Liikenne- ja viestintäministeriö

VN/24348/2020

Suojelupoliisin lausunto; Selvitys tietoturvan ja tietosuojan parantamisesta yhteiskunnan kriittisillä toimialoilla

1 Asia

Liikenne- ja viestintäministeriö on asettanut 9.11.2020 työryhmän selvittämään tietoturvan ja tietosuojan parantamista yhteiskunnan kriittisillä toimialoilla. Liikenne- ja viestintäministeriö on pyytänyt Suojelupoliisilta lausuntoa työryhmän väliraportista; *Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla*.

2 Lausunto

Suojelupoliisi katsoo, että esityksen tavoitteenasettelu on perusteltu samoin kuin useat ehdotukset poliittisiksi linjauksiksi, joilla nykytilanteen haasteisiin pyritään vastaamaan.

Suojelupoliisi haluaa kuitenkin kiinnittää työryhmän huomiota siihen, ettei selvityksessä oteta riittävällä tavalla huomioon kansallista turvallisuutta. Tarkastelusta puuttuu vielä Suojelupoliisi. Suojelupoliisin tehtävänä on suojata kansallista turvallisuutta torjumalla myös digitaalisen toimintaympäristön uhkia. Nämä uhat voivat ilmetä esimerkiksi vieraan valtion tiedustelutoimintana tai suuren ihmismäärän henkeä ja terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaavana toimintana. Edellä mainittujen lisäksi Suojelupoliisin tehtävänä on torjua vieraan valtion toimintaa, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille tai taloudellisille tai muille tärkeille eduille.

Kun tietoturvalle tai -suojalle vahinkoa aiheuttava toiminta vaarantaa myös kansallista turvallisuutta, ei riitä, että tekninen poikkeama selvitetään. Vahingon rajaamiseksi on selvitettävä myös sen syy ja taustatekijät. Suojelupoliisi tuottaa ennakoivaa ja merkityksellistä tietoa kansallista turvallisuutta vaarantavasta toiminnasta omilla toimivaltuuksillaan. Tietoa ja tilannekuvaa tuotetaan valtiojohdon lisäksi viranomaisille, kuten Kyberturvallisuuskeskukselle. Tämän lisäksi Suojelupoliisi torjuu kansallisen turvallisuuden uhkia ilmoittamalla havaitsemistaan uhkista kriittistä infrastruktuuria ylläpitäville organisaatioille sekä avustamalla näitä estämään vahinkoja omalla toiminnallaan.

Suojelupoliisi on kansallisen turvallisuuden katsauksessa tuonut esiin, että sekä Kiina että Venäjä harjoittavat aktiivisesti vakoilua Suomen intressejä vastaan. Kun tietoturvaloukkauksen toteuttajana on valtio, toimenpiteet tapahtu-

man ja sen mahdollisesti aiheuttamien vahinkojen torjumiseksi ovat erilaisia kuin jos teon taustalla olisi yksittäinen henkilö tai henkilöryhmä. Teon seuraamusmenettelykään ei kuulu tällöin vain rikosoikeuden piiriin, vaan se edellyttää ulko- ja turvallisuuspoliittista harkintaa.

Laitevalmistajiin liittyvien teknisten riskien lisäksi kriittistä infrastruktuuria sekä keskeistä tietoa ylläpitävillä organisaatioilla on oltava tietoa strategisesta riskistä, joka aiheutuu laitevalmistajiin autoritäärisistä kolmansista maista asetetuista velvoitteista. Nämä velvoitteet sitovat laitevalmistajaa vahvemmin kuin asiakassuhde valmistajan suomalaiseen asiakkaaseen.

Ehdotuksissa poliittisiksi linjauksiksi huomioidaan hyvin Liikenne- ja viestintäviraston kyberturvallisuuskeskuksen sekä poliisin verkkorikostorjunnan resurssit. Tietoturvallisuuden ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla tämä ei kuitenkaan ole riittävää. Vastaava huomio tarvitaan laaja-alaisemmin myös kansallista turvallisuutta uhkaavan valtiollisen toiminnan, eli tässä tapauksessa erityisesti kybervakoilun ja -vaikuttamisen torjuntaan ja sen resursseihin.

