Insta DefSec Oy

Lausunto

02.02.2021

Asia: VN/ 797/2021

Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Insta DefSecin lausunto kyberturvallisuuden kehittämisohjelmasta

1. Yleistä

Insta kiittää mahdollisuudesta lausua kyberturvallisuuden kehittämisohjelmasta.

Pidämme tärkeänä, että kehittämisohjelman aikajänne mahdollistaa pitkäjänteisen kehitystyön, jota useat toimeenpanosuunnitelman toimenpiteet edellyttävät. Pitkästä aikajänteestä johtuen on myös tärkeää, että etenkin ohjelman toimeenpanosuunnitelmaa arvioidaan vuosittain ohjelmassa kuvatulla tavalla ja suunnitelma rakennetaan joustavaksi ja rahoitus on riittävällä tasolla.

2. Osaaminen

Erityisen tärkeänä näemme sen, että kyberturvallisuuden opetuksen pitäisi olla sisällytettynä yleisesti teknologia-alojen koulutuksessa mm. sivuainevaihtoehtoina ja sen, että koulutuksen suunnittelussa otetaan huomioon myös elinkeinoelämän tarpeet ohjelmassa kuvatulla tavalla. Erillisten koulutusohjelmien, sivuainekokonaisuuksien ja muiden laajempien opintojen lisäksi kyberturvallisuuden perusasiat tulee sisällyttää kaikkeen teknologia-alan koulutukseen. On tärkeää, että kyberturvallisuusosaaminen ei siiloudu liiaksi yksinomaan erillisiin kyberturvallisuuden koulutusohjelmiin. Vastaavasti on tärkeää, että myös esimerkiksi liiketoimintajohdolla on riittävästi

kyberturvallisuusosaamista, ja koulutusta tulisi olla tarjolla sekä täydennyskoulutuksena että muiden alojen koulutuksen yhteydessä.

Kansalaisten kyberturvataitojen kehittämisen kannalta pidämme tärkeänä, että ohjelman mukaan kyberturvallisuus sisällytetään jo varhaiskasvatuksen ja peruskoulun opetussuunnitelmaan ja että kyberturvallisuustaidot on tässä yhdistetty muihin digitaaliseen toimintaympäristöön liittyviin taitoihin.

3. Yhteistyö ja harjoitustoiminta

Osallistuminen ja vaikuttaminen kansalliseen ja kansainväliseen kyberturvallisuuden yhteistyöhön on hyvä määritellä: mikä organisaatio osallistuu esim. EU-tason yhteistyöhön ja miten tietoa jaetaan Suomessa muille toimijoille.

Jatkossa tarvitaan esitettyäkin vahvempi panostus harjoitustoimintaan sekä panostuksen jakaminen nyt esitettyä useamman eri voimavaran kehittämiseen ja ylläpitämiseen. Panostusta tulisi suunnata toimintamallien kehittämiseen sekä harjoitustoiminnan laajemman työkalukokonaisuuden (erilaiset ratkaisut, alustat ja sovellukset) mahdollistamiseen.

Harjoitustoiminnan kehittämispanosten vaikuttavuuden arvioimiseksi tulisi määritellä kansallisella tasolla suositus harjoitustoiminnan vähimmäisvaatimuksiksi ja tavoitetilat eri kohderyhmille.

Harjoitustoiminnan kohteena tulisi huomioida myös koko julkishallinto. Toimialaharjoitusten lisäksi tulisi tukea valituissa kohderyhmissä myös organisaatiokohtaista harjoitustoimintaa.

Harjoitustoimintapalveluita ja ratkaisuja tuottavat yritykset ja yhdistykset tulee osallistaa mukaan kansallisen harjoitustoiminnan kehittämiseen kautta linjan.

Harjoitustoiminnan kehittäminen tulee huomioida osana uuden osaamiskeskuksen toimintaa ja oppilaitosyhteistyötä.

Harjoitustoimintapalveluidenkin osa-alueella tulee edistää uusia skaalautuvia ja kaupallista potentiaalia omaavia innovaatioita kansallisiin ja kansainvälisiin tarpeisiin.

Harjoitus- ja koulutustoiminnan yhteyksiä kannattaisi vahvistaa - esim. luomalla harjoituskalenteriin sidottu kyberturvallisuuden häiriötilanteiden hallinnan johtamisen kurssikokonaisuus organisaatioiden johdolle ja avainasiantuntijoille. Vrt. AVI:en ja Pelastusopiston alueellinen valmiusharjoitustoiminta, jossa harjoituksiin liittyy alueen kunnille suunnattuja varautumisen ja valmiuden peruskursseja.

4. Kotimainen kyberteollisuus

Teollisuuden rooli on olennainen, koska se tarjoaa työpaikkoja ja sitoo osaamista Suomeen.

