Euroopan unionin neuvosto

Bryssel, 14. syyskuuta 2017
(OR. en)

Toimielinten välinen asia:
2017/0225 (COD)

12183/17
ADD 2

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

SAATE

Lähettäjä:	Euroopan komission pääsihteerin puolesta Jordi AYET PUIGARNAU, johtaja
Vastaanottaja:	Jeppe TRANHOLM-MIKKELSEN, Euroopan unionin neuvoston pääsihteeri
Kom:n asiak. nro:	SWD(2017) 501 final
Asia:	KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA TIIVISTELMÄ VAIKUTUSTEN ARVIOINNISTA Oheisasiakirja Ehdotukseen EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI EU:n kyberturvallisuusvirastosta ENISAsta ja asetuksen (EU) 526/2013 kumoamisesta sekä tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (”kyberturvallisuusasetus”)

Valtuuskunnille toimitetaan oheisena asiakirja SWD(2017) 501 final.

Liite: SWD(2017) 501 final

EUROOPAN
KOMISSIO

Bryssel 13.9.2017
SWD(2017) 501 final

KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA

TIIVISTELMÄ VAIKUTUSTEN ARVIOINNISTA

Oheisasiakirja

Ehdotukseen EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI

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

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. TOIMIA TARVITAAN

Mikä on ongelma ja miksi se on ongelma?

Digitaaliset teknologiat ja internet ovat keskeisen tärkeitä EU:n taloudelle ja yhteiskunnalle. Kriittiset talouden alat, kuten liikenne, energia, terveydenhuolto ja rahoitus, ovat tulleet yhä riippuvaisemmiksi verkko- ja tietojärjestelmistä keskeisen toimintansa ylläpitämiseksi. Esineiden internet yhdistää esineet ja ihmiset viestintäverkkojen välityksellä. Tämä uusi todellisuus tarjoaa ennennäkemättömiä mahdollisuuksia, mutta siihen liittyy myös riskejä. Kyberturvallisuuspoikkeamien määrä onkin kasvussa. Niiden monimutkaisuuden, toistumistiheyden ja kohteena olevien alojen kirjon – keskeisistä palveluista demokraattisiin prosesseihin – odotetaan kasvavan edelleen.

Tässä yhteydessä on kartoitettu seuraavat toisiinsa liittyvät ongelmat:

- kyberturvallisuuspolitiikan ja -lähestymistapojen hajanaisuus jäsenvaltioissa;
- hajanaiset resurssit ja yhtenäisen linjan puute kyberturvallisuuslähestymistavoissa EU:n toimielimissä, virastoissa ja elimissä;
- kansalaisten ja yritysten riittämätön tietoisuus kyberuhkista ja riittämätön tiedotus kansalaisten ja yritysten ostamien tieto- ja viestintätekniikan tuotteiden ja palvelujen turvallisuusominaisuuksista yhdistettynä yhä useampien erillisten kansallisten ja alakohtaisten sertifiointijärjestelmien käyttöönottoon.

Nämä ongelmat vaikuttavat koko EU:n kykyyn sietää kyberuhkia (kyberresilienssi) ja heikentävät sisämarkkinoiden tehokasta toimintaa.

Mitä olisi saavutettava?

Aloitteen toimintapoliittiset erityistavoitteet ovat seuraavat:

1. Jäsenvaltioiden ja yritysten valmiuksien ja varautumiskyvyn lisääminen erityisesti kriittisten infrastruktuurien osalta.
2. Yhteistyön ja koordinoinnin lisääminen jäsenvaltioiden ja EU:n toimielinten, virastojen ja elinten välillä.
3. EU-tason valmiuksien lisääminen jäsenvaltioiden toimien täydentämiseksi erityisesti rajat ylittävien kyberkriisien yhteydessä.
4. Kansalaisten ja yritysten tietoisuuden lisääminen kyberturvallisuuteen liittyvistä kysymyksistä.
5. Yleisen avoimuuden lisääminen tieto- ja viestintäteknisten tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa, jotta voidaan lisätä luottamusta digitaalisiin sisämarkkinoihin ja digitaalisiin innovaatioihin.
6. Hajanaisuuden välttäminen sertifiointijärjestelmissä EU:ssa ja niihin liittyvissä turvallisuusvaatimuksissa ja arviointiperusteissa jäsenvaltioissa ja eri aloilla.

