CSC-Tieteen tietotekniikan keskus Oy

Lausunto
17.10.2017
Asia: LVM/1616/03/2016

Lausunto Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta annetuista laeista

Yleiset huomiot

Yhteiskunnan toiminnan kannalta keskeisten palveluiden määrittäminen

CSC - Tieteen tietotekniikan keskus kiittää mahdollisuudesta vastata lausuntopyyntöön Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta annetuista laeista. CSC on suomalainen tutkimuksen, koulutuksen ja julkishallinnon ICT osaamiskeskus, joka ylläpitää opetus- ja kulttuuriministeriön toimeksiannosta korkeakoulujen valtakunnallista keskitettyä tietotekniikkainfrastruktuuria ja tarjoaa sen avulla kansallisia tietotekniikkapalveluita tutkimuksen, tieto-, opetus- ja tutkimushallinnon, sekä kirjastojen, arkistojen, museoiden ja kulttuurin tarpeisiin.

CSC, itsekin huoltovarmuuskriittisenä toimijana, näkee että on erittäin perusteltua päivittää ja uudistaa luetteloa yhteiskunnan toiminnan kannalta keskeisistä palveluista. On myös perusteltua, että tietoyhteiskuntakaaren velvoitteet kattavat arkipäivän IT-palveluiden toimittajat. Merkittävät katkot kansalaisten, yritysten sekä julkishallinnon päivittäisissä IT-palveluissa aiheuttavat vakavia häiriötä koko maalle. Hallitusohjelman mukainen digitalisaation edistäminen edellyttää, että keskeisten IT-palveluiden toimintakyky on varmistettu joustavalla ja tehokkaalla tavalla kaikissa olosuhteissa.

Toiminnanharjoittajille ehdotettavat tietoturvallisuutta koskevat riskienhallintavelvoitteet

Riskienhallinta on hyvä lähtökohta tietoturvallisuuden varmistamiselle. On kuitenkin tärkeää asettaa riskienhallinnalle tiettyjä vähimmäiskriteerejä, jotka sisältävät myös riskien riittävän kattavan tunnistamisen, niiden lieventämisen sekä lieventämistoimenpiteiden vastuuttamisen. Kansainväliset sekä kansalliset hyvät tietoturvakäytännöt (esim. VAHTI) ovat hyvä referenssi sille, mikä on riittävä riskienhallinta.

Palveluntarjoaja voi osoittaa toimivansa hyvien tietoturvakäytäntöjen mukaisesti esimerkiksi sertifioimalla riskienhallintansa ja tietoturvansa hallinnan. Vastaavaa käytäntöä suositellaan myös

tietosuoja-asetuksessa. Myös ulkopuolinen, luotettava ja riippumaton arvioija voi varmistaa riskienhallinnan laadun ja luotettavuuden

Valvontaviranomaisen tehokkaat ja riittävät toimivaltuudet (ml. seuraamukset ja sanktiot)

CSC katsoo, että salassa pidettäviä tietoja voidaan tietyin edellytyksin luovuttaa toisille jäsenvaltioille kansalaisten ja valtion riittävän turvallisuuden varmistamiseksi. Salassa pidettävien tietojen luovutus voi koskea vain merkittäviin turvallisuusuhkiin liittyviä yksittäistapauksia. CSC suosittelee, että jo käytettävissä olevien ei-salassa pidettävien tietojen vaihtamiseen liittyvää yhteistyötä kehitetään edelleen. Edellytys salassa pidettävien tietojen jakamiselle jäsenvaltioiden kesken on varmistuminen siitä, etteivät valtion tai yritysten luottamuksellinen tieto tai kansalaisten tietosuoja vaarannu. Tätä varten tulee kehittää riippumattomia varmistusmekanismeja.

CSC katsoo myös, että jäsenvaltioiden on välttämätöntä ilmoittaa toisilleen tarpeellisista, salassa pidettävistä tietoturvallisuuteen liittyvistä häiriöistä. Tässäkin tapauksessa on varmistettava, etteivät valtion tai yritysten luottamukselliset tiedot tai kansalaisten tietosuoja vaarannu. Varmistamisen voi toteuttaa riippumattoman valvontaelimen avulla.

Muut yleiset huomiot

CSC on samaa mieltä työryhmän kanssa siitä, että direktiivin mukaiset velvoitteet tulisi lähtökohtaisesti pyrkiä ottamaan kansallisesti osaksi sektorikohtaista lainsäädäntöä oman erityislain sijaan, jottei syntyisi päällekkäisiä velvoitteita tai raportointikäytäntöjä.

