RO/ Tuomo Rusila
Vanhempi osastoesiupseeri, everstiluutnantti

Suuri valiokunta

Valtioneuvoston kirjelmä eduskunnalle ehdotuksista CSA2-asetukseksi ja NIS2-muutosdirektiiviksi

Suuri Valiokunta on pyytänyt puolustusministeriön kirjallista asiantuntijalausuntoa valtioneuvoston kirjelmästä eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS2-muutosdirektiiviksi sen käsittelyä varten. Tässä lausunnossa käsitellään CSA2-asetusta ja NIS2-muutosdirektiiviä maanpuolustuksen ja kyberpuolustuksen näkökulmasta.

Kyberturvallisuuden ja -resilienssin kehittäminen sekä ICT-toimitusketjujen turvallisuuden vahvistaminen ovat toimia, jotka sisämarkkinoiden häiriöttömän toiminnan, yhteiskuntien vakauden ja teknologisen suvereniteetin edistämisen lisäksi tukevat myös laajemmin maanpuolustusta sekä luovat pohjaa kyberpuolustuksen kehittämiselle.

NIS2- sääntelyn yksinkertaistaminen on kannatettavaa kuten myös sen yhdenmukaistaminen CSA2-asetuksen kanssa. Esitettyjen muutosten osalta on kuitenkin huomioitava esimerkiksi laajennetun tiedonvaihdon tai komissiolle esitetyn toimivallan muutoksien mahdolliset seurannaisvaikutukset kansalliseen turvallisuuteen ja maanpuolustukseen ja varmistaa näiden osalta riittävä kansallinen liikkumavara eri turvallisuustilanteissa.

Kriittisten toimialojen tieto- ja viestintätekniikan kyberturvallisuudella ja toimitusketjujen turvallisuudella on vaikutuksia myös puolustus- ja sotilasinfrastruktuurin turvallisuuteen. NIS2:n sovellusalueeseen liittyvät muutokset ovat sääntelyn yksinkertaistamisen lähtökohdista perusteltuja, mutta samalla toimijarajan nostamisella myös maanpuolustukselle keskeisiä kansallisia siviilikomponentin toimijoita jäisi nykyistä laajemmin kynnyksien alapuolelle. Näiden toimijoiden osalta tulee jatkossa erilaisin kansallisin toimin varmistaa minimivaatimustason täyttyminen. Samalla tulee arvioida esitettyjen muutosten vaikutusta kaksoiskäyttöinfrastruktuurin omistajiin ja operoiviin tahoihin.

Euroopan kyberturvallisuusvirasto ENISA:n tehtävien ja resurssien osalta tulee huomioida tarve ENISA:n nykyistä tiiviimmälle ja systemaattisemmalle yhteistyölle niin EU:n kuin Naton kyberpuolustusorganisaatioiden kanssa. Tällä hetkellä toiminnassa on niin toimivallallisia kuin prosessillisia, toimintakulttuurillisia ja teknisiä rajoitteita. Yleisesti siviili-sotilasyhteistyö ja sen mahdollistaminen alkaen tiedonvaihdosta tulisi olla integraalinen osa myös EU:n kyberturvallisuusnormistoa. Esitys ENISA:n päivitetystä mandaatista ei ole tällä hetkellä riittävän kunnianhimoinen tältä osin. Käytännössä siviili-sotilasyhteistyön tulisi olla osa ENISA:n säädettyä normaalia tehtäväkenttää ja siten mahdollistaa ENISA:lle sekä tiedonvaihto että operatiivinen yhteistyö kyberpuolustustoimijoiden kanssa. Tämä myös pienentää mahdollisten erillisten kaksoissuorituskykyjen luomisen tarvetta EU:n siviili- ja sotilasvirastoille ja auttaa siten hallitsemana muun muassa kustannuksiin ja henkilöstöresursseihin liittyviä ongelmia.