Mikä on EU-tason toiminnasta saatava lisäarvo?

Koska talouden ja yhteiskunnan vuorovaikutuksella ja digitalisoitumisella on maailmanlaajuisia vaikutuksia, ongelmat ulottuvat paljon yhden jäsenvaltion aluetta laajemmalle. Tämä edellyttää, että toimiin ryhdytään unionin tasolla. Nykyisessä tilanteessa ja tulevaisuuden skenaarioita tarkastellen näyttää siltä, että jäsenvaltioiden yksittäiset toimet ja hajanainen lähestymistapa kyberturvallisuuteen ja erityisesti sen vahvaan rajatylittävään ulottuvuuteen eivät lisää unionin kollektiivista kyberresilienssiä.

B. RATKAISUT

Millä vaihtoehdoilla tavoitteet saavutettaisiin? Onko jokin vaihtoehto arvioitu parhaaksi?

Tässä vaikutustenarvioinnissa tarkastellaan eri toimintavaihtoehtoja Euroopan unionin verkko- ja tietoturvaviraston (ENISA) ja tieto- ja viestintäteknologian turvallisuussertifioinnin uudelleentarkastelun perusteella.

ENISAn uudelleentarkastelu

Vaihtoehto 0 – Perusskenaario – Tässä vaihtoehdossa mikään ei muutu. ENISAn toimeksiantoa jatkettaisiin ja sen tavoitteet ja tehtävät säilyisivät pääosin ennallaan, mukaan lukien sittemmin EU:n lainsäädännössä (esim. verkko- ja tietoturvadirektiivissä) ENISAlle annetut tehtävät.

Vaihtoehto 1 – ENISAn toimeksiannon päättäminen (ENISAn lakkauttaminen). Tämä vaihtoehto johtaisi ENISAn lakkauttamiseen sen nykyisen toimeksiannon päättyessä (kesäkuussa 2020) ja mahdollisesti toimivallan ja toimintojen uudelleenjakamiseen EU:n ja/tai kansallisella tasolla.

Vaihtoehto 2 – ”Uudistettu ENISA”. Tämä vaihtoehto perustuisi ENISAn nykyiseen toimeksiantoon, johon tehtäisiin valikoituja muutoksia, joissa otetaan huomioon kyberturvallisuustilanteen kehitys. ENISAlle annettaisiin pysyvä toimeksianto, jonka pohjana olisivat seuraavat keskeiset osatekijät: tuki EU:n politiikan kehittämiselle ja täytäntöönpanolle; valmiuksien kehittäminen; tietämys ja tiedotus; markkinoihin liittyvät tehtävät; tutkimus ja innovointi; ja operatiivinen yhteistyö ja kriisinhallinta.

Vaihtoehto 3 – EU:n kyberturvallisuusvirasto, jolla on täydet operatiiviset valmiudet. Tämä vaihtoehto koskee ENISAn uudistamista siten, että sillä olisi seuraavat kolme päätehtävää: 1. poliittinen/neuvoa-antava tehtävä; 2. tieto- ja osaamiskeskus; ja 3. tietotekniikan kriisiryhmä (CERT). Tämä vaihtoehto aiheuttaisi suurelta osin samoja muutoksia toimeksiantoon kuin vaihtoehto 2. ENISAlle annettaisiin kuitenkin uusia tehtäviä tietoturvaloukkauksiin reagoinnin ja kriisinhallinnan aloilla, jotta sen toimeksianto kattaisi kyberturvallisuuden koko elinkaaren ja sillä olisi valmiudet kyberturvallisuuspoikkeamien ennaltaehkäisyyn, havaitsemiseen ja niihin reagointiin.

Sertifiointi

Vaihtoehto 0 – Perusskenaario – mikään ei muutu. Tässä vaihtoehdossa komissio säilyttää vallitsevan tilanteen eikä ryhdy toimintapoliittisiin tai lainsäädännöllisiin toimiin.

