

Eduskunnan liikenne- ja viestintävaliokunta

Päiväys/Datum
11.10.2021

LiV(at)eduskunta.fi

Dnro/Dnr
TRAFICOM/484370/03.03.01/2021

Viite/Referens
HE 146/2021 vp

Liikenne- ja viestintäviraston lausunto aiheesta kyberturvallisuuden haasteet ja kehittäminen talousarvioesityksen näkökulmasta

Kyberturvallisuuteen esitettyä rahoitusta on toistuvasti leikattu

Suomen panostukset kyberturvallisuuteen ovat viimeisen vuosikymmenen ajan jääneet merkittävästi jälkeen kyberturvallisuusympäristön ja -uhkien kehittymisestä. Toistamiseen Suomen kyberturvallisuuden kehittämisen toimenpiteille asiantuntijoiden arvioimia ja määrittämiä rahoitustarpeita on leikattu, jonka seurauksena toimenpiteet toteutetaan vaillinaisesti ja jätetään osin kokonaan toteuttamatta. Samaan aikaan viranomaisille asetetaan uusia tehtäviä ilman riittäviä taloudellisia resursseja. Näistä viimeisimpiä esimerkkejä ovat kyberturvallisuuden kehittämisohjelma, tietoturvallisuuden ja tietosuojan kehittäminen kriittisillä toimialoilla -raportin toimenpiteet, kansallisen tietoturvan sertifiointiviranomaisen tehtävät ja kansallisen koordinaatiokeskuksen tehtävät, joiden kaikkien osalta asiantuntijoiden esittämää rahoitusesityksiä on leikattu ja osassa tapauksissa jopa jätetty myöntämättä.

Kyberturvallisuuden korjausvelkaa ei saa syntyä

Samaan aikaan kyberturvallisuusongelmissa Kyberturvallisuuskeskuksen apua tarvitsevia kansalaisia ja yhteiskunnan kriittisten toimialojen toimijoita on joka vuosi entistä enemmän. Kasvavaan tuen tarpeeseen vastaaminen tulee edellyttämään lisärahoitusta.

Nyt viimeistään Suomen tulisi ajaa kiinni kyberturvallisuuden korjausvelka, joka vuosikymmenen aikana on syntynyt, ja turvata yhteiskunnan elintärkeät toiminnot. Mikäli nyt jäämme jälkeen Suomen kyberturvallisuuden perustan rakentamisessa, tulevat tulevaisuuden kustannukset kyberturvallisuuden toimenpiteiden laiminlyönnistä olemaan moninkertaisesti suhteessa nyt esitettyihin panostuksiin. Kyse ei ole enää ainoastaan taloudellisista menetyksistä, vaan myös demokratiaan ja hyvinvointiin liittyvistä sekä henkisistä kärsimyksistä, joista Coop-kauppaketjun kauppohenkilöstön sulkeminen Ruotsissa ja Vastaamo-tapauksen seuraukset Suomessa ovat vain yksi esimerkki. Riittävän rahoituksen puute ei vaivaa ainoastaan Liikenne- ja viestintäviraston Kyberturvallisuuskeskusta, vaan myös muita viranomaisia, jotka valvovat ja tukevat kriittisten sektorien toimijoiden kyberturvallisuutta ja kyberturvallisuuden kehittämistä. Jos yhteiskuntaan iskisi kaksi yhtäaikaista vakavaa kybertapausta ei Kyberturvallisuuskeskuksella eikä muilla turvallisuusviranomaisilla olisi resursseja hoitaa molempia tapauksia.

Kyberturvallisuus on tärkeä osa yhteiskunnan turvallisuutta ja toimivuutta

Kyberturvallisuus on poikkihallinnollinen ja koko yhteiskuntaa läpileikkaava kivijalka ja kyberturvallisuus on digitalisoituvan yhteiskunnan kotivakuutus.

Kyberturvallisuushkat tulevat entistä konkreettisemmin ihmisten iholle vaikuttaen samalla tavoin kuin fyysisessä maailmassa kohtaamamme turvallisuushkat. Kyberturvallisuushkan toteutuessa menetykset ovat taloudellisten menetysten lisäksi entistä useammin henkisiä, ja maailmalla on jo jopa raportoitu ensimmäisistä kyberturvallisuusloukkausten kuolonuhreista. Kyberturvallisuushkat eivät ole enää virtuaalisen maailman vitsaus, vaan jokapäiväiseen elämäämme vaikuttava uhka.

