Euroopan unionin
virallinen lehti

L 237

64. vuosikerta

Suomenkielinen laitos **Lainsäädäntö**

5. heinäkuuta 2021

Sisältö

FI

Säädökset, joiden otsikot on painettu laihalla kirjasintyypillä, ovat maatalouspolitiikan alaan kuuluvia juoksevien asioiden hoitoon liittyviä säädöksiä, joiden voimassaoloaika on yleensä rajoitettu.

Kaikkien muiden säädösten otsikot on painettu lihavalla kirjasintyypillä ja merkitty tähdellä.

II

(Muut kuin lainsäätämisjärjestyksessä hyväksyttävät säädökset)

SUOSITUKSET

KOMISSION SUOSITUS (EU) 2021/1086,
annettu 23 päivänä kesäkuuta 2021,
yhteisen kyberturvallisuusyksikön perustamisesta

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 292 artiklan,

sekä katsoo seuraavaa:

(1) Kyberturvallisuus on olennaisen tärkeää talouden ja yhteiskunnan digitalisaatiokehityksen onnistumisen kannalta. EU on sitoutunut ennennäkemättömän suuriin investointeihin sen varmistamiseksi, että ihmiset, yritykset ja viranomaiset voivat luottaa digitaalisiin välineisiin.

(2) Covid-19-pandemia on lisännyt yhteenliitettävyyden merkitystä ja Euroopan riippuvuutta vakaista verkko- ja tietojärjestelmistä sekä osoittanut, että koko toimitusketju pitää suojata. Luotettavat ja turvalliset verkko- ja tietojärjestelmät ovat erityisen tärkeitä pandemian torjunnan etulinjassa oleville tahoille, kuten sairaaloille, lääkevirastoille ja rokotevalmistajille. Koordinoimalla EU:n toimia, joilla pyritään ehkäisemään, havaitsemaan, torjumaan, estämään ja lieventämään vaikutuksiltaan voimakkaimpia tällaisiin tahoihin kohdistuvia kyberhyökkäyksiä ja reagoimaan niihin, voitaisiin ehkäistä ihmishenkien menetyksiä ja yrityksiä heikentää EU:n kykyä voittaa pandemia mahdollisimman nopeasti. Lisäksi lujittamalla EU:n kykyä torjua kyberhyökkäyksiä tehokkaasti edistetään maailmanlaajuista, avointa, vakaata ja turvallista kybertoimintaympäristöä.

(3) Kyberturvallisuusuhkien rajatylittävän luonteen sekä monimutkaisempien, laajalle ulottuvien ja kohdennettujen hyökkäysten ([1]) jatkuvan lisääntymisen vuoksi asiaankuuluvien kyberturvallisuusinstituutioiden ja -toimijoiden olisi parannettava valmiuksiaan vastata tällaisiin uhkiin ja hyökkäyksiin hyödyntämällä olemassa olevia resursseja ja parantamalla toimien koordinointia. Kaikkien asiaankuuluvien toimijoiden EU:ssa on tarpeen varautua reagoimaan kollektiivisesti ja vaihtamaan tietoja pikemminkin tiedonjakotarpeen kuin tiedonsaantitarpeen perusteella.

(4) Vaikka jäsenvaltioiden välisessä kyberturvallisuutta koskevassa yhteistyössä, jota on tehty erityisesti verkko- ja tietoturva-alan yhteistyöryhmässä (NIS-yhteistyöryhmä) ja Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148 ([2]) nojalla perustetussa tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden (CSIRT) verkostossa, on edistytty merkittävästi, ei ole vieläkään yhteistä EU:n alustaa, jolla eri kyberturvallisuusyhteisöissä kerättyjä tietoja voitaisiin vaihtaa tehokkaasti ja turvallisesti ja jossa asiaankuuluvat toimijat voisivat koordinoida ja ottaa käyttöön operatiivisia valmiuksia. Tästä johtuen kyberuhkien ja -poikkeamien käsittely on siiloutunutta, minkä vuoksi tehokkuus kärsii ja haavoittuvuus lisääntyy. Lisäksi EU:n tason kanava yksityisen sektorin kanssa tehtävää teknistä ja operatiivista yhteistyötä varten puuttuu sekä tietojen jakamisen että kyberturvallisuus-poikkeamiin reagoinnin tukemisen osalta.

([1]) ENISA, 2020 Threat Landscape; Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020.

([2]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (EUVL L 194, 19.7.2016, s. 1).

(5) Nykyiset puitteet ja rakenteet sekä jäsenvaltioissa ja asiaankuuluvissa EU:n toimielimissä, elimissä ja virastoissa käytettävissä olevat resurssit ja asiantuntemus muodostavat vahvan perustan kollektiiviselle reagoinnille kyberturvallisuusuhkiin, -poikkeamiin ja -kriiseihin ([3]). Tähän olemassa olevaan arkkitehtuuriin kuuluvat operatiivisella puolella suunnitelma nopeasta ja koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin, jäljempänä 'Blueprint-suunnitelma' ([4]), CSIRT-verkosto ja Euroopan kyberkriisien yhteysorganisaatioiden verkosto (EU-CyCLONe) ([5]) sekä Euroopan kyberrikostorjuntakeskus (EC3) ja yhteinen kyberrikollisuuden torjunnan työryhmä (J-CAT) Euroopan unionin lainvalvontayhteistyövirastossa (Europol) ja EU:n lainvalvonnan hätäaputoimien protokolla (EU LE ERP). NIS-yhteistyöryhmä, EU:n tiedusteluanalyysikeskus (EU INTCEN) sekä pysyvän rakenteellisen yhteistyön (PRY) ([6]) puitteissa käynnistetyt kyberdiplomatian välineistö ([7]) ja kyberpuolustukseen liittyvät hankkeet edistävät myös osaltaan poliittista ja operatiivista yhteistyötä kyberturvallisuusyhteisöissä. Euroopan unionin kyberturvallisuusviraston (ENISA) tehtävänä on vahvistetun toimeksiantonsa nojalla tukea verkko- ja tietojärjestelmien kyberturvallisuuteen liittyvää operatiivista yhteistyötä ([8]) sekä tällaisten järjestelmien käyttäjiä ja muita henkilöitä, joihin kyberuhat ja -poikkeamat vaikuttavat. Poliittisen kriisitoiminnan integroitujen järjestelyjen (IPCR) avulla EU pystyy koordinoimaan poliittisia toimiaan suurissa kriiseissä, myös laajamittaisten kyberhyökkäysten tapauksessa.

(6) Vielä ei kuitenkaan ole olemassa mekanismia, joka auttaisi hyödyntämään olemassa olevia resursseja ja antamaan keskinäistä apua kaikissa kyberyhteisöissä verkko- ja tietojärjestelmien turvallisuuden, kyberrikollisuuden torjunnan, kyberdiplomatian toteuttamisen ja tarvittaessa kyberpuolustuksen osalta mahdollisessa kriisitilanteessa. EU:n tasolla ei myöskään ole kattavaa mekanismia tilannetietoisuuden, varautumisen ja reagoinnin tekniselle ja operatiiviselle yhteistyölle kaikkien yhteisöjen välillä. Lisäksi olisi saatava aikaan synergiaa lainvalvonta- ja tiedusteluyhteisöjen kanssa Europolin ja INTCEN:n välityksellä.

(7) Komissio, unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustaja, jäljempänä 'korkea edustaja', jäsenvaltiot sekä asiaankuuluvat EU:n toimielimet, elimet ja virastot tunnustavat, että on tärkeää analysoida viime vuosina luodun EU:n nykyisen kyberturvallisuusarkkitehtuurin vahvuuksia, heikkouksia, puutteita ja päällekkäisyyksiä. Komissio on laatinut jäsenvaltioita kuullen ja korkean edustajan myötävaikutuksella yhteisen kyberturvallisuusyksikön toimintamallin vastauksena tältä pohjalta tehtyyn analyysiin ja merkittävänä osana turvallisuusunionistrategiaa ([9]), digitaalistrategiaa ([10]) ja kyberturvallisuusstrategiaa ([11]).

([3]) Jäsenvaltiot ovat perustaneet Euroopan kyberkriisien yhteysorganisaatioiden verkoston (EU-CyCLONe) vastauksena Blueprint-suunnitelman suositukseen. Se on kansallisten operatiivisten ja kriisinhallinnan asiantuntijoiden verkosto, jota komissio ehdotti kodifioitavaksi joulukuussa 2020 ehdotetulla direktiivillä toimenpiteistä yhteisen korkeatasoisen kyberturvallisuuden varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta, COM(2020) 823 final, 2020/0359 (COD).

([4]) Komission suositus (EU) 2017/1584, annettu 13 päivänä syyskuuta 2017, koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja –kriiseihin (EUVL L 239, 19.9.2017, s. 36).

([5]) Tässä suosituksessa otetaan huomioon Blueprint Operational Level Exercise (Blue OLEx) 2020 After Action Report ja erityisesti puheenjohtajan yhteenveto yhteistä kyberturvallisuusyksikköä koskevasta strategisesta keskustelusta.

