15.11.2021

Kyberturvallisuuden rahoitus

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. Jäljempänä on esitetty, mitä tällä hetkellä liikenne- ja viestintäministeriön hallinnonalalla myönnetyllä rahoituksella saadaan tehtyä ja mitä jää tekemättä.

1) Kyberturvallisuuden kehittämisohjelma

Valtioneuvosto antoi periaatepäätöksen kyberturvallisuuden kehittämisohjelmasta 10.6.2021. Suomen kyberturvallisuusstrategian mukaisesti kehittämisohjelma ulottuu yli hallituskausien, aina vuoteen 2030 saakka. Kehittämisohjelma perustuu hallitusohjelman linjauksiin ja lisäksi kehittämisohjelma on osa yhteiskunnan turvallisuusstrategian ja EU:n kyberturvallisuusstrategian toimeenpanoa.

Toteutuessaan kyberturvallisuuden kehittämisohjelma vahvistavaa kansallista kyberturvallisuutta, pienentäen samalla nykyisistä puutteista tai kapeikoista johtuvia kyberturvariskejä. Kehittämisohjelma luo Suomeen kyberturvallisuuden ekosysteemin, joka tuottaa elinvoimaa ja kasvua, lisää alan työpaikkoja, luo tarvittavaa osaamista ja parantaa digitaalisen yhteiskunnan kestävyyttä sekä sietokykyä kybertoimintaympäristön eri ilmiöitä vastaan.

Kehittämisohjelman rahoitus vuodelle 2022

Vuodelle 2022 kehittämisohjelman toimeenpanoon on käytettävissä n. 2,2 milj. euroa. Jäljellä olevassa rahoituksessa on myös kyberturvallisuusjohtajan tehtävän palkkaus vuodelle 2022.
Kehittämisohjelman rahoitusta edellyttävistä toimenpiteistä vuonna 2022 pystytään toteuttamaan:

- Kaikkia koulutusasteita koskeva tutkimus koulutusohjelmien muutostarpeista kyberturvallisuuden osalta, valmistuu 31.5.2022.
- Tunnistetaan yhteiskunnan kannalta kriittiset tietovarannot, -palvelut ja -järjestelmät ja aloitetaan toimenpiteet, joilla varmistetaan näiden toiminta sekä turvallisuus.
- Turvallisuusviranomaisten keskitetysti järjestetyt tekniset kyberturvakoulutukset kansallisten kyvykkyyksien kehittämiseksi.
- Vapaaehtoisuuteen perustuvien kyberturvayhteisöjen toiminnan tukeminen, kyberalan osaajapulan paikkaamiseksi.
- Kotimaiseen teknologiaan perustuvan turvallisen puhekommunikaation käyttöönoton edistäminen valtion johdolle ja eri viranomaisille.
- Pieniä panostuksia ekosysteemin kehittämiseen mm. osaaminen ja suomalaisen osaamisen viennin edistäminen.

Liikenne- ja viestintäministeriö
Käyntiosoite Eteläesplanadi 16 Helsinki
Postiosoite PL 31 00023 Valtioneuvosto
Puhelin 029516001
www.lvm.fi
etunimi.sukunimi@lvm.fi
kirjaamo@lvm.fi

Kehittämisohjelman rahoitusvaje

Ilman pitkäaikaista rahoitusta kehittämisohjelman kärjet, kotimainen salaustuoteperhe ja AQUA-statuksen saavuttaminen jäävät toteutumatta.
Digitaalisessa toimintaympäristössä on ensiarvoisen tärkeää, että salassa pidettävien ja henkilötietojen eheys sekä luottamuksellisuus säilyvät. Kotimaisen salaustuoteperheen kehittämisen, testauslaboratoriokyvykkyyden ja tutkimuksen avulla Suomi voi hakea EU:n salaustuotteiden sertifiointeja hyväksyvän AQUA-maan (Appropriately Qualified Authority) asemaa viimeistään vuonna 2028. Pelkästään salaustuotteiden EU-markkinat ovat miljardiluokkaa. Eräiden arvioiden mukaan ruotsalaiselle kyberteollisuudelle AQUA-maan asema ja tarvittavan salaustuotelaboratoriotoiminnan kehittäminen ovat synnyttäneet suoraan ja välillisesti tuhansia työpaikkoja.

