Euroopan parlamentti
2019-2024

Perussopimus-, työjärjestys- ja toimielinasioiden valiokunta

2022/0085(COD)

31.1.2023

LAUSUNTO

perussopimus-, työjärjestys- ja toimielinasioiden valiokunnalta

teollisuus-, tutkimus- ja energiavaliokunnalle

ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Valmistelija: Markéta Gregorová

PA_Legam

LYHYET PERUSTELUT

Euroopan unionin toimielimet, elimet ja virastot toimivat ympäristössä, joka on viime vuosina digitalisoitunut yhä enemmän. Teknologia kehittyy jatkuvasti ja tämä heijastuu kyberturvauhkien tasoon. Kyberturvauhkatilannetta ovat pahentaneet covid-19-terveyskriisin puhkeaminen ja muun muassa lisääntynyt etätyön tekeminen. Näiden aikana monista eri lähteistä tulevien sofistikoituneiden hyökkäysten määrä kasvoi entisestään.

Tällä hetkellä kyberturvallisuusympäristö, esimerkiksi hallinta, kyberhygienia, yleiset valmiudet ja kehitystaso, vaihtelee unionin toimielinten, elinten ja virastojen välillä huomattavasti, mikä muodostaa lisäesteen avoimelle, tehokkaalle ja riippumattomalle eurooppalaiselle hallinnolle.

Tämän vuoksi valmistelija yhtyy näkemykseen, että unionin toimielimet, elimet ja virastot tarvitsevat perustoimintamallin yhteisten kyberturvallisuusjärjestelmien ja -vaatimusten käyttöön ottamiseksi, jotta voidaan varmistaa, että kyberturvallisuus kehittyy samaan suuntaan, ja edistää siten eurooppalaisen hallinnon tehokkuutta ja riippumattomuutta.

Valmistelija katsoo lisäksi, että vankka ja johdonmukainen turvallisuuskehys on äärimmäisen tärkeä koko EU:n henkilöstön, datan, viestintäverkkojen, tietojärjestelmien ja päätöksentekoprosessien suojelemiseksi ja edistää siten myös Euroopan unionin demokraattista toimintaa. Unionin toimielinten, elinten ja virastojen lujitettu turvallisuuskulttuuri varmistaisi myös Euroopan digitaalisen valmiuden ja rakentaisi tulevaisuuden vaatimukset huomioon ottavaa, ihmisten palveluksessa olevaa taloutta.

TARKISTUKSET

Perussopimus-, työjärjestys- ja toimielinasioiden valiokunta pyytää asiasta vastaavaa teollisuus-, tutkimus- ja energiavaliokuntaa ottamaan huomioon seuraavat tarkistukset:

Tarkistus 1

Ehdotus asetukseksi
Johdanto-osan 1 kappale

Komission teksti	*Tarkistus*
(1) Tieto- ja viestintätekniikka on avoimen, tehokkaan ja riippumattoman unionin hallinnon kulmakivi digiaikakaudella. Alati kehittyvä teknologia sekä digitaalisten järjestelmien yhä suurempi monimutkaisuus ja keskinäinen riippuvuus lisäävät kyberturvallisuusriskejä, minkä	(1) Tieto- ja viestintätekniikka on avoimen, tehokkaan ja riippumattoman unionin hallinnon kulmakivi digiaikakaudella. Alati kehittyvä teknologia sekä digitaalisten järjestelmien yhä suurempi monimutkaisuus ja keskinäinen riippuvuus lisäävät kyberturvallisuusriskejä, minkä

seurauksena unionin hallinto on yhä haavoittuvampi kyberuhkille ja poikkeamille. Tämä puolestaan vaarantaa viime kädessä hallinnon toiminnan jatkuvuuden ja kyvyn suojata tietonsa. Vaikka pilvipalvelujen kasvava hyödyntäminen, ***tietotekniikan*** laajamittainen käyttö, korkea digitalisaatioaste, etätyö sekä kehittyvä teknologia ja verkkoyhteydet ovat nykyään keskeisiä piirteitä unionin hallinnollisten yksiköiden kaikessa toiminnassa, digitaalinen häiriönsietokyky ei ole vielä riittävällä tavalla sisäänrakennettu.	seurauksena unionin hallinto on yhä haavoittuvampi kyberuhkille ja poikkeamille. Tämä puolestaan vaarantaa viime kädessä hallinnon toiminnan jatkuvuuden ja kyvyn suojata tietonsa. Vaikka pilvipalvelujen kasvava hyödyntäminen, ***tieto- ja viestintätekniikan*** laajamittainen käyttö, korkea digitalisaatioaste, etätyö sekä kehittyvä teknologia ja verkkoyhteydet ovat nykyään keskeisiä piirteitä unionin hallinnollisten yksiköiden kaikessa toiminnassa, digitaalinen häiriönsietokyky ei ole vielä riittävällä tavalla sisäänrakennettu.

Perustelu

Komission ehdotuksessa käytetään ilmausta tietotekniikka, kun pitäisi käyttää ilmausta tieto- ja viestintätekniikka eli TVT, joka on vakiotermi NIS 2 -direktiivissä ja EU:n kyberturvallisuusasetuksessa.

Tarkistus 2

Ehdotus asetukseksi
Johdanto-osan 2 kappale

Komission teksti	*Tarkistus*
(2) Unionin toimielinten, elinten ja virastojen kyberuhkaympäristö muuttuu jatkuvasti. Uhkatoimijoiden käyttämät taktiikat, tekniikat ja menettelyt kehittyvät koko ajan, kun taas hyökkäysten perussyyt arvokkaiden julkistamattomien tietojen varastamisesta aina rahan hankkimiseen, yleisen mielipiteen manipuloimiseen tai digitaalisen infrastruktuurin heikentämiseen ovat pysyneet lähes ennallaan. Uhkatoimijat toteuttavat kyberhyökkäyksiään koko ajan nopeammalla tahdilla. Lisäksi heidän kampanjansa ovat yhä kehittyneempiä ja automaattisempia, ne kohdennetaan alttiina oleville, laajeneville hyökkäyspinnoille ja niissä käytetään nopeasti hyväksi haavoittuvuuksia.	(2) Unionin toimielinten, elinten ja virastojen kyberuhkaympäristö muuttuu jatkuvasti. Uhkatoimijoiden käyttämät taktiikat, tekniikat ja menettelyt kehittyvät koko ajan, kun taas hyökkäysten perussyyt arvokkaiden julkistamattomien tietojen varastamisesta aina rahan hankkimiseen, yleisen mielipiteen manipuloimiseen tai digitaalisen infrastruktuurin heikentämiseen ovat pysyneet lähes ennallaan. Uhkatoimijat toteuttavat kyberhyökkäyksiään koko ajan nopeammalla tahdilla. Lisäksi heidän kampanjansa ***ja menetelmänsä*** ovat yhä kehittyneempiä ja automaattisempia, ne kohdennetaan alttiina oleville, laajeneville hyökkäyspinnoille ja niissä käytetään nopeasti hyväksi haavoittuvuuksia.

Tarkistus 3

Ehdotus asetukseksi
Johdanto-osan 3 kappale

Komission teksti	*Tarkistus*
(3) Unionin toimielinten, elinten ja virastojen ***tietoteknisillä ympäristöillä*** on keskinäisiä riippuvuussuhteita ja yhdistettyjä tietovirtoja, ja niiden käyttäjät tekevät tiivistä yhteistyötä. Tämä keskinäinen yhteys tarkoittaa, että vaikka häiriöt alun perin rajoittuisivatkin yhteen unionin toimielimeen, elimeen tai virastoon, niillä voi olla ketjureaktiovaikutuksia, jotka voivat aiheuttaa kauaskantoisia ja pitkäaikaisia kielteisiä vaikutuksia muihin. Lisäksi tiettyjen toimielinten, elinten ja virastojen ***tietotekniset ympäristöt*** ovat yhteydessä jäsenvaltioiden ***tietoteknisiin ympäristöihin***, minkä seurauksena yhdessä unionin yksikössä tapahtunut poikkeama aiheuttaa riskin jäsenvaltioiden ***tietoteknisten ympäristöjen*** kyberturvallisuudelle ja päinvastoin.	(3) Unionin toimielinten, elinten ja virastojen ***tieto- ja viestintäteknisillä*** ympäristöillä on keskinäisiä riippuvuussuhteita ja yhdistettyjä tietovirtoja, ja niiden käyttäjät tekevät tiivistä yhteistyötä. Tämä keskinäinen yhteys tarkoittaa, että vaikka häiriöt alun perin rajoittuisivatkin yhteen unionin toimielimeen, elimeen tai virastoon, niillä voi olla ketjureaktiovaikutuksia, jotka voivat aiheuttaa kauaskantoisia ja pitkäaikaisia kielteisiä vaikutuksia muihin. Lisäksi tiettyjen toimielinten, elinten ja virastojen ***tieto- ja viestintätekniset*** ympäristöt ovat yhteydessä jäsenvaltioiden ***tieto- ja viestintäteknisiin*** ympäristöihin, minkä seurauksena yhdessä unionin yksikössä tapahtunut poikkeama aiheuttaa riskin jäsenvaltioiden ***tieto- ja viestintäteknisten*** ympäristöjen kyberturvallisuudelle ja päinvastoin.