([6]) Erityisesti PRY-hankkeet, jotka koskevat kyberalan nopean toiminnan ryhmiä ja keskinäistä avunantoa kyberturvallisuudessa, joita Liettua koordinoi, ja kyber- ja tietoalan koordinointikeskusta, jota koordinoi Saksa.

([7]) Neuvoston päätelmät EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevista puitteista ("kyberdiplomatian välineistö"), 19.6.2017 (9916/17).

([8]) Euroopan parlamentin asetuksen (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintäteksiikan kyberturvallisuussertifionnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15) 7 artiklassa edellytetään, että virasto tukee operatiivista yhteistyötä jäsenvaltioiden, unionin toimielinten, elinten ja laitosten kesken sekä sidosryhmien välillä. Tähän sisältyy jäsenvaltioiden tukeminen CSIRT-verkoston puitteissa tehtävässä operatiivisessa yhteistyössä, turvallisuuspoikkeamia ja kyberuhkia koskevan säännöllisen ja perusteellisen EU:n kyberturvallisuuden teknisen tilanneraportin laatiminen ja osallistuminen yhteisen lähestymistavan kehittämiseen laajamittaisiin rajatylittäviin poikkeamiin tai kriiseihin vastaamiseksi unionin ja jäsenvaltioiden tasolla. Lisäksi ENISA osallistuu koulutustoimiin Euroopan turvallisuus- ja puolustusakatemian (ETPA) kanssa.

([9]) Komission tiedonanto Euroopan parlamentille, Eurooppa-neuvostolle, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle EU:n turvallisuusunionistrategiasta, COM(2020) 605 final.

([10]) Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Euroopan digitaalista tulevaisuutta rakentamassa, COM(2020) 67 final.

([11]) Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle: EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle, JOIN/2020/18 final.

(8) Kriisitilanteissa jäsenvaltioiden olisi voitava luottaa EU:n solidaarisuuteen koordinoidun avun muodossa, myös kaikkien neljän kyberyhteisön taholta, joita ovat siviiliyhteisö, lainvalvonta ([12]), diplomatia ja tarvittaessa puolustus. Yhden tai useamman yhteisön osallistumisaste voi riippua laajamittaisen poikkeaman tai kriisin luonteesta ja näin ollen siitä, minkä tyyppisiä vastatoimia tarvitaan. Kyberuhkien, -poikkeamien ja -kriisien sattuessa hyvin koulutetut asiantuntijat ja tekniset laitteet ovat keskeisiä voimavaroja, jotka auttavat välttämään vakavia vahinkoja ja palautumaan tilanteesta tehokkaasti. Näin ollen yhteisen kyberturvallisuusyksikön keskiössä ovat selkeästi määritellyt tekniset ja operatiiviset valmiudet, pääasiassa asiantuntijat ja laitteet, jotka ovat valmiita otettaviksi tarvittaessa käyttöön jäsenvaltioissa. Tässä ympäristössä osallistujat voivat ainutlaatuisessa asemassa edistää ja koordinoida tällaisia valmiuksia EU:n kyberturvallisuuden nopean toiminnan ryhmien kautta ja varmistaa samalla asianmukaisen synergian PRY:n puitteissa jo käynnistettyjen kyberturvallisuushankkeiden kanssa.

(9) Yhteinen kyberturvallisuusyksikkö tarjoaa virtuaalisen ja fyysisen alustan eikä edellytä uuden erillisen elimen perustamista. Sen perustaminen ei saisi vaikuttaa kansallisten kyberturvallisuusviranomaisten ja asiaankuuluvien unionin elinten toimivaltuuksiin. Yhteiselle kyberturvallisuusyksikölle olisi luotava perusta siihen osallistuvien tahojen välisissä yhteisymmärryspöytäkirjoissa. Sen olisi perustuttava olemassa oleviin rakenteisiin, resursseihin ja valmiuksiin ja tuotava niille lisäarvoa EU:n toimijoiden ja jäsenvaltioiden viranomaisten välisen turvallisen ja nopean operatiivisen ja teknisen yhteistyön alustana. Sen olisi myös koottava yhteen kaikki kyberturvallisuusyhteisöt eli siviili-, lainvalvonta-, diplomatia- ja puolustusyhteisöt. Osallistujilla olisi oltava joko operatiivinen tai tukitehtävä. Operatiivisia osallistujia ovat ENISA, Europol, EU:n toimielinten, elinten ja virastojen tietotekniikan kriisiryhmä (CERT-EU), komissio, Euroopan ulkosuhdehallinto (mukaan lukien INTCEN), CSIRT-verkosto ja EU-CyCLONe. Tukitehtäviä suorittaviin osallistujiin olisi kuuluttava Euroopan puolustusvirasto (EDA), NIS-yhteistyöryhmän puheenjohtaja, neuvoston kyberkysymysten horisontaalisen työryhmän puheenjohtaja ja yksi asiaan liittyvien PRY-hankkeiden edustaja ([13]). Koska jäsenvaltioilla on operatiiviset valmiudet ja toimivalta vastata laajamittaisiin kyberuhkiin, -poikkeamiin ja -kriiseihin, osallistujien olisi tavoitteensa saavuttaakseen hyödynnettävä ensisijaisesti näitä valmiuksia, asiaankuuluvien unionin elinten avulla.

(10) Yhteisen kyberturvallisuusyksikön toivotaan antavan uutta pontta Blueprint-suunnitelmalla vuonna 2017 käynnistetylle prosessille. Sen olisi jatkettava Blueprint-suunnitelman arkkitehtuurin käyttöönottoa ja autettava ottamaan ratkaiseva askel kohti eurooppalaista kyberturvallisuuden kriisinhallintakehystä, jossa tunnistetaan uhkia ja riskejä, lievennetään niitä ja vastataan niihin koordinoidusti ja oikea-aikaisesti. Yhteisen kyberturvallisuusyksikön odotetaan tällä tavoin auttavan EU:ta vastaamaan nykyisiin ja tuleviin uhkiin.

(11) Osallistumalla yhteiseen kyberturvallisuusyksikköön operatiivisten ja tukitehtäviä suorittavien osallistujien olisi voitava tehdä yhteistyötä laajemman sidosryhmäjoukon kanssa osana EU:n kyberturvallisuuden kriisinhallintakehystä. Harjoittaessaan tehtäviään toimeksiantojensa rajoissa osallistujien olisi voitava hyötyä paremmasta varautumisesta ja laajemmasta tilannetietoisuudesta, joka kattaa kaikki kyberturvallisuusuhkiin ja -poikkeamiin liittyvät näkökohdat, ja hyödynnettävä kyberturvallisuusasiantuntemusta. Osallistujien olisi esimerkiksi osallistuttava säännöllisesti yhteisöjen välisiin harjoituksiin, omaksuttava selkeästi määritelty rooli EU:n kriisinhallintasuunnitelmassa, lisättävä toimiensa näkyvyyttä yhteisellä julkisella viestinnällä ja tehtävä operatiivista yhteistyötä koskevia sopimuksia yksityisen sektorin kanssa. Yhteisen kyberturvallisuusyksikön toimintaan osallistumisen lisäksi osallistujien pitäisi samalla voida vahvistaa olemassa olevia verkostoja, kuten CSIRT-verkostoa ja EU-CyCLONea, tarjoamalla niiden käyttöön turvallisia tiedonvaihtovälineitä ja parempia havaitsemisvalmiuksia (eli turvaoperaatiokeskuksia) ja mahdollisuuksia hyödyntää käytettävissä olevia EU:n operatiivisia valmiuksia.

(12) Yhteisen kyberturvallisuusyksikön osallistujien olisi keskityttävä tekniseen ja operatiiviseen yhteistyöhön, yhteiset operaatiot mukaan luettuina. Osallistujien olisi edistettävä tällaista yhteistyötä toimeksiantojensa sallimissa rajoissa. Yhteistyön olisi perustuttava käynnissä oleviin toimiin ja täydennettävä niitä. Yhteistyön tyypistä riippuen siihen voi tulla mukaan myös muita osallistujia.

([12]) Koskee myös oikeudellista yhteistyötä.

([13]) Ks. alaviite 5. EU:n ulkosuhdehallinto (EUH) ja EDA ovat PRY:n sihteeristön ominaisuudessa yhteydessä asiaankuuluvien PRY-hankkeiden koordinaattoreihin.

(13) Alustan olisi koottava yhteen jäsenvaltioiden ja EU:n teknisiä ja operatiivisia kriisinhallinnan asiantuntijoita, jotta voidaan koordinoida reagointia kyberuhkiin, -poikkeamiin ja -kriiseihin hyödyntämällä olemassa olevia valmiuksia ja asiantuntemusta. Yhteiseen kyberturvallisuusyksikköön osallistuvat asiantuntijat voivat seurata ja suojata paljon laajempaa hyökkäyspintaa käyttämällä sekä fyysistä että virtuaalista alustaa. Tätä varten osallistujien olisi koordinoitava toimia rajat ylittävissä poikkeamissa ja kriiseissä sekä avun toimittamista poikkeamista kärsiville maille alustan kautta.

