Valtioneuvoston kanslia | PERUSMUISTIO | VNEUS2017-00676

VNEUS Lind Jouni(VNK) | 20.10.2017 JULKINEN

Asia

E-kirje tiedonantoon Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle

Kokous

U/E/UTP-tunnus

Käsittelyvaihe ja jatkokäsittelyn aikataulu

Komissio ja EU:n ulkoasioiden ja turvallisuuspolitiikan korkea edustaja julkaisivat 13.9.2017 tiedonannon Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle. Komissio ja korkea edustaja esittävät tiedonannossa näkemyksensä toimista, joita tarvitaan EU:ssa verkon vakauden turvaamiseksi, valmiuksien kohottamiseksi, strategisen riippumattomuuden ja siten kokonaisvaltaisesti kyberturvallisuuden lujittamiseksi.

Tiedonanto on osa 13.9.2017 kyberturvallisuuspakettia, joka sisältää kaksi lainsäädäntöehdotusta: asetus EU:n kyberturvallisuusvirastosta ENISAsta sekä asetus (EU) 526/2013 kumoamisesta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista. Tiedonanto sisältää myös muita aloitteita.

Tiedonannon käsittely käynnistyi syyskuussa neuvoston horisontaalisessa kybertyöryhmässä ja puheenjohtajamaan tavoitteena on valmistella asiasta päätelmät yleisten asioiden neuvoston hyväksyttäväksi 20.11.2017.

Suomen kantoja tiedonannossa mainittuihin eri aloitteisiin täsmennetään kunkin toimenpide-ehdotuksen antamisen yhteydessä.

Suomen kanta

Suomi pitää esitettyä tiedonantoa tavoitteiltaan kannatettavana. Se luo pohjaa digitaalisten sisämarkkinoiden ja liiketoiminnan kehittymiselle ja samalla turvallisuuden lujittamiselle tietojärjestelmiin perustuville yhteiskunnan rakenteille. Kyberturvalliset tuotteet ja palvelut tulee nähdä taloudellisena kasvualana ja on tärkeää edistää kansalaisten ja yritysten luottamusta internetiä ja digitaalisia toimintatapoja kohtaan.

Suomi pitää tärkeänä, että tiedonannosta johdettavat toimenpiteet ovat linjassa kansallisen sisäisen turvallisuuden strategian, kansallisen tietoturvastrategian sekä edellisen hallituksen hyväksymän kyberturvallisuusstrategian kanssa.

Suomi kannattaa Euroopan unionin verkko- ja tietoturvaviraston (ENISA) mandaatin vahvistamista sekä sen roolia jäsenvaltioiden, EU-toimielinten ja yritysten tukemisessa tietoturvallisten tuotteiden käyttöön saattamisessa. Tarkempi kanta on määritelty asiaa koskevassa omassa U-kirjeessä.

Teknologia ja osaaminen ovat olennainen osa kyberturvallisuuden vahvistamista. Suomi kannattaa kyberturvallisuusosaamiskeskusten yhteistoimintaa ja verkostoa. Jäsenvaltioiden välisessä yhteistyössä tulisi pyrkiä mahdollisimman paljon hyödyntämään jo olemassa olevia rakenteita ja yhteistyömuotoja. Selvitettäessä eurooppalaisen osaamiskeskuksen perustamista tehtävänjako ja rajapinnat olemassa olevien toimintojen kanssa on selkeytettävä. Massadatan hyötykäytön mahdollistaminen tietoturvallisella tavalla on keskeistä uusille innovaatioille ja tehokkuudelle, joita eurooppalaiset yritykset voivat olla kehittämässä.

Suomi kannattaa IPv6-protokollan käyttöönoton edistämistä. Suomi kannattaa myös mahdollista yhteistyötä ICANNin (Internet Corporation for Assigned Names and Numbers on voittoa tavoittelematon organisaatio, joka hallinnoi Internetin osoitteiden tunnuksia). kanssa. Tätä kokonaisuutta tarkastellaan jatkoselvitysten perusteella.

Suomi tukee tiedonannossa esitettyjä koulutuksellisia ja osaamisen tavoitteita.

