Teknologiateollisuus

Finnish Information Security Cluster
Kyberala

14.11.2023

Eduskunta
Sivistysvaliokunta
Viite: U 43/2023 vp

Lausunto: E-kirjeluonnos koskien komission tiedonantoa ”Kyberturvallisuuteen liittyvän osaamisvajeen pienentäminen EU:n kilpailukyvyn, kasvun ja häiriönsietokyvyn parantamiseksi (Kyberturvallisuusakatemia)” COM(2023) 207 final

Osaajapula on yksi suurimmista haasteista tietoturva-alalla Euroopassa, mutta myös globaalilla tasolla. Tämän haasteen ratkaisemiseksi Kyberala kannustaa EU-instituutioita löytämään tapoja tukea jäsenvaltioita uusien tietoturva-alan ammattilaisten kouluttamisessa suurempina määrinä. Aloitteet, jotka edistävät monipuolisista taustoista tulevien tietoturva-ammattilaisten dynaamista ja elinvoimaista eurooppalaista työmarkkinaa, ovat lämpimästi tervetulleita.

Kyberalan näkökulmasta tietoturva-asiantuntijoiden osaajapula liittyy kahteen perustavaan ongelmaan:

1. Rekrytointi ja henkilöstöpolitiikka: alan kaupalliset toimijat suosivat rekrytoinneissa kokeneita ammattilaisia, mikä heikentää alalle vasta tulleiden tai pyrkivien työllistymismahdollisuuksia. Tilanne vääristää palkkakilpailua, nostaa kustannustasoa ja kokonaisuudessaan alan työmarkkinoiden toimintaa. Asian ratkaisemisessa keskeistä on työnantajien liiketoiminnan ja rekrytointikäytäntöjen kehittäminen siten, että nuorempien ammattilaisten tuottaman lisäarvon oikeansuhtaisuus huomioidaan hinnoittelussa ja siten mahdollistetaan liiketoimintariskin kannalta uusien, aloittelevien osaajien palkkaaminen.

2. Osaajien saatavuus työmarkkinoilla on kokonaisuudessaan riittämätöntä: Tämä ongelma voidaan ratkaista lisäämällä merkittävästi koulutuksen tarjontaa ammattilaistasolla seuraavasti:

    - Uusien, tutkintoon johtavien korkeakoulujen aloituspaikkojen lisääminen tekniikan ja ICT:n aloilla kyberturvallisuutta painottaen nuorille, jotka suorittavat ensimmäisen tutkintonsa työmarkkinoille tullessaan,
    - Lisäkoulutusohjelmia niille, joilla on soveltuvia aiempia taitoja, sekä tutkinto kyberturvallisuuden lähialoilta (esim. yleiset tekniikka-, tietoliikenne-, ohjelmisto- tai sähkötekniikka-aidot)
    - Muuntokoulutusohjelmia niille, joilla on yleisesti soveltuvaa osaamista hallinnon ja elinkeinoelämän aloilta, mutta joilta puuttuu kyberturvallisuuden temaattista substanssiosaamista (esim. hallinto, myynti ja markkinointi, viestintä, projektinhallinta, palvelusuunnittelu ja muotoilu)

Kyberala suhtautuu komission tiedonantoon ja siinä esitettyihin toimiin kriittisesti. Emme näe, että esitetyn digitaalisen alustan hyödyt olisivat oikeassa suhteessa sen perustamisesta

Kyberala ry
Teknologiateollisuus ry

Eteläranta 10, PL 10, 00131 Helsinki
Puhelin 09 192 31
www.teknologiateollisuus.fi
Y-tunnus: 0215289-2

ja ylläpitämisestä aiheutuvaan hallinnolliseen työhön ja taloudellisten resurssien käyttöön. Nykyisten toimivaltuuksien puitteissa mahdollisuudet EU-tason toimille ovat koulutuspolitiikan rajapinnassa parhaimmillaankin hyvin rajalliset, ellei häviävät. Haluamme samassa yhteydessä huomauttaa komissiota myös harhaanjohtavien käsitteiden käytöstä: esityksen mukainen digitaalinen alusta ei ole akatemia tai muukaan oppilaitos, eikä sitä tulisi sellaiseksi kutsua. Epäselkeä ja harkitsematon käsitteistö on omiaan luomaan sekaannusta kyberturvallisuusalan kentällä ja pahimmillaan jopa herättää kysymyksiä unionin toimivaltuuksien ylittämisestä.

