Elinkeinoelämän keskusliitto EK

Lausunto

05.01.2021

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Kiitämme lausuntomahdollisuudesta ja toteamme seuraavaa:

Yleiset huomiot

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

Vastaamon tietomurto on toiminut hyvänä herättäjänä sekä yksityisellä että julkisella sektorilla pohtimaan tietoturvan ja tietosuojan tasoa. Kaikilla on varmasti yhteinen tahto varmistaa suomalaisen yhteiskunnan toimivuus ja turvallisuus.

Tietoturva ja tietosuoja verkottuneessa yhteiskunnassa ovat kompleksisia haasteita, 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, vaan organisaatioiden päivittäisessä työssä johdon kannustamana, riittävin resurssein ja riittävällä osaamisella. Siksi tulevaisuudessa on tärkeää huolehtia erityisesti näistä asioista, avoimesti ja yhteistyössä oppia jakaen ja kaikkia tukien sekä varautua lisäksi vahinkojen rajoittamiseen, ripeään tutkintaan, tiedottamiseen sekä oppien keräämiseen ja jakamiseen.

Ottaen huomioon, että merkittävä osa väliraportin ehdotuksista joko suoraan tai välillisesti kohdistuu yksityisen sektorin toimijoihin, pidämme tarpeellisena, että selvitystä jatkettaessa myös elinkeinoelämä otettaisiin mukaan työryhmän toimintaan.

Haluamme kiinnittää LVM:n huomiota siihen, että termi ”yhteiskunnan kriittiset toimialat” on luonteeltaan kuvaileva eikä sitä ole määritelty lain-säädännössä. Jos termiä halutaan käyttää sääntelytarkoituksissa, sen sisältöä ei näkemyksemme mukaan tule jättää asiayhteydestä pääteltäväksi, vaan termi tulee määritellä yksiselitteisesti. Sekaannusten välttämiseksi määritelmän tulisi myös olla yhteensopiva huoltovarmuuden turvaamista ja kansallista turvallisuutta koskevien sääntelyjen kanssa. Poliittisissa linjauksissa näyttäisi olevan epäjohdonmukaisuutta myös termien ”hallinnonala”, ”toimiala” ja ”sektori” käytössä, mikä vaikeuttaa linjausten kohteen, sisällön ja vaikutusten hahmottamista. Pidämme tärkeänä, että terminologia on yksiselitteistä ja linjauksista käy selvästi ilmi, miltä osin kyse on elinkeinoelämään ja miltä osin viranomaisiin kohdistuvista vaatimuksista. Kun tarkoituksena on lopulta sää-tää yksittäistä yritystä koskevia velvoittavia vaatimuksia, 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.

Monet väliraportin ehdotuksista kohdistuvat kriittisten toimialojen yrityksiin. Kiinnitämme huomiota siihen, että 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.

Kommentit ehdotetuista poliittisista linjauksista

Otamme seuraavassa lyhyesti kantaa väliraportissa ehdotettujen politiikkalinjausten osalta:

1-6:

Kannatamme ehdotuksia.

Ehdotuksen 1 osana tulisi lisäksi varmistaa, ettei ole esteitä luovuttaa tietoja viranomaisilta myös yrityksille, jos tiedot ovat tarpeen havaitun riskin realisoitumisen ehkäisemiseksi tai vaikutusten mitigoimiseksi. 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 rajata pidä rajata vain sektoriviranomaisille, 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 ja 4 osalta katsomme, että viranomaisten kyberturvallisuuteen osoitettujen resurssien parantaminen on perusteltua, mutta viranomaisen ei tule 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 5 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.

7:

Kiinnitämme huomiota, että vaatimuksia harkittaessa tulee kiinnittää huomioita vaatimusten oikeasuhtaisuuteen ja oikean kohdentumisen varmistamiseen. Vaatimusten ja velvoitteiden tulee perustua lakiin ja niiden tulee olla Suomea koskevien kansainvälisten velvoitteiden mukaisia. Linjauksessa esitetty tietoturvaa koskevien sitovien määräysten antovaltuuksien delegointi asetustakin alemmalle tasolle vaikuttaa ylimitoitetulta ja hyvien periaatteiden vastaiselta. Muutokset tietoturvan ja tietosuojan kannalta merkittävissä teknisissä tai toiminnallisissa järjestelyissä saattavat edellyttää toimijoilta merkittäviä taloudellisia panostuksia, minkä vuoksi tällaisista velvoitteista tulisi ehdottomasti säätää lain tasolla ja niiden säätämisessä tulisi käyttää erityistä harkintaa. Vain täysin välttämättömiä vaatimuksia tulisi säätää.

