EUROOPAN KOMISSIO

Bryssel 31.3.2011
KOM(2011) 163 lopullinen

KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE SEKÄ ALUEIDEN KOMITEALLE

elintärkeiden tietoinfrastruktuureiden suojaamisesta

”Saavutukset ja seuraavat vaiheet: kohti maailmanlaajuista verkkoturvallisuutta”

KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE SEKÄ ALUEIDEN KOMITEALLE

elintärkeiden tietoinfrastruktuureiden suojaamisesta

”Saavutukset ja seuraavat vaiheet: kohti maailmanlaajuista verkkoturvallisuutta”

1. JOHDANTO

Komissio antoi 30. maaliskuuta 2009 elintärkeiden tietoinfrastruktuureiden suojaamista koskevan tiedonannon ”Euroopan suojaaminen laajoilta tietoverkkohyökkäyksiltä ja häiriöiltä: valmiuden, turvallisuuden ja sietokyvyn parantaminen”[1]. Siinä esitetään toimintasuunnitelma, jolla pyritään parantamaan elintärkeiden tieto- ja viestintätekniikan (TVT) infrastruktuurien tietoturvaa ja sietokykyä. Tavoitteena oli edistää ja tukea korkean valmiusasteen, tietoturvan ja sietokyvyn kehittämistä sekä kansallisella että Euroopan tasolla. Lähestymistapa sai laajaa tukea neuvostossa vuonna 2009[2].

Toimintasuunnitelma koostuu viidestä osiosta: varautuminen ja ehkäisy, havaitseminen ja vastatoimet, häiriöiden lieventäminen ja toimintakunnon palautus, kansainvälinen yhteistyö sekä Euroopan elintärkeiden infrastruktuurien kriteerit TVT-toimialalla. Siinä esitetään komissiolta, jäsenvaltioilta ja/tai toimialalta itseltään odotetut toimet kussakin osiossa. Toimissa saadaan tukea Euroopan verkko- ja tietoturvavirastolta (ENISA).

Toukokuussa 2010 hyväksytyn Euroopan digitaalistrategian[3] ja sitä koskevien neuvoston päätelmien[4] myötä kävi selvästi ilmi yhteinen näkemys siitä, että luottamus ja tietoturva ovat ehdottomia perusedellytyksiä TVT:n laajalle käyttöönotolle ja tätä kautta Eurooppa 2020 -strategian[5] ”älykäs kasvu” -tavoitteiden saavuttamiselle. Euroopan digitaalistrategiassa korostetaan, että kaikkien sidosryhmien on yhdistettävä voimansa kokonaisvaltaisella tavalla, jotta voidaan varmistaa TVT-infrastruktuurien suoja ja sietokyky keskittymällä ennaltaehkäisyyn, valmistautuneisuuteen ja tietoon uhkista sekä kehittää tuloksellisia ja koordinoituja mekanismeja, joilla vastata uusiin ja yhä kehittyneempiin verkkohyökkäysten ja verkkorikollisuuden muotoihin. Tällä lähestymistavalla varmistetaan, että sekä ehkäisyyn että reagointiin liittyvät tämän haasteen ulottuvuudet otetaan asianmukaisesti huomioon.

Viime kuukausien aikana on toteutettu useita digitaalistrategiassa ilmoitettuja toimia. Komissio antoi syyskuussa 2010 ehdotuksen direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä[6]. Sillä pyritään vahvistamaan verkkorikollisuuden vastaista toimintaa lähentämällä jäsenvaltioiden rikoslainsäädäntöä ja parantamalla yhteistyötä lainkäyttöviranomaisten ja muiden toimivaltaisten viranomaisten välillä. Se sisältää

---

1 KOM(2009) 149.

2 Neuvoston päätöslauselma, annettu 18 päivänä joulukuuta 2009, yhteistoiminnallisesta eurooppalaisesta lähestymistavasta verkko- ja tietoturvallisuuden alalla (2009/C 321/01).

3 KOM(2010) 245.

4 Neuvoston päätelmät, annettu 31 päivänä toukokuuta 2010, Euroopan digitaalistrategiasta (10130/10).

5 KOM(2010) 2020 ja Eurooppa-neuvoston päätelmät, 25.–26. maaliskuuta 2010 (EUCO 7/10).

6 KOM(2010) 517 lopullinen.

säännöksiä myös uudentyyppisistä verkkohyökkäyksistä, erityisesti bottiverkoista. Täydennykseksi komissio antoi samalla myös ehdotuksen uudesta toimeksiannosta[7], jolla vahvistettaisiin ja nykyaikaistettaisiin Euroopan verkko- ja tietoturvavirastoa (ENISA) luottamuksen lisäämiseksi ja verkkoturvallisuuden parantamiseksi. Verkko- ja tietoturvaviraston aseman vahvistaminen ja uudistaminen auttaa EU:ta, jäsenvaltioita ja yksityissektorin sidosryhmiä kehittämään valmiuksiaan ehkäistä ja havaita tietoturvaongelmia ja reagoida niihin.

Euroopan digitaalistrategia, Tukholman ohjelma/toimintasuunnitelma[8] ja EU:n sisäisen turvallisuuden strategian toteuttamissuunnitelma[9] ovat osoituksia komission sitoutumisesta rakentamaan digitaalista ympäristöä, jossa jokainen eurooppalainen voi täysin saavuttaa taloudellisen ja sosiaalisen potentiaalinsa.

Tässä tiedonannossa tarkastellaan tuloksia, joita on saatu aikaan sen jälkeen kun elintärkeiden tietoinfrastruktuurien suojaamista koskeva toimintasuunnitelma hyväksyttiin vuonna 2009. Siinä kuvataan kullekin toimintaosiolle kaavaillut seuraavat vaiheet sekä Euroopan tasolla että kansainvälisesti. Lisäksi siinä keskitytään haasteiden maailmanlaajuiseen ulottuvuuteen ja siihen, miten maailmanlaajuiset keskinäiset riippuvuussuhteet edellyttävät yhteistyötä jäsenvaltioiden ja yksityisen sektorin kesken kansallisella, eurooppalaisella ja kansainvälisellä tasolla.

2. KEHITTYVÄ TILANNE

Elintärkeiden tietoinfrastruktuurien suojaamista koskevan toimintasuunnitelman vaikutustenarviointi[10] ja lukuisat julkisen ja yksityisen sektorin analyysit ja raportit nostavat esiin Euroopan yhteiskunnallisen, poliittisen ja taloudellisen riippuvuuden TVT:stä, mutta todistavat myös uhkien – niin luonnon kuin ihmisenkin aiheuttamien – määrän, laajuuden, monimutkaisuuden ja potentiaalisten vaikutusten jatkuvaa lisääntymistä.

