Puolustusministeriö
Försvarsministeriet
Ministry of Defence

Kirje

5.1.2021

VN/24348/2020
VN/24348/2020-PLM-47

LVM TIO Turvallisuusyksikkö

Puolustusministeriön lausunto

Puolustusministeriön lausunto liikenne- ja viestintäministeriön asettaman työryhmän selvitykseen tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla. Pääesikunta laatii erillisen puolustusvoimien lausunnon.

Lausunto selvityksen ehdotuksiin poliittisiksi linjauksiksi

Selvityksen poliittisten linjausten ja kyberturvallisuuden kehittämisohjelman suhde jää epäselväksi. Molemmissa on esitetty samankaltaisia tai ainakin toisiaan lähellä olevia toimenpiteitä. Lisäksi kyberturvallisuuden kehittämisohjelmassa on toimenpiteitä, kuten hankintaosaamisen kehittäminen ja kyberturvallisuusvaatimusten määrittely, jotka ovat myös osa tämän selvityksen poliittisia linjauksia.

EU:n kyberstrategiassa (The EU's Cybersecurity Strategy for the Digital Decade, 16.12.2020) korostetaan tiedonvaihdon ja yhteistyön merkitystä kyberuhkien estämisessä ja niihin vastaamisessa. EU:n kyberstrategian mukaiset kriittiset toimijat, joiden välistä yhteistoimintaa korostetaan, ovat "(i) NIS authorities, such as CSIRTs, and disaster response; (ii) law enforcement and judicial authorities; (iii) cyber diplomacy; and (iv) cyber defence". Esitetyt poliittiset linjaukset kohdistuvat pääosin NIS-toimijoihin (i) ja joiltain osin myös OM ja SM hallinnonaloille (ii). Poliittisia linjauksia voisi laajentaa turvallisuusviranomaisiin (iii), (iv) tai sitten lisätä uuden linjauksen, jossa todetaan, että turvallisuusviranomaisten osalta kehittämistoimenpiteet tarkastellaan kyberturvallisuuden kehittämisohjelmassa.

Edelleen tulee ottaa huomioon se, että linjaukset ovat hyödyttömiä, mikäli niitä ei panna toimeen. Linjausten perusteella toteutettavilla toimenpiteillä tulee olla vastuutaho ja toteutuksella mittarit joita seurataan.

Linjaus 1

Viranomaisten välisen yhteistyön tiivistäminen ja tiedonvaihdon lisääminen on kannatettavaa. Viranomaisten välistä tiedonvaihtoa rajoittaa salassapitosäännöt mm. poliisin osalta ja sopimukset mm. Havaron osalta. Virka-apuun liittyvää lainsäädäntöä on jo olemassa ja sitä on syytä tarkentaa kyberasioiden osalta.

Tuen ja virka-avun tulisi toimia molempiin suuntiin eli tarvittaessa muut viranomaiset voisivat tukea Kyberturvallisuuskeskusta tai Kyberturvallisuuskeskus tukea muita viranomaisia.

Postiosoite Postadress Postal Address	Käyntiosoite Besöksadress Office	Puhelin Telefon Telephone	Faksi Fax Fax	s-posti, internet e-post, internet e-mail, internet
Puolustusministeriö				
PL 31 00131 Helsinki	Eteläinen Makasiinikatu 8 Helsinki	0295 16001 +358 295 16001		kirjaamo@defmin.fi www.defmin.fi

Linjaus 2

Kyberturvallisuuskeskuksen vahvistamisessa eri toimialoille pitää varmistaa että mm. tiedonvaihto eri toimialojen välillä toimii.

Linjaus 3

Linjaus Kyberturvallisuuskeskuksen koulutustehtävästä eri sektoreiden viranomaisille voisi yhtä hyvin olla kyberturvallisuuden kehittämisohjelman toimenpide.