Kyberturvallisuuden ja puolustuksen näkökulma tulee sisällyttää EU:n yhteiseen turvallisuus- ja puolustuspolitiikkaan. Suomi kannattaa kriisinhallinnassa tiiviimpää yhteistyötä tietojenvaihdossa EU:n ja kansallisten järjestelmien välillä sekä roolien ja vastuualueiden selkeyttämistä. Suomi toimii sen eteen, että EU:n pysyvä rakenteellinen yhteistyö ja puolustusrahasto vahvistavat osaltaan kybersuorituskykyjen kehittämistä. Suomi suhtautuu tässä vaiheessa kuitenkin varauksellisesti ajatukseen erillisen kyberturvallisuuden hätäapurahaston perustamisesta.

EU-NATO yhteistyön syventäminen kyberpuolustuksen kehittämisessä on Suomelle tärkeä tavoite. Tuemme omalla toiminnallamme tätä tavoitetta osallistumalla aktiivisesti sekä NATOn että EU:n kyberpuolustusharjoituksiin. Kyberturvallisuuden tulee kattaa toiminta hybridiuhkien torjumisessa. Vasta perustettu Euroopan hybridiuhkien torjunnan osaamiskeskus Helsingissä osaltaan edistää EU:n ja Naton yhteistyötä.

Suomi pitää hyvänä, että kyberstrategia nähdään EU:n globaalina vaikuttamisena kaikilla tasoilla kansainvälisen kybertoimintaympäristön kysymyksissä. Tärkeää on kansainvälisen

oikeuden ja normien kaikenkattava huomioiminen tehtävässä yhteistyössä. Oleellisena on kyberdiplomatian työkalupakin toimeenpano sekä se, että EU jatkossakin edistää valmiuksien kehittämistä perusoikeudet huomioivassa toiminnassa yhteistyömaissa.

Pääasiallinen sisältö

Komission ja korkean edustajan tiedonanto kyberturvallisuudesta päivittää vuonna 2013 julkistettua EU:n ensimmäistä kyberturvallisuusstrategiaa ”Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö”. Tiedonannossa esitetään näkemyksiä toimista, joita tarvitaan EU:ssa verkon vakauden edistämiseksi, valmiuksien kohottamiseksi, strategisen riippumattomuuden ja siten kokonaisvaltaisesti kyberturvallisuuden lujittamiseksi.

Komissio julkisti 13.9. lainsäädäntöehdotuksen, jossa se esittää pysyvää toimeksiantoa Euroopan unionin verkko- ja tietoturvavirastolle (ENISA) sekä joitakin lisäyksiä viraston tehtäviin. ENISA muuttuisi Euroopan verkko- ja tietoturvavirastosta Euroopan kyberturvallisuusvirastoksi. Tavoitteena on luoda puitteet tieto- ja viestintäteknologiatuotteiden ja -palveluiden tietoturvasertifioinnille EU:ssa ja siten turvata sisämarkkinoiden toiminta vahvistamalla kyberturvallisuutta, sietokykyä ja luottamusta EU:ssa. ENISA:n mandaatin muutosta sekä sertifiointia käsitellään tarkemmin ko. asetusehdotusta koskevassa U-kirjelmässä.

Komissio ja korkea edustaja korostavat tiedonannossa verkko- ja tietojärjestelmien turvallisuudesta annetun direktiivin täysimääräistä täytäntöönpanoa toukokuuhun 2018 mennessä. Verkko- ja tietoturvadirektiivi parantaa kansallisia kyberturvallisuuden valmiuksia, edistää yhteistyötä jäsenvaltioiden välillä ja edellyttää, että keskeisten alojen yritykset ottavat käyttöön tehokkaita riskinhallintakäytäntöjä sekä ilmoittavat vakavista turvapoikkeamista kansallisille viranomaisille. Jäsenmaat valmistelevat parhaillaan suuntaviivoja yhdenmukaisemman direktiivin täytäntöönpanon toteuttamiseksi. Komissio antoi täytäntöönpanosta 13.9. oman tiedonannon, joka tuo esille jäsenvaltioiden parhaita käytänteitä direktiivin täytäntöönpanossa ja opastaa, miten direktiivi toimii käytännössä. Tiedonanto katsoo myös, että olisi tarpeellista laajentaa verkko- ja tietoturvadirektiivin edistämää tiedonkulkua keskeisistä strategisista aloista muillekin sektoreille.

