CSC-Tieteen tietotekniikan keskus Oy

Lausunto

03.02.2021

Asia: VN/ 797/2021

Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

CSC kiittää liikenne- ja viestintäministeriötä mahdollisuudesta antaa lausunto ehdotuksesta valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta. CSC – Tieteen tietotekniikan keskus Oy on Suomen valtion ja korkeakoulujen omistama erityistehtäväyhtiö. Palvelemme laajasti koko yhteiskuntaa tuottamalla teknologiapalveluja ja -ratkaisuja TKI-toiminnalle, koulutukselle, kulttuurille ja julkishallinnolle.

Kyberturvallisuus ymmärretään usein yhteiskunnan digitaalisten osien, erityisesti tietojärjestelmien varassa toimivan infrastruktuurin, turvallisuuteena ja toimintavarmuutena. Nykyisin kyberturvallisuus ymmärretään myös tietoturvallisuuden osana, joka koskee erilaisia verkkojen kautta tehtäviä hyökkäyksiä, tietomurtoja ja vastaavia. Tietoturva puolestaan sisältää käsitteenä myös tietojen ja palveluiden suojaamisen riskeiltä. Kyberturvallisuudesta puhutaan nykyisin myös muussa kuin valtiollisessa kontekstissa, esimerkiksi yritysten kyberturvasta. Raja kyberturvallisuuden ja tietoturvallisuuden välillä on usein häilyvä varsinkin arki- ja uutiskielessä, siksi termien käyttöä olisi hyvä täsmentää ehdotuksessa.

CSC katsoo, että lausunnon kohteena oleva kyberturvallisuuden kehittämisohjelma on nopeasta aikataulusta huolimatta kattavasti valmisteltu. Ohjelman toteutuminen, vastuutahot ja toteutumisen mittarit on määritelty jo tässä vaiheessa, mikä helpottaa ohjelman toimeenpanoa ja organisaatioiden ennakointia. On järkevää, että kehittämiselle on määritelty sekä lyhyen että pitkän aikavälin tavoitteita ja painopistealueita. Hankkeisiin esitetty erillinen rahoitus on kuitenkin hyvin vaatimaton. On tärkeää huomioida, että kyberturvallisuuden merkittävä kehittäminen edellyttää merkittävää rahoitusta,

CSC arvostaa, että kehittämisohjelman valmistelussa on kuultu laaja-alaisesti eri organisaatiota. CSC haluaa myös jatkuvasti omalta osaltaan tukea Suomen kyberturvallisuuden vahvistamista.

Ehdotuksessa on kuvattu, miten kyberturvallisuuden kehittämisohjelma suhtautuu, Haukka-toimeenpanosuunnitelman sekä Digitaalinen Turvallisuus 2030 -hankkeeseen. CSC pitää tärkeänä varmistaa aktiivisesti, että yllä mainittujen toimintojen välinen työnjako ja keskinäinen tiedonsiirto on saumatonta. Aiempien kokemusten perusteella on vaarana, että erilaiset kyber- ja tietoturvahankkeet ja ohjelmat siiloutuvat, jolloin niiden tuottamat ohjeet ovat huonosti yhteensopivia tai jopa ristiriitaisia.

CSC katsoo, että kehittämisohjelman teemat on erinomaisesti kiteytetty, mutta muistuttaa, että huippuluokan osaamisen saavuttaminen edellyttää myös merkittäviä panostuksia osaamisen kehittämiseen. Kansainvälisessä kilpailussa, jossa suurvallat panostavat miljardeja, EU on kokonaisuudessaankin pienempi toimija, yksittäisestä maasta puhumattakaan.

Ehdotus kannustaa työnantajia ja oppilaitoksia yhä tiiviimpään yhteistyöhön työharjoittelujaksojen lisäämisessä on erinomainen, mutta vaatii vielä konkreettisempia toimenpiteitä esimerkiksi erillisen käytännön hankkeen muodossa. Myös kansallisten kyber- ja tietoturvallisuuden osaamissertifiointien käyttöönottoa eri kohderyhmien osalta tulee harkita. Kyberturvallisuuden avaintehtävissä oleviltahenkilöiltä tulee edellyttää kansainvälisiä johtamiseen ja tekniseen tietoturvaan liittyviä osaamissertifiointeja (esim. CISSP, CISSP, GCED) sekä osaamisen jatkuvaa kehittämistä. Myös KATAKRI-kriteeristön vaati musten toteuttamiseen liittyvää varmistettua osaamista tulee laajentaa merkittävästi.

Kiinteän yhteistyön osalta ehdotuksessa esitetään kannatettavia toimenpiteitä. CSC:n mielestä olisi hyödyllistä myös lisätä konkreettista yhteistyötä elinkeinoelämän kanssa. Korkeakoulujen kanssa tehtävään yhteistyöhön tulee löytää tiiviimpiä järjestelyitä erilaisten yhteistyöryhmien lisäksi. Tiedon jakamista ja soveltamista käytäntöön on lisättävä niin organisaatioiden välillä kuin niiden sisällä.

CSC:n katsoo, että tavoitteet kotimaisen kyberteollisuuden vahvistamiseksi on hyvin kiteytetty, mutta jää epäselväksi, onko tavoitteita mahdollista toteuttaa normaalien toimintamenojen puitteissa. Kunnianhimoisten tavoitteiden saavuttaminen edellyttää asianmukaista resursointia.

