TIVIA ry – Tieto- viestintätekniikan ammattilaiset ry
Kirjallinen asiantuntijalausunto

Lausunnon antaja: TIVIA ry (Tieto- ja viestintätekniikan ammattilaiset ry)
Vastaanottaja: Eduskunnan liikenne- ja viestintävaliokunta
Asia: HE 179/2025 vp – Hallituksen esitys eduskunnalle kyberkestävyysasetuksen toimeenpanoa koskevaksi lainsäädännöksi
Päivämäärä: 23.2.2026

Asiantuntijalausunto hallituksen esityksestä HE 179/2025 vp

Kyberkestävyysasetuksen (CRA) toimeenpanoa koskeva lainsäädäntö

1. TIVIA ry lausunnon antajana

TIVIA ry (Tieto- ja viestintätekniikan ammattilaiset ry) on Suomen suurin tietotekniikka-alan asiantuntijayhdistys, joka edustaa laajaa joukkoa IT-alan ammattilaisia, asiantuntijoita ja organisaatioita Suomessa. TIVIA ry toimii useamman jäsenjärjestön kattoyhdistyksenä, jonka piirissä on yhteensä tuhansia alan ammattilaisia eri sektoreilta – yksityisestä elinkeinoelämästä julkiseen hallintoon, viranomaisiin ja akateemiseen tutkimukseen.

TIVIA ry:n jäsenjärjestöt kattavat laajan osaamiskentän kyberturvallisuudesta ohjelmistokehitykseen ja tietoverkkoihin. Jäsenkuntamme sisältää muun muassa tietoturva-alan ammattilaisia, penetraatiotestaajia, ohjelmistovalmistajia, IoT-ratkaisujen toimittajia sekä julkishallinnon digitalisoinnin asiantuntijoita. Tämä monialainen kokemus antaa TIVIA ry:lle erityisen pätevyyden arvioida EU:n kyberkestävyysasetuksen (CRA, Asetus (EU) 2024/2847) kansallista toimeenpanoa ja sen vaikutuksia suomalaiseen elinkeinoelämään ja yhteiskuntaan laaja-alaisesti.

2. Lausunnon kohde ja yleisarvio

Hallituksen esitys HE 179/2025 vp pyrkii toimeenpanemaan kansallisesti EU:n kyberkestävyysasetuksen (CRA) vaatimukset, täydentämään kyberturvallisuusasetuksen soveltamista kansallisesti sekä täydentämään NIS2 -direktiivin toimeenpanoa verkkotunnusvälittäjien osalta.

TIVIA ry suhtautuu esitykseen pääosin myönteisesti. Kyberkestävyysasetuksen sujuva toimeenpano on tärkeää digitaalisten tuotteiden tietoturvatason parantamiseksi koko EU:n sisämarkkinoilla. Pidämme perusteltuna hallitusohjelman mukaista linjausta, jonka mukaan EU-lainsäädännön toimeenpanon yhteydessä vältetään kansallista lisäsääntelyä. Lausunnossa nostamme kuitenkin esille kaksi kohtaa, joissa esitystä voidaan kehittää tai tarkentaa. Nämä esitykset parantaisivat Suomen ja suomalaisten tietoturvaa merkittävissä osin.

TIVIA ry:n kaksi keskeistä esitystä: 1. Suomeen tulee perustaa kansallinen, järjestövetoinen CVE-haavoittuvuusrekisteri yhteistyössä Kyberturvallisuuskeskuksen kanssa. Tämä täydentää ENISA:n eurooppalaista haavoittuvuustietokantaa ja vahvistaa Suomen kansallista kyberturvallisuuskykyä. Toimiakseen yhteiskuntaa palvelevana tietoturvan edistäjänä, tarvitsee tässä lakiuudistuksessa myös päivittää tietoturva-asiantuntijoiden oikeusturvaa: 2. Rikoslain 38 luvun 8 §:ään (tietomurto) tulee

lisätä erillinen CVD-turvasatama (safe harbour), joka suojaa hyvässä uskossa toimivia tietoturvatutkijoita syytteeseenpanolta – edellyttäen, että havaittu haavoittuvuus ilmoitetaan asianomaiselle taholle kohtuullisessa ajassa.