Linjaus 5

Ratkaisuille, jotka mahdollistavat salassa pidettävän ja turvaluokitellun tiedon turvallisen vaihtamisen viranomaisten välillä on tarvetta. Ratkaisuissa pitää päästä TLII-tasolle. Linjaus voisi yhtä hyvin olla kyberturvallisuuden kehittämisohjelman toimenpide.

Linjaus 6

Niin lainsäädännön kuin HAVARO-sopimusten on mahdollistettava tiedonjako myös muille turvallisuusviranomaisille ilman rikosepäilyä ja jopa muiden viranomaisten suora pääsy HAVARO-dataan. Samalla havainnointikyvykkyydellä pystytään näin vastaamaan usean toimijan tarpeisiin ilman, että se juurikaan kuormittaa Kyberturvallisuuskeskusta.

Linjaukset 7 ja 8

Selvityksessä tehty rajaus NIS-toimijoihin jättää mm. turvallisuusviranomaiset näiden linjausten ulkopuolelle. Vastaava linjaus pitää tehdä muissa kriittisiä toimialoja koskevissa määräyksissä, jollei tämän linjauksen kattavuutta laajenneta.

Linjaus 10

Yhteiskunnan elintärkeät toiminnot -käsite sisältää myös kansalliselle turvallisuudelle ja maanpuolustukselle tärkeät toimijat, jotka eivät kuitenkaan ole mukana linjauksessa luetelluissa vastuutahoissa.

Linjaus 11

Toimivaltaisilla viranomaisilla tulee olla tiedonsaantioikeus ja valtakunnallinen koottu tilannekuva toteutetuista auditoinneista ja hyväksynnöistä.

Linjaus 19

Poliisien resurssien lisäämiseksi tulee kehittää viranomaisyhteistyötä ja virka-apukäytänteitä.

Linjaus 20

Velvoitteen pitäisi koskea muitakin kuin NIS-sektoriviranomaisia.

Linjaus 21

Kansallisesti NIS-direktiiviä on mahdollista soveltaa laajemmin ja esim. poikkeamien ilmoitusvelvollisuus voisi koskea muitakin kuin NIS-toimijoita.

Linjaus 24

Valtorin resurssien lisäämisen lisäksi tulee luoda mallit, joissa Valtori pystyy hyödyntämään muiden viranomaisten resursseja ketterästi. Viranomaisyhteistyötä hyödyntämällä voitaisiin parantaa edellytyksiä esim. kehittyneiden uhkien havaitsemiseen ja torjuntaan.

Linjaus 26

Tavoitteena tulisi olla, että Hanselin kilpailutuksiin saadaan lisää kotimaisia kyberalan toimijoita, jolloin edistetään myös kansallista osaamista ja yritystoimintaa. Tällä on erityinen merkitys myös kansallisen turvallisuuden näkökulmasta.

Linjaus 35

Pääsy ilmoitusdataan tulee mahdollistaa myös viranomaisyhteistyöhön osallistuville viranomaisille. Tällöin jokaisella toimijalla on mahdollisuus arvioida omien tietoaineistojensa kautta uhkaa kriittiselle toiminnalle. Tietoja ei voida kaikissa tapauksissa vaihtaa viranomaisten kesken esim. KV-sopimusten takia, mutta lainsäädännön mahdollisuudet tiedonvaihtoon tulee hyödyntää.

Väliraportin muut osat, kommentit:

Kokonaisuutena on erittäin tervetullutta, että luodaan toimenpidekokonaisuus tiettyjen yhteiskunnan kannalta merkittävien toimialojen tietoturvan ja tietosuojan parantamiseksi.

Jossain kohden selvitystä olisi todettava se, minkä tasoinen asiakirja tästä selvityksestä on tarkoitus tulla. Tuleeko tästä selvityksestä valtioneuvoston periaatepäätös, VN päätös, ohje vai jääkö tämä vain asetetun työryhmän selvitykseksi? Ja mikä asiakirjan suhde on kansalliseen kyberturvallisuusstrategiaan ja sen perusteella käynnistettävään kehittämisohjelmaan?