On myös huomioitava, että jos esim. vain osa yrityksen toiminnasta on määritellyltä kannalta kriittistä, vaatimusta ei tule ulottaa yrityksen kaikkeen toimintaan. Vaatimusten tulee aina perustua riskiin, tiukka vaatimus varmuuden vuoksi riskin tasosta riippumatta ei ole hyväksyttävää. Lisäksi 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. Ennakoitavuuteen ja jatkuvuuteen on kiinnitettävä erityistä huomiota. Ei ole kenenkään etu, että vaatimukset muuttuisivat usein tai ennakoimattomasti.

Kriittisten toimialojen nykyinen sääntely on tasoltaan ja sisällöltään eritasoista. Alat myös poikkeavat toisistaan samoin kuin niihin liittyvät keskeisimmät riskit. Nykyinen sääntely ja alojen ominaispiirteet ja riskit on luonnollisesti huomioitava vaatimuksia harkittaessa.

8-9:

Kannatamme ehdotuksia. Ehdotuksen nro 8:n osalta on kuitenkin epäselvää, mihin ”toimialoille säädetään velvoite pyytää…” kohdistuu. Ei vaikuta siltä, että kohdassa olisi tarkoitettu asettaa yrityksille velvoite pyytää lausuntoa, vaan että toimialojen vastuuviranomaisten pitää pyytää lausunto ajatelluista vaatimuksista. Tätä olisi syytä selventää.

10-13:

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 elinkeinonvapauteen, mitä tuskin voidaan pitää perusteltuna, tarpeellisena tai edes mahdollisena. Toteutuessaan näin raskaat velvoitteet todennäköisimmin johtaisivat vain siihen, että asianomaisten palvelujen tarjonta siirtyisi kansallisen lisäsääntelyn ulottumattomiin Suomen rajojen ulkopuolelle. 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 10-13 kuitenkin päätetään toteuttaa:

- Ehdotuksen 10 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 11 osalta katsomme, että myös sisäinen / itseauditointi tulisi hyväksyä ja auditointia ei tulisi edellyttää liian usein. Kustannusvaikutus isoissa yrityksissä, jotka toimivat kokonaisuudessaan kriittisillä toimialoilla, voi olla erittäin merkittävä, erityisesti mikäli auditoinnin tulisi olla hankittu ulkopuoliselta palveluntarjoajalta. Auditointimallin riskiperusteiseen määrittelyyn tulee kiinnittää erityistä huomiota, jotta se on selkeä. Samoin on määriteltävä, mikä taho riskiperusteisuuden

harkitsee ja päättää. Jos yritys itse omistaa riskin, sillä tulee olla päätösvalta myös sen hallintatoimista.

- Ehdotuksen 12 osalta katsomme, että on tarkkaan määriteltävä, mitä tarkoitetaan kriittisten toimialojen merkittävimmillä toimijoilla ja millä perusteilla merkittävyys määritellään. Määritelmän on oltava täysin yksiselitteinen.

Katsomme, että 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. Sertifiointiprosessin kustannusriski on merkittävä. Raportin sivulla 31 käytettyyn malliesimerkkiin kustannuslaskelmia ei tule perustaa. Ne voivat todellisuudessa olla moninkertaisia riippuen mm. lähtötasosta, toimialasta, yrityksen koosta ja toiminnan ja järjestelmien kompleksisuudesta.

Raportissa mainittiin kriittisillä toimialoilla olevan lähes 58 000 yritystä. Huoltovarmuuskriittisiä organisaatioita Suomessa on alle 2 000. ISO 27001 -sertifikaatteja on Suomessa alle 100 yrityksellä. Mikäli sertifiointeja edellytettäisiin kaikilta kriittisten toimialojen yrityksiltä, kyseessä olisi erittäin merkittävä muutos.

Lisäksi olisi syytä harkita muidenkin mahdollisten standardien soveltuvuutta tarpeeseen.