Laki tietoyhteiskuntakaaren muuttamisesta

CSC:n näkemyksen mukaan esitetyt muutokset ovat pääpiirteittäin perusteltuja. CSC katsoo kuitenkin, että muutoksiin tulee lisätä varmistusmekanismeja estämään tietojen asiatonta paljastumista. Lisäksi lakia tulee soveltaa siten, että myös pienillä toimijoilla on mahdollisuus tarjota jäljempänä mainittuja palveluita.

CSC toteaa, että on perusteltua laajentaa tietoyhteiskuntakaarta kattamaan tietoverkossa toimivat markkinapaikat, hakukonepalvelut sekä pilvipalvelut, koska kyseiset toiminnat ovat kriittisiä tietoyhteiskunnan toimintakyvyn kannalta. CSC ehdottaa, että lain perusteluissa mainittaisiin pilvipalveluita koskevia kansainvälisiä standardeja, kuten ISO/IEC 17788:2014 (Information technology – Cloud computing – Overview and vocabulary) ja ISO/IEC 19086-1:2016 (Information technology – Cloud computing – Service level agreement (SLA) framework).

Ehdotetussa uudessa 247a §:ssä "Verkossa toimivan markkinapaikan, hakukonepalvelun sekä pilvipalvelun tarjoajan velvollisuus huolehtia tietoturvasta" sekä esityksessä mainitut

riskienhallinnan asianmukaisuus ja kattavuus, sekä tunnettujen tietoturvallisuusstandardien noudattaminen ovat perusteltuja ja erittäin kannatettavia. Turvallisuusvaatimusten soveltaminen tulee kuitenkin toteuttaa joustavasti siten, etteivät ne estä pienempien toimijoiden kehittymistä tai pääsyä markkinoille. Samoin suojaamistoimenpiteet tulee suhteuttaa suojattavan kohteen merkitykseen mahdollisen tietovuodon tai palvelukatkon tapahtuessa. Tämän vuoksi CSC ehdottaa lisättäväksi 247a §:n ensimmäiseen lauseen loppuun: "...suhteessa suojattavaan etuun".

Ehdotus Viestintävirastolle lisättävästä velvollisuudesta toimittaa tiivistelmäraportti komissiolle ja Euroopan verkko- ja tietoturvavirastolle on johdonmukainen ja kokonaisturvallisuuden parantamista tukeva.

CSC pitää perusteltuna, että 308 §:ään "Yhteistyö eri viranomaisten kanssa" lisätään uusi 3 momentti, jossa säädettäisiin Viestintäviraston velvoitteesta toimia tarvittaessa yhteistyössä muiden jäsenvaltioiden verkko- ja tietoturvallisuuteen liittyvien eri viranomaisten kanssa. CSC kuitenkin katsoo, että kyseiseen momenttiin tulee lisätä lause, jossa edellytetään, että yhteistyön puitteissa ei saa ilman laillista perustetta luovuttaa henkilötietoja tai luottamuksellista tietoa. Yhteistyön kehittäminen CSIRT-toimijoiden kanssa on kannatettavaa, mutta tiedonvaihdossa tulee huomioida kansalaisten oikeus tietosuojaan sekä yhteisöjen tarve tiedon luottamuksellisuudelle. CSC esittää, että 308 §:n 3 momenttiin lisätään seuraava lause: "Tiedonvaihdossa tulee varmistaa, että kansalaisten yksityisyys ja yhteisöjen tiedon luottamuksellisuus turvataan".

CSC puoltaa tehokkuus- ja tarkoituksenmukaisuussyistä, että 313 §:n "Valvonta-asioiden käsittely Viestintävirastossa" 2 momentin 2 kohtaan lisättäisiin Viestintävirastolle oikeus jättää asia tutkimatta, jos asialla on 247a §:ssä tarkoitettujen palveluiden riskinhallinnan kannalta vain vähäinen merkitys.

CSC puoltaa 318 §:n mukaista mahdollisuutta luovuttaa tietoja keskeisten valvontaviranomaisten välillä, mutta tässäkin tulee varmistaa kansalaisten yksityisyyden ja yhteisöjen tiedon luottamuksellisuuden tarve.

Laki sähkömarkkinalain muuttamisesta

CSC kannattaa esitettyjä muutoksia lakiin sähkömarkkinalain muuttamisesta.

CSC-Tieteen tietotekniikan keskus Oy

Toimitusjohtaja Kimmo Koski Tietoturvapäällikkö Urpo Kaila