EUROOPAN KOMISSIO

LEHDISTÖTIEDOTE

Bryssel 7. helmikuuta 2013

Avointa internetiä ja verkon vapautta ja mahdollisuuksia suojellaan EU:n kyberturvallisuussuunnitelmalla

Euroopan komissio on julkistanut yhdessä unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan kanssa kyberturvallisuusstrategian. Sen ohella komissio on antanut verkko- ja tietoturvaa koskevan direktiiviehdotuksen.

Kyberturvallisuusstrategia – ”Avoin, turvallinen ja vakaa verkkoympäristö” – edustaa EU:n kattavaa visiota siitä, miten verkon häiriöitä ja verkkohyökkäyksiä voidaan parhaiten ehkäistä ja torjua. Näin edistetään eurooppalaisia vapauden ja demokratian arvoja ja varmistetaan, että digitaalitalous voi kasvaa turvallisesti. Erityistoimilla pyritään parantamaan tietojärjestelmien sietokykyä ja vähentämään verkkorikollisuutta sekä vahvistamaan EU:n kansainvälistä kyberturvallisuuspolitiikkaa ja verkkopuolustusta.

EU:n kyberturvallisuutta koskeva visio koostuu viidestä strategisesta painopisteestä:

- Verkon vakaus
- Verkkorikollisuuden huomattava vähentäminen
- Verkkopuolustuspolitiikan ja yhteiseen turvallisuus- ja puolustuspolitiikkaan (YTPP) liittyvien valmiuksien kehittäminen
- Kyberturvallisuuteen liittyvien teollisten ja teknologisten voimavarojen kehittäminen
- Johdonmukaisen kansainvälisen verkkotoimintapolitiikan luominen Euroopan unionille sekä EU keskeisten arvojen edistäminen.

Kansainvälisessä verkkotoimintapolitiikassa EU edistää EU:n perusarvoja, määrittelee vastuullisen toiminnan normeja ja tehostaa verkkoa koskevien voimassa olevien lakien soveltamista sekä auttaa EU:n ulkopuolisia maita parantamaan kyberturvallisuusvalmiuksiaan ja edistää kansainvälistä yhteistyötä verkkoon liittyvissä asioissa.

EU on ottanut merkittäviä askelia kansalaistensa suojaamiseksi verkkorikollisuudelta. Se on muun muassa perustanut Euroopan verkkorikostorjuntakeskuksen IP/13/13, tehnyt tietoturvahyökkäyksiä koskevia lainsäädäntöehdotuksia (IP/10/1239ja käynnistänyt maailmanlaajuisen kumppanuuden verkossa esiintyvän lasten seksuaalisen hyväksikäytön torjumiseksi IP/12/1308. Strategialla pyritään myös kehittämään ja rahoittamaan verkkorikollisuuden torjunnan kansallisten osaamiskeskittymien verkostoa koulutuksen helpottamiseksi ja valmiuksien vahvistamiseksi.

Ehdotettu verkko- ja tietoturvaa koskeva direktiivi on yleisstrategian keskeinen osa ja siinä edellytetään, että kaikki jäsenvaltiot, keskeiset internetin toiminnan mahdollistajat ja elintärkeiden infrastruktuurien (sähköisen kaupankäynnin alustat, verkkoyhteisöpalvelut jne.) ylläpitäjät ja (mm. energia-, liikenne- pankki- ja terveysalan) palvelun tarjoajat varmistavat, että digitaaliympäristö on turvallinen ja luotettava koko EU:ssa. Direktiiviehdotuksessa esitetään muun muassa seuraavia toimenpiteitä:

a) jäsenvaltioissa laaditaan verkko- ja tietoturvastrategia sekä nimitetään kansallinen toimivaltainen viranomainen, jolla on riittävät taloudelliset ja henkilöstöresurssit turvariskien ja -poikkeamien ennaltaehkäisyä ja käsittelyä ja niihin reagoimista varten,

b) luodaan jäsenvaltioiden ja komission välinen yhteistyömekanismi, jotta voidaan antaa varhaisvaroituksia turvariskeistä ja -poikkeamista suojatun infrastruktuurin kautta, tehdä yhteistyötä ja järjestää säännöllisiä vertaisarviointeja,

c) tiettyjen alojen (rahoituspalvelut, liikenne, energia, terveys) kriittisten infrastruktuurien ylläpitäjät, tietoyhteiskunnan palvelujen toiminnan mahdollistajat (erityisesti sovelluskaupat, sähköisen kaupankäynnin alustat, internet-välitteiset maksupalvelut, pilvipalvelut, hakukoneet ja verkkoyhteisöpalvelut) ja julkishallinnot ottavat käyttöön riskinhallintakäytänteitä ja raportoivat keskeisiin palveluihin kohdistuvista merkittävistä turvapoikkeamista.

