Elinkeinoelämän keskusliitto EK

Lausunto

03.03.2021

Asia: VN/3501/2021

Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; lausuntopyyntö (Huom! Lausuntoaika päättyy 3.3.2021)

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Kiitämme mahdollisuudesta lausua. Viittaamme aiemmin työryhmän väliraportista antamaamme lausuntoon ja toteamme seuraavaa:

Yleiset huomiot

Huomautamme, että näin tärkeässä, moneen elinkeinoelämän osa-alueeseen vaikuttavassa asiassa olisi kohtuullista varata pidempi lausuntoaika kuin nyt annettu yksi vuorokausi. Lausuntopyyntö on viety lausuntopalveluun 2.3. ja lausuntojen antamisen määräaika on 3.3.

Pidämme hyvänä, että liikenne- ja viestintäministeriö (LVM) on käynnistänyt selvityshankkeen tietoturvan ja tietosuojan parantamiseksi yhteiskunnan eri sektoreilla ja valmistellut nyt lausuttavana olevan luonnoksen.

Tietoturvan ja tietosuojan haasteet verkottuneessa yhteiskunnassa ovat kompleksisia, jolloin luonnollisesti ratkaisutkin ovat monitahoisia ja vaativia. Tietoturvapoikkeamilta on mahdotonta välttyä kokonaan, joten on tärkeää ymmärtää kokonaiskuva ja välttää ylilyöntejä. Tietoturva ei myöskään toteudu tarkastamalla ja valvomalla, vaan ensisijaisesti organisaatioiden päivittäisessä työssä johdon kannustamana, riittävin resurssein ja riittävällä osaamisella. Siksi näemme, että tärkeintä on huolehtia näistä asioista, avoimesti ja yhteistyössä oppia jakaen ja kaikkia toimijoita tukien sekä varautua lisäksi vahinkojen rajoittamiseen, ripeään tutkintaan, tiedottamiseen sekä oppien keräämiseen ja jakamiseen poikkeamista.

Ottaen huomioon, että merkittävä osa väliraportin ehdotuksista joko suoraan tai välillisesti kohdistuu yksityisen sektorin toimijoihin, pidämme tarpeellisena, että jatkotyössä myös elinkeinoelämä otettaisiin mukaan toimenpiteiden käytännön suunnitteluun.

Haluamme kiinnittää huomiota siihen, että termit ”kriittiset toimialat” ja "kriittiset toiminnot" ovat luonteeltaan kuvailevia eikä niitä ole määritelty lainsäädännössä, kuten ei myöskään nyt lausuttavana olevassa luonnoksessa. Jos termiä halutaan käyttää sääntelytarkoituksissa, sen sisältöä ei tule jättää asiayhteydestä pääteltäväksi, vaan termi tulee määritellä yksiselitteisesti. Sekaannusten välttämiseksi määritelmän tulisi myös olla yhteensopiva huoltovarmuuden turvaamista ja kansallista turvallisuutta koskevien sääntelyjen kanssa, eikä se saa olla ristiriidassa myöskään esim. valmisteltavana olevien NIS2-direktiivin tai CER-direktiivin kanssa.

Kiinnitämme huomiota myös siihen, että osa nyt esitetyistä linjauksista vaikuttaa hyvin samantyyppisiltä kuin on esitetty Kyberturvallisuuden kehitysohjelmassa, joka sekin on tulossa valtioneuvoston käsittelyyn ja on tarkoitus vahvistaa valtioneuvoston periaatepäätöksellä. On tärkeää varmistaa myös se, ettei näiden kahden välille jää ristiriitaa.

Pidämme tärkeänä, että määritelmät ovat yksiselitteistä. On erittäin tärkeää, että yritys kykenee selvästi ymmärtämään, onko se sääntelyn kohteena ja jos on, miltä osin. Varsinkin isompien yritysten osalta on tyypillistä, että kaikki niiden harjoittama toiminta ei välttämättä ole tarkoitetulla tavalla kriittistä, joten sen, mitä toimintaa yrityksen kokonaisuudessa vaatimukset koskevat, tulee ilmetä täysin yksiselitteisesti.

Kiinnitämme huomiota siihen, että kriittisten toimialojen yrityksillä on itselläänkin merkittävä intressi panostaa omaan tietoturvallisuuteensa ja tietosuojavaatimusten toteutumiseen sekä laajemmin riskienhallintaansa. Yritykset tarvitsevat tuekseen ennen kaikkea tietoa. Viime vuosina viranomaisten tuottaman ja yhdessä toimialoilla tuotetun tilannekuvatiedon laatu ja kattavuus ovat parantuneet, mutta jatkossakin tulisi panostaa enenevästi siihen, että riskeistä ja uhista olisi saatavilla tietoa ja analyysejä mahdollisimman etupainotteisesti, kun ne eivät vielä ole realisoituneet Suomessa tai toimialoilla. Erityisesti digitaalisen maailman riskit eivät tunne maiden rajoja ja jos keskitytään liiaksi siihen, millaisia tapauksia on jo tullut esiin ja millaisia riskejä realisoitunut, ollaan auttamattomasti myöhässä.