Tarkistus 4
Ehdotus asetukseksi
Johdanto-osan 4 kappale

Komission teksti	*Tarkistus*
(4) Unionin toimielimet, elimet ja virastot ovat houkuttelevia kohteita erittäin taitaville uhkatoimijoille, joilla on käytössään paljon resursseja, ja niihin kohdistuu myös muita uhkia. Samalla kyseisten yksikköjen välillä on suuria eroja kyberuhkien sietokyvyssä ja sen kehitystasossa sekä kyvyssä havaita haitallinen kybertoiminta ja reagoida siihen. Eurooppalaisen hallinnon toimivuuden kannalta on siksi välttämätöntä, että unionin toimielimet, elimet ja virastot saavuttavat yhteisen	(4) Unionin toimielimet, elimet ja virastot ovat houkuttelevia kohteita erittäin taitaville uhkatoimijoille, joilla on käytössään paljon resursseja, ja niihin kohdistuu myös muita uhkia. Samalla kyseisten yksikköjen välillä on suuria eroja kyberuhkien sietokyvyssä ja sen kehitystasossa sekä kyvyssä havaita haitallinen kybertoiminta ja reagoida siihen. Eurooppalaisen hallinnon toimivuuden kannalta on siksi välttämätöntä, että unionin toimielimet, elimet ja virastot saavuttavat yhteisen

korkean kyberturvatason ottamalla käyttöön kyberturvallisuuden perustason (kyberturvallisuutta koskevat vähimmäissäännöt, joita verkko- ja tietojärjestelmien sekä niiden tarjoajien ja käyttäjien on noudatettava kyberturvallisuusriskien ***minimoimiseksi***), vaihtamalla tietoja ja tekemällä yhteistyötä.	korkean kyberturvatason ottamalla käyttöön kyberturvallisuuden perustason (kyberturvallisuutta koskevat ***yhteiset*** vähimmäissäännöt, joita verkko- ja tietojärjestelmien sekä niiden tarjoajien ja käyttäjien on noudatettava kyberturvallisuusriskien ***rajoittamiseksi***), vaihtamalla tietoja ja tekemällä yhteistyötä ***säännöllisesti ja tehokkaasti ja tarjoamalla kyberturvallisuuskoulutusta***.

Tarkistus 5

Ehdotus asetukseksi
Johdanto-osan 7 kappale

Komission teksti	*Tarkistus*
(7) Unionin toimielinten, elinten ja virastojen välisten erojen vuoksi täytäntöönpanossa tarvitaan joustavuutta, koska yksi ratkaisu ei sovi kaikille. ***Toimenpiteisiin*** yhteisen korkean kyberturvatason varmistamiseksi ***ei*** pitäisi ***sisältyä velvoitteita, jotka heikentävät suoraan*** unionin toimielinten, elinten ja virastojen tehtävien hoitamista ***tai rajoittavat*** niiden ***hallinnollista riippumattomuutta***. Näin ollen unionin toimielinten, elinten ja virastojen olisi laadittava omat kehyksensä kyberturvallisuusriskien hallintaa ja valvontaa varten sekä hyväksyttävä oma perustasonsa ja kyberturvallisuussuunnitelmansa.	(7) Unionin toimielinten, elinten ja virastojen välisten erojen vuoksi täytäntöönpanossa tarvitaan joustavuutta, koska yksi ratkaisu ei sovi kaikille. Toimenpiteillä yhteisen korkean kyberturvatason varmistamiseksi pitäisi ***tukea*** unionin toimielinten, elinten ja virastojen tehtävien hoitamista***, ja niissä pitäisi ottaa huomioon*** niiden ***hallinnollinen riippumattomuus***. Näin ollen unionin toimielinten, elinten ja virastojen olisi laadittava omat kehyksensä kyberturvallisuusriskien hallintaa ja valvontaa varten sekä hyväksyttävä oma perustasonsa ja kyberturvallisuussuunnitelmansa ***ottaen huomioon kehystensä johdonmukaisuus ja yhteentoimivuus ja tässä asetuksessa säädetyn yhteisen kehyksen pohjalta***.

Tarkistus 6
Ehdotus asetukseksi
Johdanto-osan 8 kappale

Komission teksti	*Tarkistus*
(8) Jotta unionin toimielimille, elimille ja virastoille ei aiheutuisi kohtuutonta	(8) Jotta unionin toimielimille, elimille ja virastoille ei aiheutuisi kohtuutonta

taloudellista ja hallinnollista rasitetta, kyberturvallisuusriskien hallintaa koskevien vaatimusten olisi ***oltava oikeassa suhteessa*** asianomaisen verkko- ja tietojärjestelmän ***aiheuttamaan riskiin***, ottaen huomioon näiden toimenpiteiden viimeisin kehitys. Unionin kunkin toimielimen, elimen ja viraston olisi pyrittävä osoittamaan oman kyberturvatasonsa parantamiseen ***riittävä prosenttiosuus tietotekniikkamenoistaan. Pitkällä aikavälillä tavoitteena olisi oltava noin 10 prosenttia***.	taloudellista ja hallinnollista rasitetta, kyberturvallisuusriskien hallintaa koskevien vaatimusten olisi ***vastattava*** asianomaisen verkko- ja tietojärjestelmän ***aiheuttamaa riskiä***, ottaen huomioon näiden toimenpiteiden viimeisin kehitys. Unionin kunkin toimielimen, elimen ja viraston olisi pyrittävä osoittamaan oman kyberturvatasonsa parantamiseen ***keskipitkällä aikavälillä vähintään 10 prosenttia tieto- ja viestintätekniikkamenoistaan ja pitkällä aikavälillä tarvittaessa enemmän***.

Tarkistus 7

Ehdotus asetukseksi
Johdanto-osan 9 kappale

Komission teksti	*Tarkistus*
(9) Yhteinen korkea kyberturvataso edellyttää, että kyberturvallisuus on unionin kunkin toimielimen, elimen ja viraston ylimmän johdon valvonnassa. Ylimmän johdon olisi hyväksyttävä kyberturvallisuuden perustaso, jonka olisi torjuttava kunkin toimielimen, elimen ja viraston perustaman kehyksen mukaisesti tunnistettuja riskejä. Kyberturvallisuuskulttuuriin eli kyberturvallisuuden käytännön harjoittamiseen ***puuttuminen on*** keskeinen osa kyberturvallisuuden perustasoa kaikissa unionin toimielimissä, elimissä ja virastoissa.	(9) Yhteinen korkea kyberturvataso edellyttää, että kyberturvallisuus on ***EU:n yhteisen lautakunnan ja*** unionin kunkin toimielimen, elimen ja viraston ylimmän johdon valvonnassa. Ylimmän johdon olisi hyväksyttävä kyberturvallisuuden perustaso, jonka olisi torjuttava kunkin toimielimen, elimen ja viraston perustaman kehyksen mukaisesti tunnistettuja riskejä. Kyberturvallisuuskulttuuriin eli kyberturvallisuuden käytännön harjoittamiseen ***puuttumisesta olisi tultava*** keskeinen osa kyberturvallisuuden perustasoa kaikissa unionin toimielimissä, elimissä ja virastoissa.

Tarkistus 8

Ehdotus asetukseksi
Johdanto-osan 10 kappale

Komission teksti	*Tarkistus*
(10) Unionin toimielinten, elinten ja virastojen olisi arvioitava toimittajien ja	(10) Unionin toimielinten, elinten ja virastojen olisi arvioitava toimittajien ja

palveluntarjoajien, myös datatallennus- ja -käsittelypalvelujen tai tietoturvapalveluntarjoajien (MSSP), kanssa solmittaviin suhteisiin liittyviä riskejä ja toteutettava asianmukaiset toimet näiden riskien hallitsemiseksi. Näiden toimenpiteiden olisi muodostettava osa kyberturvallisuuden perustasoa, ja niitä olisi tarkennettava CERT-EU:n julkaisemissa ohjeasiakirjoissa tai suosituksissa. Toimenpiteitä ja ohjeita määriteltäessä olisi otettava asianmukaisesti huomioon asiaan liittyvä EU:n lainsäädäntö ja toimintapolitiikat, mukaan lukien NIS-yhteistyöryhmän julkaisemat riskinarvioinnit ja suositukset, kuten EU:n koordinoitu riskinarviointi ja 5G-kyberturvallisuutta koskeva EU:n välineistö. Lisäksi ***voitaisiin edellyttää*** asiaan liittyvien tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sertifiointia asetuksen (EU) 2019/881 49 artiklan nojalla hyväksyttyjen erityisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti.

palveluntarjoajien, myös datatallennus- ja -käsittelypalvelujen tai tietoturvapalveluntarjoajien (MSSP), kanssa solmittaviin suhteisiin liittyviä riskejä ja toteutettava asianmukaiset toimet näiden riskien hallitsemiseksi. ***Näistä toimittajista ja palveluntarjoajista olisi tehtävä perusteellinen selvitys ottaen huomioon koko toimitusketju sekä taloudellinen ja poliittinen ympäristö, jossa ne toimivat. Jos suhteet näihin toimittajiin ja palveluntarjoajiin aiheuttavat riskin unionin demokraattisten prosessien luotettavuudelle, ne olisi katkaistava ilman aiheetonta viivytystä.*** Näiden toimenpiteiden olisi muodostettava osa kyberturvallisuuden perustasoa, ja niitä olisi tarkennettava CERT-EU:n julkaisemissa ohjeasiakirjoissa tai suosituksissa. Toimenpiteitä ja ohjeita määriteltäessä olisi otettava asianmukaisesti huomioon asiaan liittyvä EU:n lainsäädäntö ja toimintapolitiikat, mukaan lukien NIS-yhteistyöryhmän julkaisemat riskinarvioinnit ja suositukset, kuten EU:n koordinoitu riskinarviointi ja 5G-kyberturvallisuutta koskeva EU:n välineistö. Lisäksi***, kun otetaan huomioon uhkamaisema ja sietokyvyn parantamisen merkitys, olisi edellytettävä unionin toimielimissä, elimissä ja virastoissa käytettyjen*** asiaan liittyvien tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sertifiointia asetuksen (EU) 2019/881 49 artiklan nojalla hyväksyttyjen erityisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti.