Kansallisten kyvykkyyksien kehittäminen ja AQUA-statuksen saavuttaminen ovat edellytys kansallisen kyberomavaraisuuden kehittämiselle ja kansalliselle turvallisuudelle. Lisäksi edellä mainitut toimenpiteet edesauttaisivat suomalaisten salaustuotteita kehittävien yritysten pääsyä kansainvälisille markkinoille, edistäisivät alan työllisyyttä ja lisäisivät Suomen turvallisuusviranomaisiin kohdistuvaa kansainvälistä luottamusta.

Vuositasolla kehittämisohjelman monivuotiset toimenpiteet ja kyberturvallisuusjohtajan tehtävän palkkaus, edellyttävät yhteensä 4,9 milj. euron vuotuista määrärahaa.

RRF-rahoituksen piiriin kuuluvat kyberturvallisuushankkeet

Kyberturvallisuushankkeisiin on kanavoitu rahoitusta myös RRF-rahoituksen kautta:

Civilian cyber security skills: EU:n laajuinen kolmevuotinen tutkimushanke, jossa tutkimuksen ja pelillistämisen avulla parannetaan kyberturvallisuusosaamista koko EU:n alueella, kaikilla virallisilla EU-kielillä. Hankkeen kilpailutus on käynnissä ja sen kokonaisrahoitus yhteensä viisi miljoonaa euroa.

Cybersecurity exercises: kansalliset teknistoiminnalliset kyberturvallisuusharjoitukset, jotka sisältyvät kyberturvallisuuden kehittämisohjelmaan. Viiden miljoonan euron rahoitus turvaa harjoitustoiminnan vuoden 2025 loppuun saakka. Harjoituksissa koulutetaan vähintään 2000 kyberturvallisuuden parissa työskentelevää julkishallinnon henkilöä.

2) Tietoturvallisuuden ja tietosuojan parantaminen kriittisillä toimialoilla

Periaatepäätöksen tehtäviin on arvioitu tarvittavan 21htv, jota on karsittu ensin 15 htv ja sitten 13 htv:hen. Rahoitus on arvioitu nyt 1,6 miljoonan euron tasolle. Alla oleva arvio perustuu oletukseen 1,6 miljoonan euron rahoituksesta.

Ottaen huomioon, että jo nykyisen lainsäädännön mukaisten valvovan viranomaisen tehtävin hoitamiseksi virastolle osoitetut resurssit ovat alimitoitetut, resurssien vähentäminen aikaisemmassa arvioinnissa esitetystä heikentää merkittävästi viraston mahdollisuuksia ohjata ja valvoa sille kuuluvia kriittisiä toimialoja, saati toteuttaa uusia toimenpiteitä tietoturvallisuuden parantamiseksi ko. toimialoilla.

Nyt uudelleen arvioiduilla resursseilla on mahdollista toteuttaa **minimitasolla** pääosa liikenne- ja viestintävirastolle jo lainsäädännössä ja TITUKRI-hankkeessa osoitetuista tehtävistä, mutta joidenkin toimenpiteiden toteuttamisesta voidaan joutua luopumaan tai suunniteltua aikataulua merkittävästi siirtää myöhemmäksi. Lisäksi joidenkin

toimenpiteiden vaikuttavuus jää suunniteltua vähäisemmäksi. Kaikkien osoitettujen tehtävien hoitaminen hyvällä tasolla ja vaikuttavasti vaatisi lisäresurssien kohdentamista virastolle jossain vaiheessa hanketta ja siinä toteutettavia toimenpiteitä. Myös TITUKRI-hankkeen myötä mahdollisesti uudet lainsäädännössä asetettavat tehtävät voivat lisätä resurssitarpeita nyt esitetystä ja näitä tulee arvioida erikseen lainsäädännön valmistelun yhteydessä.

Nyt alla olevassa uudelleen arvioinnissa on arvioitu vähimmäismäärää, jolla nykyiset lainsäädännöstä ja TITUKRI-hankkeen myötä esitetyt toimenpiteet saadaan toteutettu välttävällä tasolla. Lisäksi arvioinnissa on pienennetty yhden henkilötyövuoden kustannusta.