Tiedonanto pitää tärkeänä, että reagointia kyberhyökkäysten aikana nopeutetaan ja kehitetään. Tiedonantoon kuuluu suositus Nopean ensivasteen suunnitelmaksi (Rapid Emergency Response blueprint). Suunnitelma on luonteeltaan suositus toiminnasta laajamittaisessa kyberhäiriötilanteessa, johon jäsenmaiden toivotaan sitoutuvan. Lisäksi esitetään, että kyberturvallisuus sisällytetään olemassa oleviin EU:n kriisinhallintamekanismeihin ja määritellään jäsenvaltioiden ja EU:n toimielinten, virastojen ja elinten väliselle yhteistyölle tavoitteet

ja muodot vastattaessa laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin. Perustettaisiin jäsenvaltioiden ja EU:n toimielimien yhteinen EU:n kyberturvallisuuden kriisinhallintakehys suunnitelman toteuttamiseksi käytännössä. EU:n toimielinten oman reagoinnin osalta kybernäkökulma olisi sisällytettävä olemassa oleviin EU:n kriisinhallintamekanismeihin. Näitä ovat neuvoston puheenjohtajan koordinoimat EU:n poliittisen kriisitoiminnan integroidut järjestelyt ja nopea yleishälytysjärjestelmä. Tarve reagoida erityisen vakavaan kyberturvallisuuspoikkeamaan tai hyökkäykseen voisi olla riittävä peruste, jotta EU:n jäsenvaltio voi vedota EU:n yhteisvastuulausekkeeseen.

Tiedonanto tuo esille mahdollisuuden perustaa kyberturvallisuuden hätäapurahasto muilla EU:n politiikan aloilla olevien muiden vastaavien kriisinhallintamekanismien esimerkkiä seuraten. Rahasto voisi auttaa jäsenvaltioita hakemaan apua EU:n tasolla merkittävän poikkeaman sattuessa.

Vuonna 2016 perustettu julkisen ja yksityisen sektorin kyberturvallisuuskumppanuus edistää valmiuksien kehittämistä EU:ssa digitaalisen talouden, yhteiskunnan ja demokratian turvaamiseksi sekä kriittisten laitteistojen ja ohjelmistojen suojaamiseksi ja keskeisten kyberturvallisuuspalveluja tarjoamiseksi. Strategiassa katsotaan kuitenkin, että investointeja tarvitaan enemmän ja ehdottaa jatkotoimena EU:n kyberturvallisuusvalmiuden vahvistamista kyberturvallisuuden osaamiskeskusten verkoston avulla. Sen keskiössä olisi eurooppalaisen kyberturvallisuuden tutkimus- ja osaamiskeskus. Tämä verkosto ja osaamiskeskus edistäisivät teknologian kehittämistä ja käyttöönottoa kyberturvallisuuden alalla. Asiasta käynnistetään vaikutustenarviointi. Ensimmäisenä toimena ja tulevaan suunnitteluun varautumiseksi komissio ehdottaa pilottivaiheen käynnistämistä Horisontti 2020 -ohjelman puitteissa.

Komissio ja korkea edustaja ehdottavat, että verkoston ja sen keskuksen toista vaihetta voitaisiin edelleen kehittää kyberpuolustukseen liittyvän ulottuvuuden osalta. Tältä osin noudatettaisiin yhteistä turvallisuus- ja puolustuspolitiikkaa koskevia perustamissopimuksen määräyksiä. Komissio mainitsee, että yritysten kehittämät kyberpuolustushankkeet tai -teknologiat voisivat saada rahoitusta Euroopan puolustusrahastosta tutkimus- ja kehittämisvaiheessa.