Esiin on noussut uusia ja teknisesti yhä kehittyneempiä uhkia. Niiden globaalit geopoliittiset ulottuvuudet alkavat asteittain käydä selvemmiksi. Kehityssuuntana on, että TVT:tä käytetään poliittisiin, taloudellisiin ja sotilaallisiin päämääriin, myös hyökkäysvalmiuksien kautta. Tässä yhteydessä mainitaan joskus verkkosodankäynti ja verkkoterrorismi.

Lisäksi kuten eteläisen Välimeren alueen hiljattaiset tapahtumat osoittavat, eräät hallinnot ovat valmiita ja kykeneviä estämään poliittisista syistä omien kansalaistensa mahdollisuuden käyttää sähköisiä viestintävälineitä, etenkin internetiä ja matkaviestintää, tai ainakin haittaamaan niiden käyttöä. Tällaisilla yksipuolisilla maan sisäisillä interventioilla voi olla vakavia seurauksia muualla maailmassa[11].

Jotta saadaan kattavampi kuva näistä erilaisista uhkista, voi olla hyödyllistä luokitella ne seuraaviin ryhmiin:

---

7 KOM(2010) 521.
8 KOM(2010) 171.
9 KOM(2010) 673.
10 SEC(2009) 399.
11 Yhteinen tiedonanto demokratiaan ja yhteiseen vaurauteen tähtäävästä kumppanuudesta eteläisen Välimeren alueen kanssa, KOM(2011) 200, 8.3.2011.

– **hyödyntavoittelutarkoitukset**, kuten ”pysyväisluonteiset kehittyneet uhat”[12] taloudellisiin ja poliittisiin vakoilutarkoituksiin (esim. GhostNet[13]), identiteettivarkaudet ja hiljattaiset hyökkäykset päästökauppajärjestelmää[14] ja valtiollisia tietojärjestelmiä[15] vastaan,

– **häirintätarkoitukset**, kuten bottiverkoilla toteutetut hajautetut palvelunestohyökkäykset tai roskapostitukset (esim. 7 miljoonan koneen Conficker-verkosto ja Espanjasta ohjattu 12,7 miljoonan koneen Mariposa-verkosto[16]), Stuxnet[17] ja viestintäkanavien sulkeminen,

– **tuhoamistarkoitukset**. Tämä skenaario ei vielä ole toteutunut, mutta koska TVT on yhä keskeisemmässä asemassa elintärkeissä infrastruktuureissa (esim. älykkäät sähköverkot ja vedenjakelujärjestelmät) sitä ei tulevina vuosina voida sulkea pois[18].

3. EUROOPAN UNIONI JA YHTEYDET MUUHUN MAAILMAAN

Edessä olevat haasteet eivät koske pelkästään Euroopan unionia, eikä EU selviydy niistä yksin. TVT:n ja internetin jatkuva yleistyminen mahdollistaa entistä tehokkaamman, toimivamman ja edullisemman viestinnän, koordinoinnin ja yhteistyön eri toimijoiden välillä ja luo elinvoimaisen innovaatioekosysteemin kaikilla elämän aloilla. Uhat voivat nykyään kuitenkin olla lähtöisin mistä päin maailmaa hyvänsä, ja aiheuttaa maailmanlaajuisten yhteenliitäntöjen takia vaikutuksia missä tahansa maailmankolkassa.

Puhtaasti eurooppalainen lähestymistapa ei riitä haasteisiin vastaamiseksi. Vaikka onkin edelleen hyvin tärkeää luoda EU:n sisällä johdonmukainen ja yhteistyötä korostava lähestymistapa, se on kytkettävä maailmanlaajuiseen koordinointistrategiaan, joka tavoittaa keskeiset kumppanimme olivat ne sitten yksittäisiä kansakuntia tai kansainvälisiä organisaatioita.

Meidän on saavutettava globaali ymmärrys riskeistä, joita TVT:n laaja ja massiivinen käyttö aiheuttaa kaikilla yhteiskuntalohkoilla. Tätäkin tärkeämpää on laatia strategiat näiden riskien hallitsemiseksi (ennaltaehkäisy, vastatoimet, vaikutusten lieventäminen ja reagointi). Digitaalistrategian mukaisesti ”*asianomaisten toimijoiden välinen yhteistyö on organisoitava maailmanlaajuisesti, jotta sen avulla voitaisiin tehokkaasti torjua ja lieventää turvallisuusuhkia*” ja tavoitteena on toimia ”*yhteistyössä globaalien sidosryhmien kanssa erityisesti* ***maailmanlaajuisen riskienhallinnan*** *lujittamiseksi digitaalisessa ja fyysisessä ympäristössä, ja [toteuttaa] kansainvälisesti koordinoituja kohdennettuja toimia tietokonepohjaisen rikollisuuden ja tietoturvahyökkäysten torjumiseksi*”.

---

12 Eli jatkuvat koordinoidut hyökkäykset valtiollisia laitoksia ja julkista sektoria vastaan. Nämä uhat ovat nyt leviämässä myös yksityiselle sektorille (ks. *RSA 2011 cybercrime trends report*).

13 Ks. *Information Warfare Monitor* -hankkeen raportit: *Tracking GhostNet: investigating a Cyber Espionage Network* (2009) ja *Shadows in the Cloud: Investigating Cyber Espionage 2.0* (2010).

14 Ks: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=en.

15 Esim. hiljattaiset hyökkäykset Ranskan hallitusta vastaan.

16 Ks. OECD:n/IFP:n hanke "Future Global Shocks", "Reducing systemic cyber-security risks", 14. tammikuuta 2011, http://www.oecd.org/dataoecd/3/42/46894657.pdf.

17 Ks. http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis.

18 Ks. World Economic Forum, *Global Risks 2011*.

4. ELINTÄRKEIDEN TIETOINFRASTRUKTUURIEN SUOJAAMISTA KOSKEVAN TOIMINTASUUNNITELMAN TOTEUTUS: MUUTAMIA ESIMERKKEJÄ

Koko raportti toimintasuunnitelman saavutuksista ja seuraavista vaiheista on liitteenä. Seuraavassa nostetaan esiin muutamia esimerkkejä tämänhetkisestä tilanteesta.