(14) Yhteisen kyberturvallisuusyksikön perustaminen edellyttää vaiheittaista prosessia, jossa hyödynnetään ja vahvistetaan tässä suosituksessa mainittuja jo olemassa olevia puitteita ja rakenteita, mukaan lukien yhteistyömekanismit, joita on perustettu jäsenvaltioiden johtamilla foorumeilla (esim. CSIRT-verkosto, EU-CyCLONe, neuvoston kyberkysymysten horisontaalinen työryhmä, J-CAT ja asiaankuuluvat PRY-hankkeet), sekä EU:n toimielimien, elimien ja virastojen puolella ENISAn ja CERT-EU:n sekä toimielinten välisen kybertuvallisuutta koskevan tietojenvaihtoryhmän välinen jäsennelty yhteistyö. Lisäksi olisi otettava riittävällä tavalla mukaan hybridiuhkia ja pelastuspalvelua ([14]) koskevat sekä alakohtaiset kehykset ([15]). Vastaavasti olisi luotava jäsennelty yhteys IPCR-järjestelyihin ([16]). Näin kriisitilanteessa voidaan toimittaa nopeasti ja tehokkaasti tietoja neuvostossa kokoontuville poliittisille päätöksentekijöille.

(15) Yhteisen kyberturvallisuusyksikön perustamisessa olisi sen vuoksi noudatettava vaiheittaista ja läpinäkyvää prosessia, joka saatetaan päätökseen seuraavien kahden vuoden aikana. Tästä syystä tässä suosituksessa asetetut tavoitteet olisi saavutettava nelivaiheisella menettelyllä, joka kuvaillaan tämän suosituksen liitteessä. Kahdessa ensimmäisessä vaiheessa olisi käynnistettävä ENISAn järjestämä ja tukema valmisteluprosessi, johon osallistuu operatiivisia ja tukitehtäviä suorittavia osallistujia EU:n ja jäsenvaltioiden tasolla, ja se olisi toteutettava komission perustaman työryhmän puitteissa. Valmistelutyössä olisi noudatettava keskinäisen sitoutumisen, osallistavuuden ja yksimielisyyden rakentamisen periaatteita. Olisi edistettävä kaikkien osallistujien sitoutumista, jotta mahdollistetaan erilaiset näkemykset ja kannat ja voidaan pyrkiä löytämään ratkaisuja, jotka saavat mahdollisimman laajaa kannatusta. Tässä suosituksessa esitettyjen eri vaiheiden aikataulua voidaan mukauttaa tarpeiden ja asianmukaisesti perusteltujen olosuhteiden mukaan.

(16) Ensimmäisessä vaiheessa valmisteluprosessi olisi aloitettava määrittämällä käytettävissä olevat EU:n operatiiviset valmiudet ja käynnistämällä arviointi osallistujien rooleista ja vastuista. Toiseen vaiheeseen olisi sisällyttävä Blueprint-suunnitelman mukainen EU:n kyberturvapoikkeama- ja -kriisinhallintasuunnitelma ([17]), EU:n lainvalvonnan hätäaputoimien protokolla ja varautumiseen ja tilannetietoisuuteen liittyvien toimien käyttöönotto kyberturvallisuusasetuksen ja Europol-asetuksen ([18]) mukaisesti sekä osallistujien rooleja ja vastuualueita koskevan arvioinnin loppuun saattaminen. Työryhmän olisi esitettävä arvioinnin tulokset komissiolle ja korkealle edustajalle, jotka ilmoittavat tulokset neuvostolle. Komission ja korkean edustajan olisi yhteistyössä toimivaltuuksiensa mukaisesti laadittava tähän arviointiin perustuva yhteinen raportti ja kehotettava neuvostoa hyväksymään se neuvoston päätelmillä.

(17) Hyväksymisen jälkeen yhteinen kyberturvallisuusyksikkö saatetaan toimintavalmiiksi, jotta prosessin kaksi jäljellä olevaa vaihetta voidaan saattaa päätökseen. Kolmannessa vaiheessa osallistujien olisi voitava osoittaa yhteiseen kyberturvallisuusyksikköön EU:n nopean toiminnan ryhmiä EU:n kyberturvapoikkeama- ja -kriisinhallintasuunnitelmassa määriteltyjen menettelyjen mukaisesti hyödyntäen sekä fyysistä että virtuaalista alustaa ja osallistumalla eri tavoin poikkeamatilanteisiin vastaamiseen (julkisesta viestinnästä jälkihoitoon ja palautumiseen). Neljännessä vaiheessa yksityisen sektorin sidosryhmiä, myös kyberturvallisuusratkaisujen ja -palvelujen käyttäjiä ja tarjoajia, pyydetään mukaan osallistumaan, jotta osallistujat voivat parantaa tiedonvaihtoa ja tehostaa EU:n koordinoitua reagointia kyberturvallisuusuhkiin ja -poikkeamiin.

([14]) Tässä yhteydessä yhteisen kyberturvallisuusyksikön olisi luotava synergioita EU:n pelastuspalvelumekanismin kanssa, jotta voidaan parantaa Euroopan varautumista ja reagointia multikatastrofien ja sellaisten hätätilanteiden varalta, joihin sisältyy kyberturvallisuuselementti.

([15]) Kuten Euroopan parlamentin ja neuvoston asetuksessa (EU) 2021/xx* tarkoitettu finanssiala [DORA].

([16]) Ks. johdanto-osan 5 kappale.

([17]) Ks. alaviite 3.

([18]) Euroopan parlamentin ja neuvoston asetus (EU) 2016/794, annettu 11 päivänä toukokuuta 2016, Euroopan unionin lainvalvontayhteistyövirastosta (Europol) sekä neuvoston päätösten 2009/371/YOS, 2009/934/YOS, 2009/935/YOS, 2009/936/YOS ja 2009/968/YOS korvaamisesta ja kumoamisesta (EUVL L 135, 24.5.2016, s. 53).

(18) Nelivaiheisen prosessin loppuun mennessä osallistujien olisi laadittava komissiolle ja korkealle edustajalle toimintakertomus suosituksessa esitettyjen neljän vaiheen toteuttamisen edistymisestä ja siinä kohdatuista haasteista. Komission ja korkean edustajan olisi tämän kertomuksen perusteella arvioitava näitä tuloksia ja tehtävä päätelmät yhteisen kyberturvallisuusyksikön tulevaisuudesta.

(19) Komission, ENISAn, Europolin ja CERT-EU:n olisi annettava yhteiselle kyberturvallisuusyksikölle hallinnollista, taloudellista ja teknistä tukea tämän suosituksen IV jaksossa esitetysti ja edellyttäen, että määrärahoja ja henkilöresursseja on käytettävissä. Asiaankuuluvien EU:n toimielinten, elinten ja virastojen operatiivisten kyberturvallisuusvalmiuksien vahvistaminen on keskeistä yhteisen kyberturvallisuusyksikön tehokkaan valmistelun ja kestävyyden turvaamiseksi. Komissio aikoo varmistaa, että tuleva asetus EU:n toimielimiä, elimiä ja virastoja koskevista yhteisistä sitovista kyberturvallisuussäännöistä (lokakuu 2021) muodostaa oikeusperustan osallistumiselle CERT-EU:n tapauksessa.

(20) Koska ENISAn toimeksiantoa on vahvistettu asetuksella (EU) 2019/881, jäljempänä 'kyberturvallisuusasetus', se voi ainutlaatuisen asemansa takia organisoida ja tukea yhteisen kyberturvallisuusyksikön valmistelua sekä edistää sen toimintavalmiuteen saattamista. Kyberturvallisuusasetuksen säännösten mukaisesti ENISA perustaa parhaillaan Brysseliin toimistoa tukemaan jäsenneltyä yhteistyötään CERT-EU:n kanssa. Tämä jäsennelty yhteistyö, mukaan lukien lähellä toisiaan sijaitsevat toimistot, tarjoaa hyödyllisen kehyksen, jolla helpotetaan yhteisen kyberturvallisuusyksikön perustamista ja myös sille varattavaa fyysistä tilaa, joka olisi annettava tarvittaessa osallistujien sekä muiden asiaankuuluvien EU:n toimielinten, elinten ja virastojen henkilöstön käyttöön. Fyysiseen alustaan olisi yhdistettävä virtuaalinen alusta, joka muodostuu yhteistyöstä ja turvatuista tiedonvaihtovälineistä. Näillä välineillä hyödynnetään sitä runsasta tietoa, jota on kerätty EU:n kyberturvallisuusjärjestelyn ([19]) kautta, mukaan lukien turvaoperaatiokeskukset (SOC) ja tietojen jakamisen ja analysoinnin keskukset (ISAC).

