EUROOPAN KOMISSIO

Bryssel 30.9.2010
SEC(2010) 1123 lopullinen

KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA

TIIVISTELMÄ VAIKUTUSTEN ARVIOINNISTA

Oheisasiakirja

ehdotukseen

EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVIKSI

tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS kumoamisesta

{COM(2010) 517 final}
{SEC(2010) 1122 final}

TIIVISTELMÄ VAIKUTUSTEN ARVIOINNISTA

1. ONGELMAN MÄÄRITTELY

Tietojärjestelmiin kohdistuvien hyökkäysten määrä on kasvanut merkittävästi sen jälkeen, kun puitepäätös tietojärjestelmiin kohdistuvista hyökkäyksistä tehtiin. Eräs johtava internet-turvallisuusyritys raportoi, että luottamuksellisiin tietoihin kohdistuvat uhat (julkiseen tietoon verrattuna) lisääntyivät huomattavasti vuonna 2008 eli 624 267:stä 1 656 227:ään havaittuun uhkaan vuonna 2008.[1] Lisäksi on tehty useita ennennäkemättömän laajamittaisia ja vaarallisia hyökkäyksiä, esimerkiksi Virossa vuonna 2007 ja Liettuassa vuonna 2008. Maaliskuussa 2009 valtiollisten ja yksityisten organisaatioiden tietokonejärjestelmät 103 maassa joutuivat kaapattujen tietokoneiden muodostaman verkon hyökkäyksen kohteeksi. Tällöin siepattiin arkaluontoisia ja luokiteltuja asiakirjoja.[2] Hyökkäys tehtiin bottiverkkojen[3] avulla. Bottiverkot muodostuvat haittaohjelmien saastuttamista tietokoneista, joita voidaan hallita etäältä. Tällä hetkellä maailmalla leviää Conficker-bottiverkko (joka tunnetaan myös nimillä Downup, Downadup ja Kido). Se on levinnyt ennennäkemättömän laajalti marraskuusta 2008 alkaen ja vaikuttanut miljooniin tietokoneisiin eri puolilla maailmaa.[4]

Toiseksi jäsenvaltioiden ja erityisesti EU:n lainvalvonta- ja oikeusviranomaisten riittämättömän yhteistyön vuoksi on vaikea vastata näihin hyökkäyksiin koordinoidusti ja tehokkaasti. Vaikka tietojärjestelmiin kohdistuvista hyökkäyksistä tehtyä puitepäätöstä koskevasta täytäntöönpanokertomuksesta ilmenee, että useimmat jäsenvaltiot ovat perustaneet puitepäätöksen 11 artiklassa edellytetyt vakinaiset yhteyspisteet, kiireellisiin yhteistyöpyyntöihin vastaamisessa ja vastaamisvalmiudessa on edelleen ongelmia.[5]

Yhteyspisteen olemassaolo ei takaa sen toimivuutta. Komissiolle lähettämissään ilmoituksissa eräät jäsenvaltiot totesivat, että vaikka ne olivat perustaneet yhteyspisteet, ne eivät toimineet ympäri vuorokauden kuten puitepäätöksessä edellytetään. Tämä tarkoittaa, että ne eivät voi vastata kiireellisiin pyyntöihin virka-ajan ulkopuolella. Julkisen ja yksityisen sektorin yhteistyötä haittaa usein yhteyspisteiden tehottomuus tai niiden kyvyttömyys vastata yksityisen sektorin yhteistyöpyyntöihin.

Kolmanneksi tietoverkkohyökkäyksiä samoin kuin poliisin ja oikeusviranomaisten jatkotoimia koskevaa tietoa on edelleen saatavilla vain vähän. Kaikki jäsenvaltiot eivät kerää tietoverkkohyökkäyksiä koskevia tietoja. Ne, jotka keräävät tietoja, tekevät sen tavalla, joka estää vertailun, sillä jäsenvaltiot käyttävät erilaisia tilastointimenetelmiä.

---

1 http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf, s. 10.