Strategiassa todetaan, että kyberturvallisuuden ammattilaisia ennustetaan puuttuvan Euroopan yksityiseltä sektorilta 350 000 kappaletta vuoteen 2022 mennessä. Jäsenmaiden toivotaan vastaavan koulutustarpeisiin. Koulutuksen kehittäminen tulee integroida kyberturvallisuuden osa-alueiden toimintoihin. Yksi näkökohta lisätä tietoturvallisuutta on tehdä tietoturvan kysymyksistä näkyvämpiä ja hallinnoitavampia kuluttajille.

Komissio ja korkea edustaja katsovat, että EU:n olisi kehitettävä lisäksi portaali, johon kootaan keskitetysti yhteen välineet, jotka opastavat

välttämään haittaohjelmien uhriksi joutumista ja ratkaisemaan näitä tilanteita. Jäsenvaltioiden olisi nopeutettava kyberturvallisempien välineiden käyttöä sähköisen hallinnon kehittämisen yhteydessä sekä hyödynnettävä kaikin tavoin osaamisverkostoa.

Keskeisessä asemassa ovat myös tehokkaammat lainvalvontatoimet, jotka keskittyvät kyberrikollisten tunnistamiseen, jäljittämiseen ja syytteeseenpanoon. EU kannustaa Europolin kyberrikollisuusyksikön vahvistamiseen, uuden yhteyskäytännön (IPv6) laajempaan käyttöönottoon ja verkkotunnusten väärinkäytön estämiseen. IPv6:n laajemman käyttöönoton ajatuksena on mahdollistaa yhden IP-osoitteen osoittaminen kullekin käyttäjälle, mikä auttaisi lainvalvonnassa ja kyberturvallisuustutkinnoissa. IPv6-protokollaan siirtyminen lisäisi uniikkien IP-osoitteiden saatavuutta ja vähentäisi tarvetta jakaa samoja IP-osoitteita useiden käyttäjien kesken. Tämä parantaisi myös viranomaisten mahdollisuuksia selvittää tietoverkkorikoksia.

Kyberhyökkäysten torjunnassa tärkeän pelotteen muodostaa kyberrikosten tehokas tutkinta ja syytteeseenpano. Tätä varten komissio aikoo, antaa vuoden 2018 alussa ehdotuksia sähköisen todistusaineiston rajat ylittävän saatavuuden helpottamiseksi.
Komissio esittää tulokset salauksen rooliin rikostutkinnassa lokakuuhun 2017 mennessä.
Nykyistä parempaan pääsyyn rajat ylittävään todistusaineistoon tarvitaan sekä lainsäädännöllisiä että käytännön toimenpiteitä. Tarkemmat Suomen kannat määritellään myöhemmin.

Lähtökohtana rikosten torjunnassa ja selvittämisessä tulee olla keskinäisen oikeusavun toimivuus ja sitä koskevien menettelytapojen kehittäminen. Tärkeää on kuitenkin huolehtia riittävässä määrin tietosuojasta ja perusoikeuksien turvaamisesta sekä valtioiden suvereniteetista; käyttäjillä tulee olla mahdollisuus suojata luottamuksellinen viestintänsä ja digitaaliset tietonsa asiakastarpeiden mukaan kehittyvillä salaus- ja suojausohjelmistoilla sekä muilla teknologisilla ratkaisuilla.

Komissio tutkisi yhdessä sidosryhmien kanssa kansallisia lähestymistapoja uusien ratkaisujen löytämiseksi ns. pimeän verkon olemassa olosta ja toiminnasta. Pimeä verkko on avannut rikollisille uusia mahdollisuuksia saada käsiinsä laitonta materiaalia ja kyberrikollisuudessa käytettäviä välineitä, mm. haittaohjelmia ja hakkerointityökaluja.

Komissio ja korkea edustaja ehdottavat tiukennuksia rikkomusten ehkäisyyn verkkomaksuissa: direktiivi muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten ja väärennysten torjumisesta. Sen tarkoituksena on päivittää alan säännöt ja tehostaa lainvalvonnan valmiuksia tällaisiin rikoksiin puuttumiseksi. Muihin maksuvälineisiin kuin käteisrahaan liittyvän rikollisuuden torjunnasta annettuun lainsäädäntöehdotukseen määritellään kanta omassa U-kirjeessä.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

Strategia ei ole lainsäädäntöesitys.

