Jyväskylän yliopisto

Lausunto

03.02.2021

Asia: VN/ 797/2021

Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

”3 Huippuluokan osaaminen” 3. kappale

”Nykyinen koulutusjärjestelmä ei suoraan tuota tarvittavaa osaamista suomalaiselle kyberturvateollisuudelle, elinkeinoelämälle ja viranomaisille. Tämä johtaa tilanteeseen, jossa eri tahot joutuvat myös kilpailemaan jatkuvasti samoista osaajista, sekä jatkokouluttamaan uutta henkilöstöään merkittävästi työtehtävien aloittamisen yhteydessä. Parhaimman vaikuttavuuden varmistamiseksi kyberturvallisuuden koulutusjärjestelmän tuottamat tutkinto-opinnot tulee suunnitella yhteistyössä eri toimijoiden kanssa ja opintojen sisältöjä tulee päivittää säännöllisesti vastaamaan eri toimijoiden tarpeita.”

JYU:n vastaus: Tämä pitää paikkansa. Ongelmaksi tässä muodostuu se, että ei ole oikein olemassa sellaista foorumia, jolla tätä yhteistyötä voitaisiin suunnitella ja tehdä. Sellainen olisi ehkä syytä perustaa. Lisäksi haasteeksi tulee helposti korkeakoulujen rahoitusmalli: niin tutkintokoulutuksen kuin jatkuvan oppimisen malleissakin opetuksen tuottaja hyötyy, mikä vaikeuttaa yhteistyötä muiden saman mallin mukaisesti toimivien tahojen kanssa. Jos yhteistyötä koulutuksen toteutuksessa oikeasti halutaan, sitä pitäisi myös resursoida ohi normaalien rahoitusmallien.

”3 Huippuluokan osaaminen” 3. kappale

Edelleen kyberturvallisuuden opetuksen pitäisi olla sisällytettynä niissä tutkintoopinnoissa, joissa luodaan osaamista teknologia-aloille.

JYU:n vastaus: Samaa mieltä sillä täydennyksellä, että peruskyberturvallisuusosaamisen pitäisi sisältyä kaikkiin korkeakoulututkintoihin. Tämä tukisi myös tavoitetta arjen kyberturvallisuusosaamisen lisäämisestä. Tämän osalta voisi harkita jopa asetustason muutosta niin,

että tutkintoasetuksiin kirjattaisiin osaamistavoitteeksi modernin tietoyhteiskunnan vaatima perusosaaminen.

”4 Kiinteä yhteistyö” ”Ehdotetut kehittämistoimenpiteet” 1. kappale (Kyberturvallisuuden harjoitustoiminnan yhteistyön vahvistaminen)

”Tehdään tiivistä yhteistyötä kyberturvallisuuden harjoitustoiminnassa viranomaisten, elinkeinoelämän ja järjestöjen välillä yhteiskunnan toimivuuden kannalta kriittisten arvoketjujen toiminnan turvaamiseksi.”

JYU:n vastaus: Harjoitustoiminnan osalta olisi perusteltua, että oppilaitokset (niin niiden opiskelijat kuin henkilökuntakin) mainittaisiin tarpeellisina yhteistyötahoina.

”4 Kiinteä yhteistyö” 4. kappale

”Kehittämisohjelma kannustaa strategisten kumppanuusmallien lisäämiseen yritysten ja yliopistojen sekä korkeakoulujen välillä. Pitkäjänteisen yhteistyön tulisi mahdollistaa tutkimus- ja kehitystyön kautta uusien tuote- ja palveluinnovaatioiden syntyminen. Tämä edistää kotimaisen kyberturvateollisuuden tuotteiden ja ratkaisujen kaupallistamista.”

JYU:n vastaus: Tämä on tärkeä asia. Pitäisi pyrkiä varmistamaan, että strategisia kumppanuussuhteita syntyy. Mahdolliset yhteistyöryhmät voisivat edistää tätä pelkän kannustuksen lisäksi.