Vaihtoehto 1 – **Muut kuin lainsäädäntötoimet (ei-sitovat toimenpiteet)**. Tässä vaihtoehdossa komissio käyttäisi ei-sitovia poliittisia välineitä (esim. tulkitsevat tiedonannot, EU:n laajuisten itsesääntelyaloitteiden tukeminen ja standardointitoimet) avoimuuden parantamiseksi ja hajanaisuuden vähentämiseksi.

Vaihtoehto 2 – Unionin säädös, jolla SOGIS-sopimus laajennetaan kaikkiin jäsenvaltioihin. Tässä toimintavaihtoehdossa komissio antaisi lainsäädäntöehdotuksen, jolla jäsenyys laajennettaisiin koskemaan kaikkia jäsenvaltioita.

Vaihtoehto 3 – **Yleinen EU:n kehys tieto- ja viestintätekniikan turvallisuussertifioinnille**. Tässä vaihtoehdossa perustettaisiin eurooppalainen kehys tieto- ja viestintätekniikan turvallisuussertifioinnille (mukaan luettuna kansallisista viranomaisista koostuva asiantuntijaryhmä), joka perustuisi mahdollisimman pitkälti nykyisiin tieto- ja viestintäteknologian turvallisuussertifiointijärjestelmiin. Kehys mahdollistaisi sellaisten EU:n sertifiointijärjestelmien perustamisen, jotka hyväksyttäisiin kaikissa jäsenvaltioissa.

Parhaaksi arvioitu vaihtoehto on vaihtoehdon 2 (ENISAn uudistaminen) ja vaihtoehdon 3 (sertifiointi) yhdistelmä.

Mitkä ovat eri sidosryhmät? Mitkä toimijat kannattavat mitäkin vaihtoehtoa?

Suuri enemmistö kuulemisiin vastanneista kaikissa sidosryhmäluokissa (jäsenvaltiot, toimiala, EU:n toimielimet, tutkimusyhteisö) vaikuttaa olevan tyytyväinen parhaaksi arvioituun vaihtoehtoon, sillä ne kannattavat ENISAn vahvistamista ja eurooppalaisen kehyksen luomista tieto- ja viestintäteknologian turvallisuussertifiointia varten.

Erityisesti sidosryhmät ovat yksimielisiä siitä, että tarvitaan (ainakin) hyvin toimiva EU:n virasto, jolla on pysyvä toimeksianto, riittävät resurssit ja valtuutus käsitellä nykyisiä ja tulevia kyberturvallisuuden haasteita. Sidosryhmät ovat laajalti yksimielisiä myös vapaaehtoisuuteen perustuvan, laajennettavissa olevan eurooppalaisen kehyksen luomisesta.

Teollisuuden sidosryhmistä kyseistä sertifiointiratkaisua tukevat yritykset, joihin jo sovelletaan sertifiointivaatimuksia ja jotka hyötyisivät EU:n laajuisesta sertifikaattien vastavuoroiseen tunnistamiseen perustuvasta mekanismista. Sertifiointiratkaisu saa kannatusta myös pk-yrityksiltä, jotka kärsivät eniten eri sertifiointiprosessien käynnistämisestä eri jäsenvaltioissa. Jotkut jäsenvaltiot – erityisesti ne, joilla on vähemmän resursseja – sekä jotkut teollisuudenalan edustajista ja EU:n toimielimistä kertoivat suhtautuvansa myönteisesti myös vaihtoehtoon 3 (ENISAn uudistaminen).

C. PARHAAKSI ARVIOIDUN VAIHTOEHDON VAIKUTUKSET

Mitkä ovat parhaaksi arvioidun vaihtoehdon hyödyt (jos parhaaksi arvioitua vaihtoehtoa ei ole, päävaihtoehtojen hyödyt)?