Tarkistus 9

Ehdotus asetukseksi
Johdanto-osan 13 kappale

Komission teksti	*Tarkistus*
(13) Lyhytnimi CERT-EU olisi säilytettävä nimen tunnettuuden vuoksi. Monet kyberhyökkäykset ovat osa laajempia kampanjoita, jotka kohdistuvat unionin toimielinten, elinten ja virastojen ryhmiin tai etuyhteisöihin, joihin sisältyy unionin toimielimiä, elimiä ja virastoja. Jotta voitaisiin havaita ongelmat etukäteen, reagoida poikkeamiin tai toteuttaa lieventäviä toimenpiteitä, unionin toimielinten, elinten ja virastojen olisi ilmoitettava CERT-EU:lle merkittävistä kyberuhkista, haavoittuvuuksista ja poikkeamista sekä jaettava sen kanssa asianmukaiset tekniset tiedot, jotka mahdollistavat samankaltaisen kyberuhkien, haavoittuvuuksien ja poikkeamien tunnistamisen tai lieventämisen sekä niihin reagoimisen muissa unionin toimielimissä, elimissä ja virastoissa. Direktiivissä [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] määritetyn lähestymistavan mukaisesti silloin, kun toimija saa tietoonsa merkittävän poikkeaman, sitä olisi vaadittava toimittamaan ***ensimmäinen ilmoitus*** CERT-EU:lle 24 tunnin kuluessa. Tällaisen tietojenvaihdon olisi mahdollistettava se, että CERT-EU levittää tiedot muille unionin toimielimille, elimille ja virastoille sekä asianmukaisille vastaavaa tehtävää hoitaville viranomaisille, jotta voidaan auttaa suojaamaan unionin ***tietoteknisiä*** järjestelmiä ja unionin kumppaneiden ***tietoteknisiä*** järjestelmiä samankaltaisilta poikkeamilta, uhkilta ja haavoittuvuuksilta.	(13) Lyhytnimi CERT-EU olisi säilytettävä nimen tunnettuuden vuoksi. Monet kyberhyökkäykset ovat osa laajempia kampanjoita, jotka kohdistuvat unionin toimielinten, elinten ja virastojen ryhmiin tai etuyhteisöihin, joihin sisältyy unionin toimielimiä, elimiä ja virastoja. Jotta voitaisiin havaita ongelmat etukäteen, reagoida poikkeamiin tai toteuttaa lieventäviä toimenpiteitä, unionin toimielinten, elinten ja virastojen olisi ilmoitettava CERT-EU:lle merkittävistä kyberuhkista, haavoittuvuuksista ja poikkeamista sekä jaettava sen kanssa asianmukaiset tekniset tiedot, jotka mahdollistavat samankaltaisen kyberuhkien, haavoittuvuuksien ja poikkeamien tunnistamisen tai lieventämisen sekä niihin reagoimisen muissa unionin toimielimissä, elimissä ja virastoissa. Direktiivissä [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] määritetyn lähestymistavan mukaisesti silloin, kun toimija saa tietoonsa merkittävän poikkeaman, sitä olisi vaadittava toimittamaan ***varhaisvaroitus*** CERT-EU:lle ***ilman aiheetonta viivytystä ja joka tapauksessa viimeistään*** 24 tunnin kuluessa. ***Unionin toimielimille, elimille ja virastoille olisi osoitettava riittävät resurssit, jotta ne voivat täyttää raportointivelvoitteensa nopeasti ja tehokkaasti sen varmistamiseksi, että suunniteltu järjestelmä toimii oikein.*** Tällaisen tietojenvaihdon olisi mahdollistettava se, että CERT-EU levittää tiedot muille unionin toimielimille, elimille ja virastoille sekä asianmukaisille vastaavaa tehtävää hoitaville viranomaisille, jotta voidaan auttaa suojaamaan unionin ***tieto- ja viestintäteknisiä*** järjestelmiä ja unionin kumppaneiden ***tieto- ja viestintäteknisiä*** järjestelmiä samankaltaisilta poikkeamilta,

uhkilta ja haavoittuvuuksilta.

Tarkistus 10

Ehdotus asetukseksi
Johdanto-osan 14 kappale

Komission teksti	*Tarkistus*
(14) Sen lisäksi, että CERT-EU:lle annetaan enemmän tehtäviä ja sen roolia laajennetaan, olisi perustettava toimielinten välinen kyberturvallisuuslautakunta (IICB). Sen olisi edistettävä yhteistä korkeaa kyberturvatasoa unionin toimielimissä, elimissä ja virastoissa seuraamalla tämän asetuksen täytäntöönpanoa unionin toimielimissä, elimissä ja virastoissa, valvomalla sitä, miten CERT-EU panee täytäntöön yleiset painopisteet ja tavoitteet, ja antamalla CERT-EU:lle strategista ohjausta. IICB:n olisi varmistettava toimielinten edustus ja otettava mukaan virastojen ja elinten edustajia unionin virastojen verkoston kautta.	(14) Sen lisäksi, että CERT-EU:lle annetaan enemmän tehtäviä ja sen roolia laajennetaan, olisi perustettava toimielinten välinen kyberturvallisuuslautakunta (IICB). Sen olisi edistettävä yhteistä korkeaa kyberturvatasoa unionin toimielimissä, elimissä ja virastoissa seuraamalla tämän asetuksen täytäntöönpanoa unionin toimielimissä, elimissä ja virastoissa, valvomalla sitä, miten CERT-EU panee täytäntöön yleiset painopisteet ja tavoitteet, ja antamalla CERT-EU:lle strategista ohjausta. IICB:n olisi varmistettava toimielinten ***tasapuolinen*** edustus ja otettava mukaan virastojen ja elinten edustajia unionin virastojen verkoston kautta.

Tarkistus 11

Ehdotus asetukseksi
Johdanto-osan 16 kappale

Komission teksti	*Tarkistus*
(16) IICB:n olisi valvottava tämän asetuksen noudattamista, ohjeasiakirjojen ja suositusten jatkotoimien toteuttamista sekä CERT-EU:n antamien toimintakehotusten noudattamista. Teknisissä asioissa IICB:n tukena olisi oltava teknisiä neuvoa-antavia ryhmiä***, joiden koostumuksesta päättää IICB***. Niiden olisi tehtävä tiivistä yhteistyötä CERT-EU:n, unionin toimielinten, elinten ja virastojen sekä ***tarvittaessa*** muiden sidosryhmien kanssa. Tarvittaessa IICB:n olisi annettava ***ei-sitovia*** varoituksia ja	(16) IICB:n olisi valvottava tämän asetuksen noudattamista, ohjeasiakirjojen ja suositusten jatkotoimien toteuttamista sekä CERT-EU:n antamien toimintakehotusten noudattamista. Teknisissä asioissa IICB:n tukena olisi oltava teknisiä neuvoa-antavia ryhmiä. Niiden olisi tehtävä tiivistä yhteistyötä CERT-EU:n, unionin toimielinten, elinten ja virastojen sekä ***tapauksen mukaan*** muiden sidosryhmien kanssa. Tarvittaessa IICB:n olisi annettava varoituksia ja

suositeltava tarkastuksia.	***tarkastussuosituksia***.

Tarkistus 12

Ehdotus asetukseksi
Johdanto-osan 17 kappale

Komission teksti	*Tarkistus*
(17) CERT-EU:n tarkoituksena olisi oltava edistää kaikkien unionin toimielinten, elinten ja ***virastojen tietoteknisen*** ympäristön turvallisuutta. CERT-EU:n olisi toimittava vastaavassa tehtävässä kuin direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 6 artiklassa tarkoitettu Euroopan haavoittuvuusrekisteriin tehtävää koordinoitua haavoittuvuuksien ilmaisemista varten unionin toimielimille, elimille ja virastoille nimetty koordinaattori.	(17) CERT-EU:n tarkoituksena olisi oltava edistää kaikkien unionin toimielinten, elinten ja ***laitosten tieto- ja viestintäteknisen*** ympäristön turvallisuutta. CERT-EU:n olisi toimittava vastaavassa tehtävässä kuin direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 6 artiklassa tarkoitettu Euroopan haavoittuvuusrekisteriin tehtävää koordinoitua haavoittuvuuksien ilmaisemista varten unionin toimielimille, elimille ja virastoille nimetty koordinaattori.