Huomiot esitetyistä poliittisista linjauksista

Otamme seuraavassa lyhyesti kantaa ehdotettuihin politiikkalinjauksiin:

Ehdotukset 1 - 8:

Kannatamme ehdotuksia.

Ehdotuksen 1 osana on tärkeää varmistaa, ettei ole esteitä luovuttaa tietoja viranomaisilta myös yrityksille, jos tiedot ovat tarpeen havaitun riskin realisoitumisen ehkäisemiseksi tai vaikutusten lieventämiseksi. Sillä, että tiedonkulkuun kiinnitetään erityistä huomiota ja tietoa annetaan myös yksityisille yrityksille, on iso merkitys negatiivisten vaikutusten rajaamiseksi ja monissa tapauksissa jopa tapausten ennalta ehkäisemiseksi kokonaan.

Ehdotuksen 2 osalta tulisi huomioida, ettei vastuuvirkamiesten toimialakohtaista neuvontaa pidä rajata vain sektoriviranomaisille annettavaksi, vaan sen tulee ulottua myös asianomaisen toimialan yrityksiin. Merkittävä osa kriittisestä infrastruktuurista on yksityisten toimijoiden hallussa, joten viranomaisten keskinäisen kommunikoinnin lisäksi on huomioitava elinkeinoelämä. On myös välttämätöntä, että Kyberturvallisuuskeskuksen resurssien riittävyys ja selkeät toimintaperiaatteet varmistetaan niin, etteivät mahdolliset uudet tehtävät vaaranna nykyistä hyvin sujuvaa ja luottamuksellista yhteistyötä.

Ehdotusten 2 - 4 osalta katsomme, että viranomaisten kyberturvallisuuteen osoitettujen resurssien parantaminen on perusteltua, mutta viranomaisen ei tule myöskään rakentaa yritysten palveluiden kanssa kilpailevaa julkista palvelutarjontaa. Viranomaisen tulee keskittyä edistämään ja mahdollistamaan yhteiskunnan kriittisten toimijoiden käyttämien palveluntarjoajien toimintaa ja välttää kilpailua jo nyt rajallisesta osaavasta työvoimasta yritysten kanssa.

Ehdotuksessa 7 esitettyjen yhdenmukaisten, kattavien, luotettavien ja turvallisten teknisten tiedonsiirtoratkaisujen tarve on ilmeinen ja ne tulisi toteuttaa mahdollisimman nopealla aikataululla. Hallinnonalojen sisäisten ja välisten siirtojen ohella ratkaisujen tulisi mahdollistaa myös hallinnonalojen ja yritysten väliset tietojen siirrot. Ratkaisujen tulisi olla yleisesti käytössä oleviin ratkaisuihin (esim. O365) integroituvia siten, että yrityksiltä ei edellytetä erillisiä kommunikointityökaluja viranomaisyhteyksiin.

Ehdotukset 9 - 11:

Kriittisten toimialojen ja toimintojen selkeä määrittely on keskeistä, kuten edellä olemme todenneet. Sääntelyn ristiriidattomuus yleisen ja sektorikohtaisen sääntelyn ja toisaalta kotimaisen ja EU-tasoisten sääntelyn välillä on erittäin tärkeää. Vaatimukset tulee säätää lain tasolla, eikä sisällöllisten vaatimusten antovaltuutta tule delegoida tätä alemmas, koska vaatimuksilla on tyypillisesti merkittävä taloudellinen vaikutus yritysten toimintaan. Vaatimuksilta tulee edellyttää myös riittävää pysyvyyttä ja ennakoitavuutta, jotka toteutuvat parhaiten lain tasoisilla säädöksillä.

Vaatimusten riskiperusteisuus, oikeasuhteisuus ja oikea kohdentuminen tulee varmistaa. Pitää huolehtia esim. siitä, että vaatimus kohdentuu vain siihen osaan yrityksen toimintaa, joka perustellusti ja riskiperusteisesti voidaan katsoa kriittiseksi.

Vaatimuksia määriteltäessä tulee välttää yksityiskohtaisia, teknisiä vaatimuksia toteutustapojen osalta, koska teknologioiden kehittyessä tällaiset vaatimukset vanhentuvat nopeasti. Sen sijaan on keskityttävä vaatimuksiin, joissa määritellään tarvittava turvallisuuden taso ja jättää toteutustapa toimijan itsensä päätettäväksi.