Kansalliset kyberkyvykkyydet on tunnistettu osuvasti. Niiden vahvistamisen osalta ohjelma ei kuitenkaan vastaa kysymykseen, miten harmonisoidaan huoltovarmuuskriittisten sektoreiden ja -yritysten kyberturvavaatimuksia yhteisen turvallisuustason määrittelemiseksi ei-luokitellun tiedon osalta. CSC:n mielestä on syytä määritellä nykyisiä KATAKRI-kriteeristöä joustavammat kriteerit ”harkiten annettavalle”, sillä muutoin kyseisen tiedon suojausvaatimukset jäävät epäselviksi. Asiaa voisi täsmentää esimerkiksi liitteen kohdassa 10.

Ohjelman seurannan ja raportoinnin tulisi sisältää itse ohjelman seurannan lisäksi seurantaa myös toteutetuista turvallisuusarvioinneista ja -sertifioinneista.

Nimipalvelun turvallisuusominaisuuksien nykyistä laajempi ja kattavampi hyödyntäminen on erittäin kannatettava toimenpide. Ehdotuksessa voisi myös mainita muita konkreettisia toimenpiteitä, joilla olisi huomattava vaikutus, kuten turvallisuusselvitysten teettämiseen liittyvän ohjeistusten selkiyttäminen edelleen selvitystä tekevien organisaatioiden osalta, turvallisuussopimusten merkittävä uudistaminen ja virtaviivaistaminen, sekä haavoittuvuuskartoitusten säännöllinen ja kattava seuranta.

Kehittämisohjelmaehdotuksessa on hyvin kuvattu kyberturvallisuuden nykytila ja kehittämistarpeet toteuttamissuunnitelmineen. Teknologian kehityksen vuoksi kyberturvallisuuden haasteet muuttuvat koko ajan. Uusiin riskeihin tulee pyrkiä varautumaan proaktiivisesti ennakoiden. Riskien lisäksi tulevaisuus ja teknologinen kehitys tuo mukanaan myös paljon mahdollisuuksia.

Kehitysohjelman tavoitteellisuutta tuleekin mahdollisuuksien mukaan täydentää lisäämällä siihen osuus kyberturvallisuuden tulevaisuudennäkymistä. Uudet teknologiat ja toimintaympäristöt, kuten kriittisen tiedon siirtyminen kansainvälisiin pilvipalveluihin, tuovat mukanaan uusia uhkia, ja toisaalta mahdollistavat haavoittuvuuksien löytymisen odottamattomista paikoista.

Esimerkiksi kvanttiteknologia tulee muuttamaan vaatimuksia tietoturvalle. Kvanttiturvallisia salausmenetelmiä on jo kehitetty, toisaalta jotkin nykyiset salausmenetelmät ovat purettavissa kvanttitietokoneilla. Suomessa on hyvät mahdollisuudet panostaa kvanttiteknologiaan ja muodostaa alan osaamiskeskittymä yhdessä yritysten, tutkimuslaitosten ja korkeakoulujen kanssa. Kvanttiteknologian tuomat mahdollisuudet ja toisaalta myös uhat tulee tarkemmin huomioida myös käsillä olevassa kyberturvallisuuden kehittämisohjelmassa.

Uudet teknologiat tulevat myös muuttamaan tietoturvauhkia niin valtioiden, yritysten kuin kansalaisten näkökulmasta. Jo nyt esimerkiksi deepfake-tyyppiset videohuijaukset murentavat median luotettavuutta. Laskentatehojen ja tekoälyn kehittyessä niitä tullaan käyttämään entistä enemmän myös vilpillisiin tarkoituksiin. Tällaisten uhkien torjuminen vaatii tietoturvavalmiuksien tai kyberlukutaidon parantamista niin yksilön kuin organisaatioiden tasolla. On koko ajan yhä tärkeämpää, että tietoturvallisuustaitoja opetetaan, mutta on tärkeää myös tutkia, miten taitoja voidaan ja osataan soveltaa käytäntöön monien muidenkin vaatimusten ristipaineessa.

Esimerkkinä suomalaisesta osaamisesta ja mahdollisuuksista tekoälytutkimuksessa on Kajaaniin sijoitettava, maailman tehokkaimpiin kuuluva supertietokone LUMI, joka tulee olemaan yksi maailman edistyksellisimmistä alustoista tekoälylle. LUMI mahdollistaa tekoälyn menetelmien, erityisesti syväoppimisen, perinteisten laajan skaalan simulaatioiden sekä suurten datamassojen analytiikan yhdistymisen saman haasteen ratkaisemisessa.

Panostaminen kvanttiteknologian ja muiden uusien teknologioiden tutkimukseen, kehitykseen ja koulutukseen vahvistaisi Suomen asemaa maailmanluokan toimijana tietoturvan ja kyberturvallisuuden alalla. Tähän on erinomaiset edellytykset muun muassa LUMI-supertietokoneen sekä käynnissä olevien kvanttiteknogiahankkeiden avulla, joiden ympärille on mahdollista rakentaa erilaisia osaamiskeskittymiä ja ekosysteemejä.

CSC tukee ja kannattaa niin kansallista kuin kansainvälistä yhteistyötä kyberturvallisuuden alalla kaikkien luotettavien toimijoiden kanssa. Kyberturvallisuutta koskevaa tutkimusta kannattaa resursoida korkeakouluihin, tutkimuslaitoksiin ja yrityksiin. Erilaiset verkostot kannattaa myös pitää mukana keskusteluissa, hyvänä esimerkkinä Suomen aloitteesta perustettu ja Suomessa toimiva Hybridiuhkien osaamiskeskus. Myös kyberturvallisuuteen liittyvää tutkimustietoa tulee seurata ja hyödyntää kattavammin.

Kaila Urpo
CSC-Tieteen tietotekniikan keskus Oy