4.1. Varautuminen ja ehkäisy

- **Euroopan jäsenvaltiofoorumi** (EFMS) on merkittävästi kyennyt edistämään viranomaisten keskustelua ja tiedonvaihtoa hyvistä toimintavaihtoehdoista TVT-infrastruktuurien suojaamisen ja sietokyvyn alalla. Jäsenvaltiot pitävät EFMS:ää tärkeänä keskustelufoorumina ja keinona vaihtaa kokemuksia hyvistä toimintamalleista[19]. EFMS tulee saamaan jatkossakin toiminnalleen tukea ENISAlta ja keskittyy yhteistyöhön kansallisten/valtiollisten tietotekniikan kriisiryhmien eli CERT-ryhmien (*Computer Emergency Response Team*) välillä. Se pyrkii määrittelemään taloudellisia ja sääntelyllisiä kannustimia turvallisuuden ja sietokyvyn parantamiseen (sovellettavien kilpailu- ja valtiontukisääntöjen puitteissa), arvioimaan verkkoturvallisuustilannetta Euroopassa, edistämään yleiseurooppalaisia harjoituksia sekä keskustelemaan painopisteistä kansainvälisessä tietoinfrastruktuurien suojaamiseen ja sietokykyyn liittyvässä yhteistyössä.

- **Sietokykyä käsittelevä eurooppalainen julkis-yksityinen kumppanuus** (EP3R) luotiin Euroopan laajuiseksi ohjausjärjestelmäksi TVT-infrastruktuurien sietokykyä koskevissa asioissa. Sen avulla pyritään edistämään julkisen ja yksityisen sektorin välistä yhteistyötä turvallisuuteen ja sietokykyyn liittyvissä strategisissa kysymyksissä. ENISA on avustanut EP3R:n toimintaa. Komission vuonna 2010 antaman ENISAn uudistusehdotuksen mukaan ENISAn on tarkoitus tarjota EP3R:lle pitkän aikavälin kestävät puitteet. EP3R toimii myös kanavana kansainväliselle tiedonvaihdolle yhteiskuntapoliittisista, taloudellisista ja markkinakysymyksistä, joilla on merkitystä tietoinfrastruktuurien suojaamisen ja sietokyvyn kannalta. Erityistavoitteena on vahvistaa maailmanlaajuista TVT-infrastruktuurien riskinhallintaa.

- Kansallisille/valtiollisille CERT-ryhmille on laadittu **perusvalmiuksia ja -palveluja koskevat vähimmäisvaatimukset**[20] ja niihin liittyvät **toimintasuositukset**[21], jotta ne voisivat toimia tuloksellisesti ja olla keskeinen osa kansallisissa valmiuksissa, jotka liittyvät valmistautuneisuuteen, tiedonvaihtoon, koordinointiin ja reagointiin. Näiden tulosten pohjalta voidaan luoda kaikkiin jäsenvaltioihin vuoteen 2012 mennessä ENISAn tuella hyvin toimiva kansallisten/valtiollisten CERT-ryhmien verkosto. Tämä verkosto toimii perustana kansalaisille ja pk-yrityksille suunnatussa eurooppalaisessa tiedonjako- ja hälytysjärjestelmässä (EISAS), joka toteutetaan kansallisten resurssien ja valmiuksien pohjalta vuoteen 2013 mennessä.

---

19 Yhdistyneen kuningaskunnan hallitus toteaa toimintasuunnitelmaa koskevassa viidennessä raportissaan ylähuoneen EU-valiokunnalle, että EFMS ”*on ollut menestys ja vastannut politiikantekijöiden todelliseen tarpeeseen löytää kanava kokemusten vaihtoa varten*”.

20 Ks. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

21 Ks. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

4.2. Havaitseminen ja vastatoimet

- ENISA on laatinut ylätason etenemissuunnitelman eurooppalaisen tiedonjako- ja hälytysjärjestelmän (**EISAS**) luomiseksi vuoteen 2013 mennessä[22]. Se muodostuu kansallisten/valtiollisten CERT-ryhmien tasolla toteutettavista *peruspalveluista* sekä *yhteentoimivuuspalveluista*, joilla kansalliset tiedotus- ja varoitusjärjestelmät liitetään EISAS-järjestelmään. Yksi keskeinen osa-alue tässä toiminnassa on henkilötietojen asianmukainen suojaaminen.

4.3. Häiriöiden lieventäminen ja toimintakunnon palautus

- Tähän mennessä ainoastaan 12 jäsenvaltiota on järjestänyt laajamittaisia verkkoturvallisuusharjoituksia[23]. ENISA on laatinut **hyvien käytänteiden oppaan kansallisia harjoituksia varten**[24]. Lisäksi se on antanut kansallisia strategioita koskevia **suosituksia**[25] jäsenvaltioiden toimien – joita on tehostettava – tueksi.

- Ensimmäinen **yleiseurooppalainen suuren mittakaavan verkkoturvallisuusharjoitus** (*Cyber Europe 2010*) järjestettiin 4. marraskuuta 2010. Mukana olivat kaikki jäsenvaltiot, joista 19 osallistui harjoitukseen aktiivisesti. Lisäksi mukana olivat Sveitsi, Norja ja Islanti. Tulevissa yleiseurooppalaisissa harjoituksissa olisi eittämättä hyötyä yhteisistä puitteista, jotka perustuvat kansallisille varautumissuunnitelmille ja linkittyvät niihin. Puitteet tarjoaisivat perusmekanismit ja -menettelyt jäsenvaltioiden yhteydenpitoa ja yhteistyötä varten.

4.4. Kansainvälinen yhteistyö

- EFMS:n puitteissa laadittiin **internetin sietokykyä ja vakautta koskevat yhteiseurooppalaiset periaatteet ja ohjeet**[26]. Komissio keskustelee näistä periaatteista ja edistää niitä eri sidosryhmien kanssa, erityisesti yksityisen sektorin kanssa (EP3R:n kautta), kahdenvälisesti keskeisten kansainvälisten kumppanien, erityisesti Yhdysvaltojen, kanssa sekä monenvälisesti. Toimivaltansa puitteissa se keskustelee asiasta eri foorumeilla, kuten G8-ryhmässä, OECD:ssä, NATOssa (erityisesti sen marraskuussa 2010 hyväksytyn uuden strategisen mallin ja verkkopuolustusyhteistyön osaamiskeskuksen (*Cooperative Cyber-defense Center of Excellence*) pohjalta), ITU:ssa (verkkoturvallisuusalan valmiuksien parantamisen yhteydessä), ETYJ:ssä (sen turvallisuusyhteistyöfoorumin kautta), ASEANissa ja Meridianissa[27]. Tavoitteena on tehdä näistä periaatteista ja ohjeista yhteiset puitteet yhteisille kansainvälisille pyrkimyksille taata internetin pitkän aikavälin sietokyky ja vakaus.

---

22 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

23 Lähde: ENISA.

24 Ks. http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

25 Ks. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

26 Ks. http://ec.europa.eu/information_society/policy/nis/index_en.htm.

27 Meridian-prosessissa pyritään tarjoamaan hallituksille kaikkialta maailmasta välineet, joiden avulla ne voivat keskustella poliittisen tason yhteistyöstä elintärkeiden tietoinfrastruktuurien suojaamisessa (CIIP). Ks. http://meridianprocess.org/.