Ehdotuksessa on muotoiltu, että pyritään rahoittamaan erityisesti pk-yritysten kyberturvallisuuden tutkimushankkeita ja kyberturvallisuuden kompetenssien kehittämistä. On huomattava, että suomalainen suuryritysten määritelmä on kansainvälisesti varsin pieni. Lisäksi useissa ei-pk –yrityksissä kyberturva saattaa olla oma toimialueensa. Tämä tarkoittaa, että yritysten tukemisen ohjaaminen vain/ensisijaisesti pk-yrityksille saattaa aiheuttaa, että haluttuja merkittäviä kehitysaskelia ei voida ottaa suuremmissa yrityksissä.

Hyvänä näemme halun tukea kotimaisen kyberturvateollisuuden innovaatioita, tuotteita ja ratkaisuita, siten että niitä hyödynnetään entistä laajemmin ja rohkeammin. Tämä on esimerkiksi vientimahdollisuuksien kannalta tärkeää, koska kotimaisten referenssien arvo on suuri.

Kotimaisen kyberteollisuuden kehittämisessä myös julkiset hankinnat ovat merkittävässä roolissa. Hankintaosaamisen kehittämisen rinnalla tulisikin varmistaa, että julkisissa hankinnoissa hankintakriteerit ovat selkeät ja niissä keskitytään hankinnan kohteen kannalta olennaisiin seikkoihin.

5. Kansalliset kyberkyvykkyydet sekä kotimaisen salausteknologian luonti

Kansallinen salaustuoteperhe on uusi käsite, tarkoitetaanko tällä hyväksyttyjä teknologiavalintoja? On huomattava, että eri käyttökohteissa on ratkaisuille erilaiset tarpeet ja kun huomioidaan teknologian nopea kehittyminen, niin liian pitkälle menevä määrittely ei ole tarkoituksenmukaista.

Salausteknologian kehittämisessä Puolustusvoimat on ollut edelläkävijä ja siellä jo käynnissä olevaa strategiatyötä, kryptolaboratoriota sekä laajaa yritysten, tutkimuslaitosten ja viranomaisten muodostamaa verkostoa kannattaa hyödyntää sen sijaan että rakennettaisiin uutta.

Lause ”Tunnistetaan kansallisesti kriittiset kyberturvayhtiöt ja turvataan niiden kansalliset omistusosuudet.” on ongelmallinen mm. seuraavista syistä

- Valtion omistus tietoturvatuotteita tekevissä yrityksissä aiheuttaa haasteita vientimahdollisuuksien osalta.

- Valtion omistus yrityksissä vääristää markkinatilannetta, kun joku toimija on erikoisasemassa. Se myös vähentää muiden yritysten kiinnostusta investoida tuotekehitykseen ja tämä johtaa väistämättä osaamisen kuihtumiseen.

- Hajautunut omistus tekee vastuista epäselviä.

- Yhteenvetona näemme, että salausteknologian osalta ehdotukset ovat ristiriitaisia muihin esitettyihin tavoitteisiin.

Yritysten ja valtionkin kannalta kansallisen turvallisuuden varmistaminen on tarkoituksenmukaisempaa toteuttaa ilman pakotetta omistuksesta. Omistusosuuden ei ole tarpeen olla proaktiivisesti varmistettu vaan se voidaan hoitaa muillakin tavoilla. Suomessa toimii esimerkiksi puolustusteknologian alueella useita yrityksiä, jossa samat tunnistetut haasteet on pystytty hallitsemaan vuosikymmeniä. Jo nykyinen lainsäädäntö sallii puuttua esimerkiksi yrityskauppatilanteisiin, joissa yrityskaupan kohteena on puolustusteollisuusyritys tai yritys, joka tuottaa tai toimittaa yhteiskunnan turvallisuuden kannalta kriittisiä tuotteita tai palveluita viranomaisille.

Asia voidaan muotoilla esimerkiksi näin: ”Kriittisten kyberturvayhtiöiden osalta tulee varmistaa, että mahdollisissa kansallisen intressin kannalta haitallisissa määräysvallan siirtymistilanteissa sopimuksin on mahdollistettu järjestelyt, joilla valtion etu voidaan turvata.”

6. Seuranta ja raportointi

Kyberturvallisuuden kehittämissuunnitelman haasteena on toisaalta nopeasti muuttuvat teknologiat ja uhkatilannekuva ja toisaalta tarve pitkäjänteiselle sekä määrätietoiselle kehittämiselle. Molempien näkökulmien huomioonottaminen vaatii strategioiden ja toimintasuunnitelmien joustavuutta sekä ajantasaisuutta eli riittävän taajaan tehtyjä tarkasteluja ja päivityksiä.

Hautakangas Marko
Insta DefSec Oy