2 www.theglobeandmail.com/servlet/story/RTGAM.20090328.wspy0328/BNStory/International/home?cid=al_gam_mostemail

3 ”Bottiverkolla” tarkoitetaan haittaohjelmien (tietokonevirusten) saastuttamaa tietokoneverkkoa. Tällainen kaapattujen tietokoneiden (zombie-koneiden) muodostama verkko voidaan saada toimimaan halutulla tavalla, esimerkiksi hyökkäämään tietojärjestelmiä vastaan (tietoverkkohyökkäykset). Näitä zombie-koneita voi hallita toinen tietokone usein käyttäjien sitä tietämättä. Tätä isäntäkonetta kutsutaan myös komentopalvelimeksi. Komentopalvelinta hallinnoivat henkilöt ovat myös rikoksentekijöitä, sillä he käyttävät kaapattuja tietokoneita käynnistääkseen hyökkäyksiä tietojärjestelmiä vastaan. Näitä henkilöitä on erittäin vaikea jäljittää, sillä bottiverkon muodostavat ja hyökkäyksen tekevät tietokoneet voivat olla eri paikassa kuin rikoksentekijä itse.

4 http://www.lemonde.fr/technologies/article/2009/03/31/virus-conficker-catastrophe-ou-poisson-d-avril_1174916_651865.html

5 Komission kertomus neuvostolle tietojärjestelmiin kohdistuvista hyökkäyksistä 24 päivänä helmikuuta 2005 tehdyn neuvoston puitepäätöksen 12 artiklan perusteella, KOM(2008) 448 lopullinen.

Tietojärjestelmiin kohdistuvien laajamittaisten hyökkäysten kohteisiin kuuluvat tietojärjestelmiä käyttävä yleisö, keskus- ja paikallishallinto, kansainväliset järjestöt ja yksityiset yritykset.

Hyökkäys voidaan käynnistää EU:n ulkopuolella, vaikka kohde olisi EU:ssa ja päinvastoin.

2. TOISSIJAISUUS

Tietoverkkorikollisuus on kansainvälinen ongelma, jota voidaan vain harvoin torjua pelkästään kansallisin toimenpitein. Yleensä katsotaan, että sekä EU:n että kansainvälisen tason toimet ovat tarpeen tietoverkkorikollisuuden torjumiseksi ja siihen puuttumiseksi. Useimmat hyökkäykset tapahtuvat yli EU:n rajojen. Ne vaikuttavat kaikkiin jäsenvaltioihin, ja on todisteita siitä, että huomattavaan osaan niistä liittyy toimia, jotka on toteutettu yli jäsenvaltioiden rajojen. Tietojärjestelmät ovat usein teknisesti yhteydessä toisiinsa ja riippuvaisia toisistaan rajojen yli. Asiantuntijat ovatkin samaa mieltä siitä, että sekä kansainvälisiä että EU:n toimia tarvitaan, ja että tällaista rikollisuutta ei voida torjua riittävän tehokkaasti pelkästään jäsenvaltioiden toimin.

Tietoverkkorikollisuutta koskeviin kansallisiin ratkaisuihin perustuvan lähestymistavan vaarana on toimien hajanaisuus ja tehottomuus koko Euroopan kannalta katsottuna. Kansallisten lähestymistapojen erot ja järjestelmällisen rajatylittävän yhteistyön puute vähentävät merkittävästi kansallisten vastatoimien vaikuttavuutta. Tämä johtuu osittain tietojärjestelmien keskinäisistä yhteyksistä, sillä alhainen turvataso yhdessä maassa voi lisätä muiden maiden haavoittuvuutta.

3. TAVOITTEET

3.1 Yleistavoitteet, erityistavoitteet ja toiminnalliset tavoitteet

EU:n toiminnan yleistavoitteena on torjua järjestäytynyttä tai muuta rikollisuutta ja asettaa rikoksentekijät syytteeseen Euroopan unionin toiminnasta tehdyn sopimuksen 67 artiklan mukaisesti estämällä tietojärjestelmiin kohdistuvia laajamittaisia tietoverkkohyökkäyksiä.

