Työterveyslaitos

Lausunto

28.11.2023

Asia: VN/18157/2023

Lausuntopyyntö: luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

NIS2-diretiivin yleiset tavoitteet ovat hyvät. Kyberturvallisuuden merkitys on kasvanut, ja kasvanee jatkossa. Vapaaehtoisilla toimilla on saatu paljon aikaan, mutta on ilmeistä, etteivät nämä riitä, sillä osa toimijoista varautuu riittämättömästi.

Suomessa kyberturvallisuuden taso lienee korkeampi kuin muissa EU-maissa keskimäärin. Valtionhallinnossa ja koko yhteiskunnassa on pitkät perinteet tietoturvallisuuden tekemiselle, myös tekemisen strategiselle suunnittelulle. Esimerkiksi VAHTI-ohjeet täyttävät kohta neljännesvuosisadan, valtionhallinnon tietoturvallisuuden kehitysohjelma (VM:n vetämä) on tehty ensimmäisen kerran vuosille 2003-2006.

Ensimmäinen kansallinen tietoturvastrategia laadittiin vuonna 2002.

NIS2-direktiivin vaatimukset ovat pitkälti niitä, joita maassamme toteutettu hyvä tovi. Muissa Euroopan maissa tilanne ei liene yhtä hyvä.

Työterveyslaitos pitää hyvinä direktiivin tavoitteita.

Soveltamisalaa koskevat huomiot

NIS2-direktiivin soveltamisala laajenee merkittävästi NIS-direktiivistä. Tämä on luonnollinen kehitys, ja NIS3 tullee aikanaan laajentamaan sitä.

Soveltamisen alaraja valmistavan teollisuuden yrityksissä on asetettu melko alas.

Instan tekemä arvio direktiivin soveltamisen kustannuksista yrityksissä on kohtuullisen korkea. Valmistussektorilla runsaat 350 TEUR kertakustannuksena ja tämän jälkeen noin 150 TEUR/v. Selvityksestä ei jostain syystä ilmene, miten nämä suhteutuvat liikevaihtoon eli kuinka paljon kasvua on odotettavissa 0,5% 0,7% ja 0,3% osuuksille. Tulokset ovat siis mielenkiintoisia, mutta valitettavasti yhteismitattomia.

Riskienhallintavelvoitetta koskevat huomiot

Hallituksen esityksen ehkä eniten toimenpiteitä aiheuttaa kyberturvallisuuden riskienhallinnasta annetun lain 7–9§. Mukana ei ole toimia, joita emme jo tekisi, mutta joudumme tekemään aiempaa perusteellisemmin, ja dokumentoimaan tekemisemme paremmin.

On ilmeistä, että erilaisten tietoturvan johtamisen standardien kysyntä tulee kasvamaan, erityisesti riskipohjaisten ja julkishallintoon sovellettavien kuten ISO 27001 ja Julkri.

9§3 k6 tuo suomalaiseen tietoturva-alan sanastoon käsitteen, jota on käytetty lähinnä englanniksi: kyberhygieniakäytännöt. Tällä on analogia lääketieteelliseen hygieniaan, ja termillä tarkoitetaan sellaisia toistuvia perustoimia, jotka ovat rutiineja, ja yksittäinen hygieniatoimi on todennäköisesti tarpeeton. Sanavalinta ei ole paras mahdollinen, sillä tämän ryhmän toimet sisältyvät osin listan muihin kuuteen kohtaan. Toiseksi, termi on suomeksi uusi ja osin vakiintumaton. Vakiintunut vastine sanalle olisi “perustason tietoturvatoimet” tai kohdassa oleva perusluontoiset hallintatoimet. Kohta on varmasti yhdenmukainen direktiivin käännösten kanssa, mutta koska kyse on kansallisesta lainsäädännöstä soisimme siinä käytettävän vakiintunutta terminologiaa.

Sanaa kyberhygienia käytetään alan englanninkielisessä kirjallisuudessa, joten se on alan parissa työskenteleville sanana tuttu, mutta sisällöltään vähemmän vakiintunut kuin vanhemmat termit.

Termin käyttämisen ongelmista kertoo hyvin, että hallituksen esityksen sivulla 124 avataan käsitettä, ja siihen luetaan kuuluvan vuosikymmenten saatossa hyvin vakiintuneiden tietoturvatoimien, kuten ohjelmistopäivitykset ja verkon segmentointi, lisäksi uudempi käsite luottamattomuuden periaate, josta suomen kielessä puhutaan voittopuolisesti vielä lainasanalla zero-trust.

Käsite zero-trust on ilmeisen hyvä, ja edistää tietoturvallisuutta, mutta siihen siirtyminen ei tapahdu äkkiä, eikä ainakaan lokakuuhun 2024 mennessä. Suurin osa organisaatioista perustaa henkilöiden ja laitteiden tunnistamisen ainakin osittain perinteiseen turvavyöhykeajatteluun, jossa tietyltä kyberin alueelta tulevat (kuten lähiverkko) on jo tunnistettu, ja heihin voidaan luottaa.

