Turun yliopisto

Lausunto

02.02.2021 12/03/2021

Asia: VN/ 797/2021

Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Toimeenpanosuunnitelma tarvitsee lisää konkretiaa. Aikataulu on hyvin monessa esitetyssä toimenpiteessä avoin, ja rahoitus on suurimmassa osassa toimenpiteitä merkitty toteutuvaksi normaalein toimintamenoin. Monet näistä kohdista edellyttäisivät erillisen rahoituksen, jotta ne voisivat kehittämisohjelman mukaisesti realistisesti toteutua. Ilman lisärahoitusta panostus toimenpiteisiin jäänee liian vähäiseksi.

Tarvitaan kolmenlaista osaamista (koulutustarve):

1. kansalaistaito: mitä jokaisen pitää osata kyberturvallisuudesta elääkseen ja toimiakseen tietoyhteiskunnassa

2. alakohtainen perusosaaminen: mitä eri aloilla ja ammateissa pitää osata kyberturvallisuudesta

3. erityisasiantuntijat: yleiset ja alakohtaiset kyberammattilaiset

Em. kolme kohtaa pitää selvittää toimeenpanosuunnitelman kohdassa 2.1 ja kohdentaa tähän suunnattu rahoitus kaikille kolmelle osa-alueelle.

1: kaikki pitää kouluttaa tietylle perustasolle (Integraatio perusopetukseen, toimeenpanosuunnitelman kohta 2.3; integrointi lukio- ja ammatilliseen koulutukseen, kohdat 2.4-2.5). Vaatii erillisen rahoituspohjan, nyt kirjattu vain osaksi normaaleja toimintamenoja. Sama osaamisen kehittämismahdollisuus pitää tuoda kaikkien ulottuville, ei ainoastaan peruskoululaisiile ja toisen asteen opiskelijoille.

2: Työntekijöiden tulee tiedostaa, että digitalisaatio ja tekoäly muuttavat nopealla tahdilla työnkuvaa ja -kenttää. Tämä edellyttää työntekijöiltä hyvää ymmärystä kyberturvallisuudesta. Kyberturvallisuuden rakentaminen on jatkuva yhteisvastuullinen prosessi organisaatioissa. Se ei toteudu pelkästään yksittäisiä spesialisteja palkkaamalla. Tarvitaan eri aloille räätälöityä koulutusta, jota ei voida toteuttaa yleiskursseilla. Toteutukset tulisi suunnitella ko. alojen asiantuntijoiden ja kyberasiantuntijoiden yhteistyönä. Tämä tulee huomioida toimeenpanosuunnitelman kohdassa 2.6., ja tämän toteuttaminen suunnitellussa laajuudessa ei ole realistista koulutusorganisaatioiden normaalien toimintamenojen puitteissa. Tämäkin vaatii erillisen rahoituspohjan.

3: Korkeasti koulutettuja kyberturvallisuusasiantuntijoita ei ole riittävästi tarjolla vastaamaan suomalaisen yhteiskunnan ja yrityskentän tarpeisiin. Tässä avainasemassa on lahjakkaimpien huippuosaajien kouluttaminen sekä kotimaisista että kansainvälisistä opiskelijoista, ja heidän integrointinsa yhteiskunnan ja elinkeinoelämän palvelukseen. Erityisesti ulkomailta tulleiden asiantuntijoiksi valmistuneiden opiskelijoiden integroitumista Suomeen tulisi tukea voimakkaasti. Esimerkiksi Turun yliopisto on kouluttanut tietoturva-asiantuntijoita (diplomi-insinöörejä) kyberturvallisuuden maisteriohjelmassa ja tietoturvaerityisasiantuntijoita (tekniikan tohtoreita) vastaavassa tohtoriohjelmassa jo yli 10 vuoden ajan ollen alan vanhin yhtäjaksoisesti toiminut ylempien korkeakoulututkintojen koulutusyksikkö Suomessa. Turun yliopisto on myös ainoana suomalaisena yliopistona mukana yhteiseurooppalaisessa kyberturvallisuustutkinto-ohjelmassa, EIT Digital Master School in Cyber Security:ssä, jossa opintoihin kuuluu pakollisena myös laaja innovaatio- ja yrittäjyyskokonaisuus. Turun yliopiston tarjoama alan koulutus kiinnostaa hyvin paljon lahjakkaita ulkomaisia potentiaalisia opiskelijoita. Vaikka kyseessä on yliopiston diplomi-insinöörituotannoltaan suurin erikoistumislinja, valmistuneiden asiantuntijoiden määrä ei kata alan asiantuntijoiden kysyntää. Tilanne lienee sama muissa kyberturvallisuusopintoja tarjoavissa korkeakouluissa. Hakupaineen puolesta sisään otettavien opiskelijoiden määrää olisi mahdollista kasvattaa vastaamaan yhteiskunnallista tarvetta, mutta resursoinnin osalta ollaan jo nyt kantokyvyn rajoilla. Alan yliopistokoulutuksen lisäresursointi on välttämätöntä, mikäli kehittämisohjelman tavoitteet huippuluokan osaamisen lisäämisestä ja juurruttamisesta Suomeen halutaan täyttää. Todennäköisesti alalla tarvittaisiin 5- vuotiset lisärahoitetut kehitys- ja verkostointiohjelmat, jonka jälkeen ne siirtyisivät osaksi yliopistojen omaa rahoitusta ja vastuita. Ulkomaisten asiantuntijoiden juurruttamista Suomeen ja ulkomaisten huippututkijoiden rekrytointia korkeakouluihin tulisi tukea erityisin tavoin, esim. tarjoamalla ”starttipaketteja” tutkimusryhmän perustamiseen. Yleisesti ottaen suomalaisten yliopistojen

