DNA Oyj

Lausunto

18.12.2020

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

DNA kiittää mahdollisuudesta lausua väliraportista tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla. DNA:n mielestä on tärkeää, että kriittisten toimialojen tietoturvaa ja tietosuojaa koskeva sääntely on riittävän selkeää ja kullekin toimialalle asetetut velvoitteet ovat oikein kohdennettuja ja oikeasuhtaisia.

Viranomaiset toimivat yhdessä (linjaus 1)

Kuten väliraportissa todetaan, kriittisten toimialojen osalta tietoturvaloukkauksesta voi joutua tekemään kaksi erillistä ilmoitusta tietosuojavaltuutetun toimistoon sekä sektorikohtaiselle valvontaviranomaiselle.

DNA katsoo, että velvollisuus ilmoittaa kahdelle viranomaiselle samasta loukkauksesta tulisi poistaa. Uudistus parantaisi yritysten oikeusturvaa, kun olisi tiedossa, että vain yksi viranomainen käsittelee asiaa, selventäisi viranomaisten työnjakoa ja vähentäisi viranomaisten työtaakkaa (nyt sama ilmoitus on kahdella eri viranomaisella työn alla ja voi olla, että viranomaiset eivät koordinoi asiaa keskenään).

Kyberturvallisuuskeskuksen resurssien vahvistamisesta (linjaus 2)

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tehtävät ovat jo nykyisellään varsin kattavat ja toimivat teleyritysten sääntelyssä.

DNA pitää linjausta Kyberturvallisuuskeskuksen resurssien vahvistamisesta edelleen kannatettavina. Nyt tehtäviä ollaan laajentamassa niin, että Kyberturvallisuuskeskus pystyy antamaan riittävästi apua ja toimialakohtaista neuvontaa muille hallinnonaloille. Kyberturvallisuuskeskukseen esitetään

perustettavaksi jokaiselle kriittiselle toimialle oma asiantuntijapalvelunsa, joiden vastuuvirkamiehet tukevat päätoimisesti tietyn yksittäisen kriittisen toimialansa tietoturvasta vastaavaa sektoriviranomaista. Kriittisten toimialojen resursseja vahvistetaan vastaavasti.

DNA kuitenkin huomauttaa, että Kyberturvallisuuskeskuksen rahoitusmalli on poikkeuksellinen, sillä sen varat kerätään suurelta osin teletoimialalta ja täten se on vahvasti riippuvainen myös teletoimialan rahoituksesta. Kuten DNA on aiemminkin ilmaissut, kehityssuunta, jossa Kyberturvallisuusviraston tehtävät laajenevat yhä enemmän yleisyhteiskunnallisiksi sen saadessa kuitenkin valtaosan rahoituksestaan teletoimialalta, ei ole tuettava ja oikeansuuntainen.

Rahoitusmalli, jossa valtaosa toimintamenoista kerätään toimialalta liiketoimintaan sidottuina maksuina ei ole enää perusteltu, kun virasto monilta osin palvelee koko yhteiskuntaa ja nyt esitetyillä toimenpiteillä laajenisi vielä nykyisestä entisestään. Koko Liikenne- ja viestintäviraston rahoitus Kyberturvallisuuskeskus mukaan lukien tulisi viimeistään nyt saada katettavaksi kokonaan valtion budjetista ja samalla saattaa toiminnan tehokkuuden seuranta ja tulosohjaus vastaavaksi kuin muissa valtion virastoissa. DNA toivoo, että työryhmä kiinnittäisi tähän loppuraportissaan erityistä huomiota.

Kaikilla kriittisillä toimialoilla on lakisääteiset tietoturvavaatimukset (linjaus 7-9)

On tärkeää, että lakisääteiset tietoturvavaatimukset ovat tasapuolisia ja oikeasuhtaisia ja että yritys pystyy vaatimuksista huolimatta edelleen toimimaan kilpailukykyisesti kansallisella ja kansainvälisellä tasolla ja kehittämään palveluitaan. Sääntelyn tulisi asettaa minimitaso ja olisi hyvä arvioida, voiko lakisääteisen vaatimuksen sijaan toimenpiteitä ohjata esim. viranomaissuositusten avulla.

Kriittisille toimialoille säädetään velvoite määritellä kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot (linjaus 10)

DNA:n mielestä linjauksen liittyvän, mahdollisen uuden sääntelyn valmistelu tulisi tehdä toimialakohtaisesti, läheisessä yhteistyössä yritysten ja toimialojen edunvalvontajärjestöjen kanssa. Sääntelyn ennustettavuudesta, tarkkarajaisuudesta ja oikeasuhtaisuudesta on pidettävä erityistä huolta.

Velvoite siirtyä ISO 27001 -sertifiointiin vuoden 2024 loppuun mennessä (linjaus 12)

DNA katsoo, että kriittisten toimialojen tietoturvan ja tietosuojan auditointi ja sertifiointi on yksi tärkeistä kehittämiskohteista. Esitetty linjaus velvoitteeksi siirtyä ISO 27001 -sertifiointiin 2024 mennessä vaikuttaa kuitenkin vielä varsin yleiseltä ja vaatinee tarkentamista. Olisiko sertifiointi pakollinen kaikelle toiminnalle, toimintokohtainen tai vaikkapa tilakohtainen? Millaisia toimijoita uusi velvoite koskisi ja millä rajauksella? Toiminnan sertifioinnin laajuus vaikuttaa merkittävästi myös siitä syntyviin liiketoimintakustannuksiin. Asian jatkotarkastelussa tulisi kiinnittää erityistä huomiota velvoitteen taloudellisiin ja liiketoiminnallisiin vaikutuksiin yrityksille ja mahdollisen uuden velvoitteen tulisi olla tarkkarajainen ja oikeasuhtainen.

Tietosuojasääntelyllä pystytään tehokkaasti puuttumaan oikeudenloukkauksiin (linjaukset 28-34)

DNA katsoo, että tietosuojavaltuutetun toimiston resursseja varmistettaessa olisi tärkeää vahvistaa tietoturvateknologiaan liittyvää osaamista, juridisen osaamisen rinnalla.

Uudet toimintatavat tietoturvauhkista ja –loukkauksista viestimiseksi ja ilmoittamiseksi (linjaus 35)

Mikäli esitetty sovellus päädyttäisiin perustaa, olisi syytä varmistua, että se sisältää elementtejä, joiden johdosta ilmoituksissa annettavan tiedon laatu olisi hyvä ja varmistettu yksilöinti- ja näyttötietokysymyksin. Tilanne, jossa kyseisenkaltainen sovellus toimisi eräänlaisena reklamaatiovälineenä yrityksen toimittamaan palveluun liittyen, ei liene tarkoituksenmukainen. Riskinä lienee myös, että varsinaiset uhka- ja loukkausilmoitukset hukkuisivat muunlaiseen viestintään.

Kunnioittavasti,

Anna Anttinen

DNA Oyj

Väliraportin muut osat, kommentit:

-

Anttinen Anna
DNA Oyj - Lakiasiat ja regulaatio, Anna Anttinen