(21) Neuvoston vuonna 2018 hyväksymässä suuria rajatylittäviä kyberhyökkäyksiä koskevassa EU:n lainvalvonnan hätäaputoimien protokollassa annetaan Europolin Euroopan kyberrikostorjuntakeskukselle (EC3) ([20]) keskeinen rooli osana Blueprint-suunnitelman kehystä. Protokollan ansiosta EU:n lainvalvontaviranomaiset voivat vastata epäiltyihin laajamittaisiin rajatylittäviin vihamielisiin hyökkäyksiin ympärivuorokautisesti ja kaikkina viikonpäivinä nopealla tilannearviolla ja reagoimisella sekä jakamalla turvallisesti ja oikea-aikaisesti kriittisiä tietoja, jotta rajatylittäviin poikkeamiin voidaan reagoida koordinoidusti. Lisäksi protokollassa käsitellään yhteistyötä muiden EU:n toimielinten ja EU:n laajuisten kriisiprotokollien kanssa sekä kriisiyhteistyötä yksityisen sektorin kanssa. Lainvalvontayhteisön olisi tarvittaessa Europolin tuella osallistuttava yhteisen kyberturvallisuusyksikön toimintaan toteuttamalla tarvittavat toimet koko tutkintasyklin aikana rikosoikeudellisen kehyksen vaatimusten ja sovellettavien sähköisen todistusaineiston käsittelymenettelyjen mukaisesti. Europol on antanut operatiivista tukea ja helpottanut operatiivista yhteistyötä kyberuhkien torjumiseksi siitä lähtien, kun EC3 perustettiin vuonna 2013. Europolin olisi tuettava tätä uutta alustaa toimeksiantonsa ja tiedusteluperusteiseen poliisitoimintaan perustuvan lähestymistavan mukaisesti hyödyntäen samalla kaikenlaista sisäistä asiantuntemusta, tuotteita, välineitä ja palveluja poikkeamatilanne- tai kriisitoimia varten.

(22) Lisäksi tietojärjestelmiin kohdistuvista hyökkäyksistä annetussa direktiivissä 2013/40/EU edellytetään jäsenvaltioiden varmistavan, että niillä on ympärivuorokautinen ja kaikkina viikonpäivinä tavoitettavissa oleva kansallinen yhteyspiste tietojen vaihtamiseksi kyseisessä direktiivissä määritellyistä rikoksista. Operatiivisten kansallisten yhteyspisteiden verkoston olisi myös osaltaan edistettävä yhteisen kyberturvallisuusyksikön toimintaa varmistamalla tarvittaessa jäsenvaltioiden lainvalvontaviranomaisten osallistuminen.

(23) EU:n kyberdiplomatian yhteisö edistää ja suojelee maailmanlaajuista, avointa, vakaata ja turvallista kybertoimintaympäristöä ja ehkäisee ja estää haitallisia kybertoimia ja reagoi niihin. EU loi vuonna 2017 puitteet EU:n yhteiselle diplomaattiselle vastaukselle haitallisiin kybertoimiin ("kyberdiplomatian välineistö"). Nämä puitteet ovat osa EU:n laajempaa kyberdiplomatiapolitiikkaa. Ne edistävät osaltaan konfliktien ehkäisyä ja kansainvälisten suhteiden vakautta. Niiden ansiosta EU ja jäsenvaltiot voivat, tarvittaessa yhteistyössä kansainvälisten kumppaneiden kanssa, käyttää kaikkia yhteisen ulko- ja turvallisuuspolitiikan (YUTP) toimenpiteitä niiden toteuttamiseksi sovellettavien menettelyjen mukaisesti edistääkseen yhteistyötä, lieventääkseen uhkia ja vaikuttaakseen nykyiseen ja mahdolliseen tulevaan haitalliseen käyttäytymiseen kybertoimintaympäristössä. Kyberdiplomatiayhteisön olisi tehtävä yhteistyötä yhteisen kyberturvallisuusyksikön puitteissa käyttämällä ja tukemalla kaikkia diplomaattisia toimenpiteitä, erityisesti julkista viestintää, yhteisen tilannetietoisuuden tukemista ja yhteistyötä kolmansien maiden kanssa kriisitilanteessa.

([19]) JOIN/2020/18 final, 1.2 kohta.
([20]) Perustettu asetuksella (EU) 2016/794.

(24) Korkean edustajan pitäisi Blueprint-suunnitelman puitteissa, muun muassa INTCEN:n kautta, osallistua yhteisen kyberturvallisuusyksikön toimintaan tarjoamalla jatkuvaa tiedusteluun perustuvaa yhteistä tilannetietoisuutta nykyisistä ja kehittymässä olevista uhkista, mukaan lukien tarvittava strateginen tilannetietoisuus jostakin tietystä yksittäisestä tapahtumasta.

(25) Kyberpuolustusyhteisössä EU ja jäsenvaltiot pyrkivät vahvistamaan kyberpuolustusvalmiuksia ja lisäämään synergiaa, koordinointia ja yhteistyötä asiaankuuluvien EU:n toimielinten, elinten ja virastojen välillä sekä jäsenvaltioiden kanssa ja niiden välillä, myös yhteisen turvallisuus- ja puolustuspolitiikan (YTPP) operaatioiden osalta. Yhteisöjen toiminnot perustuvat hallitustenväliseen hallintotapaan EU:n tasolla, kansallisiin sotilaallisiin komentorakenteisiin ja sotilaallisiin tai kaksikäyttövalmiuksiin ja -resursseihin. Kyberpuolustusyhteisön erilaisen luonteen vuoksi olisi luotava erityisiä rajapintoja yhteisen kyberturvallisuusyksikön kanssa, jotta mahdollistetaan tietojen jakaminen sen kanssa ([21]).

(26) Pysyvä rakenteellinen yhteistyö on Lissabonin sopimuksella ([22]) käyttöön otettu oikeudellinen kehys, joka perustettiin vuonna 2017 unionin puitteissa. Jäsennelty yhteistyö on johtanut useisiin kyberalan PRY-hankkeisiin, mikä osaltaan on auttanut täyttämään sitoumuksen 11 ([23]), jossa sitoudutaan ”varmistamaan, että kyberpuolustusyhteistyöhön kuuluvia toimia, kuten tietojen jakamista, koulutusta ja operatiivista tukea, lisätään”. EUH, mukaan lukien EU:n sotilasesikunta ja EDA, muodostaa PRY:n sihteeristön, joka toimii yhteyspisteenä unionin puitteissa kaikissa PRY-asioissa, mukaan lukien PRY-hankkeisiin liittyvät tuki- ja koordinointitehtävät (esim. uusien hanke-ehdotusten arviointi, hankkeiden edistymisraporttien laatiminen jne.). Asiaankuuluvien PRY-hankkeiden edustajien olisi tuettava yhteistä kyberturvallisuusyksikköä erityisesti tilannetietoisuuden ja varautumisen osalta.

(27) Osallistujien olisi yhteisen kyberturvallisuusyksikön välityksellä otettava myös yksityisen sektorin sidosryhmiä, kuten kyberturvallisuusratkaisujen ja -palvelujen tarjoajat ja käyttäjät, mukaan tukemaan soveltuvalla tavalla eurooppalaista kyberturvallisuuden kriisinhallintakehystä, ottaen asianmukaisesti huomioon tietojen jakamista ja tietoturvaa koskeva oikeudellinen kehys. Kyberturvallisuusratkaisujen tarjoajien olisi osallistuttava aloitteeseen jakamalla uhkia koskevaa tiedustelutietoa ja antamalla saataville poikkeamiin reagoinnin asiantuntijoita, jos on tarpeen nopeasti tehostaa yksikön valmiuksia reagoida laajamittaisiin hyökkäyksiin ja kriiseihin. Kyberturvallisuustuotteiden ja -palvelujen (pääasiassa verkko- ja tietoturvadirektiivin soveltamisalaan kuuluvien) käyttäjien olisi voitava hakea apua ja neuvoja nykyisin vielä puuttuvien jäsenneltyjen kanavien kautta, jotka on liitetty EU:n tason tietojen jakamisen ja analysoinnin keskuksiin (ISAC) ([24]). Alusta voisi myös osaltaan auttaa vahvistamaan yhteistyötä kansainvälisten kumppaneiden kanssa.

(28) Tilannetietoisuuden kehittäminen ja ylläpitäminen edellyttää huipputason valmiuksia tietomurtojen havaitsemisessa ja ennaltaehkäisyssä. Yhteisen kyberturvallisuusyksikön olisi voitava tukeutua huipputasoiseen verkostoon, joka pystyy analysoimaan haitallisia uhkia ja poikkeamia, jotka voivat vaikuttaa keskeisiin viestintä- ja tietojärjestelmiin kaikkialla unionissa. Tämä tarkoittaa, että yhteisessä kyberturvallisuusyksikössä olisi hyödynnettävä muiden lähteiden ohella kansallisten, alakohtaisten ja rajat ylittävien turvaoperaatiokeskusten seuraamista viestintäverkoista saatua uhkatietoa, jotta osallistujat voivat paremmin arvioida EU:n uhkakuvia.

(29) Operatiivisten tietojen, mahdollisesti myös luottamuksellisen aineiston, vaihdon tukemiseksi olisi käytettävä asianmukaisesti suojattuja viestintäkanavia. Ne voisivat perustua esimerkiksi jo olemassa olevaan infrastruktuuriin, kuten Europolin ja lainvalvontayhteisön käyttämään suojattuun tiedonvaihtoverkkosovellukseen (SIENA). Kuten kyberturvallisuusstrategiassa ilmoitettiin, EU:n toimielinten, elinten ja virastojen välineiden käytössä olisi noudatettava tietoturvasääntöjä, joita komissio aikoo lähiaikoina ehdottaa.

