Wärtsilä

Lausunto

02.02.2021 VN/ 797/2021

Asia: VN/ 797/2021

Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Lausunnon antaja: Wärtsilä Oyj Abp, Yhteiskuntasuhteet ja Lakiasiat; Kyberturvallisuus

Kehittämisohjelman tavoitteena on synnyttää suomalainen kyberturvallisuuden ekosysteemi ja parantaa koko yhteiskunnan tieto- ja kyberturvallisuutta. Wärtsilä haluaa kuitenkin painottaa, että kehittämisohjelman kannattaa kansallisen ekosysteemin lisäksi ottaa huomioon myös kansainväliset aloitteet ja vaatimukset, koska kybermaailmaa ei voida rajoittaa perinteisten kansallisten rajojen mukaan. Kybermaailma on globaali.

Yksi suurimmista tekijöistä nykyiseen digitalisaation mukanaan tuomankorkean kyberriskin olemassaoloon on sekä 1.) yhteisen globaalin/kansainvälisen että 2.) kansallisen teknologia- ja kyberhallinnon sääntelyn, vaatimusten ja ohjeiden puute tai niiden riittämättömyys.

Tällä hetkellä digitaalisen kehityksen mukanaan tuomassa vauhdissa monet yritykset ja organisaatiot ovat menneet markkinoiden mukaan yhteisten kyberturvallisuusvaatimusten ja toimintamallien puuttuessa. Tuotteita ja palveluita suunnitellessa ei välttämättä oteta kyberturvallisuutta huomioon tarpeellisella tavalla, vaan markkinoilla saatetaan edetä liiketoimintavaatimusten (ns. ”first to market” periaate) ja lyhyen aikavälin tavoitteiden saavuttamiseksi. Tämä nopea digitaalisten tuotteiden ja palveluiden kehitys- ja toimintamalli jättää yrityksiltä kyberturvallisuuden ja testaamisen vapaaehtoiseksi toiminnaksi, joka helposti jätetään pois kustannussyistä tai on vain jälkikäteen tehty riittämätön toimenpide.

Näiden kyberturvallisuuteen liittyvien yhteisten toimintamallien ja yhteisen hallintomallin puutteen poistamiseksi Kyberturvallisuuden kehittämisohjelma voisi suunnata yhteisiä resursseja

kokonaisvaltaisten kansainvälisten ja kansallisten toimintamallien ja vaatimusten kehittämiseen; sekä ketterien hallintomallien parantamiseen dynaamisten, toisiinsa liittyvien kyberturvallisuusongelmien ja -kysymysten ratkaisemiseksi. Wärtsilällä kansainvälisenä meri- ja energia-alojen johtavana toimijana, ja näiden alojen kyberturvallisuusasiantuntijana, olisi paljon annettavaa edellä mainittujen toimintamallien kehittämisessä.

On tärkeää että näiden toimintamallien luomiseen osallistuvat sekä julkinen että yksityinen sektori. Molempien sektoreiden osallistuminen mahdollistaa sekä markkinoiden ja teollisuusalojen vaatimusten huomioon ottamisen että koko yhteiskunnan kyberturvallisuuden parantamisen. (alhaalta ylös = markkinat ja teollisuus, ylhäältä alas = julkinen sektori ja yhteiskunta).

Toisena konkreettisena ehdotuksena suomalaisen kyberturvallisuuden ekosysteemin luomiseksi Wärtsilä kannattaa kansallista Centers of Excellence (CoE) -mallia ja metodeja.

Lausuntopyynnön väliotsikoiden mukaisesti CoE-mallia voidaan soveltaa julkisen ja yksityisen sektorin yhteistyöllä ainakin seuraavissa teemoissa:

Teema 2: Kyberturvallisuuden koulutusjärjestelmän kehittäminen

- Kyber-koulutus ja tutkimus (julkinen ja yksityinen)
- Akateeminen ja ammatillinen kyber-koulutus, urapolku työelämään / alalle

Teema 3: Kyberturvallisuuden harjoitustoiminnan yhteistyön vahvistaminen

- Kyberuhkien simulointi, harjoittelu ja kriisijohtaminen (eri teollisuusalat)

Teema 4: Kansallisen kyberturvallisuuden tutkimus- ja kehitysyhteistyön edistäminen

- Resurssointi, tukeminen, käyttö

Teema 5: Aktiivinen osallistuminen ja vaikuttaminen kansalliseen ja kansainväliseen kyberturvallisuuden yhteistyöhön

- Viranomaiset ja julkishallinto, yhteistyö ja tiedonjako (Tietosuojavaltuutetut, EK, Kyberturvallisuuskeskus / HaVaRo, SuPo, Puolustusvoimat, KRP/Poliisi, muut)

Teema 6: Kotimaisten kyberturvatuotteiden ja -palveluiden kasvun ja kansainvälistymisen tukeminen

Teema 8: Jatkokehitetään poikkihallinnollisesti viranomaisten varautumista laajoihin kyberhäiriötilanteisiin

- Tilannekuva: Uhkatiedon ja kybertiedustelun suorittaminen, analysointi ja jakaminen
- Kyber-näkyvyyden / monitoroinnin parantaminen OT ja IT ympäristöissä
- Incident response OT ja IT ympäristöissä

Teema 10: Harmonisoidaan turvallisuusvaatimuksia ja parannetaan havainnointikykyä

- Testaus & riskiassesmointi (tuotteet ja palvelut): kyberturvallisuus vaatimusten testaaminen ja todentaminen
- Tuotteiden kyberuhka ja kybertapahtumien estäminen / korjaamien (PSIRT = Product Security Incident Response)

Wärtsilä on erittäin sitoutunut parantamaan kansallista ja kansainvälistä kyberuhkiin liittyvää yhteistyötä sekä olemaan kokonaisvaltaisesti mukana turvallisemman digitaalisen tulevaisuuden rakentamisessa.

Eronen Teemu
Wärtsilä - Wärtsilä Oyj Abp, Yhteiskuntasuhteet ja Lakiasiat, Kyberturvallisuus