Osoittamisvaatimus ei mielestämme myöskään saa tarkoittaa sitä, että osoittaminen on mahdollista vain ulkopuolisen palveluntarjoajan ISO 27001 - auditoinnilla, vaan yrityksellä olisi mahdollisuus myös itse dokumentoida ja osoittaa vaatimustenmukaisuutensa.

14-17:

Nämä ovat toimialakohtaisia ehdotuksia. Emme ota niihin kantaa.

18-19:

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

Laajempana kysymyksenä näemme erityisesti sen, että nykyinen ajattelu vaikuttaa perustuvan ensisijaisesti kyberrikosturvallisuuden rikoksen-tekomahdollisuuksien pienentämiseen. Vain vähän

huomiota on kohdistettu toimiin, joilla voitaisiin pienentää verkkorikoksista, kuten tietomurroista, saatavia hyötyjä. Huomiota ei ole kohdistettu niiden tosiasiallisten haasteiden ratkaisemiseen, tai myöskään uusimpien oikeudellisten ja käytännöllisten mahdollisuuksien hyödyntämiseen, joiden avulla kiinnijäämisriskiä voitaisiin nostaa. Tähän kokonaisuuteen kuuluvat kokonaisuudessaan lainvalvonta- ja oikeusviranomaisten kyvykkyydet sekä toiminnan kehittäminen. Elinkeinoelämä on toistuvasti nostanut esille kyberrikostorjunnan vaikuttavuusvajeen, jossa resurssien lisäksi myös johtamisen, toiminnan ja osaamisen ketterä kehittäminen nousevat keskiöön. Vakavan ja järjestäytyneen (kyber-)rikollisuuden torjunnassa on todettu, että tosiasiallista vaikuttavuutta saadaan aikaan keskittymällä täsmällisesti rikollisen toiminnan pysäyttämiseen. Vain pieni osa mietinnössä esitetyistä toimista tukee tätä tavoitetta.

On hyvä huomioida, että kun ehdotuksessa 20 kannustettaisiin toimijoita tekemään rikosilmoituksia, epäiltyjen tietoturva- ja tietosuojaloukkausten raportointikynnyksen alentamiseksi on ensiarvoisen tärkeää laajentaa ja nopeuttaa näiden selvittelyä ja esitutkintaa sekä mitoittaa niihin 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. Rikosilmoituksen hyödyllisyyttä on nykyisessä tilanteessa vaikea perustella ainakin rikostorjunnan vaikuttavuusvajeen näkökulmasta.

20:

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.

21:

Emme kannata NIS-direktiivin soveltamisalan laajentamista. Katsomme, että asiassa tulisi edetä vapaaehtoisen varautumisen kehittämisen kautta. Näin olemme myös vuonna 2020 lausuneet valmisteltaessa Suomen kantaa.

Mikäli soveltamisalaa kuitenkin päätettäisiin laajentaa, olisi arvioitava, ovatko ehdotetut uudet toimijat energia- ja rahoitusalalta aidosti direktiivin alkuperäisen tarkoituksen mukaisia yhteiskunnan toiminnalle keskeisten palvelujen tarjoajia tai digitaalisen palvelun tarjoajia, vai tarkoittaisiko niiden sisällyttäminen direktiivin soveltamisalan tarpeetonta laajentamista. Direktiivin soveltamisalaa tai sisältöä uudelleen arvioitaessa on varmistettava, etteivät muutokset ole päällekkäisiä tai ristiriidassa toimialakohtaisten säädösvaatimusten kanssa.

22-27:

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.

Vaatimuksen 23 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 26 ja 27 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, että mm. pilvipalveluihin 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.

28-34:

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

35:

Pidämme ehdotusta kannatettavana.

Vaadittujen ilmoitusten osalta tulee kiinnittää huomiota erityisesti prosessiekonomiaan ja hallinnollisen taakan välttämiseen. Jos tapahtuneesta tulee ilmoittaa kahdelle tai useammalle

viranomaiselle, sen tulisi olla mahdollista yhdellä ilmoituksella, joka kattaa olennaiset tiedot molempien viranomaisten kannalta ja lähtee molemmille yhdellä täyttämisellä.