ICT-toimitusketjujen ei-teknisten kyberturvallisuusriskien hallintatoimien yhdenmukaistaminen EU:ssa on tärkeää myös maanpuolustuksen näkökulmasta, kunhan huomioidaan myös jäsenvaltioiden mahdollisuus asettaa komission esittämiä vaatimuksia tiukempia kriteereitä. Mainittujen NIS2-direktiivin liitteiden I ja II sektoreilla on merkittävissä määrin maanpuolustukselle ja puolustuskyvylle kriittisiä toimijoita ja infrastruk-

tuuria, joiden ICT-toimitusketjujen riskilähtöisten toimien velvoittaminen parantaa lopulta myös sotilaallista operaatiovarmuutta. Maanpuolustuksen näkökulmasta riskiperusteiden lähestymistavan tulee olla lähtökohdiltaan uhkaperusteista. Tällöin esimerkiksi niin kutsutun savuavan aseen mahdollinen edellyttäminen riskiarvioinnin kriteerinä ei edistäisi ICT-toimitusketjujen turvallisuutta aiotussa laajuudessa huomioiden eri turvallisuustilanteiden vaatimukset. Tällaista kriteeriä ei nyt esitetty, mutta jatkovalmistelussa tulee varmistaa aidon riskilähtöisen ja uhkaperusteinen arvioinnin säilyminen.

ICT-toimitusketjujen turvallisuuden hallintatoimenpiteiden osalta valvovien viranomaisten tiedonsaantioikeuksien lisäksi tulee varmistaa, että näillä viranomaisilla on myös oikeus luovuttaa tietoja muun muassa turvallisuusviranomaisille näiden uhka- ja riskiarviointien laatimisen sekä toimitusketjuihin liittyvien uhkien jatkuvan arvioinnin mahdollistamiseksi. Samalla valvovien viranomaisten tulee saada hyödyntää näiden ei-valvovien viranomaisten tuottamia arvioita ilman että se on ristiriidassa esitetyn itsenäisen roolin tai ulkoisista vaikutteista riippumattomuuden periaatteen kanssa. Tiedonluovutusoikeudella sekä ei-valvovien viranomaisten hyödyntämisellä riskiarvioinnissa on keskeinen merkitys kansallisesti niin laaja-alaisen viranomaisyhteistyön mahdollistamisessa kuin resurssien tehokkaan käytön näkökulmasta.

Esitetty sertifiointijärjestelmien kehittäminen tukee myös siviili- ja kaksoiskäyttöteknologian turvallista hyödyntämistä sotilaskäytössä. Lisäksi sertifiointijärjestelmiä voidaan soveltaa myös sotilasjärjestelmissä yleisenä viitekehyksenä näin lisäten muun muassa yhteensopivuutta siviilijärjestelmien kanssa. Kansallisten sertifiointijärjestelmien poistumisessa on huomioitava, että niiden ylläpitokyky tulee säilyttää, jos niillä on erityistä merkitystä maanpuolustukselle ja jos EU:n yhteinen sertifiointijärjestelmä ei kykene niitä maanpuolustuksen näkökulmasta korvaamaan. Kansallisten kyberturvallisuussertifioinnin viranomaisten luominen edellyttää resursseja, mikä on samalla keskeinen osa koko sertifiointijärjestelmän uskottavuutta.

NIS2-muutosdirektiivin kansallisessa implementoinnissa tulee arvioida ja toteuttaa myös kansalliset laajennukset asettamalla vastaavat minimitason vaatimukset muun muassa puolustus- ja turvallisuussektorille sekä määrittää tälle sektorille sekä valvova viranomainen että mahdolliset muut kyberturvallisuuslain viranomaistehtävät ja näiden toimivalta. Tarve tälle tunnistettiin jo kyberturvallisuuslain valmistelussa, mutta muutosta ei vielä silloin toimeenpantu. Toimenpide on osa Puolustushallinnon roolin selkeyttämistä kyberturvallisuudessa, Suomen kyberturvallisuusstrategian toimeenpanoa sekä valtioneuvoston vuoden 2024 puolustusselonteon mukaista toimenpidettä parantaa esimerkiksi puolustusteollisuuden suojaa kyberuhkilta.

Liitteet

Jakelu PLM Kansliapäällikkö
PLM RO OSPÄÄL
PLM PO OSPÄÄL
PLM erityisavustajat
PLM sotilasneuvonantaja

Tiedoksi PLM ROTI Tietohallintojohtaja

Postiosoite
Postadress
Postal Address
Puolustusministeriö
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
kirjaamo@defmin.fi
www.defmin.fi