Kyberrikollisten kyvykkyydet kehittyvät ja kohteet lisääntyvät uusien teknologioiden avaamien ovien avulla. Viime vuosina näkyvimpänä suomalaisena kyberherätyksenä olivat kuntasektoriimme kohdistuneet kyberhyökkäykset. Ne osoittivat yhteiskuntamme haavoittuvuuden ja haittasivat muun muassa kansalaisten kriittisiä palveluita ja arkea. Suomeen on myös rantautunut uusi ilmiö, jossa rikolliset vaativat suuria lunnaita kiristyshaittaohjelmahyökkäyksillä, joiden kohteina ovat kriittiset suuryritykset. Hyökkäykset ovat aiheuttaneet yrityksille vakavia toiminnan häiriöitä sekä mittavia taloudellisia tappioita. Tapaus Vastaamo oli Suomen historian yksi merkittävimmistä tietomurroista. Varastamallaan sensitiivisillä tiedoilla hyökkääjä kiristi niin Vastaamoa kuin kymmeniä tuhansia sen palveluita käyttäneitä kansalaisia. Myös suomalainen päätöksenteko on ollut uhattuna, kun Suojelupoliisi esti eduskuntaan kohdistuneen kybervakoiluoperaation, jossa yritettiin tunkeutua eduskunnan tietojärjestelmiin. Tämän lisäksi maailmalla ovat yleistyneet kyberturvallisuushkien vaikutukset suoraan fyysiseen maailmaan. Hakkerit lamauttivat Ruotsin johtavan kauppaketju Coopin kiristyshaittaohjelman avulla, ja uhreiksi joutuivat tuhannet yritykset ainakin 17 eri maassa.

Kyberturvallisuuskeskus ennaltaehkäisee, varoittaa yhteiskuntaa ja auttaa toipumaan

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus palvelee kaikkia yhteiskunnan kriittisiä sektoreita ja tekee aktiivisesti yhteistyötä eri viranomaisten kanssa. Kyberturvallisuuskeskuksella on keskeinen rooli kyberturvallisuuden kokonaistilannekuvan ylläpitämisessä ja jakamisessa ja vakavien tai laajavaikutteisten kyberuhkien ennaltaehkäisyssä. Kyberturvallisuuskeskus huolehtii pyynnöstä myös korkean turvallisuusluokan tietoja käsittelevien tietojärjestelmien tietoturvallisuuden arvioimisesta.

Kansallisen kyberturvallisuuden kehittämistä ja samalla myös Kyberturvallisuuskeskuksen toimintaa tulevat ohjaamaan kesällä hyväksytyt kaksi kyberturvallisuutta koskevaa periaatepäätöstä. Molemmat periaatepäätökset asettavat lukuisia toimenpiteitä Kyberturvallisuuskeskuksen vastuulle koko yhteiskunnan kyberturvallisuusosaamisen ja häiriönsietokyvyn kehittämiseksi. Periaatepäätöksistä ensimmäinen eli Kyberturvallisuuden kehittämisohjelma on laadittu laaja-alaisessa yhteistyössä eri viranomaisten ja yritysten kesken ja sen tavoitteena on muun muassa parantaa digitaalisen yhteiskunnan kestävyyttä sekä sietokykyä kybertoimintaympäristön eri ilmiöitä vastaan. Kyberturvallisuuden kehittämisohjelmassa on määritelty tarvittavat toimenpiteet Suomen kyberturvallisuuden kehittämiseksi. Nämä toimenpiteet vaikuttavat olennaisella tavalla koko yhteiskunnan turvallisuuden varmistamiseen ja kriisinsietokyvyn kehittämiseen.

Toisessa periaatepäätöksessä eli tietoturvan ja tietosuojan parantamiseksi kriittisillä toimialoilla on asetettu lukuisia toimenpiteitä, jotka tähtäävät kyberturvallisuutta koskevien kyvykkyyksien kehittämiseen ja velvoittavien vaatimusten täsmentämiseen kriittisillä toimialoilla. Periaatepäätöksen keskiössä on myös yhteistyön kehittäminen selkeyttäminen keskeisten viranomaistoimijoiden kesken. Monet toimenpiteistä edellyttävät Kyberturvallisuuskeskuksen aktiivista panosta joko muiden toimialojen tukemiseksi tai kokonaan uusien toimintatapojen kehittämiseksi.

Kyberturvallisuustehtäviä osoitetaan ilman onnistumisen edellytyksiä

Kyberturvallisuuskeskukselle on tullut uusia lakisääteisiä tehtäviä ja olemassa olevien tehtävien määrä ja resurssitarve on kasvanut merkittävästi kyberturvallisuuden merkityksen kasvaessa yhteiskunnassa. Kyberturvallisuuskeskuksen vastaanotettujen poikkeamailmoitusten määrä on kolminkertaistunut viimeisen kahden vuoden aikana. Lisäksi kyberturvallisuushäiriöt ja -hyökkäykset ovat yhteiskunnan kannalta entistä laajavaikutteisimpia ja niiden hoitaminen edellyttävät aiempaa suurempaa resursointia. Tietojärjestelmien arviointitoiminnan tarve on kasvanut merkittävästi ja arviointitehtävistä voidaan nykyisellä resursoinnilla hoitaa vain ne, jotka ovat valtio johdon ja yhteiskunnan toimivuuden kannalta aivan kriittisimpiä. Arviointitoiminta on yksi keskeisimmistä työkaluista, jolla eri toimijoiden kyberturvallisuuden taso voidaan varmistaa.