4.5. Euroopan elintärkeiden infrastruktuurien kriteerit TVT-toimialalla

- EFMS:ssä käytyjen teknisten keskustelujen pohjalta laadittiin **ensimmäinen luonnos TVT-toimialakohtaisista kriteereistä**, joilla voidaan tunnistaa Euroopan elintärkeät infrastruktuurit. Erityisesti niissä keskityttiin **kiinteisiin ja matkaviestintäverkkoihin ja internetiin**. Tekniset keskustelut jatkuvat ja niissä hyödynnetään kriteeriluonnoksista järjestetyissä kuulemisissa kansallisella ja Euroopan tasolla (EP3R:n kautta) yksityiseltä sektorilta saatuja kommentteja. Komissio tulee keskustelemaan jäsenvaltioiden kanssa myös TVT-toimialakohtaisista elementeistä, joita harkitaan Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä sen suojaamisen parantamistarpeen arvioinnista annetun direktiivin[28] uudelleentarkastelun yhteydessä vuonna 2012.

5. MITÄ SEURAAVAKSI?

Elintärkeitä tietoinfrastruktuureja koskevan toimintasuunnitelman toteutus on täynnä myönteisiä saavutuksia, jotka liittyvät varsinkin sen tunnustamiseen, että verkko- ja tietoturvaan tarvitaan yhteistyöhön perustuvaa lähestymistapaa, jossa ovat mukana kaikki sidosryhmät. Toimintasuunnitelma etenee suurin piirtein vuonna 2009 asetettujen välitavoitteiden ja aikataulujen mukaisesti. Tähän ei ole kuitenkaan syytä tyytyä, sillä sekä kansallisella että Euroopan tasolla on vielä paljon tehtävää, jotta pyrkimyksissä onnistuttaisiin.

On myös erityisen tärkeää nivoa toimintaa osaksi globaalia koordinointistrategiaa ja siten ulottaa nämä pyrkimykset myös kansainväliselle tasolle kaikkien asiaan liittyvien sidosryhmien kanssa, jotta voidaan tavoittaa ne muut alueet, maat ja organisaatiot, jotka kamppailevat samojen kysymysten parissa, sekä luoda kumppanuuksia yhteisten lähestymistapojen ja toimien määrittelemiseksi ja päällekkäisen työn välttämiseksi.

Meidän on edistettävä globaalia riskinhallintakulttuuria. Tässä olisi keskityttävä aikaansaamaan koordinoituja toimia kaikenlaisten häiriöiden – niin luonnon kuin ihmisenkin aiheuttamien – ehkäisemiseksi, huomaamiseksi, lieventämiseksi ja korjaamiseksi sekä verkkorikollisten saamiseksi vastuuseen teoistaan. Tähän kuuluvat myös kohdennetut toimet turvallisuusuhkia ja tietokonerikollisuutta vastaan.

Tätä varten **komissio**

- **edistää internetin sietokykyä ja vakautta koskevia periaatteita** – Internetin sietokykyä ja vakautta koskevat kansainväliset periaatteet olisi laadittava yhdessä muiden maiden, kansainvälisten organisaatioiden ja tarvittaessa globaalien yksityisen sektorin organisaatioiden kanssa käyttäen hyväksi olemassa olevia foorumeja ja prosesseja esimerkiksi internetin hallinnon saralla. Näistä periaatteista olisi luotava kaikille sidosryhmille apuväline ohjaamaan toimia, jotka liittyvät internetin sietokykyyn ja vakauteen. Tässä voitaisiin käyttää pohjana yleiseurooppalaisia periaatteita ja ohjeita.

- **perustaa strategisia kansainvälisiä kumppanuuksia** – Strategisten kumppanuuksien pohjana olisi käytettävä jo meneillään olevaa toimintaa kriittisillä aloilla, kuten verkkoturvallisuuspoikkeamien hallinnassa. Tähän kuuluvat myös harjoitukset ja CERT-ryhmien yhteistyö. Globaalisti toimivan yksityisen sektorin osallistuminen on äärimmäisen

[28] Neuvoston direktiivi 2008/114/EY.

tärkeää. EU:n ja Yhdysvaltojen huippukokouksessa marraskuussa 2010 perustettu EU:n ja Yhdysvaltojen verkkoturvallisuus ja -rikollisuustyöryhmä on tärkeä askel tähän suuntaan. Työryhmä keskittyy verkkoturvallisuuspoikkeamien hallintaan, julkisen ja yksityisen sektorin kumppanuuksiin, asiaa koskevan tietoisuuden lisäämiseen ja verkkorikollisuuteen. Se voi harkita yhteistyötä myös muiden alueiden ja maiden kanssa, jotka pohtivat vastaavia kysymyksiä. Näin voitaisiin luoda yhteisiä lähestymistapoja ja toimia sekä välttää päällekkäinen työ. Tarvitaan lisää yhteyksiä ja koordinaatiota kansainvälisillä foorumeilla, varsinkin G8-ryhmässä. Euroopan puolella taas tärkeitä menestystekijöitä ovat hyvä koordinointi kaikkien EU-toimielinten, erillisvirastojen (erityisesti ENISA ja Europol) ja jäsenvaltioiden välillä.

- **lisää luottamusta pilvipalveluihin** – On lisättävä keskustelua parhaista hallintotavoista uusia globaalisti vaikuttavia teknologioita, kuten etäresurssipalveluja eli pilvipalveluja, varten. Näissä keskusteluissa olisi luonnollisesti käsiteltävä myös tarvittavia puitteita henkilötietojen suojan takaamiseksi. Luottamus on ensiarvoisen tärkeää, jotta uusista teknologioista saadaan täysi hyöty[29].

Koska turvallisuus on kaikkien yhteisellä vastuulla, kaikkien jäsenvaltioiden on varmistettava, että niiden kansalliset toimet ja pyrkimykset yhdessä tukevat koordinoitua eurooppalaista lähestymistapaa pyrittäessä ehkäisemään, huomaamaan ja lieventämään kaikenlaisia verkkoon kohdistuvia häiriöitä ja hyökkäyksiä ja reagoimaan niihin. Tässä suhteessa **jäsenvaltioiden olisi sitouduttava**

- **kohottamaan EU:n valmiusastetta luomalla hyvin toimivien kansallisten/valtiollisten CERT-ryhmien verkosto vuoteen 2012 mennessä.** EU-toimielimet luovat vastaavasti omat CERT-ryhmänsä vuoteen 2012 mennessä. Kaikissa näissä pyrkimyksissä olisi hyödynnettävä asiaan liittyviä ENISAn laatimia perusvalmiuksien ja -palvelujen vähimmäisvaatimuksia ja niitä koskevia toimintasuosituksia. ENISA jatkaa tukeaan näille aloitteille. Tämä toiminta edistää myös eurooppalaisen tiedonjako- ja hälytysjärjestelmän (EISAS) kehittämistä laajemmalle yleisölle vuoteen 2013 mennessä.