Suojelupoliisi katsoo, että toimijoiden tietoturvallisuuden hallintajärjestelmien arviointi ja auditointi ovat tärkeitä hallintakeinoja organisaation tietoturvallisuuden kehittämisessä. Luonnoksessa esitetty linjaus (linjaus 12.) ISO 27001-sertifioinnin vaatimisesta on kuitenkin Suojelupoliisin näkemyksen mukaan arvioitava kriittisesti ja kytkettävä laajemmin edellytettäviin auditointiprosesseihin. Arviointilaitosten määrän lisääminen (linjaus 13.) ei Suojelupoliisin näkemyksen mukaan sellaisenaan lisää tietoturvallisuutta. Erityisen kriittisesti tulee arvioida arviointilaitosten hyväksymismenettelyn keventämistä, jota esitys hyväksymismenettelyn tehostamisesta käytännössä tarkoittaisi.

Luvussa 4 (sivu 15) käsitellään hankintojen suorittamista ja niissä huomioitavaa säätelyä. Suojelupoliisi painottaa, että hankinnoissa on syytä huomioida mahdollisuus niiden tekemiseen julkisista puolustus- ja turvallisuushankinnoista säädetyn lain pohjalta. Tällöin mahdollistuu myös tietoturvaan liittyvien seikkojen huomiointi eri tavalla. Samassa luvussa todetaan, että kilpailutushankintaprosesseissa tulisi kiinnittää aktiivisemmin huomiota esimerkiksi eri toimijoiden tarjoamien palvelujen ja järjestelmien sertifioinnin tasoon. Työryhmä katsoi lisäksi, että tietosuojaan ja tietoturvaan liittyvää hankintaosaamista olisi mahdollista kehittää esimerkiksi julkishallinnolle tukitoimintoja tarjoavan Hansel Oy:n kautta.

Suojelupoliisi toteaa edellä mainittuun kappaleeseen sekä poliittisiin linjausehdotuskohtiin 26 ja 27 liittyen, että voimassa oleva turvallisuusselvityslaki (726/2014, 5. luku) antaa mahdollisuuden selvittää erilaisten toimijoiden tietoturvallisuuden tasoa Suojelupoliisin ja Kyberturvallisuuskeskuksen yhteistyönä ja tämä olemassa olevan lainsäädännön tuoma mahdollisuus tulisi ottaa mukaan huomioitaessa eri ratkaisuja tietoturvan parantamiseksi kriittisillä toimialoilla.

Kohdassa 26 mainittu Hansel Oy:n rooli tietoturvallisuuden varmistamisessa on tunnistettu jo aiemmin turvallisuusselvityslain valmistelussa. Laissa (726/2014, 33§) todetaan, että yritysturvallisuusselvitystä voi hakea "...viranomaisen toimeksiannosta valtionhallinnon hankinnoista vastaava yksikkö", jolla tarkoitetaan Hansel Oy:tä. Hansel Oy:n on mahdollista hakea yritysturvallisuusselvitystä julkisiin hankintoihin liittyvistä yrityksistä. Tämän lisäksi ja

linjauskohtaan 27 viitaten, yritysturvallisuusselvityksiä on mahdollista tehdä myös terveydenhuollon sekä energia- ja vesihuollon toimijoiden tietoturvallisuuden selvittämiseksi siinä laajuudessa, miten turvallisuusselvityslaissa esitetyt laatimisen edellytykset (36 §) täyttyvät.

Selvityksessä todetaan myös (sivu 23), että "tällä hetkellä vain osa yhteiskunnan kriittisen toimialan toimijoista tilaa auditointipalveluja tai omaa tietoturvaa koskevia sertifikaatteja. Erityisesti kuntasektorilla, logistiikassa, elintarvikehuollossa ja teollisuustuotannossa auditointeja tehdään työryhmän saaman selvityksen mukaan vähän" Edelliseen viitaten, Suojelupoliisin on mahdollista laatia yritysturvallisuusselvityksiä myös kuntasektorin ja muiden kappaleessa mainittujen toimialojen tietoturvallisuuden tason selvittämiseksi nykyisen turvallisuusselvityslainsäädännön (726/2014) puitteissa.