Kyberturvallisuuskeskuksella on oltavat osaavat ja hyvin resursoidut vastinparit viranomaistönsä ja elinkeinoelämässä. Ilman tätä yhteiskuntaan ei pystytä luomaan tulevia vuosia varten riittävää osaamista ja kyvykkyyksiä, jotka ovat välttämättömiä sietokyvyn lisäämiseksi kyberhäiriöitä ja -hyökkäyksiä vastaan ja toisaalta niistä toipumiseksi. Muun muassa Kyberturvallisuuden kehittämisohjelma sekä tietoturvan ja tietosuojan parantamista kriittisillä toimialoilla koskevan periaatepäätös tähtäävät näiden varmistamiseen. Näiden toimenpiteille ei kuitenkaan ole osoitettu riittävää rahoitusta, jolloin vaarana on Suomen kyberturvallisuuden tilan heikentyminen ja puutteellinen kyky vastata kyberturvallisuushaasteisiin. Seuraavassa on listattu muita Kyberturvallisuuskeskuksen tehtäviä, joiden budjettirahoitus ei ole tällä hetkellä varmistunut.

Sertifiointiviranomaistehtävä

Kyberturvallisuuskeskus on sähköisen viestinnän palveluista annetun lain (SVPL) 304 §:ssä nimetty EU:n kyberturvallisuusasetuksen (EU) 2019/881 mukaiseksi sertifiointiviranomaiseksi, mutta lakiin perustuvan tehtävän hoitamiseksi ei ole myönnetty budjettirahoitusta. EU:n sertifiointikehyksestä aiheutuvien tehtävien hoitamiseksi ja niiden edellyttämään resursointiin on haettu 0,39 milj. € vuodelle 2022 ja vuodesta 2023 alkaen vuosittaista 0,65 milj. € määrärahaa. Tämä määräraha-tarve on vähimmäisrahoitustarve, joka mahdollistaa tyydyttävällä tasolla tehtävien hoitamisen. Ilman rahoitusta tehtäviä ei voida hoitaa tai sen edellyttämät resurssit joudutaan irrottamaan muusta toiminnasta. Sertifiointitoiminnan tarkoituksena on varmistua siitä, että tuotteen tai palvelun kyberturvallisuuden taso on riittävä.

EU:n kyberkompetenssikeskuksen kansallisen koordinaatiopisteen tehtävät

Hallituksen esityksessä (HE 157/2021) esitetään tarvittavia muutoksia SVPL:ään ja Liikenne- ja viestintävirastosta annettuun lakiin Kyberturvallisuuskeskuksen nimeämiseksi EU:n Kyberosaamiskeskusta koskevassa asetuksessa (EU) 2021/887 tarkoitettuksi kansalliseksi koordinaatiokeskukseksi. Kyberturvallisuuskeskukselle nimeämisen myötä tulevia uusia tehtäviä olisivat erityisesti kansallisen tason kyberturvallisuusalan sidosryhmistä koottavan ekosysteemin rakentamiseen, koordinointiin ja osaamis yhteisön kansallisena verkostojohtajana toimimiseen liittyvät tehtävät. Tehtävän hoitamiseksi on ehdotettu 0,5 milj. € vuosittaista pysyvää määrärahaa vuodesta 2022 alkaen.

Kyberturvallisuuskeskuksen nimeämisestä kansalliseksi koordinoitikeskukseksi aiheutuvia määrärahatarpeita ei voida kattaa Liikenne- ja viestintäviraston nykyisistä määrärahoista. Koordinoitikeskuksen tehtävien hoitamisen edellyttämä jatkuva vuosittainen rahoitustarve on 1,0 milj. € vuodesta 2022 alkaen. Tästä rahoitustarpeesta 50 prosenttia eli puuttuvat 0,5 milj. € katetaan EU-rahoituksella, jonka osalta aikataulu on tällä hetkellä vielä epävarma. EU-rahoituksen saamiseksi tarvitaan vastaava määrä eli ehdotetut 0,5 milj. € kansallista rahoitusta. Kansallisen rahoituksen puuttuminen tarkoittaa, että ilman kansallista rahoitusta kansallinen

koordinointikeskus ei tule myöskään samaan Suomelle varattua EU-rahoitusta. Mikäli EU-rahoitus myöhemmin lakkaisi, puuttuva rahoitustarve tulisi kattaa lisämäärärahalla tai toiminnan supistamisella.

