Kyberturvallisuuden rahoitus, ydinviestit

- **Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on Suomen kyberturvallisuuden kivijalka**. Muuttunut uhkaympäristö, virastoihin kohdistuvat tuottavuustoimenpiteet sekä uudet lakisääteiset tehtävät edellyttävät Kyberturvallisuuskeskuksen riittävän rahoituksen varmistamista ja toiminnan turvaamista.

- Kyberturvallisuuden rahoitustarpeet on priorisoitu. **Rahoitusta esitetään vain niille toimenpiteille, joiden arvioidaan olevan kaikista kriittisimmät kyberturvallisuuden tason säilyttämiseksi muuttuneessa turvallisuusympäristössä.**

- Ilman riittäviä panostuksia kyberturvallisuuteen ei voida ylläpitää yhteiskunnan kokonaisturvallisuutta. Kyky reagoida ja varautua yhteiskuntaa uhkaaviin kyberhyökkäyksiin heikkenee ja **alttius vakaviin tietomurtoihin, yhteiskunnan ydintoimintoihin kohdistuviin kiristyshaittaohjelmahyökkäyksiin ja vihamielisten toimijoiden kybervakoilulle kasvaa merkittävästi**, mikäli resursointia ei ole turvattu.

- **Kyberturvallisuuskeskuksen toimintamenot vuodelle 2025 ovat noin 28 miljoonaa euroa**. Vuoden 2025 TAE:ssa Kyberturvallisuuskeskukselle myönnettiin lisärahoitusta NIS2-toimeenpanoon sekä HAVARO- ja Hyöky-palveluiden tuottamiseen 2,66 miljoonaa euroa. Tuottavuustoimien ja toimintamenosäästöjen vuoksi lisärahoituksella saavutettiin nettovaikutus mahdollistaen vain nykyisten toimintojen ylläpidon. **Tuottavuustoimenpiteitä ei voi jatkossa kohdistaa kyberturvallisuuden tehtäviin ilman, että ne heikentäisivät kansallista kyberturvallisuutta.**

- **Vuoden 2026 osalta tunnistettu lisärahoitustarve kaikista tärkeimpien toimenpiteiden osalta on 4,7 miljoonaa euroa. Vuosille 2026-2029 rahoitustarve on yhteensä noin 30 miljoonaa euroa**.

- Lisärahoitusta tarvitaan tietojärjestelmien ja turvallisuuskriittisten tuotteiden arviointitoiminnan kehittämiseen, kyberkestävyyssäädöksen tehokkaaseen toimeenpanoon, kyberuhkien havainnoinnin kehittämiseen sekä Huoltovarmuuskeskuksen rahoittamien palveluiden siirtämiseen valtion talousarvioon. Vuodesta 2027 eteenpäin rahoitusta tarvitaan myös kansallisten kyberturvallisuusharjoitusten (KYHA) toteuttamiseen ja harjoitusten laajentamiseen useammille organisaatioille.

    - **Näiden toimintojen ja palveluiden kehittäminen ja jatkuvuuden turvaaminen ovat tärkeä osa hallitusohjelman mukaisesti valmistellun kyberturvallisuusstrategian toimeenpanoa.**

- **Kyberturvallisuuden rahoituksella luodaan Suomeen myös kasvua** ja vahvistetaan Suomen asemaa kyberturvallisuusratkaisuiden ja -innovaatioiden kehittäjänä. Salaustuotteiden tehokas arviointi- ja hyväksyntäprosessi edistää kansallista ja EU-tason kyberturvallisuuden omavaraisuutta. **Vuoden 2026 täydentävään talousarvioesitykseen LVM ehdottaa 860 000 euron pysyvää määrärahaa salaus- ja turvallisuuskriittisten tuotteiden ja tietojärjestelmien vaatimustenmukaisuuden arviointitoiminnan tehostamiseen**

Tausta-aineisto

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen palveluilla ennaltaehkäistään ja havaitaan kyberhäiriöitä, reagoidaan niihin ja tuetaan niistä palautumisessa. Kyberturvallisuuskeskuksen palveluilla voidaan mm. havaita valtakunnallisesti tietoverkoissa olevia vakavia kyberuhkia. Keskus tuottaa tilannekuvaa kyberuhista valtiojohdolle, viranomaisille ja yksityiselle sektorille. Harjoitustoiminnalla harjoitellaan häiriötilanteita ennalta ja luodaan osaamista kyberhyökkäyksiin vastaamiseksi. Kyberturvallisuuskeskus toimii myös esimerkiksi kansallisena salaustuotteiden ja turvallisuusjärjestelyiden hyväksyntäviranomaisena.

