonaiskustannukset ovat. Väliraportista ei käy ilmi, onko tarvittavista toiminnanmuutoksista ja esimerkiksi järjestelmäkehittämisestä aiheutuvat kustannukset huomioitu esitetyssä ISO 27001 – tietoturvasertifikaatin hankkimisen kokonaiskustannuksessa.

Millä resursseilla sertifiointi voidaan toteuttaa satoihin organisaatioihin esitetyssä ajassa? Sertifiointiprosessi kestää arviolta 1-2 vuotta organisaation koosta ja maturiteetista riippuen. Jotta hallintajärjestelmä voidaan toteuttaa ja ottaa käyttöön useassa organisaatiossa saman aikaisesti, on varmistetta osaamisen riittävyys. Tältä osin nousee huolenaiheeksi laskutusautomaatin muodostuminen ISO27001 sertifiointia tarjoaville yrityksille.

Täyttääkö ISO27001 sertifointi aiemman auditointitarpeen jos sertifoininin voimassa ololta edellytetään sellaista?

Viranomaisvaatimusten ja valvonnan lisääminen toimialallemme tasapuolistaa eri verkkoyhtiöiden ja energiayhtiöiden investointitarvetta tietoturvaan ja tietosuojaan.

Väliraportin muut osat, kommentit:

-

Paananen Heikki
Helen Oy/Digitaaliset ratkaisut - Digitaaliset Ratkaisut