Tarkistus 13

Ehdotus asetukseksi
Johdanto-osan 18 kappale

Komission teksti	*Tarkistus*
(18) CERT-EU:n johtoryhmä asetti CERT-EU:lle vuonna 2020 uuden strategisen tavoitteen, joka on perusteellisen, soveltuvan laajuisen ja syvällisen kyberpuolustustason varmistaminen kaikissa unionin toimielimissä, elimissä ja virastoissa ja sen jatkuva mukauttaminen nykyisiin tai tuleviin uhkiin, kuten mobiililaitteisiin, pilviympäristöihin ja esineiden internetiä käyttäviin laitteisiin kohdistuviin hyökkäyksiin. Tämä strateginen tavoite sisältää myös laaja-alaiset turvaoperaatiokeskukset, jotka seuraavat verkkoja, sekä erittäin vakavien uhkien ympärivuorokautisen seurannan. CERT-	(18) CERT-EU:n johtoryhmä asetti CERT-EU:lle vuonna 2020 uuden strategisen tavoitteen, joka on perusteellisen, soveltuvan laajuisen ja syvällisen kyberpuolustustason varmistaminen kaikissa unionin toimielimissä, elimissä ja virastoissa ja sen jatkuva mukauttaminen nykyisiin tai tuleviin uhkiin, kuten mobiililaitteisiin, pilviympäristöihin ja esineiden internetiä käyttäviin laitteisiin kohdistuviin hyökkäyksiin. Tämä strateginen tavoite sisältää myös laaja-alaiset turvaoperaatiokeskukset, jotka seuraavat verkkoja, sekä erittäin vakavien uhkien ympärivuorokautisen seurannan. CERT-

EU:n olisi tuettava unionin suurten toimielinten, elinten ja virastojen ***tietotekniikan*** turvallisuudesta vastaavia ryhmiä, myös ympärivuorokautisessa ensivaiheen seurannassa. Lisäksi CERT-EU:n olisi tarjottava kaikki palvelut pienille ja joillekin keskikokoisille unionin toimielimille, elimille ja virastoille.	EU:n olisi tuettava unionin suurten toimielinten, elinten ja virastojen ***tieto- ja viestintätekniikan*** turvallisuudesta vastaavia ryhmiä, myös ympärivuorokautisessa ensivaiheen seurannassa. Lisäksi CERT-EU:n olisi tarjottava kaikki palvelut pienille ja joillekin keskikokoisille unionin toimielimille, elimille ja virastoille.

Tarkistus 14

Ehdotus asetukseksi
Johdanto-osan 19 a kappale (uusi)

Komission teksti	*Tarkistus*
	(19 a) Jotta voidaan varmistaa unionin toimielinten, elinten ja virastojen kyberturvallisuustoimenpiteiden ja suuntaviivojen parempi täytäntöönpano ja vahvistaa niiden kyberturvallisuuskulttuuria, CERT-EU:n olisi myös tehostettava yhteistyötä Euroopan kyberturvallisuuden osaamisverkoston ja -keskuksen kanssa.

Tarkistus 15

Ehdotus asetukseksi
Johdanto-osan 20 kappale

Komission teksti	*Tarkistus*
(20) CERT-EU:n olisi operatiivista kyberturvallisuutta tukiessaan hyödynnettävä saatavilla olevaa Euroopan unionin kyberturvallisuusviraston asiantuntemusta Euroopan parlamentin ja neuvoston asetuksessa (EU) 2019/881[5] tarkoitetun jäsennellyn yhteistyön kautta. ***Tarvittaessa*** tällaisen yhteistyön käytännön toteutus olisi määriteltävä erityisin järjestelyin näiden kahden yksikön välillä päällekkäisten tehtävien välttämiseksi. CERT-EU:n olisi tehtävä yhteistyötä Euroopan unionin	(20) CERT-EU:n olisi operatiivista kyberturvallisuutta tukiessaan hyödynnettävä saatavilla olevaa Euroopan unionin kyberturvallisuusviraston asiantuntemusta Euroopan parlamentin ja neuvoston asetuksessa (EU) 2019/881[5] tarkoitetun jäsennellyn yhteistyön kautta. Tällaisen yhteistyön käytännön toteutus olisi määriteltävä erityisin järjestelyin näiden kahden yksikön välillä päällekkäisten tehtävien välttämiseksi. CERT-EU:n olisi tehtävä yhteistyötä Euroopan unionin

kyberturvallisuusviraston kanssa uhka-analyysissa ja jaettava säännöllisesti uhkaympäristöä koskeva raporttinsa viraston kanssa.

kyberturvallisuusviraston kanssa uhka-analyysissa ja jaettava säännöllisesti uhkaympäristöä koskeva raporttinsa viraston kanssa.

---

[5] Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15).

[5] Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15).

Tarkistus 16
Ehdotus asetukseksi
Johdanto-osan 24 kappale

Komission teksti	*Tarkistus*
(24) Koska CERT-EU:n palvelut ja tehtävät ovat unionin kaikkien toimielinten, elinten ja virastojen edun mukaisia, unionin kunkin toimielimen, elimen ja viraston, jolla on ***tietotekniikkamenoja***, olisi osoitettava ***oikeudenmukainen*** rahoitusosuus näihin palveluihin ja tehtäviin. Nämä rahoitusosuudet eivät rajoita unionin toimielinten, elinten ja virastojen ***itsenäistä budjettivaltaa***.	(24) Koska CERT-EU:n palvelut ja tehtävät ovat unionin kaikkien toimielinten, elinten ja virastojen edun mukaisia, unionin kunkin toimielimen, elimen ja viraston, jolla on ***tieto- ja viestintätekniikkamenoja***, olisi osoitettava ***suhteellinen*** rahoitusosuus näihin palveluihin ja tehtäviin. Nämä rahoitusosuudet eivät rajoita unionin toimielinten, elinten ja virastojen ***budjettikapasiteettia***.

Tarkistus 17

Ehdotus asetukseksi
Johdanto-osan 25 kappale

Komission teksti	*Tarkistus*
(25) IICB:n olisi tarkasteltava ja arvioitava tämän asetuksen täytäntöönpanoa CERT-EU:n avustuksella ja raportoitava havainnoistaan komissiolle. Komission olisi näiden tietojen perusteella annettava ***kertomus*** Euroopan	(25) IICB:n olisi tarkasteltava ja arvioitava tämän asetuksen täytäntöönpanoa CERT-EU:n avustuksella ja raportoitava havainnoistaan komissiolle. Komission olisi näiden tietojen perusteella annettava ***vähintään kolmen vuoden***

parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle,	***välein kertomus*** Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle,

Tarkistus 18

Ehdotus asetukseksi
1 artikla – 1 kohta – a alakohta

Komission teksti	*Tarkistus*
a) unionin toimielimille, elimille ja virastoille asetettavista sisäisen kyberturvallisuusriskien hallinta- ja valvontakehyksen perustamisvelvoitteista;	a) unionin toimielimille, elimille***,*** ***toimistoille*** ja virastoille asetettavista sisäisen kyberturvallisuusriskien hallinta- ja valvontakehyksen perustamisvelvoitteista;

Tarkistus 19

Ehdotus asetukseksi
1 artikla – 1 kohta – c alakohta

Komission teksti	*Tarkistus*
c) unionin toimielinten, elinten ja virastojen kyberturvallisuuskeskuksen (CERT-EU) organisaatioon ja toimintaan sekä toimielinten välisen kyberturvallisuuslautakunnan organisaatioon ja toimintaan sovellettavista säännöistä.	c) unionin toimielinten, elinten ja virastojen kyberturvallisuuskeskuksen (CERT-EU) organisaatioon ja toimintaan sekä toimielinten välisen kyberturvallisuuslautakunnan ***(IICB) käytäntöihin,*** organisaatioon ja toimintaan sovellettavista säännöistä.

Tarkistus 20

Ehdotus asetukseksi
2 a artikla (uusi)

Komission teksti	*Tarkistus*
	2 a artikla
	Henkilötietojen käsittely
	CERT-EU:n, IICB:n ja kaikkien unionin toimielinten, elinten ja laitosten tämän asetuksen mukainen henkilötietojen käsittely toteutetaan Euroopan

parlamentin ja neuvoston asetuksen (EU) 2018/1725 mukaisesti.

Tarkistus 21

Ehdotus asetukseksi
3 artikla – 1 kohta – 2 alakohta

Komission teksti	*Tarkistus*
2) ’verkko- ja tietojärjestelmällä’ direktiivin [ehdotus NIS 2 -direktiiviksi] ***4*** artiklan 1 kohdassa ***tarkoitettua*** verkko- ja tietojärjestelmää;	2) ’verkko- ja tietojärjestelmällä’ direktiivin [ehdotus NIS 2 -direktiiviksi] ***6*** artiklan 1 kohdassa ***määriteltyä*** verkko- ja tietojärjestelmää;

Tarkistus 22

Ehdotus asetukseksi
3 artikla – 1 kohta – 4 alakohta

Komission teksti	*Tarkistus*
4) ’kyberturvallisuudella’ ja ’kyberturvalla’ ***direktiivin [ehdotus tarkistetuksi verkko- ja tietoturva -direktiiviksi] 4*** artiklan ***3*** kohdassa ***tarkoitettua*** kyberturvallisuutta ja kyberturvaa;	4) ’kyberturvallisuudella’ ja ’kyberturvalla’ ***Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/8811 a 2*** artiklan ***1*** kohdassa ***määriteltyä*** kyberturvallisuutta ja kyberturvaa;
	[1a]Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15).

