Kimmo Halunen

Lausunto

03.02.2021

Asia: VN/ 797/2021

Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Lausunto kyberturvallisuusstrategian toimeenpano-ohjelmaan "Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta".

Uusi strategia on erinomaisen hyvä ja lähtökohtaisesti hyvä entistä laajemmalla pohjalla valmisteltuna. Strategian lisäksi tämä kehittämisohjelma on tarpeellinen ja siinä kuvataan paljon tärkeitä toimenpiteitä tavoitteiden saavuttamiseksi. Haluamme kuitenkin nostaa esiin muutamia näkökulmia koulutuksesta ja kriittisestä infrastruktuurista.

Kyberturvallisuuden koulutus

Panostukset koulutukseen ovat hyvä lähtökohta. On erinomaista, että koulutusta katsotaan kaikilla tasoilla peruskoulusta ja esikoulusta lähtien. Laaja-alainen koulutus tukee kansalaisten perustaitoja, parantaa kansallista toimintakykyä, ja antaa hyvän lähtötason luoda kansainvälistä osaamista.

Mielestämme huomiota pitäisi keskittää merkittävästi kouluttajien koulutukseen, sillä tämä voi muodostua pullonkaulaksi koulutuksen, erityisesti täydennyskoulutuksen, suhteen. Huoltovarmuudelle kriittisten yrityksen määräksi on arvioitu yli 1500 (https://www.defmin.fi/files/3130/1_Raija_Viljanen_MATINE_seminaari_17_3_2015.pdf), joten jotta jokaisessa yrityksessä olisi edes muutama hiljattain koulutettu asiantuntija, niin vuosittaisen koulutettavien määrä pitäisi olla tuhansia. Näin ollen myös asiantuntevia kouluttajia tulee olla kymmenittäin pelkästään tällä sektorilla.

Kriittinen infrastruktuuri

Jo mainittu panostus laaja-alaiseen koulutukseen tukee Suomen kriittisen infrastruktuurin kykyä selvitä kriisitilanteista. Ehdotuksessa ei kuitenkaan juurikaan viitata kolikon toiseen puoleen, joka on tietoturvan sisäänrakentaminen kansalliseen infrastruktuuriin. Yksityisten, yritysten ja julkisen tahon käyttämien laitteiden, verkkojen ja järjestelmien laatuun ja tietoturvaan pitää kiinnittää enemmän huomiota.

Ehdotus viittaa .fi-domainin sisäänrakennettujen turvallisuusominaisuuksien kehittämiseen. Tämä on toki kannatettava kehityskohde, mutta vain yksi yksityiskohta laajassa teknisessä toimintaympäristössä.

Järjestelmien kyberturvallisuuden parantamisen tulee sisältää teknistä ohjeistusta, joista esimerkkinä voidaan mainita Kyberturvallisuuskeskuksen Tonttu-ohjelma (https://www.kyberturvallisuuskeskus.fi/fi/tonttu). Tällaisen ohjeistuksen ja avun tarpeen osoittavat viimeaikaiset Vastaamon ja Eduskunnan tietomurrot. Toisaalta järjestelmien sertifiointia ja niiden riippumatonta tietoturvan arviointia tulisi tukea. Esimerkkeinä ovat Kyberturvallisuuskeskuksen Tietoturvamerkki (https://tietoturvamerkki.fi/) ja tutkimus, jota tehdään eri yliopistoissa ja muissa tutkimuslaitoksissa. Myös monet suomalaiset ja kansainväliset yritykset suorittavat arviointeja, mutta näiden arviointien hinta on korkea ja saatavuus rajoitettua.

Julkisia hankintaprosesseja pitäisi kehittää ja julkisen puolen pitäisi lisätä tietoturvavaatimuksia tietojärjestelmien hankintakriteeristöön. Toimittajan tulisi sitoutua järjestelmän tietoturvan jatkuvaan päivitykseen, kun uhista saadaan uutta tietoa vaikkapa ulkopuolisten arviointien seurauksena tai ehdotuksessakin mainittujen "bug bounty"-ohjelmien tuloksena.

Ehdotuksessa korostettu yksityisten ja julkisten organisaatioiden yhteistyö ja tietojenvaihto on erittäin kannatettavaa. Tätä voisi vielä täydentää elinkeinoelämän, korkeakoulujen ja valtionhallinnon välisillä henkilöstön vaihto-ohjelmilla. Tämä edesauttaa asiantuntijuuden siirtymistä eri organisaatioiden välillä.

Kehitysohjelmassa esitetyt rahalliset panostukset ovat esitettyihin haasteisiin nähden melko vaatimattomia ja painottuvat erityisesti AQUA-statukseen liittyviin toimiin. Myös muut aiheet tarvitsevat riittävät resurssit ja voi olla, että normaalien toimintamenojen puitteissa ei kaikkia tavoitteita ole mahdollista saavuttaa.

Kimmo Halunen
Oulun yliopisto / Oulu University Secure Programming Group (OUSPG)