Komission tiedonannossa listaamat toimet eivät tosiasiassa edesauta osaajapulan ratkaisemista, sillä ne eivät itsessään synnytä alalle uutta ammattiosaamista luovaa koulutustarjontaa. Komission perustelu digitalisen alustan toimimisesta kybeturvallisuusalan houkuttelevuutta lisäävänä tekijänä on kyseenalainen, sillä näkemyksemme mukaan alan koulutustarjonnan vetovoima on jo nykyisellään hyvällä tasolla ja politiikkatoimien tulisi tämän vuoksi keskittyä siihen, että mahdollisimman moni alasta kiinnostunut myös pääsisi ammattilaistason osaamista tuottavan koulutuksen piiriin tarjontaa lisäämällä. Suuri osa tästä houkuttelevuudesta, toisin sanoen opintoalan vetovoimasta on riippuvaista teknologia- sekä luonnontiedealojen kiinnostavuudesta tulevaisuuden työllisyyden ja hyvän ansiotason turvaajana. Tiedonannon mukaan esitetyn digitaalisen alustan luominen auttaisi ymmärtämään kyberturvallisuuden osaajatarpeita eurooppalaisella tasolla. Todellisuudessa tarve tällaisen ymmärtämisen hankkimiselle ylimitoitettujen toimien kautta on vähintäänkin kyseenalainen.

Kyberala haluaa korostaa sekä komission tiedonantoon että E-kirjeluonnokseen liittyen, että laajojen kansanosien ”kybervalmiuksia” kehittävä työ, kuten yleisen kyberriskitietoisuuden lisääminen ja henkilökohtaisesta tietoturvasta huolehtimisen edellytysten parantaminen eroavat olennaisesti kyberturvallisuusalan ammattilaistason osaamiseen tähtäävästä koulutuksesta eikä niitä tule temaattisesti tai varsinkaan politiikkatoimien puitteissa sekoittaa toisiinsa. Samoin on tärkeä tunnistaa, että informaatiovaikuttamiseen, eli kansanomaisemmin propagandan tunnistamiseen tai sosiaalisen median syötteiden vaikutuksen alaiseksi joutumisella ei ole yhtenevyyttä tietoturvallisuuden ammattilaistason osaamiseen. Viittaukset tähän olisi perusteltua poistaa niin E-kirjeestä kuin edellyttää komissiota rajaamaan tiedonvälitykseen liittyvät toimet ja tavoitteet muihin säädösehdotuksiin.

E-kirjeluonnoksessa nostetaan asianmukaisesti esille, että tiedonannosta jää epäselväksi, mitä ehdotuksessa tarkoitetaan koulutuksen kehittämisellä EU-tasolla ja että jäsenvaltiot päättävät tutkintojen viitekehysten sisällöstä sekä osaamisen tunnustamisesta. Samalla painotetaan viisaasti jäsenmaiden koulutusjärjestelmien kehittämisen sekä jäsenmaiden strategisen yhteistyön merkitystä. Kuten E-kirjeluonnoksessa mainitaan, Euroopan kyberturvallisuusvirasto (ENISA) on jo tehnyt työtä kyberosaamisen ammattilaisten profiilien määrittelemiseksi eurooppalaisen kyberosaamisen viitekehyksen (ECSF) alla. Tätä viitekehystä tulee yleisesti ottaen kehittää ja hyödyntää soveltuvin osin. On kuitenkin havaittu, että ECSF-profiilit eivät vastaa kovinkaan täsmällisesti kyberturvallisuusalan toimenkuvia ja ovat muutoinkin suhteellisen laajan ”kompromissin” tuloksia. Näin ollen tuleekin jatkossa harkita, miten ja miltä osin siinä määritellyt osaamisprofiilit olisivat hyödyllistä liittää osaksi ESCO-ammattiluokitusjärjestelmää. Tätä työtä ei tule tehdä ehdotuksessa kuvatuissa EDIH-kokoonpanoissa, vaan jättää koulutuspolitiikan ammattilaisten organisoitavaksi.