Viitatun kohdan muut esimerkit ovat tietoturvallisuuden perustason asioita, mikä tekee uuden käsitteen ottamisen mukaan oudoksi.

Käsite zero-trust on tullut yleisesti käytetyksi ehkä viimeisen viiden vuoden aikana. NIST määrittelee sen ohjeissaan 2018. Iso-Britannian NCSC suosittelee sitä uusien verkkojen suunnitun perustaksi vuodesta 2019 alkaen. HE olettaa myös vanhojen verkkojen muutettava.

Sana zero trust esiintyy hallituksen esityksen perusteissa, mutta ei itse laissa.

Sen toteuttaminen etenkin pienissä yrityksissä on vaikeaa, lain voimaantuloon mennessä mahdotonta.

Raportointivelvoitetta koskevat huomiot

Raportointivelvoite on uusi ja laaja, ja ilmoituskynnys on säädetty varsin alas. Ilmoittamisen ehdot on määritelty niin, että valvova viranomainen saattaa hukkua yhteiskunnan kannalta mitättömiin ilmoituksiin.

Jos määritelmää tulkitaan tiukasti 11§1 kohdasta “toimijan on ilmoitettava.. [24 tunnin kuluessa] ...poikkeama, joka voi aiheuttaa taloudellisia tappioita” on jokainen verkkopalvelun katkos tällainen; ainakin, jos siellä myydään jotain.

Näkisimme, että taloudellisen menetyksen raja asetettaisiin samaksi kuin kyseisen kohdan muiden vahinkojen osalta, siis että vain huomattavat vahingot on ilmoitettava.

Ehdottamamme muutos on tosin hankalasti toteutettavissa, sillä Direktiivin kohta 23 (3) a) puhuu vain taloudellisista tappioista.

Samasta syystä tiukkoja aikarajoja tuskin voitaneen muuttaa

Valvontaa koskevat huomiot

Ehdotettu valvonta on linjassa tietoturvallisuuden yleisen valvonnan kanssa. Traficomin ja muiden valvovien viranomaisten on ehdottomasti saatava tarvitsemansa lisäresurssit joko suoraan itselleen tai osin valvomiensa tietoturvallisuuden arviointilaitosten kautta.

Yleisesti ottaen valvonta on säädetty riittävän hyvin ja istuu suomalaisen julkishallinnon vakiintuneisiin valvontakäytäntöihin.

Valvonnan järjestäminen kullakin hallinnonalalla on oma lukunsa. Toivoimme, että tätä tehdään jokaisella hallinnonalalla, ja että valvonta ja ohjaus aloitetaan mahdollisimman pian.

Valvomisen aloittamisen kynnys muille kuin keskeisille toimijoille on asetettu varsin korkeaksi. (26§3)

Seuraamusmaksua koskevat huomiot

Seuraamusmaksu on melko suuri, vaikka pienempi kuin esimerkiksi tietosuojapoikkeamissa.

Julkishallinnon toimijana seuraamusmaksu ei koskisi meitä.

CSIRT-yksikön tehtäviä koskevat huomiot

CSIRT-yksikön tehtävät ovat laissa hyvin määriteltyjä, jos tosin käsityksemme mukaan Traficom tuottaa jo nyt suurimman osan niistä.

CSIRT-yksikön toiminnan laajuus määritellään kohdassa 19§1 3k varsin laajasti. Jos ilmoituksia tulee melko vähäisistä poikkeamista ja CSIRT:n odotetaan avustavan niiden hallinnassa, on tilanteessa ristiriita.

Kaupallisia CSIRT-palveluita on saatavilla, ja olisi hyvä, ettei viranomainen omilla toimillaan laajenisi tälle markkinalle.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Julkishallintoa koskevien velvoitteiden sisällyttämistä tiedonhallintalakiin voidaan lähtökohtaisesti pitää järkevänä ratkaisuna. Uuden 4 a luvun soveltamisalan suhdetta kyberturvallisuuden riskienhallinnasta annettavan lain soveltamisalaan tulisi kuitenkin vielä selkeyttää.

Ehdotetun lain 2§k25 on yhdenmukainen direktiivin ja kyberturvallisuuden riskihallintaa säätelevän lain vastaavien kohtien kanssa, mutta euron taloudellinen tappio on lain mukaan merkittävä poikkeama, mitä se ei arkijärjellä ole

Verkkotunnusvälittäjiä koskevat huomiot

Ei kommenttia.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei kommenttia.

Vaikutustenarviointia koskevat huomiot

Ei kommenttia.

Muut huomiot ja avoin palaute esityksestä

Ei kommenttia.

Koivula Antti
Työterveyslaitos

Saarni Leena
Työterveyslaitos - Tietoturvapäällikkö Olli-Pekka Soini, p. 030 474 3415