Tarkistus 23

Ehdotus asetukseksi
3 artikla – 1 kohta – 5 alakohta

Komission teksti	*Tarkistus*
5) ’ylimmällä johdolla’ kaikkein ylimpään johtotasoon kuuluvaa johtajaa, hallinto- tai koordinointi- ja valvontaelintä unionin kunkin toimielimen, elimen tai viraston korkean tason hallintojärjestelyt huomioon ottaen;	5) ’ylimmällä johdolla’ kaikkein ylimpään johtotasoon kuuluvaa johtajaa, hallinto- tai koordinointi- ja valvontaelintä***, jolla on valtuudet tehdä tai vahvistaa päätöksiä,*** unionin kunkin toimielimen, elimen tai viraston korkean tason hallintojärjestelyt huomioon ottaen;

Tarkistus 24

Ehdotus asetukseksi
3 artikla – 1 kohta – 7 alakohta

Komission teksti	*Tarkistus*
7) ’merkittävällä poikkeamalla’ mitä tahansa poikkeamaa, ***lukuun ottamatta sellaisia, joilla*** on ***vähäinen vaikutus ja joihin ei todennäköisesti liity juurikaan epäselvyyksiä menetelmän*** tai ***teknologian osalta;***	7) ’merkittävällä poikkeamalla’ mitä tahansa poikkeamaa, ***joka on aiheuttanut tai voi aiheuttaa vakavaa toimintahäiriötä unionin yksikön toiminnalle tai taloudellista tappiota kyseiselle unionin yksikölle tai joka*** on ***vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista*** tai ***aineetonta vahinkoa.***

Tarkistus 25

Ehdotus asetukseksi
3 artikla – 1 kohta – 11 alakohta

Komission teksti	*Tarkistus*
11) ’merkittävällä kyberuhkalla’ kyberuhkaa***, jonka tarkoituksena on aiheuttaa, jolla saatetaan aiheuttaa tai jolla kyetään aiheuttamaan merkittävä poikkeama***;	11) ’merkittävällä kyberuhkalla’ ***direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 6 artiklan 11 kohdassa määriteltyä*** kyberuhkaa;

Tarkistus 26

Ehdotus asetukseksi
3 artikla – 1 kohta – 14 alakohta

Komission teksti	*Tarkistus*
14) ***'kyberturvallisuusriskillä'*** mitä tahansa ***kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti verkko- ja tietojärjestelmien turvallisuuteen***;	14) ***'riskillä'*** mitä tahansa ***direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 6 artiklan 9 kohdassa määriteltyä riskiä***;

Tarkistus 27

Ehdotus asetukseksi
3 artikla – 1 kohta – 14 a alakohta (uusi)

Komission teksti	*Tarkistus*
	14 a) 'tieto- ja viestintäteknisellä ympäristöllä' mitä tahansa asetuksen (EU) 2019/881 2 artiklan 12, 13 ja 14 kohdassa määriteltyä fyysistä tai virtuaalista tieto- ja viestintätekniikan tuotetta, palvelua tai prosessia taikka mitä tahansa verkko- ja tietojärjestelmää, jonka unionin toimielin, elin tai virasto omistaa ja jota se käyttää tai jota kolmas osapuoli ylläpitää tai käyttää, mukaan lukien mobiililaitteet, yritysverkot ja internetiin liittämättömät liiketoiminnan verkot ja kaikki tieto- ja viestintätekniseen ympäristöön liitetyt laitteet;

Perustelu

Käsite on siirretty tämän ehdotuksen 4 artiklan 2 kohdasta määritelmiä koskevaan artiklaan, koska käsitettä käytetään johdonmukaisesti kaikkialla tekstissä. Tälle käsitteelle ehdotettu määritelmä perustuu sen osatekijöiden määritelmiin, jotka on esitetty kyberturvallisuusasetuksen (EU) 2019/881 2 artiklassa.

Tarkistus 28

Ehdotus asetukseksi
3 artikla – 1 kohta – 15 alakohta

Komission teksti	*Tarkistus*
15) 'yhteisellä kyberturvallisuusyksiköllä' unionissa	***Poistetaan.***

toimivien eri kyberturvallisuusyhteisöjen yhteistyötä varten perustettua virtuaalista ja fyysistä alustaa, jossa keskitytään toimien operatiiviseen ja tekniseen koordinointiin 23 päivänä kesäkuuta 2021 annetussa komission suosituksessa tarkoitetuissa suurissa rajat ylittävissä kyberturvallisuusuhkissa ja -poikkeamissa;

Tarkistus 29
Ehdotus asetukseksi
4 artikla – 1 kohta

Komission teksti	*Tarkistus*
1. Unionin kukin toimielin, elin ja virasto laatii ylimmän johtonsa valvonnassa sisäisen kyberturvallisuusriskien hallinta- ja valvontakehyksen, jäljempänä ’kehys’, tukemaan kyseisen yksikön toimeksiantoa ja käyttäen institutionaalista itsemääräämisoikeuttaan. Tätä työtä valvotaan kyseisen yksikön ylimmällä hallintotasolla, ***jotta voidaan varmistaa*** kaikkien kyberturvallisuusriskien ***tehokas*** ja ***järkevä hallinta***. Kehyksen on oltava käytössä viimeistään … päivänä …kuuta … [15 kuukauden kuluttua tämän asetuksen ***voimaantulosta]***.	1. Unionin kukin toimielin, elin ja virasto laatii ***täysimittaisen turvallisuustarkastuksen perusteella*** ylimmän johtonsa valvonnassa sisäisen kyberturvallisuusriskien hallinta- ja valvontakehyksen, jäljempänä ’kehys’, tukemaan kyseisen yksikön toimeksiantoa ja käyttäen institutionaalista itsemääräämisoikeuttaan ***ja ottaen huomioon kehyksensä johdonmukaisuuden ja yhteentoimivuuden muiden asiaankuuluvien toimielinten, elinten ja virastojen kehysten kanssa***. Tätä työtä valvotaan kyseisen yksikön ylimmällä hallintotasolla, ***joka on vastuussa*** kaikkien kyberturvallisuusriskien ***tehokkaan*** ja ***järkevän hallinnan varmistamisesta***. Kehyksen on oltava käytössä viimeistään … päivänä …kuuta … [15 kuukauden kuluttua tämän asetuksen ***voimaantulopäivästä]***.

Tarkistus 30

Ehdotus asetukseksi
4 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. Kehyksen on katettava	2. Kehyksen on katettava

asianomaisen toimielimen, elimen tai viraston koko ***tietotekninen*** ympäristö, mukaan lukien sen tiloissa oleva ***tietotekninen*** ympäristö, pilvipalveluympäristöissä olevat tai kolmansien osapuolten ylläpitämät ulkoistetut resurssit ja palvelut, mobiililaitteet, yritysverkot, internetiin liittämättömät liiketoiminnan verkot ja kaikki ***tietotekniseen*** ympäristöön liitetyt laitteet. Kehyksessä on otettava huomioon toiminnan jatkuvuus ja kriisitilanteiden hallinta, toimitusketjun turvallisuus sekä sellaisten inhimillisten riskien hallinta, jotka voisivat vaikuttaa unionin asianomaisen toimielimen, elimen tai viraston kyberturvallisuuteen.	asianomaisen toimielimen, elimen tai viraston koko ***tieto- ja viestintätekninen*** ympäristö, mukaan lukien sen tiloissa oleva ***tieto- ja viestintätekninen*** ympäristö, pilvipalveluympäristöissä olevat tai kolmansien osapuolten ylläpitämät ulkoistetut resurssit ja palvelut, mobiililaitteet, yritysverkot, internetiin liittämättömät liiketoiminnan verkot ja kaikki ***tieto- ja viestintätekniseen*** ympäristöön liitetyt laitteet. Kehyksessä on otettava huomioon toiminnan jatkuvuus ja kriisitilanteiden hallinta, toimitusketjun turvallisuus sekä sellaisten inhimillisten riskien hallinta, jotka voisivat vaikuttaa unionin asianomaisen toimielimen, elimen tai viraston kyberturvallisuuteen.

Tarkistus 31
Ehdotus asetukseksi
4 artikla – 4 kohta

Komission teksti	*Tarkistus*
4. Unionin kullakin toimielimellä, elimellä ja virastolla on oltava käytössä tehokkaat mekanismit sen varmistamiseksi, että ***riittävä prosenttiosuus tietotekniikkamenoista*** käytetään kyberturvallisuuteen.	4. Unionin kullakin toimielimellä, elimellä ja virastolla on oltava käytössä tehokkaat mekanismit sen varmistamiseksi, että ***keskipitkällä aikavälillä vähintään 10 prosenttia yhteenlasketuista tieto- ja viestintätekniikkamenoista*** käytetään kyberturvallisuuteen.

