

Asia: VN/ 797/2021

Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämishojelmasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Cyberwatch Finland kiittää mahdollisuudesta lausua mielipiteensä kyberturvallisuuden kehittämishojelmasta.

Kansallisen koko yhteiskunnan läpileikkaava kyberturvallisuuden kehittämishojelma on välttämätön strategian toimeenpanemiseksi ja kansallisen kyberkyvykkyyden kehittämiseksi. Se luo suuntaviivat Suomen kyvyille vastata tulevaisuuden haasteisiin, sekä muovaa suomalaista identiteettiä ja kyberturvakulttuuria. Kehittämishojelma pohjautuu yhteistyöhön, mahdollisuuksiin ja osaamisen kehittämiseen. Lähestymistapa on hyvä ja se tukee kansallisen kilpailukyvyyn kehittymistä myös kansainvälisesti niin lyhyellä kuin pitkällä tähtäimellä. Kansallisen kyberturvallisuuden kehittämishojelma toteuttaa Suomen kyberturvallisuusstrategia 2019:n mukaista suunnitelmaa. Kehittämishojelman valmisteluun ja työpajoihin on osallistunut yli 80 eri organisaatiota muun muassa elinkeinoelämä, kyberturvateollisuus, valtionhallinto, yliopistoja, sekä eri järjestöjä. Tämä antaa hyvät lähtökohdat kehityshojelman jalkauttamiseen ja sitouttamiseen tiivistäen julkisen hallinnon ja elinkeinoelämän kyberturvallisuuden yhteistyötä. Kansallinen kyberkyvykkyys muodostuu osaamisesta, digitaalisista toimintatavoista ja kyberturvateknologiasta, sekä niiden kokonaisvaltaisesta johtamisesta ja kehittämisestä.

Huippuluokan osaaminen avainasia

Kansalaisten kybertaitojen parantaminen koulutuksen kautta on tärkeä tavoite, joka vahvistaa Suomea korkean koulutuksen ja osaamisen maana ja luo pohjan tulevaisuuden yhteiskunnalle. Elinkeinoelämää ja yhteiskuntaa tukevan tutkintopohjaisen koulutustarjonnan lisäksi tulisi panostaa

joustavaan täydennyskoulutukseen ja elinikäistä oppimista tukevaan kurssi- ja koulutustarjontaan. Suomen huippuluokan kyberosaamista on kehitettävä kolmella tasolla:

- digi- ja kyberinnovaatioiden tutkimukseen on panostettava jatkuvasti pärjätäksemme kansainvälisessä kilpailussa ja turvataksemme kansainvälisen huippuosaamisen Suomessa
- akuuteissa tilanteissa on varmistettava yritysten ja julkisen sektorin päättäjien ymmärrys, jotta kyetään luomaan riittävä kansallinen kyberturvallisuuden osaaminen ja johtamiskapasiteetti
- pitkällä tähtäimellä on luotava kansallinen kyberoppimispolku alkaen alakoulusta ja päättyen korkeakoulutasoon

Kyberturvallisuus ja digitaidot on saatava osaksi opetussuunnitelmia kaikilla koulutasoilla. Kyberkoulutuksen kansallinen intressi on, että koulujärjestelmän, tutkimustyön ja liike-elämän yhteistyön rajapinnat tuottavat kansainvälisiä vientituotteita myös koulutusviennin osa-alueella. On rakennettava liityntäpinta koulutusjärjestelmän, organisaatioiden ja yritysten välille, sekä tiekartta koulutusviennin integrointiin ja jalkauttamiseen.