A Erityistavoite: asettaa syytteeseen ja tuomita laajamittaisista hyökkäyksistä vastuussa olevat rikolliset lähentämällä tietoverkkojärjestelmiin kohdistuvia hyökkäyksiä koskevaa rikoslainsäädäntöä

B Erityistavoite: parantaa lainvalvontaviranomaisten välistä yhteistyötä rajojen yli

C Erityistavoite: ottaa käyttöön tehokkaat valvonta- ja tiedonkeruujärjestelmät

4. TOIMINTAVAIHTOEHDOT

4.1 Toimintavaihtoehto 1: nykytilanteen säilyttäminen / ei uusia EU:n toimia

Tämä vaihtoehto tarkoittaa sitä, että EU ei toteuta uusia toimia tämäntyyppisen tietoverkkorikollisuuden torjumiseksi. Käynnissä olevia toimia jatketaan, erityisesti ohjelmia, joiden tavoitteena on lujittaa elintärkeän tietoinfrastruktuurin suojaamista ja parantaa julkisen ja yksityisen sektorin yhteistyötä tietoverkkorikollisuuden torjumiseksi.

4.2 Toimintavaihtoehto 2: ohjelman laatiminen tietojärjestelmiin kohdistuvien hyökkäysten torjunnan lujittamiseksi muilla kuin lainsäädännöllisillä toimenpiteillä

Elintärkeän tietoinfrastruktuurin suojaamiseen tähtäävän ohjelman lisäksi muissa kuin lainsäädännöllisissä toimenpiteissä keskityttäisiin rajatylittävään lainvalvontaan ja julkisen ja yksityisen sektorin yhteistyöhön. Niillä myös parannettaisiin toimintojen koordinointia EU:n tasolla. Ei-lainsäädännölliseen ehdotukseen sisältyisi lainvalvontaviranomaisten yhteyspisteistä koostuvan nykyisen ympärivuorokautisen verkoston lujittaminen, tietoverkkorikollisuuden asiantuntijoista ja lainvalvontaviranomaisista koostuvan julkisen ja yksityisen sektorin yhteyspisteiden muodostaman EU:n verkoston perustaminen ja vakiomuotoisen EU:n palvelusopimuksen laatiminen yksityisen sektorin toimijoiden kanssa tehtävää lainvalvontayhteistyötä varten.

4.3 Toimintavaihtoehto 3: puitepäätöksen kohdennettu päivittäminen tietojärjestelmiin kohdistuvien laajamittaisten hyökkäysten uhkaan puuttumiseksi

Tässä vaihtoehdossa otetaan käyttöön kohdennettu (ts. rajoitettu) lainsäädäntö tarkoituksena torjua tietojärjestelmiin kohdistuvia erityisen vaarallisia laajamittaisia hyökkäyksiä. Kohdennettu lainsäädäntö liittyisi toimenpiteisiin, joiden tarkoituksena on lujittaa tietojärjestelmiin kohdistuvien hyökkäysten torjumiseen tähtäävää rajatylittävää operatiivista yhteistyötä ja koventaa vähimmäisseuraamuksia. Tässä vaihtoehdossa nykyistä tietojärjestelmiin kohdistuvista hyökkäyksistä tehtyä puitepäätöstä päivitettäisiin täydentämällä sitä muilla kuin lainsäädännöllisillä toimenpiteillä, joita olisivat esimerkiksi elintärkeän tietoinfrastruktuurin suojaamiseen liittyvien valmiuksien, turvallisuuden ja kestävyyden parantaminen, rajaylittävässä lainvalvontayhteistyössä käytettävien välineiden ja menettelyjen lujittaminen ja parhaiden käytänteiden vaihto.

4.4 Toimintavaihtoehto 4: tietoverkkorikollisuuden torjumiseen tähtäävän kattavan EU:n lainsäädännön käyttöön ottaminen

Tarve ryhtyä nopeasti toimiin tietojärjestelmiin kohdistuvia kehittyneitä hyökkäyksiä vastaan herättää kysymyksen siitä, olisiko aiheellista antaa tietoverkkorikollisuutta yleensä koskevaa laajempaa EU:n lainsäädäntöä. Tämän lainsäädännön piiriin eivät kuuluisi pelkästään tietojärjestelmiin kohdistuvat hyökkäykset, vaan myös sellaiset seikat kuin talousalan tietoverkkorikollisuus, laiton internetsisältö, sähköisten todisteiden kerääminen/säilyttäminen/siirtäminen ja lainkäyttövaltaa koskevat yksityiskohtaisemmat säännöt. EU:n lainsäädäntöä sovellettaisiin rinnakkain tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen kanssa, jota täydennettäisiin erityisesti EU:n kannalta tarpeellisiksi katsotuilla uusilla säännöksillä.