Tarkistus 32

Ehdotus asetukseksi
4 artikla – 5 a kohta (uusi)

Komission teksti	*Tarkistus*
	5 a. Paikallinen kyberturvallisuusvastaava tekee yhteistyötä asetuksen (EU) 2018/1725 43 artiklassa tarkoitetun tietosuojavastaavan kanssa hoitaessaan päällekkäisiä tehtäviä ja soveltaa kyberturvallisuustoimenpiteisiin

	sisäänrakennettua ja oletusarvoista tietosuojaa ja valitsee sellaisia kyberturvallisuustoimenpiteitä, joihin sisältyy henkilötietojen suoja, integroitu riskinhallinta ja yhdennetty turvallisuuspoikkeamien käsittely.

Tarkistus 33

Ehdotus asetukseksi
5 artikla – 1 kohta

Komission teksti	*Tarkistus*
1. Unionin kunkin toimielimen, elimen ja viraston ylin johto hyväksyy kyberturvallisuuden perustason 4 artiklan 1 kohdassa tarkoitetussa kehyksessä eriteltyjen riskien torjumiseksi. Se tekee tämän tukeakseen toimeksiantoaan ja käyttäen institutionaalista itsemääräämisoikeuttaan. Kyberturvallisuuden perustason on oltava käytössä viimeistään … päivänä …kuuta … [18 kuukauden kuluttua tämän asetuksen ***voimaantulosta]***, ja sen on katettava liitteessä I luetellut osa-alueet ja liitteessä II luetellut toimenpiteet.	1. Unionin kunkin toimielimen, elimen ja viraston ylin johto hyväksyy kyberturvallisuuden perustason 4 artiklan 1 kohdassa tarkoitetussa kehyksessä eriteltyjen riskien torjumiseksi. Se tekee tämän tukeakseen toimeksiantoaan ja käyttäen institutionaalista itsemääräämisoikeuttaan ***täysin tämän asetuksen vaatimusten mukaisesti ja ottaen huomioon kehyksensä johdonmukaisuuden ja yhteentoimivuuden muiden asiaankuuluvien toimielinten, elinten ja virastojen kehysten kanssa sekä IICB:n CERT-EU:n ehdotuksesta hyväksymät ohjeasiakirjat ja suositukset sekä sovellettavat eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät***. Kyberturvallisuuden perustason on oltava käytössä viimeistään … päivänä …kuuta … [18 kuukauden kuluttua tämän asetuksen ***voimaantulopäivästä]***, ja sen on katettava liitteessä I luetellut osa-alueet ja liitteessä II luetellut toimenpiteet.

Tarkistus 34

Ehdotus asetukseksi
5 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. Unionin kunkin toimielimen, elimen ja viraston ylempi johto osallistuu säännöllisesti erityiskoulutukseen riittävien tietojen ja taitojen hankkimiseksi, jotta he voivat ymmärtää ja arvioida kyberturvallisuusriskejä ja -hallintakäytäntöjä sekä niiden vaikutusta organisaation toimintoihin.	2. Unionin kunkin toimielimen, elimen ja viraston ylempi johto osallistuu säännöllisesti erityiskoulutukseen riittävien tietojen ja taitojen hankkimiseksi, jotta he voivat ymmärtää ja arvioida kyberturvallisuusriskejä ja -hallintakäytäntöjä sekä niiden vaikutusta organisaation toimintoihin***, ja niiden käytössä on oltava riittävästi resursseja. Tällaisen erityiskoulutuksen lisäksi ja kyberturvallisuuskulttuurin luomiseksi ja lujittamiseksi kyberturvallisuussuunnitelmaan on sisällytettävä henkilöstön jäsenten säännöllinen kyberturvallisuuskoulutus ja sitä on päivitettävä vähintään kahden vuoden välein. On varmistettava riittävät resurssit laadukkaan koulutuksen tarjoamiseksi.***

Tarkistus 35

Ehdotus asetukseksi
6 artikla – 1 kohta

Komission teksti	*Tarkistus*
Unionin kukin toimielin, elin tai virasto suorittaa vähintään joka ***kolmas*** vuosi kyberturvallisuuden kehitystason arvioinnin ja sisällyttää siihen kaikki 4 artiklassa tarkoitetut ***tietoteknisen*** ympäristönsä osatekijät ottaen huomioon 13 artiklan nojalla hyväksytyt asiaan liittyvät ohjeasiakirjat ja suositukset.	Unionin kukin toimielin, elin tai virasto suorittaa ***viimeistään … päivänä …kuuta … [6 kuukauden kuluttua tämän asetuksen voimaantulosta] ja sen jälkeen*** vähintään joka ***toinen*** vuosi kyberturvallisuuden kehitystason arvioinnin ja sisällyttää siihen kaikki 4 artiklassa tarkoitetut ***tieto- ja viestintäteknisen*** ympäristönsä osatekijät ottaen huomioon 13 artiklan nojalla hyväksytyt asiaan liittyvät ohjeasiakirjat ja suositukset. ***Kyberturvallisuuden kehitystason arvioinnin on perustuttava sellaisten tarjoajien tekemiin riippumattomiin kyberturvallisuustarkastuksiin, joista on tehty selvitys.***

Tarkistus 36

Ehdotus asetukseksi
7 artikla – 1 kohta

Komission teksti	*Tarkistus*
1. Kehitystason arvioinnista saatujen johtopäätösten perusteella ja ottaen huomioon 4 artiklan nojalla tunnistetut resurssit ja riskit unionin kukin toimielin, elin ja virasto hyväksyy kyberturvallisuussuunnitelman ilman aiheetonta viivytystä sen jälkeen, kun riskien hallinta- ja valvontakehys sekä kyberturvallisuuden perustaso on määritetty. Suunnitelman tavoitteena on nostaa asianomaisen yksikön yleistä kyberturvallisuutta ja edistää siten yhteisen korkean kyberturvatason saavuttamista tai parantamista unionin kaikissa toimielimissä, elimissä ja virastoissa. Yksikön toimeksiannon tukemiseksi sen institutionaalisen itsemääräämisoikeuden pohjalta suunnitelman on sisällettävä vähintään liitteessä I luetellut osa-alueet, liitteessä II luetellut toimenpiteet sekä poikkeamiin varautumiseen ja reagoimiseen ja niistä toipumiseen liittyvät toimenpiteet, kuten turvallisuuden seuranta ja kirjaaminen. Suunnitelmaa on tarkistettava vähintään joka ***kolmas*** vuosi 6 artiklan mukaisesti tehtyjen kehitystason arviointien perusteella.	1. Kehitystason arvioinnista saatujen johtopäätösten perusteella ja ottaen huomioon 4 artiklan nojalla tunnistetut resurssit ja riskit unionin kukin toimielin, elin ja virasto hyväksyy kyberturvallisuussuunnitelman ilman aiheetonta viivytystä sen jälkeen, kun riskien hallinta- ja valvontakehys sekä kyberturvallisuuden perustaso on määritetty. Suunnitelman tavoitteena on nostaa asianomaisen yksikön yleistä kyberturvallisuutta ja edistää siten yhteisen korkean kyberturvatason saavuttamista tai parantamista unionin kaikissa toimielimissä, elimissä ja virastoissa. Yksikön toimeksiannon tukemiseksi sen institutionaalisen itsemääräämisoikeuden pohjalta suunnitelman on sisällettävä vähintään liitteessä I luetellut osa-alueet, liitteessä II luetellut toimenpiteet sekä poikkeamiin varautumiseen ja reagoimiseen ja niistä toipumiseen liittyvät toimenpiteet, kuten ***toimittajien ja palvelujen*** turvallisuuden ***arviointi,*** seuranta ja kirjaaminen. Suunnitelmaa on tarkistettava vähintään joka ***toinen*** vuosi 6 artiklan mukaisesti tehtyjen kehitystason arviointien perusteella.

Tarkistus 37

Ehdotus asetukseksi
7 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. Kyberturvallisuussuunnitelman on sisällettävä henkilöstön jäsenten tehtävät ja	2. Kyberturvallisuussuunnitelman on sisällettävä henkilöstön jäsenten tehtävät***, varautuminen*** ja vastuut sen

vastuut sen täytäntöönpanossa.

täytäntöönpanossa.

Tarkistus 38

Ehdotus asetukseksi
7 artikla – 3 kohta

Komission teksti	*Tarkistus*
3. ***Kyberturvallisuussuunnitelmassa*** on ***otettava huomioon*** CERT-EU:n ***julkaisemat soveltuvat ohjeasiakirjat*** ja ***suositukset***.	3. ***Kyberturvallisuussuunnitelmaan*** on ***sisällytettävä kaikki*** CERT-EU:n ***julkaisemissa soveltuvissa ohjeasiakirjoissa*** ja ***suosituksissa ehdotetut toimenpiteet***.

Tarkistus 39

Ehdotus asetukseksi
7 artikla – 3 a kohta (uusi)

Komission teksti	*Tarkistus*
	3 a. Unionin toimielimet, elimet ja virastot toimittavat kyberturvallisuussuunnitelmansa IICB:lle. Nämä suunnitelmat on mahdollisuuksien mukaan jaettava ilman, että vaarana on, että luvattomille kolmansille osapuolille paljastetaan tai julkistetaan arkaluonteisia tai luottamuksellisia tietoja unionin elimen erityisistä teknisistä kyberturvallisuusjärjestelyistä ja -valmiuksista.