([21]) Erityisesti EUH:n edustuksen kautta, jotta voidaan mahdollistaa kyberpuolustusyhteisön asianmukainen osallistuminen, mikä perustuu vapaaehtoisiin kansallisiin panoksiin.

([22]) SEU-sopimuksen 42 artiklan 6 kohta, 46 artikla ja pöytäkirja n:o 10.

([23]) Kukin pysyvään rakenteelliseen yhteisyöhön osallistuva jäsenvaltio tekee 20 yksittäistä sitoumusta viidellä keskeisellä alalla, jotka on vahvistettu Euroopan unionista tehtyyn sopimukseen liitetyssä pysyvää rakenteellista yhteistyötä koskevassa pöytäkirjassa n:o 10 olevassa 2 artiklassa.

([24]) Esimerkkejä olemassa olevista tietojen jakamisen ja analysoinnin keskuksista, jotka voisivat osallistua tällaiseen jakamiseen, ovat varsinkin Euroopan energia-alan ISAC (EE-ISAC) ja Euroopan finanssilaitosten ISAC (FI-ISAC).

(30) Komissio tukee – pääasiassa Digitaalinen Eurooppa -ohjelman kautta – tarvittavia investointeja fyysisen ja virtuaalisen alustan perustamiseksi, turvattujen viestintäkanavien ja koulutusvalmiuksien luomiseksi ja ylläpitämiseksi sekä havaitsemisvalmiuksien kehittämiseksi ja käyttöönottamiseksi. Lisäksi Euroopan puolustusrahasto voisi auttaa rahoittamaan keskeisiä kyberpuolustusteknologioita ja kyberpuolustusvalmiuksia, mikä lujittaisi kansallisen kyberpuolustuksen varautumisvalmiuksia,

ON ANTANUT TÄMÄN SUOSITUKSEN:

I TÄMÄN SUOSITUKSEN TARKOITUS

1) Tämän suosituksen tarkoituksena on määritellä tarvittavat toimet, jotta voidaan koordinoida EU:n toimia laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien ehkäisyä, havaitsemista, torjumista, estämistä ja lieventämistä ja niihin reagoimista yhteisen kyberturvallisuusyksikön avulla. Tätä varten tässä suosituksessa määritellään jäsenvaltioille ja EU:n toimielimille, elimille ja virastoille myös prosessit, välitavoitteet ja aikataulu tällaisen alustan perustamiseksi ja kehittämiseksi.

2) Jäsenvaltioiden ja asiaankuuluvien EU:n toimielimien, elinten ja virastojen olisi varmistettava, että ne koordinoivat laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien tapauksessa toimensa yhteisen kyberturvallisuusyksikön kautta, mikä mahdollistaa keskinäisen avunannon ([25]) käyttämällä jäsenvaltioiden viranomaisten ja asiaankuuluvien EU:n toimielimien, elimien ja virastojen asiantuntemusta. Yhteisen kyberturvallisuusyksikön olisi myös mahdollistettava osallistujien yhteistyö yksityisen sektorin kanssa.

II MÄÄRITELMÄT

3) Tässä suosituksessa tarkoitetaan

a) 'EU:n kyberturvapoikkeama- ja kriisinhallintasuunnitelmalla' tehtävien ja menettelytapojen yhdistelmää, jonka pohjalta toteutetaan koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin 13 päivänä syyskuuta 2017 annetun komission suosituksen, jäljempänä 'Blueprint-suunnitelma', 1 kohdassa tarkoitettu EU:n kyberturvallisuuden kriisinhallintakehys.

b) 'kyberturvallisuusyhteisöillä' siviili-, lainvalvonta-, diplomatia- ja puolustusyhteistyöryhmiä, jotka edustavat sekä jäsenvaltioita että asiaankuuluvia EU:n toimielimiä, elimiä ja virastoja ja vaihtavat tietoja kyberturvallisuuteen liittyvien yhteisten tavoitteiden, etujen ja operaatioiden edistämiseksi.

c) 'yksityisen sektorin osallistujilla' kyberturvallisuusratkaisuja ([26]) ja -palveluja ([27]) tarjoavien tai käyttävien yksityisen sektorin toimijoiden edustajia.

d) 'laajamittaisella poikkeamalla' direktiivin (EU) 2016/1148 4 artiklan 7 kohdassa määriteltyä poikkeamaa, jolla on merkittävää vaikutusta vähintään kahdessa jäsenvaltiossa.

e) 'yhdennetyllä EU:n kyberturvallisuuden tilanneraportilla' raporttia, jossa kerätään tietoja yhteisen kyberturvallisuusyksikön osallistujilta ja joka perustuu asetuksen (EU) 2019/881 7 artiklan 6 kohdassa määriteltyyn unionin kyberturvallisuuden tekniseen tilanneraporttiin.

f) 'EU:n kyberturvallisuuden nopean toiminnan ryhmällä' tunnustetuista kyberturvallisuusasiantuntijoista muodostettua ryhmää, joka koostuu erityisesti jäsenvaltioiden CSIRT-toimijoista ENISAn, CERT-EU:n ja Europolin tuella ja joka on valmis avustamaan etäyhteyden välityksellä osallistujia, joihin laajamittaiset poikkeamat ja kriisit vaikuttavat.

g) 'yhteisymmärryspöytäkirjoilla' osallistujien välistä sopimusta, jossa vahvistetaan tarvittavat yhteistyötä koskevat yksityiskohtaiset säännöt, mukaan lukien sellaisten voimavarojen ja menettelyjen määrittely, joita tarvitaan EU:n kyberturvallisuuden nopean toiminnan ryhmien perustamiseksi ja aktivoimiseksi sekä keskinäisen avunannon mahdollistamiseksi.

([25]) Direktiivissä (EU) 2016/1148 ja SEUT-sopimuksen 222 artiklassa vahvistetun lähestymistavan ja periaatteiden mukaisesti ja rajoittamatta Euroopan unionista tehdyn sopimuksen 42 artiklan 7 kohdan soveltamista.

([26]) Mukaan lukien ohjelmistojen myyjät.

([27]) Mukaan lukien uhkia koskeva tiedustelu.

III YHTEISEN KYBERTURVALLISUUSYKSIKÖN TAVOITE

4) Jäsenvaltioiden ja asiaankuuluvien EU:n toimielinten, elinten ja virastojen olisi varmistettava **EU:n koordinoitu vastaus** laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin ja palautuminen niistä. Erityisesti tällainen vastaus olisi varmistettava operatiivisten osallistujien, joita ovat ENISA, Europol, CERT-EU, komissio, Euroopan ulkosuhdehallinto (mukaan lukien INTCEN), CSIRT-verkosto ja EU-CyCLONe, ja tukitehtäviä suorittavien osallistujien välillä, joista jälkimmäisiä ovat NIS-yhteistyöryhmän puheenjohtaja, neuvoston kyberkysymysten horisontaalisen työryhmän puheenjohtaja, Euroopan puolustusvirasto ja yksi asiaan liittyvien PRY-hankkeiden edustaja ([28]). Operatiivisten osallistujien pitäisi voida nopeasti ja tehokkaasti saada käyttöön keskinäisen avunannon operatiivisia resursseja yhteisessä kyberturvallisuusyksikössä. Tätä varten yhteisessä kyberturvallisuusyksikössä olisi koordinoitava keskinäisen avunannon mekanismeja, jos yksi tai useampi jäsenvaltio sitä pyytää.

5) Tehokkaan koordinoidun vastauksen varmistamiseksi 4 kohdassa lueteltujen operatiivisten ja tukitehtäviä suorittavien osallistujien olisi voitava jakaa parhaita käytäntöjä, harjoittaa **jatkuvaa jaettua tilannetietoisuutta** ja turvata tarvittava **varautuminen** toimeksiantojensa rajoissa. Osallistujien olisi otettava huomioon jo olemassa olevat prosessit ja eri kyberturvallisuusyhteisöjen asiantuntemus.

IV YHTEISEN KYBERTURVALLISUUSYKSIKÖN TOIMINNAN MÄÄRITTELY

6) Jäsenvaltioiden ja asiaankuuluvien EU:n toimielinten, elinten ja virastojen olisi asetuksen (EU) 2019/881 7 artiklan 7 kohdassa kuvaillulla ENISAn tuella varmistettava **koordinoitu vastaus** laajamittaisiin poikkeamiin ja kriiseihin ja palautuminen niistä seuraavien avulla:

a) **EU:n kyberturvallisuuden nopean toiminnan ryhmien** perustaminen, koulutus, testaus ja koordinoitu käyttöönotto asetuksen (EU) 2019/881 7 artiklan 4 kohdan ja asetuksen (EU) 2016/794 3 ja 4 artiklan pohjalta;

b) sellaisen **virtuaalisen ja fyysisen alustan** koordinoitu käyttöönotto asetuksen (EU) 2019/881 7 artiklan 4 kohdan mukaisen ENISAn ja CERT-EU:n jäsennellyn yhteistyön pohjalta, jonka olisi toimittava osallistujien välisen teknisen ja operatiivisen yhteistyön tuki-infrastruktuurina ja kerättävä osallistujilta asiaankuuluvaa henkilöstöä ja muita resursseja;

c) selvityksen laatiminen ja ylläpito **operatiivisista ja teknisistä valmiuksista, joita on saatavilla EU:ssa** eri kyberturvallisuusyhteisöissä ([29]) ja jotka ovat valmiita otettaviksi käyttöön laajamittaisten kyberturvallisuuspoikkeamien tai -kriisien yhteydessä;

d) raportointi komissiolle ja korkealle edustajalle **kyberturvallisuutta koskevista operatiivisista yhteistyötoimista** saaduista kokemuksista kyberturvallisuusyhteisöissä ja niiden välillä.

