

Eduskunta

Valtiovarainvaliokunta, hallinto- ja turvallisuusjaosto

Viite: HE 154/2022 vp, lausuntopyyntö

Lausunto: Esitys valtion talousarvioksi 2023

Teknologiateollisuus sekä Kyberala kiittävät mahdollisuudesta lausua asiasta. Finnish Information Security Cluster – Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa. Viittaamme tässä yhteydessä Teknologiateollisuuden lausuntoon, päivätty 11.10.2022.

Suomessa toimivalla kyberturvallisuusteollisuudella on kaksinaisrooli: alan tuotteet, palvelut ja osaaminen varmistavat kansallista, koko yhteiskunnan laajuista resilienssiä, huoltovarmuutta ja kyberturvallisuutta, mutta alalla on myös merkittävä potentiaali vientiteollisuutena. Näin ollen kyberturvallisuuden rahoitusta tulisikin kohdentaa optimaalisemmin:

- Toimeenpanemalla kyberturvallisuuden kehittämisohjelma täysimääräisesti kansallisen ekosysteemin luomiseksi sekä kohdistamalla rahoitusta kyberturvallisuuden tutkimukseen ja tuotekehitykseen sekä tehokkaaseen markkinoille saattamiseen
- Alan yritysten tuotteita ja ratkaisuja koskevat salaustuotteiden hyväksyntäjonot tulisi purkaa, kansallinen AQUA-status (EU Appropriately Qualified Authority) varmistaa, sekä hyväksyä ennakollisesti riittävällä laajuudella tulevan kyberkestävyyssäädöksen edellyttämiä arviointilaitoksia digitaalisia elementtejä sisältävien tuotteiden turvallisuusarviointeja varten.
- PK-sektorin yritysten digiturvan parantamista on edelleen tuettava jatkamalla ja laajentamalla tänä vuonna hyväksytyn ns. tietoturvasetelin avulla.
- Oikeus- ja sisä- asiainhallinnon osalta panostuksia tulee kohdentaa täsmällisemmin kyberrikosten rikosvastuun toteuttamiseen tähtäävään toimintaan, sillä muu yhteiskunta ei kykene yksinään huolehtimaan rikoksilta suojautumisesta.
- Puolustusvoimien tutkimus-, kehittämis- ja innovaatiotoiminnan (TKI) rahoituksen erillisyydestä pidetään kiinni ja sen taso turvattava.

Alla täsmällisempi kuvaus toimista ja budjetoinnista hallinnonaloittain.

Liikenne- ja viestintäministeriön hallinnonala:

1. AQUA-status ja suomalaisen salauserhetuotteen kehittämisen tukeminen

Salaustuotteet ovat digitaalisen turvallisuuden kulmakivi, joille on EU-tasolla miljardien eurojen markkinat. Salaustuotteilla on merkittävä rooli suomalaisen kyberteollisuuden ekosysteemin kehittämisen, sekä yhteiskunnan laaja-alaisen kyber-resilienssin vahvistamisen osalta.

25.10.2022

Suomalaisten yritysten edellytyksiä salaustuotteiden kehittämiseen ja valmistamiseen on määrätietoisesti edistettävä. Suomessa on huomattavaa salaustuotteisiin liittyvää osaamista, jonka avulla on mahdollista suojata suomalaista tietoyhteiskuntaa nykyistä paremmin. Samalla voidaan luoda tilaisuuksia viennille, erityisesti kun Suomen lähestyvä Nato-jäsenyys avaa tulevaisuudessa kokonaan uusia mahdollisuuksia kaupalliseen yhteistyöhön läntisten kumppanimaiden kanssa. Tämä kuitenkin edellyttää panostuksia kansallisen salaustuoteperheen parantamiseen sekä kryptologiastrategiatyön vakiinnuttamiseen.

Suomalaisen korkean tason salaustuotteisiin liittyvän osaamisen ulosmittaaminen edellyttää, että Suomi tavoittelee AQUA-statusuksen (Appropriately Qualified Authority) saavuttamista, eli kansainvälisiä tietoturvahyväksyntöjä myöntävän maan asemaa. AQUA-status on myönnetty toistaiseksi Ranskalle, Saksalle, Italialle, Alankomaille ja Ruotsille. Vientimarkkina on laajuudeltaan miljardeja euroja.

Jäsenvaltio, jolle AQUA-status on myönnetty, kykenee tuottamaan ja hyväksymään kansainvälisesti hyväksyttyjä salausratkaisuja, joita voidaan hyödyntää salaisen tai luottamukselliseksi luokitellun EU-tiedon salaamisessa tai välittämässä. Vaatimuksena on riittävä osaamispohja, joka mahdollistaa salausratkaisujen jatkuvan kehittämisen ja tuottamisen, sekä riittävän testauslaboratoriotoiminnan tuotteiden testaamista varten.

Kyberala ry ehdottaa, että AQUA-statusuksen saavuttamiseksi vaadittavien kyvykkyyksien rakentamista, sekä kansallisen salaustuoteperheen parantamista ja kryptologiastrategian vakiinnuttamista varten myönnetään Liikenne- ja viestintäministeriön hallinonalalle **5 miljoonaa euroa vuosittain** vuoden 2023 ja 2024 aikana.

2. Kyberturvallisuuskeskuksen kansallisen kyberturvallisuuden sertifiointiviranomaisen lakisääteisen tehtävän eli CAA-viranomaistoiminnan salaustuotteiden hyväksyntätoiminnon työjonon poistaminen.