Kiinteä yhteistyö ja vahva kotimainen kyberturvateollisuus

Kehittämishjelmassa tulisi ottaa mukaan myös kansallista turvallisuutta ja kyberpuolustusta kehittävät toimenpiteet. Suomen tulisi hyödyntää tehokkaammin yleisen asevelvollisuuden ja puolustusvoimien roolia kansallisen turvallisuuden, osaamisen ja elinkeinoelämän kyberturvallisuuspalveluiden, -innovaatioiden, -yritysten ja ekosysteemin kehittämisessä. Kaikkien viranomaisten ja elinkeinoelämän yhteistyömuotoja on edelleen tiivistettävä. Erityisesti puolustusvoimien kriisiajan kapasiteettia on kyettävä hyödyntämään arkielämän kyberhäiriötilanteissa. Se on kustannustehokkain tapa kehittää kansallista kyberpuolustuskykyä. Puolustusvoimien lakisääteisten tehtävien mukaan sillä tulee olla kyky kybervirka-avun antamiseen. Maanpuolustuskoulutuksen kyberpuolustuskapasiteettia tulisi hyödyntää tehokkaammin ja se tulisi ottaa osaksi koulutuksen kokonaistarjoamaa. Myös kybervapaehtoisorganisaatioiden ja -aktivistien hyödyntäminen tulisi ottaa osaksi kokonaisykyvyyden rakentamista.

Kansallisesti olisi päätettävä, mikä taho tarjoaa kyberharjoitusympäristön, jossa kaikki toimijat voisivat toimia yhteistyössä kehittämässä kyberpuolustusvalmiutta.

Usein parhaat kyberturvainnovaatiot syntyvät startup- ja pk-yrityksissä, sekä tutkimusmaailmassa. Niiden tukemiseksi ja yhdistämiseksi tulisi miettiä parempi kansallinen koordinointi ja resurssointi. Kansallisessa kehittämissuunnitelmassa tulisi olla selkeät tavoitteet ja toimenpiteet niihin pääsemiseksi, sekä onnistumisen mittarit.

Perustettava osaamiskeskus voi tarjota hyvät edellytykset yhteistyön tiivistämiseksi eri toimijoiden kesken.

Tehokkaat kansalliset kyberturvakyvykkyudet ja lainsäädäntö

Kybertilannekuva tulisi olla ”kansallisomaisuutta”, jonka jakavat kaikki tuottamalla itsekin siihen lisäarvoa.

Kehittämissuunnitelmassa tulisi olla toimenpiteet myös kansallisen kyberjohtamisen, strategisen tilannekuvan ja nopean reagointikyvyn kehittämiseen. Kriisitilanteessa nopean toiminnan mahdollistava lainsäädäntö, toimintavaltuudet ja rakenteet tulee olla jo valmiina.

Suomeen tulisi luoda kokonaisvaltainen kyberturvallisuuslainsäädäntö. Tällä hetkellä kyberturva-alaa säätelee monen ministeriön hallinnaloilla olevat sirpaleiset säädökset. Lisäksi lainsäädäntö tulisi harmonisoida suhteessa EU-lainsäädäntöön. Lainsäädännön kehitystarpeet tulisi myös olla osana kehittämissuunnitelmaa, mikä kattaisi myös kriittisten kyberturvallisuusyritysten tunnistamisen ja turvaamisen kansallisessa omistuksessa.

Seuraaminen ja raportointi

On hyvä, että kehittämissuunnitelman toimeenpanosuunnitelmassa on määritelty vastuutahot ja mittarit. Osa määritellyistä tavoitteista ja mittareista jää melko yleiselle tasolle. Kehittämissuunnitelman tulisi olla jatkuva prosessi, jolla mitataan ja seurataan myös toimenpiteiden vaikuttavuutta. Mittaristoon tulisi ottaa mukaan toimenpiteiden säännöllinen vaikuttavuuden arviointi. Tämä toimisi johtamisen työkaluna toimenpiteiden, kehityskohteiden, sekä investointien kohdentamisessa.

Toimenpidesuunnitelma vaatii selvästi suurempaa rahoitusta. Kehitystoimenpiteiden toteuttaminen osana ”normaaleja toimintamenoja” ohjaa toki kybertietoista kehittämistä ja tekemisen kulttuuria laajemmin yhteiskunnan tasolla, mutta merkittäviä muutoksia ei saa ilman merkittävää rahoituksen lisäämistä.

Kyberturvallisuus liittyy kaikkeen digitalisoituvan yhteiskunnan tekemiseen ja toimintaan. Kansallisen turvallisuuden, kyberturvallisen yhteiskunnan ekosysteemin ja innovaatioiden vientipolun voisi

nostaa valtion kärkihankkeeksi, mikä lisäisi yhdessä kehittämisen painoarvoa ja rakentaisi Suomeen todellisen kyberturvallisuuskulttuurin.

Waltzer Kim
Cyberwatch Finland