Liikennesektorin vaikutukset:

Ilmailun, merenkulun, raideliikenteen ja tieliikenteen osalta TiTUKRIrissa esitettyjen toimintaa koskevien tietoturvamääräysten antaminen sekä prosessien määrittelyn ja auditointien ohjaus ja valvonta edellyttävät liikennemuotojen, alan organisaatioiden ja logistiikkaketjujen erittäin laaja-alaista ymmärtämistä. Liikennemuodoille ei ole annettu tällä hetkellä riittäviä määräyksiä liikennemuotojen tietoturvallisuudesta. Lisäksi kriittisille toimialoille säädetään velvoite määritellä kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot sekä auditoida säännöllisesti kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot. Virastolla ei ole käytettävissään resursseja valmistella, antaa tai valvoa määräysten tai uusien velvoitteiden noudattamista.

Vuodelle 2021 nyt suunnitellulla rahoituksella voidaan aloittaa TITUKRIrissa määriteltyjen toimenpiteiden suorittaminen. Rahoitustaso ei kuitenkaan mahdollista kaikkia liikennemuotoja koskevan riittävän tietoturvaosaamistason rakentamista virastolle. Vastaavasti rahoituksen määräaikaisuus estää vakituisen henkilöstön palkkaamisen, mikä rajoittaa merkittävästi rekrytointimahdollisuuksia ja estää suunnitelmallisen osaamisen kehittämisen. TITUKRIssa määriteltyjä toimenpiteitä ei pystytä niiden pysyväisluonteesta johtuen saattaa osaksi viraston normaalia toimintaa, eikä esimerkiksi kaikkia määräyksiä saataisi valmistelua vuoden kuluessa. Myöskään määräysten kehittämistä ja valvontaa sekä muun toiminnan ohjausta ja valvontaa ei pystyttäisi toteuttamaan siten, että sillä olisi riittävä ohjaava vaikutus erittäin haastavassa taloudellisessa tilanteessa toimiviin alan yrityksiin ja muihin tahoihin.

Viestintäsektorin vaikutukset:

TITUKRI:n kiireellisyysluokan kartoituspalvelua ei voitaisi tehdä lainkaan. Tämä tarkoittaisi että, Suomen 15 suurimman kunnan tietoturvan ja tietosuojan tasoa terveydenhuollossa, sosiaalihuollossa, energiahuollossa ja vesihuollossa ei voitaisi selvittää. Suomen 15 suurimman kunnan kriittiset palveluiden mahdolliset haavoittuvuudet jäävät selvittämättä, joka altistaa ne mahdollisille kyberhyökkäyksille.

Kyberturvallisuuskeskus ei pystyisi tarjoamaan tietoturvan koulutusta lainkaan NIS-sektoreiden tietoturvaa valvoville viranomaisille. Tämä tarkoittaisi sitä, että eri sektoreilla tietoturvavalvonnan parissa työskentelevien tietotaito olisi puutteellinen.

Yksityishenkilöille ja organisaatioiden edustajille suunnattu palvelu (esimerkiksi mobiili-päätelaitteeseen asennettava sovellus), jonka kautta on mahdollista saada kohdennetusti ajankohtaista tietoa tietoturvauhkista ja -loukkauksista ja tietoturvallisuutta koskevista ohjeista sekä ilmoittaa tietoturvauhkista ja -

loukkauksista Kyberturvallisuuskeskukselle, kriittisen toimialan valvovalle viranomaiselle ja/tai poliisille, jää kokonaan toteuttamatta.

3) Kansallisen kyberturvallisuuden sertifiointiviranomaisen lakisääteinen tehtävä

Haettu rahoitusta vuonna 2020 8htv ja 2021 5htv. Rahoitusta ei ole myönnetty lainkaan. Sertifiointiviranomaisen tehtävien hoitamiseen liittyvä työ menisi sertifiointien osalta CAA-viranomaistoiminnan salaustuotehyväksyntätoiminnon työjonoon, jossa on jo noin 12 kk työjono. Samassa jonossa olisi aikanaan muun muassa kansallinen TL II -salain ja muut kehittämisohjelman tavoitteet. Sertifiointitoimijoiden akkreditointi menisi arviointilaitoksien ohjauksen ja valvonnan työjonoon. Arviointilaitoksien ohjauksen ja valvonnan resursointi on tällä hetkellä 1 htv ja työjonoa 8 kk. Sertifiointitoiminnassa ei voi olla työjonoa tuotteiden ja palveluiden nopean elinkaaren vuoksi. Tehtäviä ei kyettäisi siis hoitamaan lainkaan siten, että sertifikaattitoiminnasta saataisiin hyötyjä ja elinkeinoelämän odotukset täyttyisivät.