palkkakilpailukyky on heikko verrattuna toisaalta elinkeinoelämään ja toisaalta ulkomaisiin yliopistoihin sekä nykyisten huippuasiantuntijoiden pitämisessä että uusia rekrytoitaessa; kyberturvallisuuden alalla tilanne on erityisen haastava. (ISC)2 -konsortion vuoden 2020 tutkimusraportti ”Cybersecurity workforce study, 2020” toteaa, että maailmanlaajuisesti kyberturvallisuusasiantuntijana työskentelee 3,50 miljoonaa työntekijää, ja maailmanlaajuinen kyberturvallisuusasiantuntijavaje on tällä hetkellä 3,12 miljoonaa työntekijää. Asiantuntijoita tarvittaisiin siis lähes kaksinkertainen määrä nykyiseen verrattuna. Tutkimuksen mukaan vaje Euroopassa on tällä hetkellä n. 170 000 asiantuntijaa. Alakohtainen kohdennettu taloudellinen tuki kilpailukykyisiin palkkauksiin yliopistoissa mahdollistaisi nykyistä paremmin parhaiden osaajien kotimaisen ja kansainvälisen rekrytoinnin tutkimus- ja koulutustehtäviin.

Ei ole olemassa absoluuttista turvallisuutta, vaan toiminnassa minimoidaan kyberkriisin todennäköisyyttä ja mahdollisia seurauksia. Tässä lainsäändännöllä ja yhteiskunnan prosesseilla on vahva rooli. Esityksessä näkökulmana on nyt selkeästi yhteiskunta ja organisaatiot, siinä saisi olla vahvemmin mukana myös ihmisnäkökulma. Monessa tilanteessa kansalaisten kyberturvallisuus perustuu monelta osin ns. pakotettuun luottamukseen liittyen yhteiskunnan prosesseihin ja instituutiohin. Tästä johtuen näiden suunnitteluun pitää saada myös niiden käyttäjien näkökulma. Lainsäädäntötyön pitää olla proaktiivista suhteessa kyberturvallisuuteen ja yhteiskunnan digitalisaatioon. Nykyinen pitkälti reagoiva lähestymistapa ei toimi kunnolla mm. kyberuhkien ja niiden vaikutusten torjunnassa. Näitä varten pitäisi perustaa pitkälti yliopistojen tutkijoihin ja muihin asiantuntijoihin perustuva oikeusoppineiden, yhteiskunnallisten prosessien sekä kyberturvallisuus- ja digitalisaatioammattilaisten yhteinen ennakointityöryhmä, joka tuottaa aloitteita mm. lainsäädännön ja yhteiskunnan prosessien puolelle. Lisähaasteena on, että kyberrikokset eivät tunne/noudata valtioiden rajoja.

Kola Jukka
Turun yliopisto

Våg Hans
Turun yliopisto - Jouni Isoaho, Professori Seppo Virtanen, Apulaisprofessori