3. Keskeiset huomiot

3.1 Haavoittuvuusrekisteri: kansallisen rekisterin ja järjestövetoisen koordinaation tarve

TIVIA ry pitää haavoittuvuuksien hallintaa koskevaa sääntelyä erityisen tärkeänä ja haluaa kiinnittää valiokunnon huomion kansallisen haavoittuvuusrekisterin ja järjestövetoisen koordinaation mahdollisuuksiin.

3.1.1 Nykytilan puutteet ja HE:n lähestymistapa

HE 179/2025 vp:n kohdassa 3.1.4 todetaan, että Suomessa ei ole nykyisin voimassa horisontaalista sääntelyä, jolla velvoitettaisiin ilmoittamaan viranomaiselle ohjelmiston haavoittuvuuksista. Kyberturvallisuuskeskuksen vastaanottamat haavoittuvuusilmoitukset perustuvat vapaaehtoisuuteen ja yhteistyöhön sidosryhmien kanssa.

CRA:n toimeenpanon myötä CSIRT-yksikkö tulee vastaanottamaan kolmenlaisia haavoittuvuusilmoituksia: pakollisia 14 artiklan mukaisia ilmoituksia, vapaaehtoisia 15 artiklan mukaisia ilmoituksia sekä muita vapaaehtoisia ilmoituksia. Ilmoitusten määrän arvioidaan kasvavan merkittävästi – pelkästään vuonna 2024 Kyberturvallisuuskeskukselle ilmoitettiin 489 haavoittuvuutta, ja proaktiivisesti otettiin yhteyttä yli tuhannen organisaation kanssa. CRA laajentaa ilmoitusvelvollisuuksia huomattavasti.

3.1.2 Kansallinen haavoittuvuusrekisteri – tarve järjestövetoiselle mallille

TIVIA ry esittää, että Suomeen tulisi harkita kansallisen haavoittuvuusrekisterin perustamista, jota ylläpitäisivät ensisijaisesti alan kansalliset ammattijärjestöt ja -yhteisöt yhteistyössä Kyberturvallisuuskeskuksen kanssa. Tällainen malli ei ole uusi – muun muassa Yhdysvaltojen NVD (National Vulnerability Database), Saksan BSI:n CERT-Bund sekä Ranskan CERT-FR ovat osoittaneet, että viranomaisten ja järjestöjen välinen yhteistyö tuottaa laadukkaamman ja kattavamman haavoittuvuustietokannan kuin puhtaasti viranomaisvetoinen malli.

Järjestövetoisen kansallisen haavoittuvuusrekisterin etuja olisivat:

- Tekninen asiantuntemus: Alan ammattilaiset pystyvät arvioimaan haavoittuvuuksien vakavuuden ja vaikutukset nopeammin ja syvällisemmin kuin pelkkä viranomaisbyrokratia.
- Luottamuksellisuus ja raportoinnin kynnys: Turvallisuustutkijat ja eettiset hakkerit ilmoittavat herkemmin haavoittuvuuksista neutraalille, järjestövetoiselle taholle kuin suoraan viranomaiselle, etenkin jos ilmoittajaan kohdistuu riski oikeudellisista seuraamuksista.
- Nopeus: Järjestövetoiset koordinointimekanismit voivat toimia viranomaista joustavammin ja nopeammin, erityisesti kriittisissä tilanteissa.
- Kansainvälinen integraatio: Ammattijärjestöt voivat ylläpitää suorempia yhteyksiä kansainvälisiin CVE-järjestelmiin (Common Vulnerabilities and Exposures) ja FIRST-verkostoon (Forum of Incident Response and Security Teams).
- Pk-sektori: Suomessa toimivien pienten ja keskisuurten ohjelmistoyritysten on helpompi ottaa yhteyttä tuttuihin ammattijärjestöihin kuin viranomaisiin, mikä parantaa kattavuutta.