7) Jäsenvaltioiden ja asiaankuuluvien EU:n toimielinten, elinten ja virastojen olisi asetuksen (EU) 2019/881 7 artiklan ja asetuksen (EU) 2016/794 3 artiklan mukaisia tavoitteita noudattaen varmistettava, että yhteinen kyberturvallisuusyksikkö tarjoaa jatkuvaa jaettua **tilannetietoisuutta** ja **varautumista** kyberturvallisuuskriiseihin eri kyberturvallisuusyhteisöjen välisesti ja niiden sisällä. Tätä varten jäsenvaltioiden ja asiaankuuluvien EU:n toimielinten, elinten ja virastojen olisi asetuksen (EU) 2019/881 ja asetuksen (EU) 2016/794 mukaisesti mahdollistettava seuraavien **tukitoimintojen** toteuttaminen:

a) **yhdennetyn EU:n kyberturvallisuuden tilanneraportin** laatiminen keräämällä ja analysoimalla kaikki asiaan liittyvät tiedot ja uhkia koskevat tiedustelutiedot;

b) asianmukaisten ja turvallisten **välineiden** käyttö asetuksen (EU) 2019/881 7 artiklan 1 kohdan mukaisesti nopeaan tietojenvaihtoon osallistujien kesken ja muiden tahojen kanssa;

c) **tietojen ja asiantuntemuksen vaihto**, joka on tarpeen, jotta unioni voi varautua laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintaan ENISAn tuella asetuksen (EU) 2019/881 7 artiklan 2 kohdan mukaisesti;

d) kansallisten **kyberturvapoikkeama- ja kriisinhallintasuunnitelmien** ([30]) hyväksyminen ja testaaminen asetuksen (EU) 2019/881 7 artiklan 2, 5 ja 7 kohdan mukaisesti;

([28]) Kyber- ja tietoalan koordinointikeskus (CIDCC) sekä kyberalan nopean toiminnan ryhmät ja kyberturvallisuuteen liittyvä keskinäinen avunanto (CRRT).

([29]) Mukaan lukien tarvittaessa kyberpuolustusyhteisö.

([30]) Ehdotettu toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta annetun direktiiviehdotuksen [COM(2020) 823 final, 2020/0359 (COD)] 7 artiklan 3 kohdan mukaisesti.

e) **EU:n kyberturvapoikkeama- ja kriisinhallintasuunnitelman** laatiminen, hallinta ja testaaminen, myös yhteisöjen välisillä harjoituksilla ja koulutuksella, Blueprint-suosituksen mukaisesti ja toimenpiteistä yhteisen korkeatasoisen kyberturvallisuuden varmistamiseksi koko unionissa annetun direktiivin (EU) 2016/1148 tarkistamista koskevan komission ehdotuksen ([31]) 7 artiklan 3 kohdan pohjalta;

f. osallistujien avustaminen tietojen jakamista koskevien sopimusten ja operatiivisten yhteistyösopimusten tekemisessä sellaisten **yksityisen sektorin toimijoiden** kanssa, jotka tarjoavat muun muassa uhkia koskevia tiedustelupalveluja ja poikkeamiin reagoimista koskevia palveluja, ENISAn tuella, josta säädetään asetuksen (EU) 2019/881 7 artiklan 1 kohdassa;

g. jäsennellyn synergian luominen kansallisten, alakohtaisten ja rajat ylittävien **seuranta- ja havaitsemisvalmiuksien**, erityisesti turvaoperaatiokeskusten, kanssa;

h. osallistujien avustaminen laajamittaisten poikkeamien ja kriisien **hallinnassa** asetuksen (EU) 2019/881 7 artiklassa säädetyn ENISAn tukitehtävän mukaisesti. Tähän sisältyy yhteisen tilannetietoisuuden edistäminen, diplomaattiset tukitoimet, poliittinen attribuutio ja attribuutio rikostutkinnan yhteydessä, myös Europolin välityksellä ([32]), julkisen viestinnän yhdenmukaistaminen ja poikkeamista selviytymisen helpottaminen.

8) Edellä olevan 6 ja 7 kohdan täytäntöön panemiseksi jäsenvaltioiden ja asiaankuuluvien EU:n toimielinten, elinten ja virastojen olisi varmistettava seuraavat:

a) yhteisen kyberturvallisuusyksikön organisatoristen näkökohtien määrittely sekä operatiivisten ja tukitehtäviä suorittavien osallistujien **roolit ja vastuualueet** alustalla, mikä mahdollistaa alustan tehokkaan toiminnan tämän suosituksen liitteessä esitettyjen näkökohtien ja periaatteiden mukaisesti;

b) niiden 4 kohdassa tarkoitettujen **yhteisymmärryspöytäkirjojen** tekeminen, joissa vahvistetaan tarvittavat yksityiskohtaiset säännöt osallistujien väliselle yhteistyölle.

9) ENISAn olisi asetuksen 2019/881 7 artiklan mukaisesti varmistettava koordinointi ja jäsenvaltioiden ja asiaankuuluvien EU:n toimielinten, virastojen ja elinten tukeminen yhteisessä kyberturvallisuusyksikössä, myös toimimalla sihteeristönä, järjestämällä kokouksia ja osallistumalla toimien täytäntöönpanoon sekä jäsenvaltioiden että EU:n tasolla. ENISAn olisi perustettava sekä virtuaalinen alusta että fyysinen tila kokouksille ja helpotettava tarvittavia täytäntöönpanotoimia.

V YHTEISEN KYBERTURVALLISUUSYKSIKÖN PERUSTAMINEN

10) Jäsenvaltioiden ja asiaankuuluvien EU:n toimielinten, elinten ja virastojen olisi varmistettava, että yhteinen kyberturvallisuusyksikkö siirtyy operatiiviseen vaiheeseen **30 päivästä kesäkuuta 2022**. Siihen mennessä operatiivisten osallistujien olisi asetettava saataville operatiiviset valmiudet ja asiantuntijat, jotka voivat muodostaa perustan EU:n kyberturvallisuuden nopean toiminnan ryhmille. Fyysistä ja virtuaalista alustaa koskevien suunnitelmien olisi oltava pitkälle edenneitä.

11) Jäsenvaltioiden ja asiaankuuluvien EU:n toimielinten, elinten ja virastojen olisi osaltaan edistettävä yhteisen kyberturvallisuusyksikön toimintaa ja varmistettava, että se on täysin toimintavalmis **30 päivään kesäkuuta 2023** mennessä. Tämä olisi tehtävä toteuttamalla seuraavat neljä vaihetta, joilla on tarkoitus saattaa päätökseen seuraavat toimet:

a) Ensimmäinen vaihe – Yhteisen kyberturvallisuusyksikön organisatoristen näkökohtien arviointi ja käytettävissä olevien EU:n operatiivisten valmiuksien määrittäminen **31 päivään joulukuuta 2021 mennessä**;

b) Toinen vaihe – Suunnitelmien laatiminen poikkeamiin ja kriiseihin vastaamiseksi ja yhteisen varautumisen toteuttaminen **30 päivään kesäkuuta 2022** mennessä;

c) Kolmas vaihe – Yhteisen kyberturvallisuusyksikön saattaminen toimintavalmiiksi **31 päivään joulukuuta 2022** mennessä;

d) Neljäs vaihe – Yhteisen kyberturvallisuusyksikön puitteissa tehtävän yhteistyön laajentaminen yksityisiin toimijoihin ja saavutetusta edistyksestä raportointi **30 päivään kesäkuuta 2023** mennessä.

Yksityiskohtaisemmat toimet, joita toteutetaan neljän peräkkäisen vaiheen aikana, esitetään tämän suosituksen liitteessä.

([31]) COM(2020) 823 final.
([32]) Asetuksen (EU) N:o 2016/794 mukaisesti.

12) Kahdessa ensimmäisessä vaiheessa ENISAn olisi organisoitava ja tuettava yhteisen kyberturvallisuusyksikön valmistelua. Komission yksiköiden olisi muodostettava työryhmä, joka kokoaa yhteen operatiiviset ja tukitehtäviä suorittavat osallistujat tällaisen valmistelutyön loppuun saattamiseksi. Komission yksiköiden olisi nimitettävä edustaja työryhmän yhdeksi puheenjohtajaksi ja kutsuttava toimimaan toisina puheenjohtajina korkean edustajan nimeämä edustaja, jolloin kumpikin näistä vastaa esityslistalla olevista asioista oman toimivaltansa mukaisesti, sekä jäsenvaltioiden valitsema edustaja.

13) Toisen vaiheen loppuun mennessä työryhmän olisi saatettava päätökseen arviointinsa yhteisen kyberturvallisuusyksikön organisatorisista näkökohdista sekä operatiivisten osallistujien tehtävistä ja vastuualueista kyseisellä alustalla. Työryhmän olisi esitettävä arvioinnin tulokset komissiolle ja korkealle edustajalle. Komission ja korkean edustajan olisi puolestaan toimitettava ne neuvostolle. Komission ja korkean edustajan olisi laadittava tämän arvioinnin pohjalta yhteinen raportti ja kehotettava neuvostoa hyväksymään se neuvoston päätelmillä.

14) Yhteisen kyberturvallisuusyksikön olisi oltava toimintavalmis kolmannesta vaiheesta alkaen.

15) ENISAn ja komission olisi varmistettava, että EU:n rahoitusohjelmien, pääasiassa Digitaalinen Eurooppa -ohjelman, olemassa olevia resursseja käytetään sovellettavien sääntöjen mukaisesti työohjelmien laatimiseen, yhteisen kyberturvallisuusyksikön osallistujien varustamiseen lisäkoulutusvalmiuksilla, viestintävalmiuksilla ja suojatulla tiedonjakoinfrastruktuurilla, joka mahdollistaa turvallisuusluokiteltujen tietojen vaihdon, myös yhteisöjen välillä.

VI **UUDELLEENTARKASTELU**

16) Jäsenvaltioiden olisi tehtävä yhteistyötä komission ja korkean edustajan kanssa näiden toimivaltuuksien mukaisesti arvioidakseen yhteisen kyberturvallisuusyksikön vaikuttavuutta ja tehokkuutta **30 päivään kesäkuuta 2025** mennessä, jotta voidaan tehdä päätelmiä yhteisen kyberturvallisuusyksikön tulevaisuudesta. Arvioinnissa olisi otettava huomioon edellä mainittujen neljän vaiheen täytäntöönpano.

Tehty Brysselissä 23 päivänä kesäkuuta 2021.

Komission puolesta
Thierry BRETON
Komission jäsen

LIITE

Yhteisen kyberturvallisuusyksikönperustamisen vaiheet

Tässä liitteessä kuvaillaan ydintoimet ja tukitoimet, joita tarvitaan yhteisen kyberturvallisuusyksikön perustamiseksi ja sen toimintavalmiuteen saattamiseksi.

1. *Ensimmäinen vaihe – Yhteisen kyberturvallisuusyksikön organisatoristen näkökohtien arviointi ja käytettävissä olevien EU:n operatiivisten valmiuksien määrittäminen*

YDINTOIMET

Yhteisen kyberturvallisuusyksikön operatiivisten osallistujien olisi komission perustamassa työryhmässä ja ENISAn tuella kerättävä tietoja nykyisistä operatiivisista valmiuksista, mukaan lukien luettelo käytettävissä olevista tunnustetuista ammattilaisista sekä tiedot heidän asiantuntemuksestaan, käytettävissä olevista poikkeamien käsittelyvälineistä, -toiminnoista ja -resursseista, saatavilla olevista koulutuksesta ja harjoituksista sekä olemassa olevista tieto- ja tiedusteluanalyysituotteista. Näiden tietojen perusteella operatiivisten osallistujien olisi laadittava **luettelo EU:n käytettävissä olevista operatiivisista valmiuksista**, jotka voidaan ottaa käyttöön kyberturvallisuuspoikkeamien tai -kriisien yhteydessä, erityisesti EU:n kyberturvallisuuden nopean toiminnan ryhmien kautta.

Työryhmän olisi käynnistettävä arviointi yhteisen kyberturvallisuusyksikön **organisatorisista näkökohdista** sekä **operatiivisten osallistujien tehtävistä ja vastuualueista kyseisellä alustalla**.

Jotta valmiuksista saataisiin kokonaiskuva ja päästäisiin yhteisymmärrykseen menettelyistä, ensimmäisen vaiheen ydintoimet ja mahdollisuuksien mukaan tukitoimet olisi saatettava päätökseen **31 päivään joulukuuta 2021 mennessä (6 kuukautta hyväksymisen jälkeen)**.

2. *Toinen vaihe – Suunnitelmien laatiminen poikkeamiin ja kriiseihin vastaamiseksi ja yhteisen varautumisen toteuttaminen*

YDINTOIMET

Työryhmän operatiivisten osallistujien olisi yhteistyössä tukitehtäviä suorittavien osallistujien kanssa valmisteltava **EU:n kyberturvapoikkeama- ja kriisinhallintasuunnitelma** kansallisten kyberturvapoikkeama- ja kriisinhallintasuunnitelmien pohjalta. EU:n kyberturvapoikkeama- ja kriisinhallintasuunnitelmaan olisi sisällytettävä EU:n varautumista, yksilöityjä menettelyjä ja suojattuja tiedonvaihtokanavia koskevat tavoitteet, mukaan lukien tiedonkäsittelytavat, sekä kriteerit keskinäiseen avunantoon perustuvan mekanismin aktivoimiseksi sovitun turvapoikkeamaluokituksen ja EU:n käytettävissä olevien valmiuksien luettelon perusteella.

Toisen vaiheen loppuun mennessä työryhmän olisi saatettava päätökseen arviointinsa yhteisen kyberturvallisuusyksikön organisatorisista näkökohdista sekä operatiivisten osallistujien tehtävistä ja vastuualueista kyseisellä alustalla. Työryhmän olisi esitettävä arvioinnin tulokset komissiolle ja korkealle edustajalle. Komission ja korkean edustajan olisi toimitettava tämä arvio neuvostolle. Komission ja korkean edustajan olisi yhteistyössä toimivaltuuksiensa mukaisesti laadittava tähän arviointiin perustuva yhteinen raportti ja kehotettava neuvostoa hyväksymään se neuvoston päätelmillä.

TUKITOIMET

EU:n kyberturvapoikkeama- ja kriisinhallintasuunnitelman olisi perustuttava kansallisten kyberturvapoikkeama- ja kriisinhallintasuunnitelmien keskeisiin osiin. Toimenpiteistä yhteisen korkeatasoisen kyberturvallisuuden varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta annetun komission direktiiviehdotuksen ([1]) mukaisesti jäsenvaltioiden olisi hyväksyttävä kansalliset kyberturvapoikkeama- ja kriisinhallintasuunnitelmat. Kansallisissa suunnitelmissa, joista voidaan mahdollisesti tehdä vertaisarviointi, olisi määriteltävä laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintaa koskevat tavoitteet ja yksityiskohtaiset säännöt. Kansallisissa suunnitelmissa pitäisi käsitellä erityisesti seuraavia:

a) kansallisten varautumiskeinojen ja -toimien tavoitteet;

b) kansallisten toimivaltaisten viranomaisten tehtävät ja vastuualueet kansallisella tasolla;

c) kansalliset kriisinhallintamenettelyt ja tiedonvaihtokanavat;

d) varautumistoimenpiteiden määrittely, mukaan lukien harjoitukset ja koulutus;

e) asiaan liittyvien julkisten ja yksityisten sidosryhmien ja infrastruktuurin yksilöinti;

f) asiaankuuluvien kansallisten viranomaisten ja elinten, myös kaikista kyberyhteisöistä vastaavien viranomaisten ja elinten väliset kansalliset menettelyt ja järjestelyt sen varmistamiseksi, että jäsenvaltiot osallistuvat tehokkaasti laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoituun hallinnointiin ja tukevat sitä EU:n tasolla.

Jäsenvaltioiden ja EU:n toimielinten, elinten ja virastojen antaman palautteen perusteella operatiivisten osallistujien olisi toteutettava yhteisen kyberturvallisuusyksikön puitteissa seuraavat tukitoimet:

a) laadittava ensimmäinen yhdennetty EU:n tilanneraportti, joka perustuu kansallisiin kyberturvapoikkeama- ja kriisinhallintasuunnitelmiin;

([1]) COM(2020) 823 final, 2020/0359 (COD), Bryssel, 16.12.2020.

b) vahvistettava viestintävalmiudet ja turvalliset tiedonvaihtovälineet;

c) helpotettava keskinäistä avunantoa koskevien protokollien hyväksymistä osallistujien kesken;

d) järjestettävä yhteisöjen välisiä harjoituksia ja koulutusta asiantuntijoille, jotka mainitaan EU:n käytettävissä olevien operatiivisten valmiuksien luettelossa;

e) laadittava monivuotinen suunnitelma harjoitusten koordinoimiseksi.

Operatiivisten osallistujien olisi tarvittaessa kuultava tukitehtäviä suorittavia osallistujia. ENISAn olisi komission, Europolin ja CERT-EU:n tuella mahdollistettava tietojen vaihtaminen ottamalla käyttöön viestintävalmiuksia ja turvallisia tiedonvaihtovälineitä.

Sen varmistamiseksi, että tarvittavat suunnitelmat laaditaan ja yhteiset toimet aloitetaan, toisen vaiheen ydintoimet ja mahdollisuuksien mukaan tukitoimet olisi saatettava päätökseen **30 päivään kesäkuuta 2022 mennessä (6 kuukautta ensimmäisen vaiheen päättymisen jälkeen)**.