Tarkistus 40

Ehdotus asetukseksi
9 artikla – 2 kohta – a alakohta

Komission teksti	*Tarkistus*
a) seurata tämän asetuksen täytäntöönpanoa unionin toimielimissä, elimissä ja virastoissa;	a) seurata tämän asetuksen täytäntöönpanoa unionin toimielimissä, elimissä ja virastoissa ***ja antaa suosituksia***

	saman korkean kyberturvallisuustason saavuttamiseksi;

Tarkistus 41

Ehdotus asetukseksi
9 artikla – 3 kohta – 1 alakohta – johdantokappale

Komission teksti	*Tarkistus*
IICB koostuu kolmesta unionin virastojen verkoston (EUAN) nimittämästä edustajasta, jotka nimitetään tieto- ja viestintätekniikkaa käsittelevän neuvoa-antavan komitean ehdotuksesta ja edustavat omaa ***tietoteknistä*** ympäristöään käyttävien virastojen ja elinten etuja, sekä yhdestä kunkin seuraavan nimeämästä edustajasta:	IICB koostuu kolmesta unionin virastojen verkoston (EUAN) nimittämästä edustajasta, jotka nimitetään tieto- ja viestintätekniikkaa käsittelevän neuvoa-antavan komitean ehdotuksesta ja edustavat omaa ***tieto- ja viestintäteknistä*** ympäristöään käyttävien virastojen ja elinten etuja, sekä yhdestä kunkin seuraavan nimeämästä edustajasta:

Tarkistus 42

Ehdotus asetukseksi
9 artikla – 3 kohta – 1 alakohta – k a alakohta (uusi)

Komission teksti	*Tarkistus*
	k a) Euroopan tietosuojavaltuutettu.

Tarkistus 43

Ehdotus asetukseksi
10 artikla – 1 kohta – a a alakohta (uusi)

Komission teksti	*Tarkistus*
	a a) hyväksyä CERT-EU:n johtajan ehdotuksen perusteella yhdelle tai kaikille unionin toimielimille, elimille ja laitoksille tarkoitetut suositukset saman korkean kyberturvallisuustason saavuttamiseksi;

Tarkistus 44

Ehdotus asetukseksi
11 artikla – 1 kohta – a alakohta

Komission teksti	*Tarkistus*
a) antaa varoituksen; jos se on tarpeen huomattavan kyberturvallisuusriskin vuoksi, varoituksen yleisö on rajattava asianmukaisesti;	a) antaa varoituksen; jos se on tarpeen huomattavan kyberturvallisuusriskin vuoksi, varoituksen yleisö on rajattava asianmukaisesti ***yhteisesti sovituilla menetelmillä***;

Tarkistus 45

Ehdotus asetukseksi
11 artikla – 1 kohta – b alakohta

Komission teksti	*Tarkistus*
b) ***suositella***, että asiaankuuluva tarkastusyksikkö tekee tarkastuksen.	b) ***määrätä***, että asiaankuuluva tarkastusyksikkö tekee tarkastuksen.

Tarkistus 46

Ehdotus asetukseksi
12 artikla – 1 kohta

Komission teksti	*Tarkistus*
1. CERT-EU:n, joka on unionin kaikkien toimielinten, elinten ja virastojen itsenäinen toimielinten välinen kyberturvallisuuskeskus, tarkoituksena on edistää unionin kaikkien toimielinten, elinten ja virastojen turvallisuusluokittelemattoman ***tietoteknisen*** ympäristön turvallisuutta neuvomalla niitä kyberturvallisuusasioissa, auttamalla niitä ehkäisemään, havaitsemaan ja lieventämään poikkeamia ja reagoimaan niihin sekä toimimalla niiden kyberturvallisuutta koskevan tietojenvaihdon ja poikkeamiin reagoimisen koordinointikeskuksena.	1. CERT-EU:n, joka on unionin kaikkien toimielinten, elinten ja virastojen itsenäinen toimielinten välinen kyberturvallisuuskeskus, tarkoituksena on edistää unionin kaikkien toimielinten, elinten ja virastojen turvallisuusluokittelemattoman ***tieto- ja viestintäteknisen*** ympäristön turvallisuutta neuvomalla niitä kyberturvallisuusasioissa, auttamalla niitä ehkäisemään, havaitsemaan ja lieventämään poikkeamia ja reagoimaan niihin sekä toimimalla niiden kyberturvallisuutta koskevan tietojenvaihdon ja poikkeamiin reagoimisen koordinointikeskuksena.

Tarkistus 47

Ehdotus asetukseksi
12 artikla – 2 kohta – d alakohta

Komission teksti	*Tarkistus*
d) mahdollisten tämän asetuksen täytäntöönpanoon sekä ohjeasiakirjojen, suositusten ja toimintakehotusten täytäntöönpanoon liittyvien ongelmien tuominen IICB:n tietoon***;***	d) mahdollisten tämän asetuksen täytäntöönpanoon sekä ohjeasiakirjojen, suositusten ja toimintakehotusten täytäntöönpanoon liittyvien ongelmien tuominen IICB:n tietoon ***ja korjausehdotusten tekeminen.***

Tarkistus 48

Ehdotus asetukseksi
12 artikla – 4 kohta

Komission teksti	*Tarkistus*
4. CERT-EU tekee jäsenneltyä yhteistyötä Euroopan unionin kyberturvallisuusviraston kanssa kyberuhkien valmiuksien kehittämisessä, operatiivisessa yhteistyössä ja kyberuhkista tehtävissä pitkän aikavälin strategisissa analyyseissa Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 mukaisesti.	4. CERT-EU tekee jäsenneltyä yhteistyötä Euroopan unionin kyberturvallisuusviraston kanssa kyberuhkien valmiuksien kehittämisessä, operatiivisessa yhteistyössä ja kyberuhkista tehtävissä pitkän aikavälin strategisissa analyyseissa Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 mukaisesti. ***Lisäksi CERT-EU voi tehdä yhteistyötä ja vaihtaa tietoja Euroopan kyberrikostorjuntakeskuksen kanssa.***

Tarkistus 49

Ehdotus asetukseksi
12 artikla – 5 kohta – johdantokappale

Komission teksti	*Tarkistus*
5. CERT-EU voi tarjota seuraavia palveluja, joita ei kuvata sen palvelujen luettelossa (veloitettavat palvelut):	5. CERT-EU voi tarjota ***unionin toimielimille, elimille ja virastoille*** seuraavia palveluja, joita ei kuvata sen palvelujen luettelossa (veloitettavat palvelut):

Tarkistus 50

Ehdotus asetukseksi
12 artikla – 5 kohta – a alakohta

Komission teksti	*Tarkistus*
a) muut kuin 2 kohdassa tarkoitetut palvelut, joilla tuetaan unionin toimielinten, elinten ja virastojen ***tietoteknisen*** ympäristön kyberturvallisuutta, palvelutasosopimusten perusteella ja saatavilla olevien resurssien mukaan;	a) muut kuin 2 kohdassa tarkoitetut palvelut, joilla tuetaan unionin toimielinten, elinten ja virastojen ***tieto- ja viestintäteknisen*** ympäristön kyberturvallisuutta, palvelutasosopimusten perusteella ja saatavilla olevien resurssien mukaan;

Tarkistus 51

Ehdotus asetukseksi
12 artikla – 5 kohta – b alakohta

Komission teksti	*Tarkistus*
b) palvelut, joilla tuetaan muita kuin toimielinten, elinten ja virastojen ***tietoteknisen*** ympäristön suojaamiseksi toteutettavia kyberturvallisuustoimia tai -hankkeita, kirjallisten sopimusten perusteella ja IICB:n etukäteisellä hyväksynnällä;	b) palvelut, joilla tuetaan muita kuin toimielinten, elinten ja virastojen ***tieto- ja viestintäteknisen*** ympäristön suojaamiseksi toteutettavia kyberturvallisuustoimia tai -hankkeita, kirjallisten sopimusten perusteella ja IICB:n etukäteisellä hyväksynnällä;

Tarkistus 52
Ehdotus asetukseksi
12 artikla – 5 kohta – c alakohta

Komission teksti	*Tarkistus*
c) palvelut, joilla tuetaan sellaisten muiden kuin unionin toimielinten, elinten ja virastojen organisaatioiden, jotka tekevät tiivistä yhteistyötä unionin toimielinten, elinten ja virastojen kanssa esimerkiksi koska niille on annettu unionin lainsäädännön mukaisia tehtäviä tai vastuita, ***tietoteknisen*** ympäristön	c) palvelut, joilla tuetaan sellaisten muiden kuin unionin toimielinten, elinten ja virastojen organisaatioiden, jotka tekevät tiivistä yhteistyötä unionin toimielinten, elinten ja virastojen kanssa esimerkiksi koska niille on annettu unionin lainsäädännön mukaisia tehtäviä tai vastuita, ***tieto- ja viestintäteknisen***

turvallisuutta, kirjallisten sopimusten perusteella ja IICB:n etukäteisellä hyväksynnällä.	ympäristön turvallisuutta, kirjallisten sopimusten perusteella ja IICB:n etukäteisellä hyväksynnällä.