Ehdotukset 12 - 15:

Ehdotuksissa esitetään tarkemmin määrittelemättömälle joukolle kriittisten toimialojen toimijoita erittäin pitkälle meneviä kansallisia velvoitteita määritellä, dokumentoida, luokitella, auditoida ja sertifioida tieto- ja tietoliikenneteknisiä prosessejaan ja toimintojaan. Tältäkin osin vaatimukset näyttäisivät merkittävällä tavalla puuttuvan ainakin elinkeinovapauteen, mitä tuskin voidaan kaikilta osin pitää perusteltuna, tarpeellisena tai edes mahdollisena. Mikäli linjauksissa ehdotettuja vaatimuksia halutaan edistää, niistä saatavat hyödyt on kyettävä osoittamaan. Lisäksi on varmistettava, että velvoitteet ovat oikeasuhtaisia eikä niistä aiheudu toimijoille kohtuutonta taloudellista, hallinnollista tai toiminnallista rasitusta.

Mikäli ehdotukset päätetään toteuttaa:

- Ehdotuksen 12 osalta kiinnitämme huomiota siihen, että määrittelyprosessi voi olla suhteellisen raskas sellaiselle toimijalle, joka sitä ei mahdollisesti tähän mennessä ole tehnyt. Tämä tulisi huomioida esim. tuki- ja neuvontatarpeissa sekä harkittaessa määräaikaa, mihin mennessä tehtävä on täytettävä.

- Ehdotuksen 13 osalta katsomme, että myös sisäinen / itseauditointi tulisi hyväksyä, eikä auditointia tulisi edellyttää liian usein. Kustannusvaikutus yrityksissä voi olla erittäin merkittävä, erityisesti mikäli auditoinnin tulisi olla hankittu ulkopuoliselta palveluntarjoajalta. Auditointimallin riskiperusteiseen ja selkeään määrittelyyn tulee kiinnittää erityistä huomiota. Samoin on määriteltävä, mikä taho riskiperusteisuuden harkitsee ja päättää. Jos yritys itse omistaa riskin tai siltä osin kuin se sen omistaa, sillä tulee olla päätösvalta myös sen hallintatoimista.

- Ehdotuksen 14 osalta katsomme, että on tarkkaan määriteltävä, mitä tarkoitetaan kriittisten toimialojen suurimmilla ja yhteiskunnan keskeisten toimintojen kannalta merkittävimmillä toimijoilla ja millä perusteilla suuruus ja merkittävyys määritellään. Määritelmän on oltava täysin yksiselitteinen.

Katsomme, että myös sertifiointivaatimuksen kohdentamiseen tulisi kiinnittää erityistä huomiota. Yrityksiä ei tulisi velvoittaa soveltamaan ISO 27001-standardia kaikessa toiminnassaan, vaan korkeintaan tiukasti rajaten vain kriittisissä prosesseissa ja toiminnoissa. Muilta osin sen tulee olla yrityksen itsensä päätettävissä.

Ehdotukset 16 - 19:

Ehdotukset ovat toimialakohtaisia. Emme ota niihin kantaa.

Ehdotukset 20 - 21:

Kannatamme ehdotuksia.

Poliisin rikostorjuntakyvystä huolehtiminen on erittäin tärkeää. Elinkeinoelämä on ollut jo pitkään huolissaan erityisesti poliisin rikostorjunnan vaikuttavuudesta sekä resurssien riittämättömyydestä seuranneista esitutkinnan kohdennus- ja rajauspäätöksistä.

On tärkeää, että keskitytään sekä kyberrikosten rikoksentekomahdollisuuksien pienentämiseen että kiinnijäämisriskin nostamiseen.

Ehdotus 22:

Ehdotuksen mukaan toimijoita ohjeistettaisiin tekemään rikosilmoituksia epäillyistä tietoturvarikoksista aina, kun epäilevät, että kyseessä on rikos.

Tämän osalta kiinnitämme huomiota kahteen asiaan:

- Raportointikynnyksen alentamiseksi on ensiarvoisen tärkeää laajentaa ja nopeuttaa ilmoitettujen epäilyjen selvittelyä ja esitutkintaa sekä mitoittaa rikoksiin liittyvät rangaistusasteikot sellaisiksi, että tekijä joutuu aidosti punnitsemaan tekonsa seuraamuksia ennen sen toteuttamista. Nykytilanteessa merkittävä osa ilmoitetuistakin tietoverkkorikoksista jäänee tutkimatta ja näin selvittämättä, jolloin uhrin kannalta rikosepäilyn ilmoittaminen merkitsee vain tarpeetonta lisätyötä.

