Elinkeinoelämän keskusliitto EK

Lausunto

02.02.2021

Asia: VN/ 797/2021

Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Kiitämme lausuntomahdollisuudesta ja toteamme ehdotuksesta seuraavaa:

Yleisesti ehdotuksesta

Tarve kehittämisohjelmalle on ilmeinen. Verkottunut maailma muuttuu vauhdilla ja asettaa kyberturvallisuuden koko ajan muuttuvien ja kasvavien haasteiden eteen. Digitalisoitumiskehitys on vauhdittunut koronakriisin myötä kaikkialla ja siinä onnistuminen edellyttää kyberturvallisuuden laajapohjaista kehittämistä ja onnistumista ja osaamista niin julkishallinnossa, yksityisen sektorin yrityksissä kuin järjestöissäkin.

Tuemme ohjelman tavoitteita ja pidämme ohjelmaa kokonaisuutena erittäin hyvänä. Nähdäksemme ohjelman toimenpidekokonaisuus kattaa melko hyvin yhteiskunnassa viime vuosina tunnistetut kyberturvallisuuden kehittämiskohteet. Hyvää on myös se, että ohjelman on tarkoitettu olevan elävä dokumentti koko aikajänteen 2021–2030; sitä on tarkoitus päivittää ja pitää ajan tasalla. Tämä onkin tarpeen huomioiden aikajänteen pituus ja jatkuvassa muutoksessa oleva aihe.

Kyberturvallisuutta on kehitetty Suomessa aiemminkin. Osin nyt ehdotetussa ohjelmassa esitellyt toimenpiteet ovat samoja tai hyvin samanlaisia kuin aiemmat. Olisi hyvä, että ohjelmassa tarkasteltaisiin lyhyesti sitä, miltä osin näissä toimenpiteissä on tai ei ole aiemmin onnistuttu ja mitä nyt pyritään tekemään toisin.

Ohjelman täytäntöönpanon riskejä ei ole ohjelmassa tarkasteltu. Nähdäksemme tämä olisi tarpeen; ohjelmasta tulisi laatia myös riskianalyysi ja riskienhallintasuunnitelma täytäntöönpanoa tukemaan.

Ohjelman onnistumisen kannalta sen tarvitsemien henkilöresurssien ja rahoituksen riittävyys ovat keskeisiä. Ehdotuksessa mainitut rahalliset panostukset, yhteensä 26,8 M€ vaikuttavat kokonaisuutena melko vaatimattomilta. Toivomme, että henkilöresurssien ja rahoituksen huolellinen suunnittelu ja varmistaminen huomioidaan jatkovalmistelussa.

Kyberturvallisuus, kuten turvallisuus yleensäkin on tuettavan ja kehitettävän prosessin, tuotteen, palvelun tai järjestelmän yksi ominaisuus, joka pitää huomioida ja jota pitää kehittää yhdessä muiden ominaisuuksien kanssa alusta lähtien (security by design). Kaipaisimme ohjelmaan mainintaa siitä, miten kyberturvallisuus huomioidaan muissa kuin ohjelmassa nimenomaan mainituissa kyberturvallisuushankkeissa. Sekä Suomessa että EU:n piirissä on meneillään useita datatalouteen ja digitalisaatioon liittyviä hankkeita, joissa kyberturvallisuuden huomioiminen on yhtä lailla tärkeää. Nähdäksemme ehdotus on tältä osin jäänyt hieman ohueksi. Jos kyberturvallisuutta kehitetään vain kyberturvaliitännäisissä erillishankkeissa, menetetään jotakin tärkeää.

Toimenpidekohtaiset kommentit (ehdotuksen liite 1)

Osa-alue 1 (Kansalaisten kyberturvataidot hyvälle tasolle)

Toimenpiteenä 1.4 kannustetaan tyttöjä ja naisia kiinnostumaan kyberalasta. Tämä on tärkeää, mutta lisäksi olisi hyvä tavoitella laajemmin opiskelijoita ja osaajia ei-perinteisillä taustoilla. Tämä auttaisi siinä, että kyberturvallisuuden tavoitteita saataisiin ajettua laajemmin ja yhä laajapohjaisemmin sen vaatimukset ymmärrettäisiin yhä useammilla aloilla.

Osa-alue 2 (Kyberturvallisuuden koulutusjärjestelmän kehittäminen)

Toimenpiteissä tunnistetaan kansainvälisten huippuosaajien tarve, mikä on aivan oikein. Koulutukseen tehtävät muutokset ovat erittäin tärkeitä. Tarvetta on kyberturvallisuuden ammateissa toimiville, mutta ehkä tätäkin tärkeämpää on varhaiskasvatuksesta lähtevän koulutuksen kautta varmistua siitä, että kaikki kansalaiset ymmärtävät kyberturvallisuuden perusteet ja työelämään siirtyvät / työelämässä olevat kykenevät ymmärtämään kyberturvallisuuden vaatimukset oman työnsä kannalta - esim. palvelu- ja tuotekehitystehtävissä toimivan on tiedettävä, miten kyberturvallisuus tulee huomioida näissä kehitystehtävissä. Erityisen tärkeä tässä suhteessa on esim. kyberturvallisuusosaaminen sovelluskehityksessä kuitenkaan muitakaan aloja unohtamatta.