Liikenne- ja viestintävirasto Traficom alainen Kyberturvallisuuskeskus hyväksyy kansainvälisten tietoturvavelvoitteiden mukaisesti salaustuotteet, joilla suojataan kansainvälistä turvallisuusluokiteltua tietoa Suomessa. Hyväksynnästä vastaa Kyberturvallisuuskeskuksen NCSA-toiminto, josta käytetään EU:ssa lyhennettä CAA (Crypto Approval Authority).

CAA-viranomaistoiminta on Suomessa kroonisen aliresursoitua, mikä on johtanut merkittäviin työjonoihin hyväksyntätoiminnossa. Työjonojen vuoksi salaustuotteita valmistavat yritykset joutuvat odottamaan hyväksyntää tuotteilleen pitkiä aikoja. Tämän seurauksena tuotteiden saattaminen markkinoille viivästyy, mikä saattaa pahimmillaan haitata merkittävästi yrityksen liiketoiminnan kehitystä sekä estää vientimahdollisuuksien syntymistä.

Kansallisen kyberturvallisuuden sertifiointiviranomaisen tehtävien resursointiin on varattu valtion talousarvioesityksessä 0,3 miljoonaa euroa vuodelle 2023. Kyberala ry vaatii, että määräraha nostetaan vähintään **0,8 miljoonaan euroon** salaustuotteiden hyväksynnän työjonon purkamisen mahdollistamiseksi.

3. EU:n tulevan kyberkestävyyssäädöksen kansallisen toimeenpanon valmistelu

25.10.2022

Euroopan komissio julkaisi 15.9. esityksen EU:n kyberkestävyyssäädöksestä, joka asettaa toteutuessaan tietoturvaan koskevat vaatimukset horisontaalisesti kaikille verkkoon kytkettäville ohjelmistoille ja laitteille niiden koko elinkaaren ajaksi, erikseen määriteltyjä poikkeuksia lukuun ottamatta.

Esitys etenee Euroopan parlamentin ja jäsenmaiden käsittelyyn. Kun esitys on hyväksytty, se astuu voimaan 24 kuukauden siirtymäajan jälkeen kaikissa EU:n jäsenmaissa. Odotettavissa oleva aikataulu edellyttää, että kyberkestävyyssäädöksen toimeenpanon kansallinen valmistelu aloitetaan vuonna 2023.

Esityksen mukaan tietoturvan näkökulmasta kriittisiksi määriteltyt ohjelmistot ja laitteet on todettava säädöksen asettamien vaatimusten mukaisiksi kolmannen osapuolen toteuttamassa hyväksyntämenettelyssä (conformity assessment). Tämä edellyttää, että säädöksessä asetettavien vaatimusten mukaisia hyväksyntämenettelyjä tekevien hyväksyntälaitosten akkreditoiminen aloitetaan vuonna 2023, ja että tähän varataan riittävät resurssit.

Sisäministeriön hallinnonala:

1. Kyberrikollisuuden torjunta

Pitkälle edennyt ja jatkuvasti kehittyvä digitalisaatio on tarjonnut alustan kyberympäristössä tapahtuvien rikosten merkittävällä kasvulla. Erilaiset tietoturvaloukkaukset aiheuttavat vuosittain maailmanlaajuisesti biljoonien eurojen kustannukset. Kyberrikollisuuden menestyksekkäs tutkiminen, sekä rikosten tekijöiden vastuuseen saattaminen ovat välttämättömyksiä turvallisille, digitalisoituneille yhteiskunnille.

Poliisitoimelle myönnetty määrärahat ovat kokonaisuudessaan oikeasuhtaiset. Määrärahoja on kuitenkin ohjattava poliisitoimen sisällä nykyistä enemmän tietojärjestelmien uudistamiseen sekä kyberrikosten torjuntaan ja tutkimiseen.

Kyberala ry vaatii, että Poliisitoimen määrärahoista korvamerkitään kyberrikosten tutkintaan ja tutkinnan valtakunnalliseen kehittämiseen yhteensä **3 miljoonaa euroa**.

Oikeusministeriön hallinnonala

1. Kyberrikosten käsittely oikeudenhoidossa

Aktiivinen ja tehokas rikollisuuden torjunta ja rikosvastuun toteutuminen digitaalisessa ympäristössä edellyttää, että kyberrikosten käsittelyyn liittyvä osaaminen vahvistuu kaikilla oikeudenhoidon osa-alueilla.

Kyberala ry vaatii, että oikeudenhoidon toteutumiseen kohdennetuista määrärahoista korvamerkitään varoja ainakin kolmen valtakunnallisen kybersyyttäjän nimittämiseksi sekä Tuomioistuinviraston tietojärjestelmäkehityksen nopeuttamiseksi yhteensä **2,5 miljoonaa euroa**.

Puolustusministeriön hallinnonala

1. TKI-toiminta ja viennin edellytysten tukeminen



25.10.2022

Kotimaisen kyberturvallisuusteollisuuden ekosysteemin kehittyminen, kyberturvallisuusteollisuuden keskeisten tuotteiden kansallisen omavaraisuuden turvaaminen sekä alan toimijoiden kansainvälistymisen kiihdyttäminen edellyttävät, että Puolustusvoimien tutkimus-, kehittämis- ja innovaatiotoiminnan (TKI) rahoituksen erillisyydestä pidetään kiinni ja sen taso turvataan.

Kansainvälistymisen edellytysten tukeminen edellyttää, että valtionhallinnon eri sektorit ottavat vientiä tekevien yritysten tarpeet toiminnassaan huomioon ja tarjoavat riittävää tukea esimerkiksi vientilupamenettelyssä.

Lisätiedot:

Toimitusjohtaja Peter Sund
sähköposti: peter.sund@teknologiateollisuus.fi
puhelin: 050 565 0621