4.5 Toimintavaihtoehto 5: tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen päivittäminen

Tämän vaihtoehdon toteutuminen edellyttäisi huomattavia uudelleenneuvotteluja nykyisestä yleissopimuksesta. Se olisi pitkällinen prosessi ja vastoin vaikutusten arvioinnissa ehdotettua toiminta-aikataulua. Kansainvälisesti ei myöskään näytä olevan halukkuutta neuvotella yleissopimus uudelleen. Yleissopimuksen päivittämistä ei sen vuoksi voida katsoa toteuttamiskelpoiseksi vaihtoehdoksi, koska se ei sovi vaaditun toiminta-aikataulun puitteisiin.

5. VAIKUTUSTEN ARVIOINTI

Vaihtoehdot	Taloudelliset vaikutukset	Sosiaaliset vaikutukset	Perusoikeuksia koskevat vaikutukset	Vaikutukset kolmansiin maihin	Merkitys tavoitteiden A, B ja C kannalta	Yhdenmukaisuu kansainvälisen oikeuden kanssa
Vaihtoehto 1: nyky–tilanteen säilyttäminen / ei uusia EU:n toimia	0	0	0	-	0	0
Vaihtoehto 2: ohjelman laatiminen tieto–järjestelmiin kohdis–tuvien hyökkäysten torjunnan lujittamiseksi muilla kuin lainsäädän–nöllisillä toimenpiteillä	-/+	++	-/+	++	A + B ++ C +	-/+
Vaihtoehto 3: puite–päätöksen kohdennettu päivittäminen, jotta voi–daan puuttua tietojärjes–telmiin kohdistuvien laajamittaisten hyökkäysten uhkaan	--/++	-/+++	-/++	+++	A +++ B +++ C +++	++
Vaihtoehto 4: tietoverkkorikollisuuden torjumiseen tähtäävän kattavan EU-lain–säädännön käyttöön ottaminen	---/+++	+++	--/++	++	A ++ B ++ C ++	-/++
Parhaaksi arvioitu vaihtoehto (vaihtoehdot 2 ja 3): muiden kuin lainsäädännöllisten toimenpiteiden ja tieto–järjestelmiin kohdis–tuvista hyökkäyksistä tehdyn puitepäätöksen kohdennetun päivit–tämisen yhdistelmä	--/+++	+++	-/++	+++	A +++ B +++ C +++	++

6. TOIMINTAVAIHTOEHTOJEN VERTAILU

6.1 Toimintavaihtoehto 1: nykytilanteen säilyttäminen

Tämä vaihtoehto heikentäisi väistämättä yksityisten toimijoiden, jäsenvaltioiden ja EU:n asemaa tietoverkkorikollisuuden torjunnassa, kun otetaan huomioon kyseisen rikollisuuden luonne ja kasvu. Vaikka nykyisten toimenpiteiden taso säilytettäisiin, koordinointia tarvittaisiin EU:n tasolla.

6.2 Toimintavaihtoehto 2: ohjelman laatiminen tietojärjestelmiin kohdistuvien hyökkäysten torjunnan lujittamiseksi muilla kuin lainsäädännöllisillä toimenpiteillä

Tällä vaihtoehdolla on kaikki sellaiset edut ja haitat, jotka liittyvät pehmeisiin sääntelyvälineisiin. Myönteistä on se, että kukin toimintavaihtoehto voidaan kuvata tavalla, joka on parhaiden kansallisten käytänteiden mukainen, ja näin voidaan helpottaa vaikuttavuudeltaan parhaiden toimenpiteiden kartoittamista.

Tämä vaihtoehto ei ole kuitenkaan yhtä tehokas tavoitteiden saavuttamisen suhteen.