- Ehdotettuihin tapahtumiin liittyen voi olla toisinaan vaikeita rajanvetotilanteita. Kyseessä voi esim. palveluksesta pois lähteneiden entisten työntekijöiden tai entisten kumppaneiden ja alihankkijoiden osalta olla sekä rikos että sopimusrikkomus. Rikosasian polku ei välttämättä kaikissa tällaisissa tilanteissa ole yrityksen etu. Lisäksi laissa on määritelty erikseen ns. asianomistajarikokset, joissa asianomistajan lähtökohtaisena oikeutena on päättää, haluaako hän vaatia epäillylle tekijälle rangaistusta. Asianomistajarikosten osalta tätä oikeutta tulee kunnioittaa, eikä yrityksiä näissä tapauksissa tule ohjeistaa tai velvoittaa tekemään rikosilmoituksia tapauksista vastoin niiden omaa päätöstä.

Ehdotus 23:

Emme kannata NIS-direktiivin soveltamisalan laajentamista. Jos näin kuitenkin päätetään tehdä, erityistä huomiota on kiinnitettävä termien ja soveltamisalan selkeään määrittelyyn sekä siihen, että eri säännökset eivät ole keskenään ristiriidassa. Muilta osin viittaamme NIS-direktiivistä muissa yhteyksissä antamiimme lausuntoihin.

Ehdotukset 24 - 29:

Ehdotukset kohdistuvat ennen kaikkea viranomaisiin ja julkishallintoon. On huomioitava, että Suomessa tietosuoja-asetuksen sanktioita ei kohdisteta julkiseen sektoriin. Julkisella sektorilla on kuitenkin tullut viime vuosina ilmi useita tietosuojaan ja tietoturvallisuuteen kohdistuneita tapauksia. Valittu sanktioimattomuuslinja näyttäisi johtavan käytännössä siihen, että tietosuojan tasoon ei ole ollut tarpeen kiinnittää niin suurta huomioita julkisella sektorilla eikä siihen ole varattu tarpeeksi resursseja. Mikäli sanktiot koskisivat kaikkia toimijoita, saattaisi tilanne olla parempi tietosuojan tason suhteen ja asiaa tulisikin arvioida tässä yhteydessä uudelleen.

Ehdotuksen 25 osalta toteamme, että Katakri edellyttää TL IV -tason tietojen sähköisen käsittely-ympäristön olevan tietyille kriittisille palveluille kokonaisuudessaan Suomen lainsäädännön alaisuudessa, toimivaltaisten viranomaisten toimivallan piirissä. On syytä täsmentää termiä ”kriittinen palvelu” ja vaatimuksia palveluiden tuottamiselle Suomessa.

Ehdotusten 27 ja 28 osalta haluamme painottaa, että julkisissa kilpailutuksissa turvallisuus- ja tietosuojavaatimusten tulee perustua aina riskiin ja vaatimukset on räätälöitävä hankittavan palvelun kannalta järkeviksi. Ns. listavaatimuksia esim. VAHTI-ohjeisiin tai Katakriin viitaten ilman palvelukohtaista räätälöintiä ei tule käyttää.

Lisäksi toteamme yleisesti pilvipalveluihin liittyen, että mm. niihin liittyvä teknologia muuttuu niin kovaa vauhtia, että vaatimukset uhkaavat jäädä teknologisesta kehityksestä jälkeen. Mikäli valtionhallinnossa kategorisesti kielletään tai rajataan pilvipalveluiden käyttöä liian laajalti, se ei lopulta ole myöskään valtionhallinnon etu, koska potentiaalisten palveluntarjoajien määrä pienenee ja palveluiden hinta kallistuu.

Ehdotukset 30 - 36:

Pidämme ehdotuksia lähtökohtaisesti kannatettavina. Tietosuojasertifiointien osalta haluamme painottaa, että näkemyksemme mukaan sertifiointi tulee säilyttää jatkossakin mahdollisuutena, eikä yrityksiä tule velvoittaa sen hankkimiseen.

Ehdotus 37:

Pidämme ehdotusta kannatettavana. Siltä osin kuin kyse on raportointivelvollisuudesta, on hyvä, jos samasta tietoturvatapahtumasta on mahdollisuus ilmoittaa kaikille asiaankuuluville viranomaisille samalla ilmoituksella, esim. tietosuojavaltuutetulle ja Traficomille.

Kunnioittavasti

Elinkeinoelämän keskusliitto EK

Lainsäädäntö ja hallinto

Tommi Toivola

Johtaja

Rajamäki Markku
Elinkeinoelämän keskusliitto EK - Lainsäädäntö ja hallinto