Kyberturvallisuuskeskuksen valtion talousarviosta rahoitettavat toimintamenot vuonna 2025 ovat noin 20,8 miljoonaa euroa. Lisäksi Huoltovarmuuskeskus ohjelmarahoitus vuodelle 2025 on noin 7 miljoonaa eurolla. Vuoden 2025 talousarviossa Kyberturvallisuuskeskukselle myönnettiin lisärahoitusta NIS2-toimeenpanoon ja sen järjestelmäinvestointeihin sekä kevennetyn HAVARO- ja Hyöky-palveluiden tuottamiseen yhteensä 2,66 miljoonaa euroa. Samalla osana tuottavuustoimenpiteitä ja toimintamenosäästöjä viraston, ml. Kyberturvallisuuskeskuksen toimintamenoihin on kohdistettu säästöjä. **Vuoden 2025 toimintamenojen lisäyksellä oli siten vain nettovaikutus, joka mahdollisti nykyisten toimintojen jatkamisen nykytasolla.**

Kyberturvallisuuskeskuksen toiminnan ja palveluiden rahoituksen turvaaminen on myös osa kansallisen kyberturvallisuusstrategian toimeenpanoa. Strategian toimeenpanosuunnitelmassa on tunnistettu yhteensä 45 toimenpidekokonaisuutta, joilla saadaan parannettua ja ylläpidettyä suomalaisen yhteiskunnan kybersietoisuutta, kehitettyä kyberpuolustusta, vahvistettua kyberturvallisuuden ekosysteemiä ja sitä kautta lisättyä työllisyyttä sekä kyberturvallisuusalan vientiä. Kyberturvallisuusstrategian täysimääräinen toimeenpano edellyttäisi vuoden 2024 arvion mukaan yhteensä 95 miljoonaa euroa lisärahoitusta kyberturvallisuuteen kehyskaudelle 2026–2029.

Kyberturvallisuusstrategian toimeenpanosuunnitelman mukaisesti liikenne- ja viestintäministeriö ehdotti Liikenne- ja viestintävirasto Traficomin toimintamenoihin yhteensä 4,7 miljoonan euron lisäystä vuoden 2026 talousarvioon. Vuosien 2026-2029 julkisen talouden suunnitelmaan esitettiin yhteensä noin 29 miljoonan euron lisäystä **Esitetyillä lisäresursseilla olisi mahdollista ylläpitää kyberturvallisuuden nykyinen taso.**

LVM:n esitys sisälsi ehdotukset kansallisen havainnointikyvyn (HAVARO) turvaamisesta, tilannekuvatoiminnan ja verkostoyhteistyön ylläpidosta, keskitettyjen kyberturvallisuuspalveluiden kehittämisestä, tietojärjestelmien palveluiden ja turvallisuuskriittisten tuotteiden arviointitoiminnan kehittämisestä sekä kyberkestävyyssäädöksen (CRA) kansallisesta toimeenpanosta.

Kyberturvallisuuskeskuksen rahoituksen osalta haasteen muodostaa myös Huoltovarmuuslainsäädäntöön esitetyt muutokset. **LVM pitää tärkeänä, että Huoltovarmuuskeskuksen rahoittamat yhteiskunnan toimivuuden kannalta kriittiset palvelut rahoitettaisiin jatkossa valtion talousarviosta HVK:n hankerahoituksen sijaan.** Niiltä osin kuin rahoitusta ei siirretä valtion talousarvioon, osana lainsäädännön uudistusta tulisi varmistaa mahdollisuus rahoittaa kyberturvallisuutta Huoltovarmuuskeskuksen rahoituksella myös jatkossa.

Myös Valtiontalouden tarkastusvirasto (VTV) on suosittanut, että LVM:n ja VM:n tulisi pyrkiä varmistamaan vaaditut resurssit kyberturvallisuusstrategian toimenpiteille. Lisäksi Onnettomuustutkintakeskus (OTKES) on Helsingin kaupungin tietomurtotapauksen tutkintaselostuksessa suosittanut, että VM:n tulisi yhdessä LVM:n kanssa varmistaa riittävät kyvykkyydet julkisen hallinnon tietoturvapuutteiden havaitsemiseksi.

Kansallisten kyberturvallisuusharjoitusten rahoitus

Kunnille, terveydenhuollolle, valtionhallinnolle ja turvallisuusviranomaisille järjestettävät kansalliset kyberturvallisuusharjoitukset (KYHA) rahoitetaan keskitetysti EU:n elvytyspaketista vuoden 2025 loppuun saakka (1 miljoona euroa/vuodessa). Harjoituksissa simuloidaan laaja-alaisesti eri yhteiskunnan toimijoihin samanaikaisesti kohdistuvia kyberpoikkeamia. Harjoitustoiminnalla pystytään ennaltaehkäisemään mahdollisista kyberhyökkäyksistä aiheutuvia merkittäviä kustannuksia yhteiskunnalle

Yleisen kustannustason nousun vuoksi sekä tarpeesta osallistaa yhä useampia organisaatioita ja -harjoituksiin, esittää LVM keskitetyn rahoituksen kasvattamista 0,5 miljoonalla eurolla vuodesta 2027 eteenpäin. Harjoitustoiminnan keskitetyn rahoituksen turvaamisella ylläpidettäisiin julkishallinnon kyberturvallisuuden taso myös jatkossa.