Parhaaksi arvioidun vaihtoehdon seurauksena EU:lla olisi virasto, joka keskittyisi jäsenvaltioiden, EU:n toimielinten ja yritysten tukemiseen aloilla, joilla se toisi eniten lisäarvoa. Näitä aloja ovat verkko- ja tietoturvadirektiivin täytäntöönpanon tukeminen, politiikan kehittäminen ja täytäntöönpano; tiedotus, tietämys ja tietoisuus; tutkimustoimet; operatiivinen yhteistyö ja kriisinhallinta; markkinat. Erityisesti ENISA tukisi EU:n politiikkaa tieto- ja viestintäteknologian turvallisuussertifioinnin alalla varmistamalla tieto- ja

viestintäteknologian turvallisuussertifioinnin eurooppalaisen kehyksen hallinnollisen ylläpidon ja teknisen hallinnoinnin. Kehyksen avulla otetaan käyttöön tieto- ja viestintäteknologian turvallisuussertifioinnin hallinnointia koskevat säännöt, joiden tarkoituksena on edistää eri jäsenvaltioissa myönnettyjen sertifikaattien vastavuoroista tunnustamista. Näiden ratkaisujen yhdistelmä on arvioitu toimintatavaksi, jonka avulla EU voi tuloksekkaimmin saavuttaa asetetut tavoitteet eli lisätä kyberturvallisuusvalmiuksia, varautumista, yhteistyötä, tietoisuutta ja avoimuutta ja estää markkinoiden pirstaloitumisen. Tämä vaihtoehto on myös parhaiten linjassa poliittisten painopistealueiden kanssa, sillä se liittyy läheisesti kyberturvallisuusstrategiaan ja sitä koskevaan toimintapolitiikkaan (esim. verkko- ja tietoturvadirektiiviin) sekä digitaalisiin sisämarkkinoihin. Lisäksi tällä vaihtoehdolla tavoitteet saavutettaisiin kohtuullisin resurssein.

Mitkä ovat parhaaksi arvioidun vaihtoehdon kustannukset (jos parhaaksi arvioitua vaihtoehtoa ei ole, päävaihtoehtojen kustannukset)?

Lisätehtävistään huolimatta ”uudistettu ENISA” säilyisi kompaktina organisaationa. Unionin talousarviosta saatava tarvittava rahoitusosuus olisi korkeampi kuin tällä hetkellä mutta silti aika paljon alhaisempi verrattuna muihin kriittisillä aloilla toimiviin virastoihin.

Tieto- ja viestintäteknologian turvallisuussertifioinnin eurooppalaisen kehyksen luominen ei lisäisi toimialalle (mukaan luettuina pk-yritykset) aiheutuvia alkuvaiheen kustannuksia. Sen sijaan siitä aiheutuisi merkittäviä säästöjä yrityksille, jotka jo sertifioivat tuotteensa tai ovat valmiita ryhtymään tuotteidensa sertifiointiin, ja niiden maailmanlaajuinen kilpailukyky paranisi. Toisaalta siihen liittyisi tiettyjä mainitun kehyksen ylläpitoa koskevia budjettisitoumuksia, jotka johtuisivat pääasiassa vaihtoehdosta ”uudistettu ENISA” ja koskisivat teknisiä ja sihteeristön tehtäviä.

Kohdistuuko jäsenvaltioiden budjettiin ja julkishallintoon merkittäviä vaikutuksia?

Ei. ENISAn vahvistamisesta aiheutuvat kustannukset katettaisiin pääosin EU:n talousarviosta. Lisäksi jäsenvaltiot voisivat edelleen maksaa virastolle vapaaehtoisia rahoitusosuuksia. Kansallisille talousarvioille ja julkishallinnoille sertifioinnista aiheutuvat kustannukset johtuisivat suurimmaksi osin mahdollisesta sertifiointiviranomaisen perustamisesta.

Onko toimenpiteellä muita merkittäviä vaikutuksia?

Ei.

Suhteellisuusperiaate

Parhaaksi arvioitu vaihtoehto koostuu tasapainoisista toimenpiteistä, jotka kaikki katsotaan tarpeellisiksi, jotta asetetut tavoitteet voitaisiin saavuttaa aiheuttamatta liiallisia rasitteita asianomaisille sidosryhmille. Näin ollen tämän aloitteen katsotaan olevan suhteellisuusperiaatteen mukainen.

D. SEURANTA

Milloin asiaa tarkastellaan uudelleen?

Ensimmäinen arviointi on määrä tehdä viiden vuoden kuluttua säädöksen voimaantulosta. Komissio laatii arvioinnista kertomuksen Euroopan parlamentille ja neuvostolle ja liittää siihen tarvittaessa uudelleentarkastelua koskevan ehdotuksen. Sen jälkeen arviointi suoritetaan viiden vuoden välein.