3.1.3 Suhde ENISA:n eurooppalaiseen haavoittuvuustietokantaan

CRA:n 17 artiklan 5 kohdan mukaisesti ENISA ylläpitää eurooppalaista haavoittuvuustietokantaa (EUVD). TIVIA ry katsoo, että kansallinen järjestövetoinen rekisteri ei ole ristiriidassa tämän kanssa, vaan toimisi syöttökanavana ja täydentävänä mekanismina. Kansallinen rekisteri voisi kerätä, esifiltteröidä ja rikastaa haavoittuvuustietoja ennen niiden välittämistä ENISA:n tietokantaan, jolloin suomalainen erityistietämys – esimerkiksi kotimaisiin kriittisiin järjestelmiin liittyvistä haavoittuvuuksista – päätyisi paremmin myös eurooppalaiseen käyttöön.

3.1.4 Eettisen hakkeroinnin ja koordinoitujen haavoittuvuusilmoitusten oikeudellinen asema

TIVIA ry:n jäsenkunta sisältää merkittävän joukon tietoturvatutkijoita ja eettisiä hakkereita, joiden työ on keskeistä haavoittuvuuksien löytämisessä ennen kuin pahantahtoiset toimijat ehtivät hyödyntää niitä. Hallituksen esityksessä käsitellään haavoittuvuusilmoittamista pääasiassa valmistajien velvollisuuksien näkökulmasta. Esityksessä ei kuitenkaan riittävässä määrin huomioida ns. koordinoidun haavoittuvuuden julkistamisen (Coordinated Vulnerability Disclosure, CVD) oikeudellista kehikkoa tutkijoiden suojan näkökulmasta.

TIVIA ry suosittaa, että kansallisessa toimeenpanossa varmistetaan selkeästi, että hyvässä uskossa toimivat tietoturvatutkijat, jotka ilmoittavat haavoittuvuuksista asianmukaisesti CSIRT-yksikölle tai järjestövetoiselle koordinaattorille, nauttivat riittävää oikeudellista suojaa. Tämä on tärkein edellytys sille, että vapaaehtoinen haavoittuvuusilmoittaminen tosiasiallisesti toimii lainsäätäjän tarkoittamalla tavalla.

3.2 Markkinavalvonta ja Pk-sektori

TIVIA ry:n jäsenkuntaan kuuluu huomattava joukko suomalaisia pieniä ja keskisuuria ohjelmisto- ja laitevalmistajia. Kyberkestävyysasetus tuo näille yrityksille merkittäviä uusia velvoitteita, erityisesti vaatimustenmukaisuuden arviointimenettelyiden, teknisten asiakirjojen sekä tietoturvapäivitysten tarjoamisen osalta.

TIVIA ry pitää tärkeänä, että Traficom/Kyberturvallisuuskeskus tarjoaa riittävästi ennakko-ohjausta ja neuvontaa suomalaisille Pk-yrityksille ennen CRA:n soveltamisen alkamista. Hallituksen esitys mainitsee yritysneuvonnan ja markkinavalvonnan, mutta resursointi tähän tehtävään tulisi varmistaa lainsäädäntömenettelyssä.

3.3 Avoimen lähdekoodin ohjelmistot ja yhteisöt

CRA:n soveltaminen avoimen lähdekoodin ohjelmistoihin on herättänyt laajaa kansainvälistä keskustelua. Asetus tekee eron kaupallisesti hyödynnettyjen ja ei-kaupallisesti hyödynnettyjen avoimen lähdekoodin ohjelmistojen välille. TIVIA ry seuraa tätä kehitystä aktiivisesti, sillä suomalaisessa ohjelmistokehitysyhteisössä on merkittävä avoimen lähdekoodin perinne.

TIVIA ry suosittaa, että kansallisessa toimeenpanossa selvennetään avoimen lähdekoodin ohjelmistovastaavien asema ja tarjotaan selkeitä ohjeita siitä, milloin vapaaehtoinen avoimen lähdekoodin kehitys kuuluu CRA:n soveltamisalaan ja milloin ei. Epäselvyys tässä kysymyksessä voi heikentää suomalaista avoimen lähdekoodin kehitysyhteisöä ja sen panosta kotimaiseen ja eurooppalaiseen ohjelmistoteollisuuteen. Epä

3.4 Kyberturvallisuussertifiointi ja osaamisen kehittäminen

TIVIA ry pitää myönteisenä, että hallituksen esitys täydentää kyberturvallisuusasetuksen mukaisten eurooppalaisten sertifiointijärjestelmien kansallista toimeenpanoa. Kyberturvallisuussertifioinnin kasvava merkitys – erityisesti CRA:n tullessa voimaan – luo merkittävän tarpeen suomalaiselle sertifiointi- ja arviointiosaamiselle.