Kuntien tietoturvallisuuden kehittäminen

Yhteiskunnan toiminnan jatkuvuuden kannalta on välttämätöntä varmistaa kaikkien yhteiskunnan keskeisten toimialojen riittävä suojautuminen ja palautuminen kyberuhkista. Kunnat ja kuntayhtymät järjestävät asukkailleen laajasti erilaisia palveluita, joista suurin osa on määritelty kuntien tehtäviksi laissa ja osa näistä voi olla kriittisiäkin. Näiden palvelujen toteuttaminen on muun yhteiskunnan tavoin yhä riippuvaisempaa erilaisista digitaalisista ohjelmistoista, järjestelmistä ja tietoverkoista. Tämä altistaa kunnat muun yhteiskunnan tavoin lisääntyvälle kyberrikollisuudelle ja tietotekniikkaan liittyville häiriöille. Kuntasektoriin kohdistuneet kyberturvallisuushäiriöt ja -hyökkäykset ovat aiheuttaneet ja voivat aiheuttaa jatkossa mittavia jopa miljoonien eurojen taloudellisia vahinkoja ja kansalaisten digitaaliseen yhteiskuntaan kohdistuvan luottamuksen horjumista. Vastaavasti näköpiirissä oleva julkisen talouden rahoitusaseman heikentyminen edellyttää yhteisiä ja kustannustehokkaita ratkaisuja kuntien kyberturvallisuuden kehittämiseksi.

Kuntasektorin palveluita suunnitellaan Liikenne- ja viestintävirastossa vuosien 2020-2022 aikana valtiovarainministeriön myöntämällä erillishoiduksella osana Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelmaa (Haukka). Kuntasektorin tukeminen ja vuosien 2020-2022 suunniteltavien palvelujen jalkauttaminen edellyttää riittävää ja pysyvää resursointia määräaikaisen rahoituksen päättymiseen varautumiseksi vuonna 2022 ja siitä eteenpäin vuodesta 2023 alkaen. Tehtävään on ehdotettu 0,13 milj. € vuodelle 2022 ja 0,49 milj. € pysyvää määrärahaa vuodesta 2023 alkaen.

Galileon PRS-palvelun toteuttaminen ja tuottaminen Suomessa sekä PRS-viranomaisen tehtävien resursointi

Tehtävien resursointiin on haettu rahoitusta osoitettua enemmän. Rahoitusta on myönnetty 0,2 milj. €, kun vuosittainen pysyvä rahoitustarve tehtävän hoitamiseen on 0,32 milj. €.

Taloudellisen tilanteen vaikutukset Liikenne- ja viestintävirastossa

Kyberturvallisuustehtäviä koskeva lainsäädäntö, kyberturvallisuuden kehittämisohjelma sekä tietoturvan ja tietosuojan parantamisesta kriittisillä toimialoilla annettu periaatepäätös ohjaavat keskeisesti Kyberturvallisuuskeskuksen toimintaa.

Lainsäädäntömuutokset ja kyberturvallisuutta koskevista periaatepäätöksistä osoittavat toimenpiteet eivät kuitenkaan aina kytkeydy valtion talousarvion valmisteluun ja sitä kautta viraston toiminnan rahoituksesta tehtäviin päätöksiin. Nykyiset toimintamenomomentin määrärahat on mitoitettu Liikenne- ja viestintävirastolle tällä hetkellä säädettyihin tehtäviin, eikä uusien lakisääteisten tehtävien hoitamiseen ole olemassa tarvittavia resursseja.

Uusien asetuksesta seuraavien tehtävien hoitaminen nykyisillä resursseilla vaarantaisi myös Liikenne- ja viestintäviraston vastuulle nykytilanteessa säädettyjen tehtävien hoitamisen, sillä nykyisillä resursseilla niitä ei enää kyettäisi hoitamaan tehtävien edellyttämällä resursseilla.

Kyberturvallisuuskeskuksen tehtävien määrä ja niiden edellyttämä resursointi suhteessa rahoitukseen on ollut epätasapainossa pitkään. Se mitä Kyberturvallisuuskeskukselta edellytetään ja vaaditaan yhteiskunnan turvaamiseksi, ei vastaa sen rahoituksen ja resurssien tasoa. Kyberturvallisuuden yhteiskuntaa läpileikkaavan

luonteen ja verkostomaisen toimintamallin vuoksi myös Kyberturvallisuuden kehittämisohjelman rahoitus on keskeistä, jotta Kyberturvallisuuskeskuksen toimintaedellytyksen sen laajan toimintakentän suuntaan voidaan turvata.



Jarkko Saarimäki
Pääjohtajan sijainen, ylijohdaja

Liikenne- ja viestintävirasto Traficom