Liikenne- ja viestintävaliokunta
liv@eduskunta.fi

Asiantuntijapyyntö pe 14.11.2017 E 83/2017 vp

Viestintäviraston lausunto valtioneuvoston selvityksestä koskien komission ja EU:n ulkoasioiden ja turvallisuuspolitiikan korkean edustajan tiedonantoa Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle

Liikenne- ja viestintävaliokunta on pyytänyt Viestintävirastolta lausuntoa valtioneuvoston selvityksestä koskien komission ja EU:n ulkoasioiden ja turvallisuuspolitiikan korkean edustajan tiedonantoa Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle.

Viestintävirasto lausuu valtioneuvoston selvityksestä seuraavaa:

Viestintävirasto tukee valtioneuvoston näkemyksiä koskien esitettyä tiedonantoa. Tiedonannossa esitetyt tavoitteet ovat lähtökohtaisesti kannatettavia. Viestintävirasto pitää valtioneuvoston tavoin tärkeänä, että tiedonannosta johdettavat toimenpiteet ovat linjassa kansallisen sisäisen turvallisuuden strategian, kansallisen tietoturvastrategian sekä kyberturvallisuusstrategian ja sen toimeenpano-ohjelman toimenpiteiden kanssa. Näiden strategioiden toimenpiteitä on jo alettu toimeenpanna ja niistä saatavat hyödyt eivät toteudu, jos tiedonannosta johdettavat toimenpiteet ovat näiden vastaisia ja johtavat vastaisten toimenpiteiden toteuttamiseen.

Alla on käsitelty tarkemmin Viestintäviraston kantaa tiedonannossa esitettyihin tavoitteisiin niiden asiakokonaisuuksien osalta, jotka liittyvät Viestintäviraston toimintaan ja toimialaan.

EU:n resilienssin kasvattaminen kyberhyökkäysten varalta

Viestintävirasto on lausunut tarkemmin liikenne- ja viestinvaliokunnalle annetussa lausunnossa komission ehdotuksesta koskien Euroopan unionin verkko- ja tietoturvavirastolle (ENISA) pysyvän mandaatin antamista ja EU:n kyberturvallisuuden sertifi-

Viestintävirasto
Kommunikationsverket
Finnish Communications Regulatory Authority

Itämerenkatu 3 A
PL 313
00181 Helsinki
Puhelin 0295 390 100
www.viestintävirasto.fi

Östersjögatan 3A
PB 313, FI-00181
Helsingfors, Finland
Telefon +358 295 390 100
www.kommunikationsverket.fi

Itämerenkatu 3A
P.O. Box 313, FI-00181
Helsinki, Finland
Telephone +358 295 390 100
www.ficora.fi

ointipuitteiden luomista.[1] Viestintävirasto lähtökohtaisesti kannattaa komission ehdotusta asettaa ENISA:lle pysyvä mandaatti ja luoda Euroopan unionin laajuinen puitekehys ICT-tuotteiden ja -palveluiden tietoturvallisuussertifioinnille.

Kansallisen kuin kansainvälisen yhteistyön tekeminen on olennaisessa osassa kyberturvallisuusuhkiin varautumisessa. Verkko- ja tietotietoturvadirektiivin toimeenpano osaltaan vahvistaa kansallista ja kansainvälistä yhteistyötä. Viestintävirasto pitääkin tärkeänä, että verkko- ja tietoturvadirektiivin kansalliseen toimeenpanoon ja sitä valvoville viranomaisille varataan riittävät resurssit tehokkaan toimeenpanon varmistamiseksi. Viestintävirasto pitää myös tärkeänä, että yhteistyön tekemiseen hyödynnetään mahdollisimman paljon jo olemassa olevia verkostoja ja tiedonvaihtovälineitä päällekkäisen toiminnan välttämiseksi.

Viestintävirasto lähtökohtaisesti kannattaa komission suurien kyberturvallisuusuhkien ja -kriisien koordinaatiota koskevassa suosituksessa[2] esille nostamia toimenpiteitä, joiden tavoitteena on kyberturvallisuusuhkiin varautuminen ja yhteistyön varmistaminen jäsenmaiden, jäsenmaiden viranomaisten ja EU instituutioiden kesken.

Viestintävirasto tukee tiedonannossa esitettyjä tavoitteita kehittää ja panostaa rahallisesti kyberturvallisuutta koskevaan tutkimukseen, koulutukseen ja osaamiseen.

Viestintävirasto tukee niiden toimien lisäämistä, millä voidaan ehkäistä ja lieventää kyberrikollisuuden vaikutuksia loppukäyttäjiin. Olennainen osa tätä on loppukäyttäjien tietoisuuden lisääminen kyberturvallisuusuhkista ja keinoista, joilla loppukäyttäjät voivat välttyä joutumasta kyberturvallisuusrikosten uhreiksi. EU:n laajuisen keskitetyn asiointipisteen luominen voisi edesauttaa tätä tietoisuuden lisäämistä. Vahva sähköinen tunnistaminen lisää myös osaltaan kyberturvallisuutta ja Viestintävirasto pitää tärkeänä, että vahvaa sähköistä tunnistautumista edistetään niin julkishallinnon palveluissa kuin yrityksissä, kuten Suomessa on jo tehtykin ja tehdään edelleen.

Toimivan kyberpeloitteen luominen

Viestintävirasto pitää tärkeänä, että IPv6-protokollan käyttöönottoa edistetään esitetyn mukaisesti eli siten, että julkisissa tietojärjestelmähankinnoissa ostettavilta järjestelmiltä vaaditaan IPv6-tukea tai että nettipalvelujen tarjoajien kanssa sovitaan vapaaehtoisesta IPv6:n käyttöönotosta. Viestintävirasto onkin jo käynyt vuoropuhelua nettipalvelujen tarjoajien kanssa IPv6:n käyttöönoton edistämiseksi Suomessa ja työn tuloksena IPv6:n käyttö loppuasiakkaiden päätelaitteissa on kasvanut alle kah-

[1] Viestintäviraston lausunto Valtioneuvoston kirjelmästä eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi ("kyberturvallisuusasetus"), dnro 1388/04/2017.
[2] C(2017)6100.

dessa vuodessa käytännössä 0 prosentista yli 20 prosenttiin.[3] IPv6:n käyttö lisää myös internetin toimivuutta sen lisäksi, että se mahdollistaa yksilöityjen IP-osoitteiden käyttämisen päätelaitteissa.

Viestintävirasto kannattaa myös muita toimenpiteitä, joiden tavoitteena on kyberrikollisuuden ennaltaehkäiseminen ja vähentäminen. Osaltaan kyberrikollisuuden ennaltaehkäisemiseen ja vähenemiseen vaikuttaa rikoksista kiinnijäämisen riskin kasvaminen. Siten toimenpiteet, joilla lisätään kyberrikollisuudesta kiinnijäämisen riskiä, ovat kannatettavia. Toimenpiteet eivät kuitenkaan saa johtaa yleisen internetin kyberturvallisuuden heikkenemiseen esimerkiksi siten, että loppukäyttäjien käyttämien viestintälaitteiden tietoturvallisuutta heikennetään tietoisesti.

[3] https://www.akamai.com/us/en/about/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp