EUROOPAN
KOMISSIO

Bryssel 4.10.2017
COM(2017) 476 final

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

Suurin hyöty verkko- ja tietoturvadirektiivistä – toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetun direktiivin (EU) 2016/1148 tehokas täytäntöönpano

Johdanto

Verkko- ja tietojärjestelmien turvallisuudesta unionissa 6. heinäkuuta 2016 annettu direktiivi (EU) 2016/1148[1] (jäljempänä ’verkko- ja tietoturvadirektiivi’ tai ’direktiivi’) on ensimmäinen horisontaalinen EU-säädös, jossa käsitellään kyberturvallisuuteen liittyviä haasteita. Se oli todellinen käännekohta Euroopan kyberresilienssin ja kyberturvallisuusyhteistyön kannalta.

Direktiivillä on kolme päätavoitetta:

- kansallisten kyberturvallisuusvalmiuksien parantaminen
- yhteistyön parantaminen EU:n tasolla ja
- riskinhallintakulttuurin ja poikkeamista raportoinnin edistäminen keskeisten talouden toimijoiden keskuudessa, joita ovat erityisesti yhteiskunnan ja talouden toimintojen ylläpitämisen kannalta keskeisiä palveluja tarjoavat toimijat (keskeisten palvelujen tarjoajat) ja digitaalisen palvelun tarjoajat.

Verkko- ja tietoturvadirektiivi on keskeinen osa EU:n vastausta niihin kasvaviin kyberuhkiin ja -haasteisiin, joita talous- ja yhteiskuntaelämän digitalisoituminen tuo mukanaan. Sen täytäntöönpano on siten olennainen osa 13. syyskuuta 2017 esitettyä kyberturvallisuuspakettia. EU:n toiminta ei voi olla täysin tehokasta niin kauan kuin verkko- ja tietoturvadirektiiviä ei ole saatettu täydessä mitassa osaksi kaikkien jäsenvaltioiden lainsäädäntöä. Tämä tunnustettiin kriittiseksi kohdaksi myös Euroopan kyberresilienssijärjestelmän vahvistamisesta vuonna 2016 annetussa komission tiedonannossa[2].

Koska verkko- ja tietoturvadirektiivi on annettu vasta hiljattain ja nopeasti muuttuva kyberuhkien ympäristö vaatii pikaisia toimia, on syytä kiinnittää erityistä huomiota haasteisiin, joita kaikki toimijat kohtaavat yrittäessään varmistaa direktiivin viipymättömän ja onnistuneen saattamisen osaksi kansallista lainsäädäntöä. Määräaika direktiivin saattamiselle osaksi kansallista lainsäädäntöä on 9. toukokuuta 2018, ja keskeisten palvelujen tarjoajat on määrä määrittää 9. marraskuuta 2018 mennessä. Näiden määräaikojen noudattamiseksi komissio on tukenut jäsenvaltioiden täytäntöönpanoprosessia ja niiden työtä yhteistyöryhmässä.

Tämä tiedonanto ja sen liite perustuvat komission valmistelutöihin ja analyysiin, jotka liittyvät verkko- ja tietoturvadirektiivin tähänastiseen täytäntöönpanoon. Näiden lisäksi se pohjautuu Euroopan verkko- ja tietoturvaviraston (ENISA) panokseen sekä keskusteluihin, joita on käyty jäsenvaltioiden kanssa etenkin yhteistyöryhmässä[3], kun direktiiviä on saatettu osaksi kansallista lainsäädäntöä. Tämä tiedonanto täydentää niitä huomattavia toimia, joita on tähän mennessä toteutettu etenkin seuraavin tavoin:

[1] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa. Direktiivi tuli voimaan 8. elokuuta 2016.
[2] COM(2016) 410 final.
[3] Verkko- ja tietoturvadirektiivin 11 artiklan mukainen jäsenvaltioiden välisen strategisen yhteistyön mekanismi.