Yhdymme periaatepäätöksessä esitettyyn näkemykseen, jonka mukaan kansallisen kyberturvallisuuden huippuosaamisen kehittäminen edellyttää riittävän osaamiskeskittymän muodostumista. Tällaisen osaamiskeskittymän luominen edellyttää esitettyä laajaa kansallista ja

kansainvälistä yhteistyötä. Kansainvälisen kilpailukyvyn saavuttaminen edellyttää, että saamme Suomeen korkeatasoisia opiskelijoita, tutkijoita ja muita alan asiantuntijoita. On välttämätöntä – myös kyberturvallisuuden kehittämisen kannalta – että Suomi on houkutteleva kohde kansainvälisille osaajille.

Muutokset kotimaisessa koulutusjärjestelmässä ja panostukset koulutukseen ovat tärkeitä, mutta vaikuttavat etupäässä vuosien viiveellä. Työperäisen maahanmuuton hidasteiden ja esteiden purkaminen on mainittu toimenpiteissä (2.9), mutta ohjelman tekstiosuuden toimenpide-ehdotuksissa keskitytään erityisesti kotimaiseen koulutukseen. Tarve on nyt. Molempia, sekä kotimaisen koulutuksen kehittämistä että työperäisen maahanmuuton esteiden purkamista tarvitaan, mutta toivomme, että näiltä osin ohjelmassa priorisoidaan lyhyellä aikavälillä tarve purkaa kansainvälisten huippuosaajien maahantulon esteitä ja hidasteita, joka on nopeavaikutteisempi toimi kuin koulutusjärjestelmän kokonaisvaltainen kehittäminen. Maahanmuuttoa on tuettava nopealla lupajärjestelmällä (esim. D-viisumi) ja monipuolisilla asettautumispalveluilla. Erityisen tärkeää on huomioida, että koronakriisistä ulos päästäessä kilpailu kansainvälisistä osaajista tulee olemaan vielä nykyistäkin kovempaa, kun se yhdistyy markkinaosuuksien osittaiseen uudelleen jakoon monilla aloilla ja ylipäätäänkin matkustuksen vapautuessa.

Kiinnitämme toimenpiteen 2.9 osalta huomiota myös siinä käytettyyn sanamuotoon ”suomalaisen teollisuuden palvelukseen”. Parempi muotoilu olisi ehkä ”suomalaisen elinkeinoelämän palvelukseen”. Teollisuus ei ole ainoa, jolla näitä tarpeita on. Suomen elinkeinorakenteessa painotus on entistä enemmän kohti palveluelinkeinoja.

Osa-alue 3 (Kyberturvallisuuden harjoitustoiminnan yhteistyön vahvistaminen

Nähdäksemme harjoituksia järjestetään Suomessa jo kohtuullisen paljon, mutta ne keskittyvät ennen kaikkea huoltovarmuuskriittisiin toimijoihin ja huoltovarmuusyhteistyöhön. Olisi keskeistä miettiä myös harjoitustoiminnan näkökulmasta, miten harjoitustoimintaan saataisiin mukaan laajempi joukko yrityksiä. Samoin olisi hyvä käydä läpi, analysoidaanko harjoitusten havainnot riittävän tarkkaan ja viestitäänkö havainnot muillekin kuin harjoitukseen osallistuneille.

Osa-alue 5 (Aktiivinen osallistuminen ja vaikuttaminen kansalliseen ja kansainväliseen kyberturvallisuuden yhteistyöhön)

Toimenpiteissä olisimme odottaneet enemmän painotusta yhteistyön lisäksi myös lainsäädäntövaikuttamiseen, erityisesti EU-edunvalvontaan ja Suomen kantojen ajamiseen nimenomaan EU-foorumeilla, muitakaan toki unohtamatta. Ymmärrämme, että se on ehkä ajateltu kohdassa mainittujen toimenpiteiden osaksi, mutta kun regulaatiosta suuri osa tulee EU:sta, se on hyvin keskeinen osa-alue.

Viestintään siitä, mitä kansainvälisillä kyberturvallisuusfoorumeilla tapahtuu, tulisi kiinnittää erityistä huomiota. Näin yritykset voisivat myös nykyistä enemmän tukea toimintaa tuomalla omia tarpeitaan ja näkemyksiään esiin.