Selvityksen soveltamisalaksi on johdannossa mainittu tietoturvan ja tietosuojan parantaminen kriittisillä toimialoilla. Missään tekstissä ei kuitenkaan ole määritelty, mitä ovat kriittiset toimialat, eikä sitä, millä perusteilla selvityksen eri toimialat on valittu toimenpiteiden kohteeksi. Monia hyvillä perusteilla kriittisiksi luokiteltavia toimialoja on jätetty pois. Turvallisuusviranomaisten lisäksi esimerkiksi (elintarvikehuoltoon liittyvät) logistiset verkostot, satamien ohjausjärjestelmät, median ja tiedonvälityksen toimivuus tai jätehuolto eivät ole selvityksen toimenpiteiden kohteena. On toki ymmärrettävää, että työn laajuuden vuoksi jonkinlainen rajaus on tehtävä, mutta rajaus olisi hyvä perustella.

Ehdotetaan harkittavaksi, että selvityksessä tukeuduttaisiin joko Yhteiskunnan turvallisuusstrategian 2017 määritelmiin yhteiskunnan elintärkeitten toimintojen turvaamisesta tai vaihtoehtoisesti Huoltovarmuuspäätöksen 2018 määrittelyyn yhteiskunnan kriittisestä infrastruktuurista. Lisäksi selvityksessä voidaan tarvittaessa todeta, että tässä vaiheessa työn laajuuden johdosta on tarkoituksenmukaista keskittyä vain tiettyihin toimialoihin.

Selvityksessä ei ole otettu kantaa uhkaan, jolta suojaudutaan. Viimeaikaisten tapahtumien valossa yhteiskunnan elintärkeiden toimintojen kannalta merkittävä uhka muodostuu kehittyneistä pysyvistä uhkista (APT), joiden taustalla olevat toimijat ovat kyvykkyydeltään ja resursseiltaan merkittäviä. Tämä haastaa yksittäisten kansallisten toimijoiden kyvyn vastata uhkaan. Kehittyneiden uhkien havaitseminen ja torjunta edellyttää kiinteää yhteistyötä ja tiedonvaihtoa.

Selvityksen alaluvussa, jossa käsitellään tietoturvan ja tietosuojan merkitystä talousjärjestelmälle pohditaan selvityksen tarkastelun kohteena olevien toimialojen vaikutusta muihin toimialoihin sekä yhteiskunnallisten toimintojen ylläpitoon. Keskinäisriippuvuudella tarkoitetaan yleisesti kahden eri asian yhteyttä tai riippuvuussuhdetta toinen toiseensa. Selvityksessä kuitenkin käytetään keskinäisriippuvuutta ilmaisuna tilanteessa, jossa on selkeästi kyse yhdensuuntaisista riippuvuuksista ja niiden kerrannaisvaikutuksista. Sähkönjakelun häiriintyminen vaikuttaa mm. raideliikenteeseen tai vedenjakeluun mutta ei päinvastoin. Ehdotetaan, että keskinäisriippuvuuksien sijaan puhuttaisiin riippuvuuksista ja niiden mahdollisista kerrannaisvaikutuksista.

Kyberturvallisuus, tietoturvallisuus ja tietosuoja on määritelty Sanastokeskuksen kokoamassa kyberturvallisuussanastossa 2018 https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf, jota mm. silloinen

Viestintävirasto oli mukana kokoamassa. Ei ole tarkoituksenmukaista, että kyberturvallisuutta ja tietoturvallisuutta käytetään toistensa synonyymeina.

Tietohallintojohtaja	Mikko Soikkeli
Tietoturvapäällikkö	Harri Mäntylä

Liitteet

Jakelu LVM TIO Turvallisuusyksikkö

Tiedoksi