- Yhteistyöryhmässä on tehty intensiivistä työtä, ja se on sopinut työsuunnitelmasta, jossa keskitytään pääasiassa verkko- ja tietoturvadirektiivin saattamiseen osaksi kansallista lainsäädäntöä ja erityisesti keskeisten palvelujen tarjoajien määrittämiseen ja niiden turvallisuusvaatimuksia ja poikkeamista ilmoittamista koskeviin velvollisuuksiin. Direktiivissä jätetään jonkin verran liikkumavaraa keskeisten palvelujen tarjoajia koskevien säännösten saattamisessa osaksi kansallista lainsäädäntöä, mutta jäsenvaltiot ovat tunnustaneet, että tässä suhteessa olisi tärkeää noudattaa yhdenmukaista lähestymistapaa[4].
- Tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden (CSIRT-toimijoiden) verkosto on perustettu ja se on aloittanut nopeasti toimintansa direktiivin 12 artiklan 1 kohdan mukaisesti. Verkosto on alkanut luoda perustaa jäsennellylle operatiiviselle yhteistyölle Euroopan tasolla.

Sekä poliittisella että operatiivisella tasolla, joita nämä kaksi rakennetta edustavat, kaikkien jäsenvaltioiden täysimittainen sitoutuminen on olennaisen tärkeää, jotta voidaan saavuttaa tavoitteena oleva yhteinen korkeatasoinen verkko- ja tietojärjestelmien turvallisuus unionissa.

Tällä tiedonannolla ja sen liitteellä vahvistetaan näitä toimia kokoamalla yhteen ja vertailemalla direktiivin täytäntöönpanoon liittyviä jäsenvaltioiden parhaita käytäntöjä, antamalla lisäohjeistusta direktiivin täytäntöönpanosta ja selittämällä tarkemmin yksittäisiä säännöksiä. Yleisenä tavoitteena on auttaa jäsenvaltioita saavuttamaan verkko- ja tietoturvadirektiivin tehokas ja yhdenmukainen täytäntöönpano kaikkialla EU:ssa.

Tätä tiedonantoa täydennetään myöhemmin verkko- ja tietoturvadirektiivin 16 artiklan 8 kohdan mukaisella komission täytäntöönpanoasetuksella, jossa määritellään tarkemmin digitaalisen palvelun tarjoajien turvallisuus- ja ilmoitusvaatimuksiin liittyvät osatekijät ja parametrit. Täytäntöönpanoasetus helpottaa direktiivin täytäntöönpanoa digitaalisen palvelun tarjoajia koskevien velvollisuuksien osalta[5].

Tiedonannossa esitetään keskeiset päätelmät niiden kysymysten analyysista, joita pidetään tärkeinä vertailukohtina ja mahdollisina inspiraation lähteinä, kun direktiiviä saatetaan osaksi kansallista lainsäädäntöä. Päähuomio on säännöksissä, jotka liittyvät jäsenvaltioiden valmiuksiin ja velvollisuuksiin direktiivin soveltamisalaan kuuluvien toimijoiden osalta. Liitteessä tarkastellaan yksityiskohtaisemmin aloja, joilla komissio katsoo olevan hyödyllisintä antaa täytäntöönpanoa koskevaa käytännön ohjeistusta, ja siinä selitetään ja tulkitaan joitain direktiivin säännöksiä ja esitellään parhaita käytäntöjä ja direktiivistä tähän mennessä saatuja kokemuksia.

[4] Yhteistyöryhmä laatii parhaillaan ohjeasiakirjoja muun muassa seuraavista kysymyksistä: kriteerit palveluntarjoajan kriittisen aseman määrittämiseksi direktiivin 5 artiklan 2 kohdan mukaisesti; olosuhteet, joissa keskeisten palvelujen tarjoajien edellytetään ilmoittavan poikkeamista 14 artiklan 7 kohdan perusteella; ja 14 artiklan 1 ja 2 kohdassa tarkoitetut keskeisten palvelujen tarjoajia koskevat turvallisuusvaatimukset.

[5] Täytäntöönpanoasetuksen luonnos on asetettu saataville julkista kuulemista varten osoitteessa https://ec.europa.eu/info/law/better-regulation/have-your-say_en

Kohti verkko- ja tietoturvadirektiivin tehokasta täytäntöönpanoa

Verkko- ja tietoturvadirektiivin tavoitteena on saavuttaa yhteinen korkeatasoinen verkko- ja tietojärjestelmien turvallisuus unionissa. Tämä tarkoittaa internetin sekä yhteiskunnan ja talouden toimintaa tukevien yksityisten verkkojen ja tietojärjestelmien turvallisuuden parantamista. Tässä suhteessa ensimmäinen tärkeä osatekijä on jäsenvaltioiden varautuminen, joka olisi varmistettava ottamalla käyttöön direktiivissä kuvaillut CSIRT-toimijoiden ja toimivaltaisten kansallisten viranomaisten laatimat kansalliset kyberturvallisuusstrategiat.

Kansallisten strategioiden kattavuus

On tärkeää, että jäsenvaltiot tarttuvat verkko- ja tietoturvadirektiivin täytäntöönpanon tarjoamaan mahdollisuuteen ja tarkastelevat uudelleen kansallisia kyberturvallisuusstrategioitaan tässä liitteessä käsiteltyjen puutteiden, parhaiden käytäntöjen ja uusien haasteiden valossa.

Vaikka direktiivissä keskitytäänkin ymmärrettävistä syistä niihin yrityksiin ja palveluihin, joilla on erityistä kriittistä merkitystä, koko talouden ja yhteiskunnan kyberturvallisuutta on tarkasteltava kokonaisvaltaisesti ja johdonmukaisesti, koska riippuvuus tieto- ja viestintätekniikasta kasvaa kaiken aikaa. Siksi sellaisten kattavien kansallisten strategioiden hyväksyminen, joissa mennään verkko- ja tietoturvadirektiivin vähimmäisvaatimuksia pidemmälle (eli jotka kattavat myös muita aloja ja palveluja direktiivin liitteissä II ja III lueteltujen lisäksi), parantaisi verkko- ja tietojärjestelmien yleistä turvallisuustasoa.

Koska kyberturvallisuus on edelleen suhteellisen uusi ja nopeasti kasvava julkisen politiikan ala, useimmissa tapauksissa tarvitaan uusia investointeja, vaikka julkisen talouden yleinen tilanne edellyttääkin leikkauksia ja säästöjä. Direktiivin tavoitteiden saavuttamisen kannalta on siksi olennaisen tärkeää tehdä kunnianhimoisia päätöksiä, joilla turvataan riittävät taloudelliset ja henkilöstöresurssit, jotta kansalliset strategiat voidaan toteuttaa tehokkaasti, mukaan lukien riittävien resurssien antaminen kansallisille toimivaltaisille viranomaisille ja CSIRT-toimijoille.

Tehokas täytäntöönpano ja sen valvonta

Velvollisuudesta nimetä kansalliset toimivaltaiset viranomaiset ja keskitetyt yhteyspisteet säädetään direktiivin 8 artiklassa. Tämä on yksi keskeinen tekijä, jolla pyritään varmistamaan verkko- ja tietoturvadirektiivin tehokas täytäntöönpano ja rajat ylittävä yhteistyö. Jäsenvaltioissa on tältä osin sovellettu sekä keskitetympiä että hajautetumpia ratkaisuja. Kun jäsenvaltiot soveltavat keskitetympää lähestymistapaa kansallisten toimivaltaisten viranomaisten nimeämiseen, vahvojen yhteistyöjärjestelyjen varmistaminen eri viranomaisten ja keskitetyn yhteyspisteen välillä on osoittautunut olennaisen tärkeäksi (*ks. liitteen 3.2 kohdan taulukko 1*). Tämä tehostaisi täytäntöönpanoa ja helpottaisi sen valvontaa.

Kriittisen tietoteknisen infrastruktuurin suojaamisesta saatujen kokemusten hyödyntäminen voi auttaa sellaisen optimaalisen hallintomallin suunnittelussa jäsenvaltioille, jolla

varmistetaan sekä verkko- ja tietoturvadirektiivin tehokas alakohtainen täytäntöönpano että yhdenmukainen horisontaalinen toimintatapa (*ks. liitteen 3.1 kohta*).