Digitaalistrategiasta vastaava Euroopan komission varapuheenjohtaja Neelie Kroes totesi, että

”Mitä enemmän ihmiset käyttävät internetiä, sitä enemmän heidän on voitava luottaa myös siihen, että sen käyttö on turvallista. Turvallinen internet suojelee vapauksia ja oikeuksia sekä mahdollisuuksia harjoittaa liiketoimintaa. On aika toteuttaa yhteisiä toimia – toimettomuus tulisi paljon kalliimmaksi kuin toimiminen.”

Unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustaja, komission varapuheenjohtaja Catherine Ashton lisäsi:

"Jotta verkko säilyisi avoimena ja vapaana, verkkotoiminnassa olisi sovellettava samoja normeja, periaatteita ja arvoja, joita EU:ssa noudatetaan reaalimaailmankin puolella. Perusoikeuksia, demokratiaa ja oikeusvaltioperiaatetta on suojeltava myös kyberavaruudessa. EU tekee yhteistyötä kansainvälisten kumppanien, kansalaisyhteiskunnan ja yksityisen sektorin kanssa näiden oikeuksien tukemiseksi maailmanlaajuisesti."

Sisäasioista vastaava komissaari Cecilia Malmström totesi vielä, että

”Strategiassa painotetaan konkreettisia toimia, joilla verkkorikollisuutta voidaan vähentää merkittävästi. Monilla EU-mailla ei ole tarvittavia välineitä järjestäytyneen verkkorikollisuuden jäljittämiseksi ja torjumiseksi. Kaikkien jäsenmaiden olisi perustettava tehokkaat kansalliset verkkorikosyksiköt, jotka voivat hyödyntää Euroopan verkkorikostorjuntakeskuksen (EC3) asiantuntemusta ja tukea."

Tausta

Kyberturvallisuuteen liittyvät turvapoikkeamat ovat tulleet yhä yleisemmiksi, laajemmiksi ja monimutkaisemmiksi, eivätkä ne tunne rajoja. Turvapoikkeamat voivat aiheuttaa merkittävää vahinkoa turvallisuudelle ja taloudelle. Niiden ennalta ehkäisyä ja niitä koskevaa yhteistyötä ja avoimuutta on parannettava.

Euroopan komission ja yksittäisten jäsenvaltioiden aiemmilla hajanaisilla toimilla ei ole pystytty vastaamaan tähän kasvavaan haasteeseen.

Tietoa kyberturvallisuustilanteesta

- Liikkeellä on päivittäin yli 150 000 virusta, ja 148 000 tietokonetta saastuu viruksesta joka päivä.
- Maailman talousfoorumin mukaan 10 prosentin todennäköisyydellä tulevan vuosikymmenen aikana tapahtuu merkittävä kriittisen tietoinfrastruktuurin kaatuminen, joka voi aiheuttaa jopa 250 miljardin dollarin tappiot.
- Suuri osa turvapoikkeamista johtuu verkkorikollisuudesta. Symantec arvioi, että verkkorikollisuuden uhrien tappiot ovat vuosittain noin 290 miljardia euroa, ja McAfeen mukaan verkkorikollisuuden tuotto on 750 miljardia euroa vuodessa.
- Vuonna 2012 tehdyn kyberturvallisuutta koskevan Eurobarometri-kyselyn mukaan EU:ssa 38 prosenttia internetin käyttäjistä on muuttanut käyttäytymistään kyberturvallisuuteen liittyvistä syistä: 18 prosenttia todennäköisesti ostaa vähemmän tavaroita verkossa ja 15 prosenttia todennäköisesti käyttää vähemmän verkkopankkia. Siitä käy ilmi myös, että 74 prosenttia vastaajista katsoi uhriksi joutumisen riskin kasvaneen, 12 prosenttia on jo joutunut verkkorikoksen kohteeksi, ja 89 prosenttia välttää henkilökohtaisten tietojen antamista verkossa.
- Verkko- ja tietoturvaa koskevan julkisen kuulemisen mukaan 56,8 prosentilla vastaajista oli ollut kuluneena vuonna verkko- ja tietoturvaongelmia, joilla oli ollut vakavia vaikutuksia heidän toimintaansa.
- Eurostatin luvut taas osoittavat, että tammikuuhun 2012 mennessä vain 26 prosenttia EU:n yrityksistä oli laatinut virallisen tietoturvallisuuspolitiikan.

Hyödyllisiä linkkejä

MEMO/13/71 Usein kysyttyjä kysymyksiä

Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö

Ehdotus direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa

Kerro mielipiteesi

Hashtag: #cybersecurity

Neelie Kroes

Seuraa Neelieä Twitterissä

EEAS verkkosivu

EEAS Twitterissä

Cecilia Malmströmin verkkosivusto

Seuraa komissaari Malmströmiä Twitterissä

Europolin (EC3) verkkosivusto

Maailmanlaajuinen kumppanuus verkossa esiintyvän lasten seksuaalisen hyväksikäytön torjumiseksi

Yhteyshenkilöt:
Ryan Heath (+32-2) 296 17 16, Twitter: @RyanHeathEU
Michele Cercone (+32-2) 298 09 63
Maja Kocijancic (+32-2) 298 65 70
Michael Mann (+32-2) 299 97 80