TIVIA ry suosittaa, että lainsäätäjä kiinnittää erityistä huomiota vaatimustenmukaisuuden arviointilaitosten (CAB) kansalliseen kapasiteettiin. Suomessa toimivien akkreditoitujen laitosten määrä vaikuttaa suoraan siihen, kuinka sujuvasti suomalaiset valmistajat pystyvät osoittamaan tuotteidensa vaatimustenmukaisuuden. Niukkuus tässä voi muodostua pullonkaulaksi markkinoillepääsyssä.

4. Erityishuomiot lakiehdotuksista

Lakiehdotuksen 1 (Laki eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista) osalta TIVIA ry pitää tärkeänä, että laissa selvästi ilmaistaan haavoittuvuusilmoitusten salassapitoa koskevat säännökset. Hallituksen esityksen perusteluissa viitataan julkisuuslain eri kohtiin (24 § 7 k., 15 k. ja 20 k.), mutta käytännön soveltamisen selkeyden kannalta olisi perusteltua harkita, tulisiko salassapidon perusteet kirjata lain tasolla yksiselitteisemmin.

TIVIA ry pitää myönteisenä, että CSIRT-yksikön tehtäväkuva säilytetään joustavana niin, että se voi edelleen vastaanottaa vapaaehtoisia haavoittuvuusilmoituksia myös CRA:n soveltamisalan ulkopuolelta. Tämä on tärkeää, jotta nykyinen toimiva sidosryhmäyhteistyö ei heikkene.

5. Suositukset

TIVIA ry esittää valiokunnalle seuraavat suositukset:

- Kansallisen haavoittuvuusrekisterin perustaminen: Lainsäätäjä harkitsee mahdollisuutta perustaa kansallinen, järjestövetoinen haavoittuvuusrekisteri, joka toimii ENISA:n eurooppalaisen haavoittuvuustietokannan täydentävänä syöttökanavana ja jota ylläpidetään Kyberturvallisuuskeskuksen kanssa yhteistyössä.
- Tietoturvatutkijoiden oikeudellinen suoja: Koordinoidun haavoittuvuusilmoittamisen (CVD) oikeudellinen viitekehys selvennetään kansallisesti, jotta hyvässä uskossa toimivat tutkijat voivat ilmoittaa haavoittuvuuksista ilman riskiä oikeudellisista seuraamuksista.
- Pk-neuvonta ja kapasiteetti: Traficomille osoitetaan riittävät resurssit yritysten ennakkoneuvontaan CRA:n vaatimusten osalta, erityisesti pk-sektorin tarpeet huomioiden.
- Avoimen lähdekoodin selkeytys: Kansallinen tulkintaohje avoimen lähdekoodin ohjelmistojen CRA-soveltuvuudesta laaditaan yhdessä alan toimijoiden kanssa.
- CAB-kapasiteetti: Vaatimustenmukaisuuden arviointilaitosten kansallinen kapasiteetti varmistetaan riittäväksi, jotta suomalaiset valmistajat eivät kohtaa aiheettomia markkinoillepääsyn esteitä.
- Salassapidon selkeytys laissa: Haavoittuvuusilmoitusten salassapidon perusteet kirjataan mahdollisuuksien mukaan selkeämmin lakitasolla, jotta soveltaminen on johdonmukaista.

6. Lopuksi

TIVIA ry kiittää mahdollisuudesta lausua hallituksen esityksestä HE 179/2025 vp. Pidämme kyberkestävyysasetuksen toimeenpanoa tärkeänä askeleena Suomen ja koko EU:n digitaalisen turvallisuuden parantamisessa. Toivomme, että lausunnossamme esittämät näkökohdat – erityisesti kansallisen järjestövetoisen haavoittuvuusrekisterin mahdollisuus – otetaan huomioon lain jatkokäsittelyssä.

TIVIA ry on valmis antamaan tarkentavia tietoja lausunnosta sekä osallistumaan asiantuntijakuulemiseen tarvittaessa.

TIVIA ry
Helsinki, 23.2.2026