VNS 3/2024 vp Lausunto

Puolustusvaliokunta

2024-10-09

WITH secure | Consulting

Lausunnon antaja

Päivämäärä	Tekijä	Muutos	Versio
2024-10-09	Antti Laatikainen, Johtava tietoturvakonsultti	Lopullinen versio	1.0

Dokumentin jakelu

Päivämäärä	Vastaanottaja	Organisaatio
2024-10-09	Puolustusvaliokunta	Eduskunta

Toimeksianto

Asia: VNS 3/2024 vp, Puolustusvaliokunnan lausuntopyyntö ulko- ja turvallisuuspoliittiseen selontekoon.

WithSecure perustaa seuraavan lausuntonsa omaan kokemukseensa, teollisuudenalan parhaisiin käytänteisiin, sekä puolustusvaliokunnan esitykseen VNS 3/2024 vp joka toimitettiin WithSecurelle pohjamateriaaliksi.

Lähtökohta lausunnolle

Maailman ja Suomen turvallisuustilanne on viime vuosien aikana muuttunut merkittävästi. Kyberturvallisuus on noussut keskeiseksi elementiksi nykyaikaisen yhteiskuntarauhan ja kansallisen turvallisuuden kannalta. Kyberturvallisuuden kansainvälinen luonne tekee siitä erityisen haastavan verrattuna perinteiseen maanpuolustukseen tai kriittisen infrastruktuurin suojaukseen, koska kybertoiminta ja digitaalinen maailma ei tunne valtiorajoja.

Ulko- ja turvallisuuspoliittinen selonteko kuvaa kattavasti ja monipuolisesti muuttunutta maailmankuvaa, sekä uusien teknologioiden huomioimista. WithSecuren näkemyksen mukaan kyberulottuvuus ja kybervaikuttamisen näkökulma ovat kuitenkin jääneet vähäiselle huomiolle, vaikka ne ovat osoittautuneet erittäin aktiivisiksi ja turvallisuuteen vaikuttaviksi elementeiksi nykyään ja lähitulevaisuudessa.

Kyberulottuvuutta tulisi korostaa tietyissä selonteon osissa, sillä Suomella on vahva kyberturvallisuuteen keskittynyt teollisuus.

LAUSUNTO

WithSecure suosittelee seuraavien kommenttien, muutosten tai lisäysten huomioimista selontekoon:

1 Uuden ajan ulko- ja turvallisuuspolitiikka

Kyberturvallisuus ja sen muodostama kokonaisulottuvuus ovat tässä luvussa vain löyhästi sidottu laajempiin asiakokonaisuuksiin. Huolimatta siitä että kyberulottuvuuden vahvistamisen ensiaskeleet on jo otettu, WithSecure pitää tärkeänä että tässä yhteydessä painotetaan Suomen asemaa kyberturvallisuuden suojauksessa ja tuessa.

On tärkeää korostaa, että Suomi on sitoutunut kehittämään kyberturvallisuuttaan ja tukemaan kansainvälisiä ponnisteluja tällä alalla.

WithSecuren näkemyksen mukaan kyberturvallisuuden merkitys kansallisen puolustuskyvyn ja yhteiskunnan toimivuuden varmistamisen kannalta olisi syytä tuoda esiin jo tässä avauskappaleessa. Kyberturvallisuus ei ole vain tekninen kysymys, vaan se on olennainen osa kansallista turvallisuusstrategiaa, joka vaikuttaa laajasti yhteiskunnan eri osa-alueisiin.

Suomen vahva osaaminen ja teollisuus kyberturvallisuuden alalla tarjoavat merkittäviä mahdollisuuksia sekä kansallisella että kansainvälisellä tasolla.

2.5 Sääntöpohjainen kansainvälinen järjestelmä

Suomen tulisi lisätä panostustaan EU:n kybersietoisuuden lisäämiseksi esimerkiksi ENISA-yhteistyön vahvistamisen kautta. Suomen tulisi myös edistää kyberturvajoukkojen kehittämistä EU:n ja YK:n piirissä. Perinteisten rauhanturvajoukkojen ja kriisinhallintajoukkojen lisäksi tulisi selvittää hybridivaikuttamiselta suojaavien joukkojen perustamista. Tämä olisi tärkeä askel kohti kattavampaa turvallisuusstrategiaa, joka vastaa nykypäivän monimuotoisiin uhkiin.