- **yhteiseurooppalaiseen verkkoturvallisuuspoikkeamia koskevaan varautumissuunnitelmaan vuoteen 2012 mennessä sekä säännöllisiin yleiseurooppalaisiin verkkoturvallisuusharjoituksiin.** Verkkoturvallisuusharjoitukset ovat tärkeä osa johdonmukaista strategiaa verkkoturvallisuuspoikkeamiin varautumisen ja niistä toipumisen suunnittelussa sekä kansallisella että Euroopan tasolla. Tulevien yleiseurooppalaisten verkkoturvallisuusharjoitusten olisi perustuttava eurooppalaiseen verkkoturvallisuuspoikkeamia koskevaan varautumissuunnitelmaan, joka taas rakentuu kansallisille varautumissuunnitelmille ja linkittyy niihin. Tällaisen suunnitelman olisi sisällettävä perusmekanismit ja -menettelyt jäsenvaltioiden yhteydenpitoa varten sekä tuettava tulevien yleiseurooppalaisten harjoitusten mitoittamista ja järjestämistä. ENISA pyrkii yhdessä jäsenvaltioiden kanssa laatimaan tällaisen eurooppalaisen verkkoturvallisuuspoikkeamia koskevan varautumissuunnitelman vuoteen 2012 mennessä. Samassa aikataulussa kaikkien jäsenvaltioiden olisi laadittava säännöllisesti tarkistettavat kansalliset varautumissuunnitelmat ja suunniteltava reagointi- ja toipumisharjoituksia.

---

[29] Ks. esimerkiksi ENISAn raportit *Cloud Computing Information Assurance Framework* (2009), http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport) ja *Security and resilience in governmental clouds* (2011), http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/).

- **eurooppalaisiin koordinoituihin pyrkimyksiin kansainvälisillä foorumeilla sekä keskusteluissa internetin turvallisuuden ja sietokyvyn parantamiseksi.** Jäsenvaltioiden olisi tehtävä keskenään ja komission kanssa yhteistyötä edistääkseen periaate- tai normipohjaista lähestymistapaa kysymykseen internetin globaalista vakaudesta ja sietokyvystä. Tässä olisi pyrittävä edistämään ennaltaehkäisyä ja valmistautuneisuutta kaikilla tasoilla ja kaikkien sidosryhmien keskuudessa, ja tasapainottamaan näiden keskustelujen nykyistä taipumusta painottua sotilaallisiin ja/tai kansallisiin turvallisuusnäkökohtiin.

6. PÄÄTELMÄ

Kokemus osoittaa, että pelkästään kansalliset tai alueelliset lähestymistavat eivät ole riittäviä vastaamaan turvallisuus- ja sietokykyhaasteisiin. Eurooppalainen yhteistyö on kehittynyt huomattavasti vuodesta 2009, ja siinä on päästy rohkaiseviin tuloksiin, joista hyvänä esimerkkinä *Cyber Europe 2010* -harjoitus. Euroopan olisi kuitenkin jatkettava pyrkimyksiään luoda koko EU:hun johdonmukainen ja yhteistyöhön perustuva lähestymistapa. Uudistetun ENISAn olisi tässä pitkän aikavälin hankkeessa lisättävä tukeaan jäsenvaltioille, EU:n toimielimille ja yksityiselle sektorille.

Jotta eurooppalaiset pyrkimykset voisivat onnistua, niiden on nivouduttava maailmanlaajuisella tasolla koordinoituun lähestymistapaan. Tätä silmällä pitäen komissio aikoo edistää verkkoturvallisuudesta käytävää keskustelua kaikilla asianmukaisilla kansainvälisillä foorumeilla.

Unkarin EU-puheenjohtajuuskaudella järjestetään 14.–15. huhtikuuta 2011 elintärkeiden tietoinfrastruktuurien suojaamista koskeva ministerikonferenssi. Se tulee tarjoamaan tärkeän mahdollisuuden vahvistaa sitoutuminen jäsenvaltioiden tiiviimpään yhteistyöhön ja koordinointiin sekä Euroopan tasolla että kansainvälisesti.

LIITE

Elintärkeiden tietoinfrastruktuurien suojaamista koskeva toimintasuunnitelma: tarkempi katsaus saavutuksiin ja seuraaviin vaiheisiin

Toimintasuunnitelma etenee yleisesti komission vuonna 2009 asettamien välitavoitteiden ja aikataulujen mukaisesti. Seuraavassa esitetään kaikkien osioiden ”saavutukset” ja ”seuraavat vaiheet”. Tässä katsauksessa on otettu huomioon, että joitain toimia on käsitelty edelleen Euroopan digitaalistrategiassa ja EU:n sisäisen turvallisuuden strategian toteuttamissuunnitelmassa.

1. Varautuminen ja ehkäisy

Perusvalmiudet ja -palvelut yleiseurooppalaista yhteistyötä varten

Saavutukset

– ENISA laati ja sopi vuonna 2009 yhdessä Euroopan CERT-ryhmien (*Computer Emergency Response Team*) kanssa vähimmäisvaatimukset perusvalmiuksille ja -palveluille, joita kansalliset/valtiolliset CERT-ryhmät tarvitsevat voidakseen toimia tuloksellisesti yleiseurooppalaista yhteistyötä tukevalla tavalla. Tässä yhteydessä päästiin yhteisymmärrykseen joukosta ehdottoman tärkeitä vaatimuksia toiminnan, teknisten valmiuksien, toimivaltuuksien ja yhteistyön alalla[30].

– Vuonna 2010 ENISA työskenteli Euroopan CERT-ryhmien kanssa muokatakseen edellä mainituista toimintasuuntautuneista vaatimuksista joukon suosituksia[31] kansallisille/valtiollisille CERT-ryhmille, jotta ne voisia toimia keskeisessä asemassa varautumiseen, tiedonvaihtoon, koordinointiin ja reagointiin liittyvissä kansallisissa valmiuksissa.

– Toistaiseksi 20 jäsenvaltiota[32] on perustanut kansallisen/valtiollisen CERT-ryhmän ja lähes kaikissa muissa jäsenvaltioissa sellainen on suunnitteilla. Komissio on ehdottanut toimenpiteitä EU-toimielinten CERT-ryhmien perustamiseksi vuoteen 2012 mennessä. Asia mainitaan Euroopan digitaalistrategiassa ja edelleen tarkemmin EU:n sisäisen turvallisuuden strategian toteuttamissuunnitelmassa.