Kansallisten CSIRT-toimijoiden paremmat valmiudet

Jos kaikkialla EU:ssa ei ole toiminnassa verkko- ja tietoturvadirektiivin 9 artikla mukaisia tehokkaita ja riittävillä resursseilla varustettuja kansallisia CSIRT-toimijoita, EU pysyy liian haavoittuvana rajat ylittäville kyberuhille. Jäsenvaltiot voisivat siksi harkita CSIRT-toimijoiden toimialan laajentamista direktiivin soveltamisalaan kuuluvien alojen ja palvelujen ulkopuolelle (*ks. liitteen 3.3 kohta*). Kansalliset CSIRT-toimijat voisivat näin antaa operatiivista tukea kyberturvallisuuspoikkeamissa, jotka tapahtuvat sellaisissa yrityksissä ja organisaatioissa, jotka eivät kuulu direktiivin soveltamisalaan mutta jotka ovat myös tärkeitä yhteiskunnan ja talouden kannalta. Jäsenvaltioiden olisi lisäksi hyödynnettävä täydessä mitassa Verkkojen Eurooppa -välineestä rahoitettavan kyberturvallisuutta koskevan digitaalipalvelujen infrastruktuuriohjelman tarjoamia lisärahoitusmahdollisuuksia; ohjelman tarkoituksena on parantaa kansallisten CSIRT-toimijoiden valmiuksia ja niiden keskinäistä yhteistyötä (*ks. liitteen 3.5 kohta*).

Keskeisten palvelujen tarjoajien määrittämisprosessin yhdenmukaisuus

Verkko- ja tietoturvadirektiivin 5 artiklan mukaisesti jäsenvaltioiden on määritettävä 9. marraskuuta 2018 mennessä toimijat, joiden katsotaan olevan keskeisten palvelujen tarjoajia. Jäsenvaltiot voisivat tähän tehtävään liittyen käyttää yhtenäisesti tässä tiedonannossa annettuja määritelmiä ja ohjeita sen varmistamiseksi, että samantyyppiset toimijat, joilla on samanlainen asema sisämarkkinoilla, määritettäisiin johdonmukaisesti keskeisten palvelujen tarjoajiksi muissakin jäsenvaltioissa. Jäsenvaltiot voisivat myös harkita verkko- ja tietoturvadirektiivin soveltamisalan laajentamista julkishallintoon, kun otetaan huomioon sen merkitys koko yhteiskunnalle ja taloudelle (*ks. liitteen 2.1 ja 4.1.3 kohta*).

Keskeisten palvelujen tarjoajien määrittämiseen sovellettavien kansallisten toimintamallien lähentäminen niin pitkälle kuin mahdollista, erityisesti noudattamalla yhteistyöryhmän laatimia ohjeita (*ks. liitteen 4.1.2 kohta*), olisi erittäin hyödyllistä, sillä se johtaisi direktiivin säännösten yhdenmukaisempaan soveltamiseen ja vähentäisi siten markkinoiden sirpaloitumisen riskiä. Tapauksissa, joissa keskeisten palvelujen tarjoajat tarjoavat näitä palveluja kahdessa tai useammassa jäsenvaltiossa, on olennaisen tärkeää, että jäsenvaltioiden kesken pyritään pääsemään sopimukseen toimijoiden yhdenmukaisesta määrittämisestä 5 artiklan 4 kohdan mukaisessa kuulemisprosessissa (*ks. liitteen 4.1.7 kohta*), koska näin vältettäisiin saman toimijan erilainen sääntelykohtelu eri jäsenvaltioiden lainkäyttöalueella.

Keskeisten palvelujen tarjoajien määrittämistä koskevien tietojen antaminen komissiolle

Direktiivin 5 artiklan 7 kohdan mukaan jäsenvaltioiden on toimitettava komissiolle tiedot kansallisista toimenpiteistä, joiden avulla keskeisten palvelujen tarjoajat voidaan määrittää, luettelo keskeisistä palveluista sekä määritettyjen keskeisten palvelujen tarjoajien lukumäärä ja tiedot niiden merkityksestä kyseessä olevalla alalla. Jäsenvaltioiden on lisäksi toimitettava

kynnysarvot, jos sellaisia on olemassa, joita määritysprosessissa on käytetty asiaankuuluvan toimitustason määrittämiseksi tai tietyn keskeisten palvelujen tarjoajan merkityksen määrittämiseksi riittävän toimitustason ylläpitämisessä. Jäsenvaltiot voisivat myös harkita, että ne toimittavat komissiolle luettelon määritetyistä keskeisten palvelujen tarjoajista, tarvittaessa luottamuksellisesti, sillä tämä auttaisi parantamaan komission arvioinnin tarkkuutta ja laatua (*ks. liitteen 4.1.5 ja 4.1.6 kohta*).