Kyberturvallisuuden ylläpito on olennaista yhteiskunnalle tärkeiden toimintojen suojaamiseksi. Esimerkiksi disinformaation ja misinformaation torjuminen on keskeinen osa sääntöpohjaisen järjestelmän suojaamista ja ylläpitoa. Suomen vahva osaaminen ja aktiivinen rooli kyberturvallisuuden alalla tarjoavat merkittäviä mahdollisuuksia sekä kansallisella että kansainvälisellä tasolla.

Suomi tekee jo nyt laaja-alaista yhteistyötä useiden kansainvälisten toimijoiden kanssa, kuten EU, NATO, YK ja ETYJ. WithSecure näkee tämän yhteistyön lisäämisen ja syventämisen tärkeänä strategisena tavoitteena.

3.1.2 Suomi panostaa kriisinkestävyyteen

Huoltovarmuuden osalta on tärkeää huomioida teollisuuden mahdollisuudet tuottaa ja kehittää tuotteitaan sekä palveluitaan. Ukrainan sota on osoittanut, että omavaraisuus osaamisessa mahdollistaa uusien luovien ratkaisujen tuottavan merkittävää suorituskykyä, jota ei ole mahdollista hankkia kriisitilanteessa. Samaa nähtiin Suomessa pandemian aikana, kun osaamista pystyttiin hyödyntämään kriittisten tarvikkeiden tuottamiseen. Suomen innovaatiopääomaa tulee vahvistaa, eikä sitä saa ohjata pelkästään kansainvälisille kentille.

Selonteossa korostetaan murroksellisten tekniikoiden, kuten tekoälyn ja kvanttilaskennan, roolia ja niiden muodostamaa uhkaa Suomen turvallisuudelle. WithSecure haluaa tuoda esiin näkemyksensä, jonka mukaan näitä tekniikoita olennaisempi ja ajankohtaisempi tietoturvan haaste on perustoimintojen puuttuminen operatiivisilta yksiköiltä ja kriittistä infrastruktuuria ylläpitäviltä yrityksiltä. Tällaisia perustoimintoja ovat esimerkiksi riskipohjainen hallintakeinojen suunnittelu, tietoturvapäivitysten levittäminen ja toimittajakentän riskien huomioon ottaminen saatavuushäiriöiden tilanteissa.

Näitä tarpeita varten ollaan muodostamassa EU NIS2 -säädökseen perustuen kyberturvallisuuslakia ja päivittämässä useita Suomen olemassaolevia lakeja. WithSecuren mukaan tietoturvan operatiivisen tehokkuuden ja hallinnan kypsyyden parantaminen näiden uusien lainsäädäntöjen mukaisesti tulisi nostaa esiin myös tässä selonteossa.

Kriittisen infrastruktuurin toimittajariskeihin sisältyy se, että toimittajat ovat usein joko monikansallisia suuryrityksiä tai ulkomailla toimivia pienempiä tahoja. Kansallinen kyky vastata tuen tarpeeseen tai kriittisten toimijoiden operatiivisiin tarpeisiin on rajallinen, etenkin kriisiajan mahdollisten kansainvälisten yhteyshäiriöiden aikana.

Nykyinen tiedonjako ja tilannekuva eivät vastaa selonteossa esitettyä tavoitetilaa rikollisuuden tai hybridivaikuttamisen uhan torjumiseksi tehokkaasti. WithSecure näkee tarpeellisena reaaliaikaisen, operatiivisen tilannekuvan luomisen jäsenvaltioihin kohdistuvan tietojärjestelmien vaikuttamisen ja kyberrikollisuuden valvonnan tueksi. Tämän tilannekuvan tarkkuus ja konkretian taso ovat olennaisia, jotta siitä saatavalla ohjauksella voidaan toteuttaa konkreettisia ennaltaehkäiseviä ja suojaavia toimenpiteitä.