Seuraavat vaiheet

– ENISA jatkaa tukeaan niille jäsenvaltioille, jotka eivät vielä ole perustaneet kansallista/valtiollista CERT-ryhmää, joka täyttäisi edellä mainitut perusvaatimukset. Tavoitteena on varmistaa, että kaikkiin jäsenvaltioihin saadaan vuoden 2011 loppuun mennessä hyvin toimiva kansallinen/valtiollinen CERT-ryhmä. Tämä välitavoite tasoittaa tietä hyvin toimivalle kansallisten CERT-ryhmien verkostolle, joka on Euroopan digitaalistrategian mukaisesti määrä luoda **vuoteen 2012 mennessä**.

---

30 Ks. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

31 Ks. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

32 Lähde: ENISA.

– ENISA pohtii yhteistyössä kansallisten/valtiollisten CERT-ryhmien kanssa, voitaisiinko perusvaatimuksia laajentaa, jotta CERT-ryhmillä olisi paremmat valmiudet tukea jäsenvaltioita niiden varmistaessa elintärkeiden TVT-infrastruktuurien sietokykyä ja vakautta, ja jotta niistä voisi muodostua selkäranka kansalaisille ja pk-yrityksille suunnatulle eurooppalaiselle tiedonjako- ja hälytysjärjestelmälle (EISAS), joka on EU:n sisäisen turvallisuuden strategian toteuttamissuunnitelman mukaisesti määrä toteuttaa kansallisten resurssien ja valmiuksien turvin **vuoteen 2013 mennessä**.

Sietokykyä käsittelevä eurooppalainen julkis-yksityinen kumppanuus (EP3R)

Saavutukset

– EP3R perustettiin vuonna 2009 Euroopan laajuiseksi ohjausjärjestelmäksi TVT-infrastruktuurien sietokyvyn alalla. Sen tarkoitus on vaalia julkisen ja yksityisen sektorin yhteistyötä turvallisuus- ja sietokykytavoitteisiin, perusvaatimuksiin, hyviin toimintamalleihin ja käytännön toimiin liittyvissä kysymyksissä. Kuten EU:n sisäisen turvallisuuden strategian toteuttamissuunnitelmassa todetaan, EP3R tekee ”*yhteistyötä myös kansainvälisten kumppanien kanssa, jotta tietoverkkojen riskinhallintaa voidaan lujittaa maailmanlaajuisesti*”. ENISA on edesauttanut EP3R:n toimintaa.

– Julkisen ja yksityisen sektorin sidosryhmiltä pyydettiin lausuntoja EP3R:n tavoitteista, periaatteista ja rakenteesta ja jotta löydettäisiin kannustimia, joilla asianomaiset sidosryhmät saataisiin aktiivisesti mukaan toimintaan[33]. EP3R:n painopistealat määriteltiin ehdotuksessa ENISAn uudistamiseksi[34].

– Samalla kun määriteltiin EP3R:n rakennetta, vuoden 2010 lopulla perustettiin kolme työryhmää, joiden aiheet olivat seuraavat: a) keskeiset voimavarat, resurssit ja toiminnot keskeytymätöntä ja turvattua sähköistä viestintää varten maiden välillä; b) sähköisen viestinnän turvallisuuteen ja sietokykyyn liittyvät perusvaatimukset; c) koordinointi- ja yhteistyötarpeet ja -mekanismit, joilla voidaan varautua ja reagoida sähköiseen viestintään vaikuttaviin suuren mittakaavan häiriöihin.

– Komission vuonna 2010 antamassa ENISAn uudistusehdotuksessa määriteltiin EP3R:lle pitkän aikavälin kestävät puitteet: ehdotuksen mukaan ENISA: ”*tukee julkisen ja yksityisen sektorin sidosryhmien yhteistyötä unionin tasolla muun muassa edistämällä tiedonvaihtoa ja tietoisuuden lisäämistä ja helpottamalla niiden pyrkimyksiä kehittää ja ottaa käyttöön normeja riskinhallintaa ja sähköisten tuotteiden, verkkojen ja palvelujen tietoturvaa varten*”.

Seuraavat vaiheet

– Vuonna 2011 vahvistetaan edelleen yhteistyötä julkisen ja yksityisen sektorin sidosryhmien välillä tavoitteena parantaa turvallisuutta ja sietokykyä innovatiivisin toimin ja menetelmin sekä määritellä sidosryhmien vastuualueet. EP3R:n työryhmät julkaisevat ensimmäiset tuloksensa, joilta odotetaan vipuvaikutusta ENISAn tukitehtäville ja tuelle. Tulevassa toiminnassa tarkastellaan myös älykkäiden sähköverkkojen verkkoturvallisuushaasteita käyttäen perustana komission ja ENISAn tekemää pohjatyötä.

[33] Ks. http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/index_en.htm.

[34] KOM(2010) 521.

– EP3R toimii kanavana maailmanlaajuisille yhteyksille yhteiskuntapolitiikkaan, talouteen ja markkinoihin liittyvissä kysymyksissä, joilla on merkitystä turvallisuuden ja sietokyvyn kannalta. Komissio aikoo EP3R:n avulla tukea EU:n ja Yhdysvaltojen verkkoturvallisuus- ja -rikollisuustyöryhmän toimintaa, jotta saadaan luotua johdonmukainen ympäristö julkisen ja yksityisen sektorin yhteistyölle sovellettavien kilpailu- ja valtiontukisääntöjen puitteissa.

– Pitkällä aikavälillä ja uuden ENISA-asetusehdotuksen mukaisesti EP3R:stä on tarkoitus tulla keskeinen osa uudistetun ENISAn toimintaa.

Euroopan jäsenvaltiofoorumi (EFMS)

Saavutukset

– EFMS perustettiin vuonna 2009, ja sillä pyritään vaalimaan asianomaisten viranomaisten välistä keskustelua ja yhteydenpitoa hyvistä toimintamalleista ja jakamaan tietoa TVT-infrastruktuurin turvallisuuteen ja sietokykyyn liittyvistä poliittisista tavoitteista ja painopisteistä muun muassa hyödyntäen suoraan ENISAn tekemää työtä ja tarjoamaa tukea. EFMS kokoontuu neljästi vuodessa, ja sen toimintaa on vuoden 2010 puolivälistä lähtien tuettu ENISAn ylläpitämällä omalla verkkosivustolla.

– EFMS on saavuttanut merkittävää edistystä seuraavilla aloilla: a) kriteerien määrittely tärkeimpien eurooppalaisten TVT-infrastruktuurien valitsemiseksi Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä annetun direktiiviin[35] yhteydessä, b) internetin sietokykyyn ja vakauteen liittyvien eurooppalaisten painopisteiden, periaatteiden ja suuntaviivojen määrittely ja c) tiedonvaihto hyvistä toimintatavoista, erityisesti verkkoturvallisuusharjoituksiin liittyen.