Kyberturvallisuusasetuksen osalta komissio ehdottaa asetuksen oikeusperustaksi Euroopan unionin toiminnasta annetun sopimuksen (SEUT) 26 ja 114 artiklaa. Ehdotus käsiteltäisiin SEUT 294 artiklan mukaisessa tavanomaisessa lainsäädäntöjärjestyksessä.

Käsittely Euroopan parlamentissa

Esittely päävaliokunnassa sisämarkkinat ja kuluttajan suoja 11.10.2017 sekä kansalaisvapaudet sekä oikeus- ja sisäasiat valiokunnassa 11.10.2017. Raportoijia ei ole nimetty.

Kansallinen valmistelu

Asiaa on valmisteltu VNK:n johdolla horisontaalisia EU-kyberturvallisuuskysymyksiä käsittelevässä ministeriöiden muodostamassa verkostossa, jossa ovat mukana VNK, TEM, OM, SM, LVM, VM, PLM ja UM.

Lausuntokierrokset:
EU19-jaosto (viestintä), kirjallinen menettely 13.10-18-10-2017
EU22-jaosto (liikenne), kirjallinen menettely 13.10.2017-18.10.2017
EU8-jaosto (sisämarkkinat), kirjallinen menettely 13.10.17-18.10.2017
EU7-jaosto (oikeus- ja sisäasiat), kirjallinen menettely 13.10.17-18.10.2017

Ahvenanmaan maakunnan kuuleminen ollut jaostolausuntojen yhteydessä.

Eduskuntakäsittely

Aihetta on käsitelty digitaalisten sisämarkkinoiden strategian välitarkastelussa (EJ 21/2017 vp, E21/2015 vp). Eduskunnan talousvaliokunta ja liikenne- ja viestintävaliokunta antoivat lausuntonsa (TaVL 38/2017 vp, LiVL 2/2015 vp).

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

Vaikutukset kansalliseen lainsäädäntöön arvioidaan strategiaan sisältyvien lainsäädäntöehdotusten antamisen yhteydessä.

Taloudelliset vaikutukset

Tiedonannolla ei tässä vaiheessa ole välittömiä taloudellisia vaikutuksia. Vaikutuksia sekä kansalliseen talousarvioon että EU:n budjettiin selvitetään. Strategiassa mainittujen yksityiskohtaisempien ehdotusten taloudelliset vaikutukset sekä ehdotusten rahoitus tulevat erikseen arvioitaviksi siinä vaiheessa, kun komission ehdotukset on

annettu ja niitä käsitellään. Erillisissä U-kirjeissä arvioidaan osana kyberpakettia annettujen ehdotusten taloudellisia vaikutuksia.

Muut asian käsittelyyn vaikuttavat tekijät

Kansallisia linjauksia: Kansallisen sisäisen turvallisuuden strategia, kansallinen tietoturvastrategia, edellisen hallituksen hyväksymän kyberturvallisuusstrategia sekä Liikenne- ja viestintäministerin maaliskuussa 2016 hyväksymän Suomen tietoturvallisuusstrategia.

Asiakirjat

Komission ja EU:n ulkoasioiden ja turvallisuuspolitiikan korkean edustajan tiedonanto: Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle JOIN(2017) 450 finalJOIN(2017) 450.

EU:n kyberturvallisuusvirastosta ENISAsta ja asetuksen (EU) 526/2013 kumoamisesta
sekä tieto- ja viestintätekniikan kyberturvallisuussertifioinnista
(”kyberturvallisuusasetus”) COM(2017) 477 final

Laatijan ja muiden käsittelijöiden yhteystiedot

Jouni Lind, VNK, p. 0295 160 448 (jouni.lind@vnk.fi)

EUTORI-tunnus

EU/2017/1434

Liitteet

Viite

Asiasanat	kyberstrategia, Euroopan digitaalistrategia
Hoitaa	**LVM, OM, PLM, SM, UM, VNK**
Tiedoksi	EUE, OKM, STM, TEM, TULLI, VM