Keskeisten palvelujen tarjoajien turvallisuus- ja ilmoitusvaatimuksia koskevien lähestymistapojen lähentäminen

Direktiivin 14 artiklan 1, 2 ja 3 kohdassa säädetään velvollisuuksista, jotka koskevat keskeisten palvelujen tarjoajien turvallisuusvaatimuksia ja niiden tekemiä ilmoituksia poikkeamista. Turvallisuusvaatimuksia ja poikkeamista ilmoittamista koskeva yhdenmukainen lähestymistapa, joka auttaisi keskeisten palvelujen tarjoajia noudattamaan vaatimuksia yli jäsenvaltioiden rajojen, edistäisi mahdollisimman laajaa sisämarkkinavaikutusta. Lähtökohtana toimii tässä edelleen yhteistyöryhmässä tehty ohjeasiakirjaa koskeva työ (*ks. liitteen 4.2 ja 4.3 kohta*).

Jos tapahtuu laajamittainen kyberturvallisuuspoikkeama, joka vaikuttaa useisiin jäsenvaltioihin, on erittäin todennäköistä, että keskeisen palvelun tarjoaja tai digitaalisen palvelun tarjoaja tekee pakollisen ilmoituksen poikkeamasta 14 artiklan 3 kohdan tai 16 artiklan 3 kohdan mukaisesti tai että jokin muu toimija, joka ei kuulu direktiivin soveltamisalaan, tekee siitä vapaaehtoisen ilmoituksen 20 artiklan 1 kohdan mukaisesti. Jäsenvaltiot voisivat koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin annetun komission suosituksen mukaisesti harkita kansallisten toimintamalliensa lähentämistä siten, että ne voivat näiden ilmoitusten perusteella antaa mahdollisimman nopeasti tietoja muiden asianomaisten jäsenvaltioiden toimivaltaisille viranomaisille tai CSIRT-toimijoille. Käytännön toimet mahdollistavat tarkat tiedot olisivat olennaisen tärkeitä poikkeaman leviämisen estämiseksi tai haavoittuvuuksien tukkimiseksi ennen kuin niitä ehditään hyödyntää.

Komissio pyrkii kumppanuuden hengessä saamaan mahdollisimman suuren hyödyn verkko- ja tietoturvadirektiivistä ja aikoo laajentaa Verkkojen Eurooppa -välineestä annettavan tuen kaikkiin tämän lainsäädännön kannalta merkityksellisiin sidosryhmiin. Painopiste on tähän saakka ollut CSIRT-toimijoiden valmiuksien rakentamisessa ja ripeän ja tehokkaan operatiivisen yhteistyön mahdollistamisessa ja siten CSIRT-verkoston vahvistamisessa, mutta komissio aikoo nyt tarkastella, kuinka Verkkojen Eurooppa -välineen rahoitus voi hyödyttää myös kansallisia toimivaltaisia viranomaisia sekä keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia.

Päätelmät

Kun otetaan huomioon verkko- ja tietoturvadirektiivin kansallisen lainsäädännön osaksi saattamisen lähestyvä määräaika 9. toukokuuta 2018 ja keskeisten palvelujen tarjoajien

määrittämisen määräaika 9. marraskuuta 2018, jäsenvaltioiden olisi toteuttava asianmukaiset toimenpiteet sen varmistamiseksi, että verkko- ja tietoturvadirektiivin säännökset ja yhteistyömallit voivat tarjota parhaat mahdolliset EU:n tason välineet yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa. Komissio pyytää jäsenvaltioita ottamaan tässä prosessissa huomioon tähän tiedonantoon sisältyvät asiaan liittyvät tiedot, ohjeet ja suositukset.

Tätä tiedonantoa voidaan täydentää muilla toimilla, mukaan lukien toimet, jotka määritellään yhteistyöryhmän käynnissä olevan työn puitteissa.