– Jäsenvaltiot pitävät EFMS:ää tärkeänä keskustelufoorumina ja keinona vaihtaa kokemuksia hyvistä toimintamalleista[36].

Seuraavat vaiheet

– Vuonna 2011 EFMS:ssä saadaan päätökseen tekniset keskustelut eurooppalaisten elintärkeiden TVT-infrastruktuurien kriteereistä. Lisäksi se määrittelee pitkän aikavälin suuntaviivat ja painopisteet eurooppalaisille suuren mittakaavan verkko- ja tietoturvaharjoituksille.

– EFMS tulee edelleen osallistumaan keskusteluihin turvallisuuteen ja sietokykyyn liittyvien kansainvälisten yhteyksien painotuksista erityisesti suhteessa EU:n ja Yhdysvaltojen verkkoturvallisuus- ja -rikollisuustyöryhmään.

– EFMS:n tulevissa toimissa, joissa hyödynnetään ENISAn suoraa tukea, keskitytään seuraaviin[37]: kansallisten/valtiollisten CERT-ryhmien tehokkaat yhteistyömenetelmät, vähimmäisvaatimukset julkisissa hankinnoissa verkkoturvallisuuden parantamiseksi,

35 Neuvoston direktiivi 2008/114/EY.

36 Yhdistyneen kuningaskunnan hallitus toteaa toimintasuunnitelmaa koskevassa viidennessä raportissaan ylähuoneen EU-valiokunnalle, että EFMS ”*on ollut menestys ja vastannut politiikantekijöiden todelliseen tarpeeseen löytää kanava kokemusten vaihtoa varten*”.

37 KOM(2010) 251.

turvallisuutta ja sietokykyä tukevat taloudelliset ja sääntelylliset kannustimet (kilpailu- ja valtiontukisääntöjen puitteissa) sekä Euroopan verkkoturvallisuustilanteen arviointi.

2. Havaitseminen ja vastatoimet

Eurooppalainen tiedonjako- ja hälytysjärjestelmä (EISAS)

Saavutukset

– Komissio on rahoittanut kahta prototyyppihanketta (FISHAS ja NEISAS), jotka ovat parhaillaan loppusuoralla.

– ENISA on laatinut vuoden 2007 toteutettavuustutkimuksensa[38] ja kansallisten ja yleiseurooppalaisten alan hankkeiden analyysin perustella ylätason etenemissuunnitelman EISAS-järjestelmän toteuttamiseksi vuoteen 2013 mennessä[39].

Seuraavat vaiheet

– Vuonna 2011 ENISA auttaa jäsenvaltioita toteuttamaan EISAS-etenemissuunnitelmaa määrittelemällä peruspalvelut, joita jäsenvaltiot tarvitsevat luodakseen kansallisten/valtiollisten CERT-valmiuksiensa pohjalta kansallisen tiedonjako- ja hälytysjärjestelmänsä (ISAS).

– Vuonna 2012 ENISA määrittelee yhteentoimivuuspalvelut, joilla kukin kansallinen ISAS saadaan toiminnallisesti liitettyä EISAS-järjestelmään. ENISA auttaa jäsenvaltioita myös testaamaan näitä palveluja kansallisten järjestelmien vaiheittaisessa yhdistämisessä.

– Vuosina 2011–2012 ENISA auttaa kansallisia/valtiollisia CERT-ryhmiä sisällyttämään ISAS-valmiudet palveluihinsa.

3. Häiriöiden lieventäminen ja toimintakunnon palautus

Kansalliset varautumissuunnitelmat ja harjoitukset

Saavutukset

– Vuoden 2010 lopulla ainoastaan 12 jäsenvaltiota oli laatinut kansallisen varautumissuunnitelman ja/tai järjestänyt harjoituksia suuren mittakaavan verkkoturvallisuuspoikkeamiin reagointia ja toimintakunnon palauttamista silmällä pitäen[40].

– ENISA laati kansallisten ja kansainvälisten kokemusten pohjalta oppaan kansallisiin harjoituksiin liittyvistä hyvistä toimintamalleista[41], järjesti jäsenvaltioiden ja eri puolilta maailmaa tulevien CERT-ryhmien kanssa kansallisiin harjoituksiin liittyviä tapaamisia ja

38 Ks. http://www.enisa.europa.eu/act/cert/other-work/files/EISAS_finalreport.pdf

39 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

40 Ks. http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

41 Ks. http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

antoi hiljattain toimintapoliittiset suositukset kansallisten strategioiden laatimisesta[42]. Suosituksissa kansallisille/valtiollisille CERT/CSIRT-ryhmille annetaan keskeinen rooli kansallisessa varautumissuunnittelussa ja testaamisessa, johon osallistuvat sekä yksityisen että julkisen sektorin sidosryhmät.

Seuraavat vaiheet

– ENISA tukee edelleen jäsenvaltioita niiden pyrkiessä laatimaan kansallisia varautumissuunnitelmia ja järjestämään säännöllisiä harjoituksia laajamittaisiin verkkoturvaloukkauksiin reagoimisessa ja kriisitilanteiden hoitamisessa. Tässä pyritään vaiheittain yleiseurooppalaiseen koordinointiin.

Yleiseurooppalaiset harjoitukset laajojen verkkoturvaloukkausten varalle

Saavutukset

– Ensimmäinen yleiseurooppalainen suuren mittakaavan verkkoturvallisuusharjoitus (*Cyber Europe 2010*) järjestettiin 4. marraskuuta 2010. Mukana olivat kaikki jäsenvaltiot, joista 19 osallistui harjoitukseen käytännön tasolla. Lisäksi mukana olivat Sveitsi, Norja ja Islanti. Harjoituksen järjesti ja arvioi ENISA[43]. Suunnitteluryhmässä oli mukana kahdeksan jäsenvaltiota ja harjoituksen teknisestä tuesta vastasi Yhteinen tutkimuskeskus.

Seuraavat vaiheet

– Vuonna 2011 keskustellaan jäsenvaltioiden kanssa vuodelle 2012 kaavaillun seuraavan yleiseurooppalaisen verkkoturvallisuusharjoituksen tavoitteista ja laajuudesta. Tässä yhteydessä harkitaan vaiheittaista lähestymistapaa, jossa toteutettavat harjoitukset ovat teknisesti pidemmälle meneviä ja osallistuvia jäsenvaltioita on pienempi määrä. Harjoituksiin voisi osallistua myös kansainvälisiä toimijoita. ENISA jatkaa tukeaan tälle prosessille.