Väliraportin muut osat, kommentit:

Kommentit väliraportin muista osista

Väliraportin sivun 9 lopussa todetaan:

" Riittävän tietosuojan ja tietoturvan taso on kuitenkin viime kädessä poliittisesti määriteltävä asia. Järjestelmän tavoitteena voi olla se, että käytännössä kaikki toimijat hankkivat riittävän tietoturvan. On myös mahdollista, että tätä ei tavoitella. Täydellinen tietoturvan taso ei välttämättä ole siinä mielessä optimaalinen, että toiminnan tehokkuuden ja tietosuojan välillä on tehtävä valinta. Enemmän tietoturvaa ja tietosuojaa tarkoittaa tehottomampaa toimintaa. Tietoturvaan ja tietosuojaan kuluu enemmän resursseja, kun on enemmän tehtävää. Lisäksi suurempi tietoturvan ja tietosuojan määrä voi aiheuttaa epätehokkuuksia tuotannossa. kun esimerkiksi järjestelmän ylläpitoon kuluu resursseja. Toisaalta vähemmän tietoturvaa tarkoittaa tehokkaampaa toimintaa, mutta suurempaa riskiä tietomurroille."

Olemme edellä lausutusta osin eri mieltä. Vaikuttaa siltä, että edellä tietosuoja ja tietoturva on mielletty ennen kaikkea tiedon luottamuksellisuudesta huolehtimisena. On kuitenkin muistettava, että tietoturvassa ja tietosuojassa ovat elementteinä luottamuksellisuuden lisäksi myös tiedon saatavuus ja eheys / kiistämättömyys. Kyse onkin usein näiden elementtien välisestä tasapainosta; se, että luottamuksellisuutta painotettaisiin tavoitteena vähemmän ei tarvitse tarkoittaa tehokkuuden korostamista luottamuksellisuuden kustannuksella, vaan sitä, että painotetaan tiedon saatavuutta luottamuksellisuuden ohella. Tietoturvallisuus ei toteudu, jos luottamuksellisuuden vaatimusta painotetaan niin paljon, ettei tieto ole siihen oikeutettujenkaan saatavilla.

Vastaamon tietomurto on erittäin ikävä tapaus. Henkilötietojen ja aivan erityisesti arkaluonteisten henkilötietojen suojaaminen on erittäin tärkeää. Samalla toimenpiteitä harkittaessa tulisi kuitenkin erittäin tarkasti varmistaa, että ei kohtuuttomasti heikennetä tiedon saatavuutta. Näin helposti käy, jos tiedon luottamuksellisuutta ylikorostetaan. Samalla täytyy varmistaa, että tieto on siihen oikeutettujen ja sitä tarvitsevien saatavilla.

Väliraportissa kiinnitetään huomiota tietoturva- ja tietosuojaosaajien puutteeseen. Samalla halutaan merkittävästi lisätä ko. resursseja erityisesti tarkastamiseen ja valvontaan. Tämä on haastava yhtälö. Suuri resurssilisäys näille alueille haastavassa osaajamarkkinassa voi tarkoittaa sitä, että tietoturva- ja tietosuojaosaajien saatavuus tärkeämmille osa-alueille – organisaatioiden palveluiden, tuotteiden ja tietoteknisten ratkaisujen tietoturvalliseen toteuttamiseen sekä jatkuvien tietoturvapalvelujen tuottamiseen heikkenee entisestään. Kuten jo väliraportin johdannossa todetaan, tietosuoja ja tietoturva on huomioitava toiminnan koko elinkaaren aikana tuote-, järjestelmä- ja palvelukehityksen lähtökohtana, eikä jälkikäteen päälle liimattavana tarrana tai laastarina. Tietoturva ja tietosuoja rakennetaan erityisesti näillä keinoilla. Jos resurssit markkinassa ohjautuvat liiaksi valvontaan, eivätkä riitä proaktiiviseen tietoturvallisuuden toteuttamiseen ja ylläpitoon, tavoitteet eivät voi toteutua.

Lopuksi toteamme, että useat väliraportissa esitetyt toimet edellyttäisivät huomattavia panostuksia sekä elinkeinoelämän että viranomaisten puolella. Tämän vuoksi pidämme välttämättömänä, että niiden taloudelliset ja hallinnolliset kustannukset arvioidaan mahdollisimman luotettavasti jatkokäsittelyn yhteydessä myös elinkeinoelämän edustajien osallistuessa työhön.

Kunnioittavasti

Elinkeinoelämän keskusliitto EK

Petri Vuorio

Johtaja

Rajamäki Markku
Elinkeinoelämän keskusliitto EK - Lainsäädäntö ja hallinto