Tilannekuvan tulisi olla jäsenmaiden viranomaisten käytettävissä erilaisiin tarkoituksiin, mukaan lukien kansainvälinen verkkorikostutkinta ja hybridivaikuttamisen torjunta. Nykyisen, viranomaisilmoituksiin perustuvan ilmoituskanavan reagointiaika on parhaimmillaankin päiviä, ja sillä saatava tietoisuus on usein vain valmiuden kohottamisen ohjaamiseen käytettävää informaatiota.

WithSecure ei näe nykyisten EU-aloitteiden, kuten Joint Cybercrime Action Taskforce [1](J-CAT) ja ENISAn alaisuudessa toimivan European Cyber Crisis Liaison Organisation Network CyCLONe[2], tuottavan kriittisen infrastruktuurin operatiiviselle tietoturvahenkilöstölle tarpeeksi ajanmukaista ja kohdennettua näkyvyyttä toisissa jäsenvaltioissa tapahtuviin häiriöihin ja hyökkäyksiin. WithSecuren näkemyksen mukaan Suomen tulisi toimia aktiivisessa roolissa nykyistä tehokkaamman ja operatiivisesti käyttökelpoisen tilannekuvan muodostamisessa. Suomessa on vahvaa osaamista tällaisten toiminnallisuuksien suunnittelussa ja rakentamisessa.

[1] https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce
[2] https://www.enisa.europa.eu/topics/incident-response/cyclone

3.2.1 Suomi edistää Euroopan unionin roolia laajan turvallisuuden tuottajana

Tässäkin kappaleessa tulisi ottaa kantaa WithSecuren edelliseen osioon (3.1.2) kirjaamiin huomioihin.

3.2.2 Suomi vahvistaa NATOn asemaa transatlanttisen turvallisuuden kulmakivenä

Suomen kyberyritysten osaamisen tuominen NATO-yhteisön saataville edellyttää osaamisen tunnistamista ja markkinointia NATO-jäsenmaille. Suomi ja Ruotsi tuovat uusina jäseninä edistyksellistä osaamista ja kyvykkyyttä, joka on tärkeää saada esille verkostoissa. Suomen tulee toimia aktiivisena suunnannäyttäjänä ja rakentajana tällaisessa yhteistyössä.

3.4 Suomi edistää kansainvälistä rauhaa ja turvallisuutta sekä kestävää kehitystä

Suomella on vahvaa osaamista, hyvä maine ja laajat verkostot rauhanvälityksen ja kansainvälisen diplomatian kyberulottuvuudessa ja kyberturvallisuudessa. Suomi voisi ottaa aktiivisemman roolin kansainvälisten hankkeiden ja yritysten tukemisessa sekä niissä operatiivisesti toimimisessa. Tämä toiminta voidaan tukea suomalaisella osaamisella tietoturvallisten viestintä- ja yhteistyökanavien sekä toimintatapojen suunnittelussa.

4 Johtopäätökset

Johtopäätöksissä ei ole huomioitu kybersietoisuutta tai digitaalista turvallisuutta, vaikka ne ovat keskeisiä monien listattujen tavoitteiden (listan kohdat 2, 3, 4, 7, 10) saavuttamisessa. Näiden osa-alueiden merkitys tulisi tuoda esiin.

WithSecure suosittelee johtopäätöksiin lisättävän oheisen tai sisällöllisesti vastaavan osion:

“Suomi vahvistaa kyberturvallisuuttaan osana kansallista puolustuskykyä ja yhteiskunnan kokonaisturvallisuutta. Kyberturvallisuus on keskeinen tekijä kaikkien aiemmin kuvattujen tavoitteiden täyttymisessä, mukaan lukien kriisinsietokyvyn parantaminen, kansainvälinen yhteistyö ja strategisten riippuvuuksien hallinta. Suomi edistää kyberturvallisuuden kehittämistä ja yhteistyötä EU:n, Naton ja muiden kansainvälisten kumppaneiden kanssa, hyödyntäen vahvaa osaamistaan ja innovaatioitaan tietoturvallisten ratkaisujen luomisessa.”

Lausunnon antaja:

Helsingissä, 9.10.2024

Antti Laatikainen

Johtava tietoturvakonsultti

WithSecure Consulting

antti.laatikainen@withsecure.com

+358406372163