– Komissio rahoittaa EuroCybex-hanketta, jossa suoritetaan vuoden 2011 jälkipuoliskolla tietokonepohjainen simulaatioharjoitus.

– Verkkoturvallisuusharjoitukset ovat tärkeä osa johdonmukaista strategiaa verkkoturvallisuuspoikkeamiin varautumisen suunnittelussa sekä kansallisella että Euroopan tasolla. Tulevien yleiseurooppalaisten verkkoturvallisuusharjoitusten olisi tämän vuoksi perustuttava eurooppalaiseen verkkoturvallisuuspoikkeamia koskevaan varautumissuunnitelmaan, joka taas rakentuu kansallisille varautumissuunnitelmille ja linkittyy niihin. Tällaisen suunnitelman olisi sisällettävä perusmekanismit ja -menettelyt jäsenvaltioiden yhteydenpitoa varten sekä tuettava tulevien yleiseurooppalaisten harjoitusten mitoittamista ja järjestämistä. ENISA pyrkii yhdessä jäsenvaltioiden kanssa laatimaan tällaisen eurooppalaisen verkkoturvallisuuspoikkeamia koskevan varautumissuunnitelman vuoteen 2012 mennessä. Samassa aikataulussa kaikki jäsenvaltiot laativat säännöllisesti tarkistettavat kansalliset varautumissuunnitelmat ja määrittelevät reagointi- ja toipumisharjoituksia. Tuloksen saavuttamisen edellyttämä koordinointi hoidetaan EFMS:n puitteissa.

---

42 Ks. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

43 Ks. http://www.enisa.europa.eu/.

Kansallisten/valtiollisten CERT-ryhmien yhteistyön lujittaminen

Saavutukset

– Yhteistyö kansallisten/valtiollisten CERT-ryhmien välillä on lisääntynyt. Kansallisten/valtiollisten CERT-ryhmien perusvalmiuksiin, CERT-harjoituksiin ja kansallisiin harjoituksiin sekä verkkoturvallisuuspoikkeamien hallintaan liittynyt ENISAn työ on auttanut aikaansaamaan ja tukemaan tiiviimpää yleiseurooppalaista yhteistyötä kansallisten/valtiollisten CERT-ryhmien välillä.

Seuraavat vaiheet

– ENISA jatkaa tukeaan kansallisten/valtiollisten CERT-ryhmien yhteistyölle. Tätä varten se laatii vuonna 2011 analyysin ja antaa ohjeistusta tarkoitukseen sopivasta suojatusta yhteydenpitokanavasta CERT-ryhmien välillä. Tähän sisältyy myös toteutusta ja jatkokehitystä koskeva etenemissuunnitelma. ENISA analysoi myös Euroopan tason toiminnalliset puutteet ja raportoi tavoista parantaa CERT-ryhmien ja eri sidosryhmien välistä rajat ylittävää yhteistoimintaa erityisesti reagointitapojen koordinoinnissa.

– Euroopan digitaalistrategiassa kehotetaan jäsenvaltioita luomaan kansallisen tason CERT-ryhmien toimiva verkosto **vuoteen 2012 mennessä**.

4. Kansainvälinen yhteistyö

Internetin sietokyky ja vakaus

Saavutukset

– EFMS:n puitteissa tehdyn työn pohjalta laadittiin internetin sietokykyä ja vakautta koskevat yhteiseurooppalaiset periaatteet ja ohjeet[44].

Seuraavat vaiheet

– Komissio aikoo vuonna 2011: tiedottaa ja keskustella periaatteista sekä kahdenvälisessä yhteistyössä kansainvälisten kumppanien, erityisesti Yhdysvaltojen, kanssa sekä monenvälisessä yhteydenpidossa G8-ryhmän, OECD:n, Meridianin ja ITU:n puitteissa; kuulla asiaan liittyviä sidosryhmiä, erityisesti yksityistä sektoria, Euroopan tasolla (EP3R:n kautta) ja kansainvälisesti (Internetin hallintofoorumin IGF:n ja muiden asianmukaisten foorumien kautta) sekä edistää keskustelua keskeisten internet-alan toimijoiden/organisaatioiden kanssa.

– Vuonna 2012 kansainväliset kumppanit pyrkivät luomaan periaatteista ja ohjeista yhteiset puitteet internetin pitkän aikavälin sietokykyyn ja vakauteen tähtääville kansainvälisille yhteisille pyrkimyksille.

Maailmanlaajuiset harjoitukset laajamittaisten internet-verkkoturvapoikkeamien hoitamista ja lieventämistä varten

Saavutukset

[44] Ks. http://ec.europa.eu/information_society/policy/nis/index_en.htm.

– Yhdysvaltain Cyber Storm III -verkkoturvallisuusharjoitukseen osallistui kansainvälisinä kumppaneina seitsemän jäsenvaltiota[45]. Komissio ja ENISA osallistuivat tarkkailijoina.

Seuraavat vaiheet

– Vuonna 2011 komissio laatii Yhdysvaltojen kanssa EU:n ja Yhdysvaltojen verkkoturvallisuus- ja -rikollisuustyöryhmän alaisuudessa vuosille 2012/2013 yhteisen ohjelman ja etenemissuunnitelman yhteisiä/yhteensovitettuja mannertenvälisiä verkkoturvallisuusharjoituksia varten. Lisäksi harkitaan yhteyksiä muihin alueisiin tai maihin samankaltaisissa kysymyksissä lähestymistapojen jakamiseksi ja yhteisen toimien toteuttamiseksi.

5. Euroopan elintärkeiden infrastruktuurien kriteerit TVT-toimialalla

Alakohtaiset kriteerit Euroopan elintärkeille TVT-infrastruktuureille

Saavutukset

– EFMS:n puitteissa käytyjen, TVT-toimialakohtaisia kriteerejä koskevien keskustelujen pohjalta laadittiin alustavat kriteerit kiinteille ja matkaviestintäverkoille sekä internet-yhteyksille.

Seuraavat vaiheet

– EFMS:ssä jatketaan teknisiä keskusteluja TVT-toimialakohtaisista kriteereistä, jotka on tarkoitus saada valmiiksi vuoden 2011 loppuun mennessä. Samaan aikaan muutamat jäsenvaltiot suunnittelevat yksityisen sektorin kuulemisia TVT-toimialan alustavista kriteereistä. Euroopan tasolla kuulemisia on tarkoitus järjestää EP3R:n kautta.

– Komissio keskustelee jäsenvaltioiden kanssa TVT-toimialakohtaisista seikoista, jotka on otettava huomioon Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä annetun direktiivin 2008/114/EY uudelleentarkastelussa vuonna 2012.

–

[45] FR, DE, HU, IT, NL, SE ja UK.