Eurooppalaiselle kyberturvallisuusosaamisen osaamisen kehittymistä arvioivalle metodologialle ei ole tiedonannossa esitetyssä muodossa tarvetta, mutta DESI:n (Digitaalinen talous ja yhteiskunta indeksi) hyödyntäminen ja edelleen kehittäminen kyberturvallisuuden osalta on muuten kannatettavaa. Kannustamme myös harkitsemaan tarkemmin, voisiko eurooppalaisen taitojen ja työpaikkojen alustan luominen tosiasiassa edistää eurooppalaista työmarkkinaa tietoturva-ammattilaisille ottaen huomioon ENISA:n Eurooppalaisen tietoturvataitojen viitekehys (ECSF) -mallin hyödyt ja haitat.

Kyberturvallisuus on kaikkia huoltovarmuuden segmenttejä ja yhteiskunnan elintärkeiden toimintoja ylläpitävä jatkuva prosessi. Kyberala haluaa erikseen korostaa, riskienhallinnan ja varautumisen käsitteellistä eroa kaikkia kyberturvallisuuteen liittyviä politiikkatoimia suunniteltaessa. Varautuminen on todellisuudessa vain yksi osa riskienhallinnan keinovalikoimaa ja koskee yksinomaan sitä, miten toimitaan, kun yhteiskunnan perustoiminnot ovat vakavan häiriön tai lamauttamisen kohteena ja tapahtumat etenevät korkealla intensiteetillä vaikeasti ennustettavasti sekä nopeasti (poikkeusolot). Etukäteisvalmistelut ovat elimellinen osa edellä mainittua ja ne vaikuttavat ensisijaisesti haitallisten seurausten minimointiin ja tilanteesta palautumisen mahdollisuuksiin.

Kyberturvallisuusalan osaajapulan ratkaiseminen edellyttää, että olemassa olevia rakenteita alan koulutuksen järjestämiseksi uudistetaan, parannetaan ja laajennetaan. Samalla on tärkeää, ettei luoda uusia byrokraattisia rakenteita, kuten sertifiointeja, jotka asettavat pahimmassa tapauksessa alan koulutusta tarjoavia oppilaitoksia eriarvoiseen asemaan ja muutoinkin haittaisivat ketteriä toimia kansallisten koulutustoimien organisoinnissa. Yksipuolisten sertifiointien sijaan tarvitsemme monimuotoisen, erilaisista toimijoista koostuvan kyberturvallisuusalan koulutuksen ekosysteemin. Samalla on syytä huomioida, että alan työvoiman osaamisen kehittyminen tapahtuu pääosin yrityksissä. Kyberturvallisuusalan osaajapulan ratkaisemisessa saavutetaan parhaita tuloksia, kun toimet perustuvat nykyisiin rakenteisiin, resursseihin ja osaamiseen. Tärkein työ ammattimaisen tietoturvaosaamisen kehittämiseksi suoritetaan oppilaitoksissa ja yrityksissä, mukaan lukien elinikäisen oppimisen toimet.

E-kirjeluonnoksen mukaan Suomi pitää tärkeänä, että koulutuksen rinnalla on käytettävissä nopeita ja dynaamisia välineitä vastaamaan nopeasti työmarkkinoiden osaamistarvemuutoksiin. Kyberala pitää valittua linjaa erinomaisena ja kyberturvallisuusalan todellisuutta vastaavana.

Kyberala ehdottaa, että tarpeettomien EU-tason rakenteiden sijaan eurooppalaista rahoitusta ja resursseja ohjataan nykyistä ja suunniteltua enemmän Euroopan tietoturvakompetenssikeskukselle (ECCC), joka voi tukea jäsenvaltioiden pyrkimyksiä vahvistaa kyberturvallisuusalan koulutuksen ekosysteemejään kansallisten koordinaatiokeskustensa kautta.

Lisätietoa:
Toimitusjohtaja Peter Sund
peter.sund@teknlogiateollisuus.fi
Puh: +358 50 565 0621

Asiantuntija Risto Rajala
risto.rajala@teknologiateollisuus.fi
Puh: +358 40 515618