Vaikutus:

Suomalaiset yritykset eivät pysty kilpailemaan eivätkä kasvattamaan liiketoimintaansa digitaalisilla sisämarkkinoilla tai niiden ulkopuolella, erityisesti datatalouden ja esineiden internetin osalta. Suomessa viranomainen ei pysty takaamaan, että sertifiointikehyksien mukaisissa tuotteissa, palveluissa ja prosesseissa (mm. valmisteilla olevat pilvipalveluiden ja IoT-laitteiden sertifiointikehykset) varmistetaan kehyksen määrittelemä peruskyberturvallisuuden taso. Kyberturvallisuussertifioinnilla on myös olennainen rooli lisättäessä viestinverkkojen ja -palvelujen turvallisuutta ja luotettavuutta sekä viestintäverkoissa käytettävien verkkolaitteiden turvallisuuden varmistamisessa.

4) EU kyberkompetenssikeskuksen kansallisen koordinaatiopisteen lakisääteiset tehtävät

Täydentävään talousarvioon on esitetty 750 000 euron rahoitusta vuodelle 2022. Valtioneuvosto antaa HE:n täydentävästä talousarviosta torstaina 18.11.2021.

5) PRS-viranomaisen tehtävät

Hallituksen talouspoliittinen ministerivaliokunta linjasi marraskuussa 2020, että Suomi ottaa vuoden 2024 aikana kansallisesti käyttöön Galileo-järjestelmän julkisesti säännellyn sijainti- ja aikapalvelun. Tämän linjauksen mukaisesti PRS-palvelun toteuttamiseksi on haettu ja myönnetty linjausta vastaava vuosittainen määräraha pois lukien vuoden 2024 osalta, jonka osalta määrärahaa myönnettiin vain 2 200 000 euroa hallituksen talouspoliittisen ministeriövaliokunnan linjaaman 4 815 000 euron sijasta. Myönnetyllä rahoituksella kyetään toteuttamaan tarvittava järjestelmähanke, mutta sen vaatimat konesalitilaratkaisut operointivaihetta ajatellen vaativat puuttuvan rahoituksen myöntämisen.

PRS-järjestelmän kansallisen infrastruktuurin toteuttaminen ja sen käytön aloittaminen hallitusti edellyttävät neljän perehdytetyn lisähenkilön työpanosta ennen palvelun käyttöönottoa vuonna 2024. Vuosien 2022-2025 kehyksessä PRS-viranomaistehtäviin on myönnetty 200 000 euroa vuodessa.

Vaikutus: Ilman vaadittavia henkilöstöresursseja, PRS-palvelua ei ole mahdollista valmistella ja ottaa tuotantokäyttöön vuonna 2024.

6) Kyberturvallisuuden korjausvelka

Kyberturvallisuusongelmissa Kyberturvallisuuskeskuksen apua tarvitsevia kansalaisia ja yhteiskunnan kriittisten toimialojen toimijoita on joka vuosi entistä enemmän. Kasvavaan tuen tarpeeseen vastaaminen tulee edellyttämään lisärahoitusta. Resurssitarve 390 000€ vuodessa.

Vaikutus: Kyberturvallisuuskeskus ei pysty hoitamaan kolmikertaistuneita tapausmääriä eikä ensivastetoiminta ole kyennyt käsittelemään kaikkia tapauksia tilanteissa, joissa on samanaikaisia kyberhäiriöitä. Kyberturvallisuuskeskuksen ensivastetoiminnon asiantuntijakäsittelyä vaativa tapausmäärä oli vuosina 2015-2019 4000-6000 tapausta vuodessa. Vuonna 2020 se oli 16 000 tapausta ja vuoden 2021 lokakuun loppuun mennessä se on ollut jo 20 000 tapausta.