”4 Kiinteä yhteistyö” ”Ehdotetut kehittämistoimenpiteet” 1. kappale (Kyberturvallisuuden harjoitustoiminnan yhteistyön vahvistaminen)

”Kyberturvallisuuden harjoitustoiminnassa hyödynnetään yhteisiä kyberharjoitusympäristöjä”

JYU:n vastaus: Näitähän ei ole olemassa ainakaan oppilaitosten näkökulmasta. Kun oppilaitoksille kuitenkin aiemmin on sälytetty kohtuullisen merkittäviäkin vastuita, pitäisi varmistaa, että niillä on pääsy tällaisiin harjoitusympäristöihin kohtuukustannuksin ja kohtuubyrokratialla. Tässäkin se jonkinlainen yhteistyöfoorumi ja kohdennettu resursointi voisivat olla perusteltuja.

”4 Kiinteä yhteistyö” ”Ehdotetut kehittämistoimenpiteet” 3. kappale (Kansallisen kyberturvallisuuden tutkimus- ja kehitysyhteistyön edistäminen)

Teoreettisten tutkimustuloksien lisäksi tunnistetaan entistä enemmän mahdollisuuksia tulosten kaupallistamiseen ja tuetaan näiden edistämistä.

JYU:n vastaus: Tämä edellyttäisi soveliaiden rahoitusinstrumenttien olemassaoloa. Esim. entisen Tekesin aiemmat tavoitetutkimusohjelmat tai niitä vastaavat instrumentit olisivat tähän hyviä; ne lisäisivät myös kaivattua yritysten kanssa tehtävää yhteistyötä. Nykyisen Business Finlandin ja Akatemian tutkimusrahoitushaut ovat monessa mielessä äärimmäisen raskaita ja työläitä niin, ettei monillakaan ole välttämättä aikaa ja halua osallistua niihin. OKM:n resurssimallin mukainen tutkimuskomponentti taas johtaa nimenomaan hyvin teoreettiseen tutkimukseen, joka lisäksi pilkotaan mahdollisimman pieniksi palasiksi JUFO-pisteiden maksimoimiseksi.

”4 Kiinteä yhteistyö” ”Ehdotetut kehittämistoimenpiteet” 3. kappale (Kansallisen kyberturvallisuuden tutkimus- ja kehitysyhteistyön edistäminen)

”Kyberturvayhteisöä aktivoidaan entistä laajemmin valtionhallinnon digitaalisten palveluiden turvallisuuden varmistamiseen. Yhteisön osaamista voidaan hyödyntää esimerkiksi turvallisen ohjelmistokoodin kehittämisessä ja käynnistämällä soveltuvin osin valtionhallinnon ”Bug Bounty” –ohjelmia, digitaalisten palveluiden turvallisuuden jatkuvaksi parantamiseksi. ”

JYU:n vastaus: Tämä tulisi laajentaa koskemaan koko julkishallintoa (valtio, kunnat, kuntayhtymät, sairaanhoitopiirit, yliopistot ja korkeakoulut), koska ne ovat merkittäviä yhteiskunnallisia toimijoita ja keskeisiä kansalaisille tarkoitettujen palveluiden tuottajia. Yleisestikin strategiassa korostuu huoltovarmuuskriittinen toiminta, mikä on sinänsä ymmärrettävää ja ehdottoman tärkeää. Olisi kuitenkin hyödyllistä korostaa toimintojen turvaamista normaalioloissa ja varmistaa kyberturvallisuuden toteutuminen ennen kuin huoltovarmuuskriittinen toiminta on vaarantunut.

”4 Kiinteä yhteistyö” ”Ehdotetut kehittämistoimenpiteet” 4. kappale (Aktiivinen osallistuminen ja vaikuttaminen kansalliseen ja kansainväliseen kyberturvallisuuden yhteistyöhön)

”Kyberturvateollisuuden osallistumista edellä mainittujen kansainvälisten yhteistyöryhmien kannan muodostamiseen tuetaan perustamalla teema-aiheisia yhteistyöryhmiä.”

JYU:n vastaus: Tämä on erittäin tervetullut lähestymistapa. Työryhmien tulee olla vahvasti poikkihallinnollisia teollisuuden edustuksen lisäksi.

Havila Marjo
Jyväskylän yliopisto - Tietoturvapäällikkö Teijo Roine, digijohtaja Ari Hirvonen, professori Martti Lehto ja lehtori Panu Moilanen.