6.3 Toimintavaihtoehto 3: puitepäätöksen kohdennettu päivittäminen tietojärjestelmiin kohdistuvien laajamittaisten hyökkäysten uhkaan puuttumiseksi

Tämä vaihtoehto tarjoaa oikea-aikaisen ja kohdennetun vastauksen havaittuihin ongelmiin. Siinä käsitellään rikosoikeudellisia seikkoja, joiden avulla rikoksentekijät voidaan panna syytteeseen tietoverkkorikoksista. Sen avulla myös parannetaan kansainvälistä yhteistyötä ottamalla käyttöön välittömään kansainväliseen avunantoon perustuva mekanismi tapauksissa, joissa on kyse kiireellisistä yhteistyöpyynnöistä, ja edistetään yksityissektorin kanssa tehtävää yhteistyötä lisätoimenpiteillä, esimerkiksi järjestämällä asiantuntijakokouksia. Tässä vaihtoehdossa otetaan käyttöön useita raskauttavia olosuhteita, joita ovat esimerkiksi hyökkäysten laajamittaisuus sekä hyökkäysten toteuttaminen salaamalla rikoksentekijän todellinen henkilöllisyys ja aiheuttamalla vahinkoa henkilöllisyyden oikealle omistajalle.

Ongelman laajuuden määrittämiseksi säädetään valvontavelvoitteista.

6.4 Toimintavaihtoehto 4: tietoverkkorikollisuuden torjumiseen tähtäävän kattavan EU:n lainsäädännön käyttöön ottaminen

Vaihtoehto 3:n tapaan tämän vaihtoehdon lisäarvona on sitovien säännösten vahvistaminen. Näin ollen vaikuttavuus paranee, jos vaihtoehto pannaan täysimääräisesti täytäntöön. Sen avulla on myös tarkoitus hyödyntää täysimääräisesti sekä lainsäädännöllisten että muiden välineiden myönteinen vaikutus monenlaisiin tietoverkkorikoksiin, ei pelkästään laajamittaisiin hyökkäyksiin. Lisäksi siinä käsiteltäisiin rikosoikeudellista kehystä ja parannettaisiin lainvalvontayhteistyötä yli rajojen. Tämä kokonaisvaltainen lähestymistapa ei kuitenkaan tällä hetkellä kuvasta sidosryhmien konsensusta asiasta, vaikka sen täytäntöönpanolla päästäisiin tietoverkkorikollisuutta koskevassa torjunnassa pidemmälle kuin muiden vaihtoehtojen avulla.

7. PARHAAKSI ARVIOITU VAIHTOEHTO

Taloudellisten, sosiaalisten ja perusoikeuksiin kohdistuvien vaikutusten analyysin perusteella vaihtoehdot 2 ja 3 tarjoavat parhaan lähestymistavan ongelmiin asetettujen tavoitteiden saavuttamiseksi.

Parhaaksi arvioitu vaihtoehto olisi toimintavaihtoehtojen 2 ja 3 yhdistelmä, sillä ne täydentävät toisiaan ja sen vuoksi niillä saavutetaan määritellyt tavoitteet parhaiten sekä sisällön että aikataulun osalta.

8. SEURANTA JA ARVIOINTI

Täytäntöönpanoa koskeva kertomus olisi julkaistava kahden vuoden kuluessa direktiivin voimaantulosta. Kertomuksessa olisi tarkasteltava sitä, miten direktiivi on todellisuudessa pantu jäsenvaltioissa täytäntöön.

Lisäksi olisi arvioitava säännöllisesti, kuinka ja missä määrin direktiivi on edistänyt siinä asetettujen tavoitteiden saavuttamista. Ensimmäinen arviointi olisi toteutettava viiden vuoden kuluessa direktiivin voimaantulosta. Tämän jälkeen komissio julkaisee arviointikertomuksen viiden vuoden välein. Kertomukset sisältävät tietoja täytäntöönpanosta. Arviointiin perustuvien päätelmien ja suositusten pohjalta komission olisi otettava huomioon direktiivin mahdollinen muuttaminen tai muu mahdollinen kehitys.