3. *Kolmas vaihe – Yhteisen kyberturvallisuusyksikön saattaminen toimintavalmiiksi*

YDINTOIMET

Kun neuvosto on hyväksynyt komission päätelmät toisen vaiheen mukaisesta raportista, operatiivisten osallistujien olisi koordinoitava **EU:n kyberturvallisuuden nopean toiminnan ryhmien** käyttöönotto yhteisessä kyberturvallisuusyksikössä ja perustettava **fyysinen alusta** ryhmien teknisille ja operatiivisille toimille. Toisessa vaiheessa tehdyn valmistelutyön perusteella osallistujien olisi viimeisteltävä EU:n kyberturvapoikkeama- ja kriisinhallintasuunnitelma. Operatiivisten osallistujien olisi varmistettava, että EU:n käytettävissä olevien operatiivisten valmiuksien luettelossa mainitut asiantuntijat ja valmiudet ovat käytettävissä ja valmiita osaltaan edistämään EU:n kyberturvallisuuden nopean toiminnan ryhmien toimintaa.

Osallistujien olisi määriteltävä vuotuinen työohjelma EU:n kyberturvapoikkeama- ja kriisinhallintasuunnitelman täytäntöön panemiseksi.

TUKITOIMET

Kyberdiplomatian yhteisö voi käyttää yhteistä kyberturvallisuusyksikköä julkisen viestinnän yhdenmukaistamiseen. Alusta voi antaa osallistujille mahdollisuuden osallistua poliittiseen attribuutioon ja attribuutioon poliisi- ja oikeusviranomaisten rikosoikeudellisissa puitteissa. Lisäksi yhteinen kyberturvallisuusyksikkö voi helpottaa tilanteista palautumista ja mahdollistaa jäsennellyn synergian kansallisten ja rajat ylittävien seuranta- ja havaitsemisvalmiuksien kanssa.

Yhteisen kyberturvallisuusyksikön toimintavalmiiksi saattamisen varmistamiseksi kolmannen vaiheen ydintoimet ja mahdollisuuksien mukaan tukitoimet olisi saatettava päätökseen **31 päivään joulukuuta 2022 mennessä (6 kuukautta toisen vaiheen päättymisen jälkeen)**.

4. *Neljäs vaihe – Yhteisen kyberturvallisuusyksikön puitteissa tehtävän yhteistyön laajentaminen yksityisiin toimijoihin ja saavutetusta edistyksestä raportointi*

YDINTOIMET

Yhteisen kyberturvallisuusyksikön osallistujien olisi laadittava **suosituksessa esitettyjen neljän vaiheen täytäntöönpanossa saavutetusta edistyksestä raportti, jossa kuvaillaan saavutukset ja kohdatut haasteet**. Raporttiin olisi sisällytettävä tilastotietoja kaikissa neljässä vaiheessa toteutetuista operatiivisista yhteistyötoimista. Raportti olisi annettava komissiolle ja korkealle edustajalle.

TUKITOIMET

EU:n kyberturvallisuuden nopean toiminnan ryhmien saatavilla olevien valmiuksien ja tietojen lisäämiseksi osallistujien olisi varmistettava, että yhteinen kyberturvallisuusyksikkö avustaa **tietojen jakamista ja operatiivista yhteistyötä koskevien sopimusten tekemisessä osallistujien ja sellaisten yksityisen sektorin toimijoiden välillä**, jotka tarjoavat muun muassa uhkia koskevaan tiedusteluun ja poikkeamisiin reagoimiseen liittyviä palveluja. Lisäksi niiden olisi muiden toimintojen ohella varmistettava, että yhteinen kyberturvallisuusyksikkö tukee säännöllisessä vuoropuhelussa ja uhkia ja haavoittuvuuksia koskevia tietoja jakamalla kyberturvallisuusratkaisujen käyttäjiä, pääasiassa niitä, jotka kuuluvat verkko- ja tietoturvadirektiivin soveltamisalaan tai kokoontuvat **EU:n tason tietojen jakamisen ja analysoinnin keskuksissa (ISAC)**.

Jäsenvaltioiden olisi tuettava alueellaan toimivia yhteisöjä ja erityisesti verkko- ja tietoturvadirektiivin soveltamisalaan kuuluvia yhteisöjä, jotta ne voivat osallistua julkisen ja yksityisen sektorin vuoropuheluihin EU:n tason ISAC-keskusten kanssa.

Yksityisen sektorin asianmukaisen osallistumisen turvaamiseksi neljännen vaiheen ydintoimet ja mahdollisuuksien mukaan myös tukitoimet olisi saatettava päätökseen **30 päivään kesäkuuta 2023 mennessä (6 kuukautta kolmannen vaiheen päättymisen jälkeen)**.

MITEN EU:N OPERATIIVISET VALMIUDET SAADAAN NOPEASTI KÄYTTÖÖN

KUKA TARJOAA VALMIUDET: Operatiiviset osallistujat

KUKA HALLINNOI VALMIUKSIA: Yhteisen kyberturvallisuusyksikön osallistujat sovittujen tehtävien ja vastuualueiden mukaisesti

Vaihe	Tavoite	Tehtävä	Ydintoimi	Tukitoimi
Ensimmäinen vaihe – Määrittely **31. joulukuuta 2021** mennessä [6 kuukautta hyväksymisen jälkeen]	VARAUTUMINEN	**Valmiuksien kartoitus**	**Operatiiviset osallistujat laativat luettelon EU:n käytettävissä olevista operatiivisista valmiuksista.**	
Toinen vaihe – Varautuminen **30. kesäkuuta 2022** mennessä [6 kuukautta ensimmäisen vaiheen päättymisestä]	VARAUTUMINEN	**Määritellään menettelyt ja järjestelyt valmiuksien aktivoimiseksi tarvittaessa**	**Operatiiviset osallistujat valmistelevat EU:n kyberturvapoikkeama- ja kriisinhallintasuunnitelman (Blueprint-suunnitelman mukainen EU:n kyberturvallisuuden kriisinhallintakehys) hyväksyttyjen kansallisten suunnitelmien perusteella**	**Operatiiviset osallistujat laativat yhdennetyt EU:n tilanneraportit unionin kyberturvallisuuden teknisen tilanneraportin pohjalta**
	VARAUTUMINEN	**Harjoitusvalmiudet**		**Osallistujat järjestävät yhteisiä harjoituksia ja koulutusta (yhteisöjen välisesti)** **Osallistujat työstävät monivuotisen suunnitelman harjoitusten koordinoimiseksi.**
	TILANNETIETOISUUS	**Välineiden luominen tietojen ja tukipyyntöjen jakamiseksi**		**Osallistujat kehittävät turvallista ja nopeaa tiedonvaihtoa**
YHTEINEN KYBERTURVALLISUUSYKSIKKÖ TOIMINTAVALMIUDESSA Osallistujien komission perustamassa työryhmässä tekemien valmistelujen perusteella				
Kolmas vaihe – käyttöönotto **31. joulukuuta 2022** mennessä [6 kuukautta toisen vaiheen päättymisestä]	VARAUTUMINEN	**Hyväksytään menettelyt, järjestelyt ja yhteisymmärryspöytäkirjat valmiuksien aktivoimiseksi tarvittaessa**	**Operatiiviset osallistujat viimeistelevät EU:n kyberturvapoikkeama- ja kriisinhallintasuunnitelman ja määrittelevät sen täytäntöönpanon vuotuisten työohjelmien avulla.**	**Osallistujat tukevat kansallisten ja rajat ylittävien seuranta- ja havaitsemisvalmiuksien toteuttamista, turvaoperaatiokeskuksien perustaminen mukaan lukien**
	KOORDINOITU REAGOINTI	**Valmiuksien käyttöönotto tarvittaessa**	**Operatiiviset osallistujat koordinoivat operatiivisia EU:n kyberturvallisuuden nopean toiminnan ryhmiä virtuaalisen ja fyysisen alustan kautta Brysselissä.**	**Osallistujat koordinoivat julkista viestintää ja edistävät osaltaan poliittista attribuutiota sekä attribuutiota rikosoikeuden alalla**

Neljäs vaihe – Laajentaminen ja raportointi **30. kesäkuuta 2023** mennessä [6 kuukautta kolmannen vaiheen päättymisestä]	TILANNETIETOISUUS KOORDINOITU REAGOINTI	**Varmistetaan skaalautuvuus ottamalla mukaan yksityinen sektori uusiin tarpeisiin vastaamiseksi**	**Osallistujat laativat saavutetusta edistyksestä toimintakertomuksen, jossa kuvaillaan saavutuksia ja haasteita tilastotietojen pohjalta.**	**Osallistujat tekevät tiedonvaihtosopimuksia ja operatiivisia yhteistyösopimuksia kyberturvallisuusratkaisujen tarjoajien kanssa** **Osallistujat tekevät tiedonvaihtosopimuksia kyberturvallisuusratkaisujen käyttäjien, pääasiassa verkko- ja tietoturvadirektiivin soveltamisalaan kuuluvien yhteisöjen ja EU:n ISAC-keskusten kanssa**

ISSN 1977-0812 (sähköinen julkaisu)
ISSN 1725-261X (painettu julkaisu)

Euroopan unionin
julkaisutoimisto
L-2985 Luxemburg
LUXEMBURG

FI