Luonnoksessa esitetään useita tietoturvallisuutta ja tietosuojan parantamiseen liittyviä toimenpiteitä, joiden tavoitteena on tietoturvan tason korottaminen niin yksityisellä, kuin julkisella puolella. Samalla esitetään Hansel Oy:n asiantuntijuuden vahvistamista ja hyödyntämistä sellaisten julkisten hankintojen osalta, joissa tietoturvan ja tietosuojan merkitys korostuu (kohta 26 ja sivu 15 toinen kappale). Tällöin Hansel Oy:n kaikki oma toiminta, kuten tietojärjestelmät, tilat, henkilöstö, prosessit ja hallinto yleensä, tulisi täyttää sellaiset turvallisuusvaatimukset, joiden perusteella Hansel Oy ja sen asiantuntijat voisivat näiden hankintojen yhteydessä käsitellä turvallisuusluokiteltua tietoa. Käytännössä tämä edellyttänee, että Hansel Oy:n toiminta täyttäisi kaikilta osin TLIII -vaatimukset. Kriittisten toimijoiden ICT-hankintoihin liittyvä tekniset kuvaukset, kuten erilaiset järjestelmien rajapintakuvaukset voivat olla TLIII -tasolle luokiteltuja, sillä niihin sisältyvät tiedot mahdollistavat taitavalle toimijalle potentiaalisia hyökkäysvektoreita tietojärjestelmiin. Samalla tulee huomioida, että tällöin Hansel Oy:n tulee todennäköisesti kerääntymään mahdollisesti erittäin huomattava määrä sellaista suomalaisen yhteiskunnan useisiin kriittisiin tietojärjestelmiin liittyvää tietoa, joka jo itsessään voi tehdä Hansel Oy:stä itse erittäin potentiaalisen kohteen vakavalle rikollisuudelle kuten vakoilulle.

3 Lopuksi

Kansalliselle turvallisuudelle vaaraa aiheuttavien riskien ja haavoittuvuuksien sekä niiden taustalla olevien monimutkaisten vaikutusketjujen arviointi ja hallitseminen on vaikeaa. Riskien minimoiminen edellyttää systemaattista ja riskilähtöistä ennalta estävää turvallisuustyötä, jossa viranomaisten ja kriittisen infrastruktuurin muiden toimijoiden toiminta on keskenään yhteen sovitettua. Tuloksellisen turvallisuustyön edellytyksenä on, että jollekin taholle on osoitettu toimivalta velvoittavasti ohjata sen toteutumista koko yhteiskunnan tasolla.

Suojelupoliisi toteaa, ettei Suomessa ole tällä hetkellä yksiselitteisesti säädetty kriittisen infrastruktuurin ja kansallisen turvallisuuden suojaamiseksi tarpeellisesta ohjausmekanismista ja siihen liittyvistä viranomaisvastuista. Vaikka poliisin hallinnosta annetun valtionneuvoston asetuksen (158/1996) 8§ esimerkiksi säätää Suojelupoliisin tehtäväksi antaa viranomaisille ja yhteisöille sellaisia ohjeita, neuvoja ja tietoja, jotka ovat tarpeen valtion turvallisuuden ylläpitämiseksi tai siihen kohdistuvien loukkausten estämiseksi, eivät säännöksen tarkoittamien ohjeiden ja neuvojen vastaanottajat ole velvoitettuja noudattamaan niitä.

Suojelupoliisin näkemyksen mukaan luonnoksesta esitettyjen toimenpiteiden ja vastuutahojen määrittelyssä tulee huomioida kattavasti Sisäministeriö (SM) ja sen hallinnonala.

Suojelupoliisin päällikkö
Poliisineuvos Antti Pelttari

Ylitarkastaja Sami Niinikorpi

Liitteet -

Jakelu Liikenne- ja viestintäministeriö.

Tiedoksi Sisäministeriö