Osa-alue 6 (Kotimaisten kyberturvatuotteiden ja -palveluiden kasvun ja kansainvälistymisen tukeminen)

Toimenpiteenä 6.6 tuetaan tuotteiden ja palveluiden tuotteistamista ja konseptointia kansainvälisen markkinan näkökulmasta. Alalla toimii paljon myös erittäin pieniä mikroyrityksiä. Voisiko näiden toiminnan ja mahdollisesti laajentumisen tueksi harkita osaajahubeja, joihin voitaisiin koota pieniä kaupallisia toimijoita / 1-2 henkilön mikroyrityksiä helpommin löydettäviksi. Näin ne voisivat yhdistää osaamistaan ja esim. tarjota palveluitaan yhdessä asiakkaille.

Osa-alue 10 (Harmonisoidaan turvallisuusvaatimuksia ja parannetaan havainnointikykyä)

Toimenpiteenä 10.1 määritellään huoltovarmuuskriittisten sektoreiden ml. yritykset kyberturvallisuusvaatimuksille yhteinen vähimmäistaso.

Tässä on tärkeä painottaa yritysten mukaanottoa määrittelyyn. On myös huomioitava, että kysymykseen liittyen on tällä hetkellä paljon hankkeita vireillä, mm. EU-tasolla NIS- direktiivin päivittäminen ja CER-direktiivin säätäminen sekä kansallisessa valmistelussa olevat toimenpiteet tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla. On tarkasti huolehdittava siitä, etteivät vaatimukset ole ristiriitaisia tai päällekkäisiä, koska ne kohdistuvat toimialoihin, joita säännellään raskaasti jo tällä hetkellä. Tarkoituksena tulee olla yritysten toiminnan tukeminen. On keskeistä, että yrityksiä kuullaan kaikissa edellä mainituissa hankkeissa ja että tämä tehdään riittävän aikaisessa vaiheessa ja niin, että yrityksillä on aito mahdollisuus vaikuttaa.

Painotamme myös sitä, että vaatimuksia säädettäessä määritellään turvallisuuden tavoitetaso käytettävien keinojen jäädessä yritysten itsensä harkittaviksi. Muu ei ole kestävää.

Kohdan tekstiosuuksissa on mainittu tarve varmistaa viranomaisten valvontaresurssit. Valvontaakin varmasti tarvitaan, mutta on hyvä muistaa, että yrityksillä itsellään on intressi kehittää kyberturvallisuuttaan. Sen vuoksi valtion tuki tälle työlle on tärkeämpää kuin viranomaisten valvontaresurssit - valvonta ei paranna tilannetta, jos tuki on muuten riittämätöntä.

Esimerkkinä yritysten tarvitsemasta tuesta voidaan mainita turvallisuusselvitykset. Kotimaiset viranomaiset edellyttävät usein palveluitaan tarjoavilta yrityksiltä turvallisuusselvitysten tekemistä

viranomaistietoa käsittelevien osalta. Taustantarkistuksia edellytetään laajasti myös kansainvälisissä tarjouskilpailuissa. On hyvä, että Suomessa on laki turvallisuusselvityksistä, joka osin vastaa näihin tarpeisiin. Vastaavaa ei kaikissa muissa maissa ole. Tällä hetkellä saamiemme tietojen mukaan tilanne on kuitenkin se, että useat turvallisuusselvitysmenettelyssä olevat suomalaisyritykset kokevat, että viime aikoina tulkinta selvitettävien tehtävien osalta on selvästi kaventunut aiemmasta huolimatta siitä, että lakia ei ole muutettu.

Osa-alue 12 (Kotimaisen salausteknologian luonti ja AQUA -statuksen saavuttaminen)

Toimenpiteenä 12.3 tunnistetaan kansallisen turvallisuuden näkökulmasta kriittiset kyberturvallisuusyhtiöt ja turvataan niiden kansalliset

omistusosuudet.

Kirjaus kaipaa mielestämme tarkentamista. Mikäli tarkoituksena on viitata ulkomaalaisten yritysostojen seurannasta annetun lain (13.4.2012 / 172) suomiin mahdollisuuksiin, joita laajennettiin turvallisuusalan yhtiöiden osalta viime vuonna, se olisi hyvä kohdassa todeta nimenomaisesti. Emme pidä hyväksyttävänä, että yksityisen sektorin yritysten omistussuhteisiin puututtaisiin yhtään laajemmin kuin mainitun lain näkökulmasta katsotaan ehdottoman välttämättömäksi. Se aiheuttaisi helposti tarpeettomia häiriöitä kilpaillulla markkinalla.

Kunnioittavasti

Elinkeinoelämän keskusliitto EK

Lainsäädäntö ja hallinto

Tommi Toivola

Johtaja

Rajamäki Markku
Elinkeinoelämän keskusliitto EK - Lainsäädäntö ja hallinto