Tarkistus 53

Ehdotus asetukseksi
12 artikla – 6 kohta

Komission teksti	*Tarkistus*
6. CERT-EU voi tarvittaessa järjestää kyberturvallisuusharjoituksia tai suositella osallistumista jo käytössä oleviin harjoituksiin tiiviissä yhteistyössä Euroopan unionin kyberturvallisuusviraston kanssa unionin toimielinten, elinten ja virastojen kyberturvatason testaamiseksi.	6. CERT-EU voi tarvittaessa järjestää kyberturvallisuusharjoituksia tai suositella osallistumista jo käytössä oleviin harjoituksiin tiiviissä yhteistyössä Euroopan unionin kyberturvallisuusviraston kanssa unionin toimielinten, elinten ja virastojen kyberturvatason testaamiseksi ***säännöllisesti. Lisäksi CERT-EU voi tukea tutkimusta ja innovointia sekä auttaa vahvistamaan unionin toimielinten, elinten ja virastojen kyberturvallisuusvalmiuksia tehostamalla yhteistyötä ja toteuttamalla yhteisiä ohjelmia Euroopan kyberturvallisuuden osaamisverkoston (ECCC) ja -keskuksen kanssa.***

Tarkistus 54

Ehdotus asetukseksi
12 artikla – 7 kohta

Komission teksti	*Tarkistus*
7. CERT-EU ***voi*** avustaa unionin toimielimiä, elimiä ja virastoja turvallisuusluokitelluissa ***tietoteknisissä*** ympäristöissä tapahtuvissa poikkeamissa, jos unionin ***asianomainen*** toimielin, elin tai virasto sitä nimenomaisesti pyytää.	7. CERT-EU avustaa unionin toimielimiä, elimiä ja virastoja turvallisuusluokitelluissa ***tieto- ja viestintäteknisissä*** ympäristöissä tapahtuvissa poikkeamissa, jos ***asianomainen*** unionin toimielin, elin tai virasto sitä nimenomaisesti pyytää ***ja jos CERT -EU on pyytänyt resursseja näin tehdäkseen tai saa tällaisia resursseja asianomaiselta yksiköltä***.

Tarkistus 55

Ehdotus asetukseksi
14 artikla – 1 kohta

Komission teksti	*Tarkistus*
CERT-EU:n johtaja toimittaa ***säännöllisesti*** kertomuksia IICB:lle ja IICB:n puheenjohtajalle CERT-EU:n toiminnasta, rahoitussuunnitelmasta, tuloista, talousarvion toteuttamisesta, tehdyistä palvelutasosopimuksista ja kirjallisista sopimuksista, yhteistyöstä vastaavaa tehtävää hoitavien elinten ja kumppanien kanssa sekä henkilöstön virkamatkoista, mukaan lukien 10 artiklan 1 kohdassa tarkoitetut kertomukset.	CERT-EU:n johtaja toimittaa ***vähintään kerran vuodessa*** kertomuksia IICB:lle ja IICB:n puheenjohtajalle CERT-EU:n toiminnasta, rahoitussuunnitelmasta, tuloista, talousarvion toteuttamisesta, tehdyistä palvelutasosopimuksista ja kirjallisista sopimuksista, yhteistyöstä vastaavaa tehtävää hoitavien elinten ja kumppanien kanssa sekä henkilöstön virkamatkoista, mukaan lukien 10 artiklan 1 kohdassa tarkoitetut kertomukset.

Tarkistus 56

Ehdotus asetukseksi
16 artikla – 1 kohta

Komission teksti	*Tarkistus*
1. CERT-EU tekee yhteistyötä ja vaihtaa tietoja jäsenvaltioissa vastaavaa tehtävää hoitavien kansallisten elinten, muun muassa CERT-yksiköiden, kansallisten kyberturvallisuuskeskusten, CSIRT-yksiköiden ja direktiivin [ehdotus NIS 2 -direktiiviksi] 8 artiklassa tarkoitettujen keskitettyjen yhteyspisteiden, kanssa kyberuhkista, haavoittuvuuksista ja poikkeamista, mahdollisista vastatoimista ja kaikista asioista, jotka ovat merkityksellisiä unionin toimielinten, elinten ja virastojen ***tietoteknisten*** ympäristöjen suojaamisen parantamisen kannalta, myös direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 13 artiklassa tarkoitetun CSIRT-verkoston kautta.	1. CERT-EU tekee yhteistyötä ja vaihtaa tietoja jäsenvaltioissa vastaavaa tehtävää hoitavien kansallisten elinten, muun muassa CERT-yksiköiden, kansallisten kyberturvallisuuskeskusten, CSIRT-yksiköiden ja direktiivin [ehdotus NIS 2 -direktiiviksi] 8 artiklassa tarkoitettujen keskitettyjen yhteyspisteiden, kanssa kyberuhkista, haavoittuvuuksista ja poikkeamista, mahdollisista vastatoimista ja kaikista asioista, jotka ovat merkityksellisiä unionin toimielinten, elinten ja virastojen ***tieto- ja viestintäteknisten*** ympäristöjen suojaamisen parantamisen kannalta, myös direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 13 artiklassa tarkoitetun CSIRT-verkoston kautta.

Tarkistus 57

Ehdotus asetukseksi
16 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. CERT-EU voi vaihtaa poikkeamakohtaisia tietoja jäsenvaltioissa vastaavaa tehtävää hoitavien kansallisten elinten kanssa, jotta voidaan helpottaa samankaltaisten kyberuhkien tai -poikkeamien havaitsemista, ilman vaikutuksen kohteena olevan unionin toimielimen, elimen tai viraston suostumusta. CERT-EU voi vaihtaa sellaisia poikkeamakohtaisia tietoja, joista käy ilmi kyberturvallisuuspoikkeaman kohteen identiteetti, ainoastaan poikkeaman kohteena ***olleen tahon*** suostumuksella.	2. CERT-EU voi vaihtaa poikkeamakohtaisia tietoja jäsenvaltioissa vastaavaa tehtävää hoitavien kansallisten elinten kanssa, jotta voidaan helpottaa samankaltaisten kyberuhkien tai -poikkeamien havaitsemista, ilman vaikutuksen kohteena olevan unionin toimielimen, elimen tai viraston suostumusta***, kunhan henkilötietojen käsittelyssä noudatetaan asetuksen (EU) 2018/1725 sovellettavia säännöksiä***. CERT-EU voi vaihtaa sellaisia poikkeamakohtaisia tietoja, joista käy ilmi kyberturvallisuuspoikkeaman kohteen identiteetti, ainoastaan poikkeaman kohteena ***olleiden unionin toimielinten, elinten tai virastojen*** suostumuksella.

Tarkistus 58

Ehdotus asetukseksi
17 artikla – 1 kohta

Komission teksti	*Tarkistus*
1. CERT-EU voi tehdä yhteistyötä muiden kuin jäsenvaltioiden vastaavien elinten kanssa, mukaan lukien vastaavat toimialakohtaiset elimet, siltä osin kuin on kyse välineistä ja menetelmistä, kuten tekniikoista, taktiikoista, menettelyistä ja parhaista käytännöistä, tai kyberuhkista ja haavoittuvuuksista. CERT-EU:n on pyydettävä ennakolta IICB:ltä hyväksyntä kaikkien tällaisten vastaavien elinten kanssa tehtävälle yhteistyölle, myös puitteissa, joissa EU:n ulkopuoliset vastaavat elimet tekevät yhteistyötä jäsenvaltioiden kansallisten vastaavien elinten kanssa.	1. CERT-EU voi tehdä yhteistyötä muiden kuin jäsenvaltioiden vastaavien elinten kanssa, mukaan lukien vastaavat toimialakohtaiset elimet, siltä osin kuin on kyse välineistä ja menetelmistä, kuten tekniikoista, taktiikoista, menettelyistä ja parhaista käytännöistä, tai kyberuhkista ja haavoittuvuuksista. CERT-EU:n on pyydettävä ennakolta IICB:ltä hyväksyntä kaikkien tällaisten vastaavien elinten kanssa tehtävälle yhteistyölle, myös puitteissa, joissa EU:n ulkopuoliset vastaavat elimet tekevät yhteistyötä jäsenvaltioiden kansallisten vastaavien elinten kanssa. ***Tällaisessa yhteistyössä on kunnioitettava EU:n demokraattista***

integriteettiä.

Tarkistus 59

Ehdotus asetukseksi
17 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. CERT-EU voi tehdä yhteistyötä muiden kumppaneiden, kuten kaupallisten toimijoiden, kansainvälisten järjestöjen, Euroopan unionin ulkopuolisten kansallisten yksikköjen tai yksittäisten asiantuntijoiden, kanssa kerätäkseen tietoa yleisistä ja erityisistä kyberuhkista, haavoittuvuuksista ja mahdollisista vastatoimista. CERT-EU hakee IICB:ltä etukäteen hyväksynnän tällaisten kumppanien kanssa tehtävälle laajemmalle yhteistyölle.	2. CERT-EU voi tehdä yhteistyötä muiden kumppaneiden, kuten kaupallisten toimijoiden, kansainvälisten järjestöjen, Euroopan unionin ulkopuolisten kansallisten yksikköjen tai yksittäisten asiantuntijoiden, kanssa kerätäkseen tietoa yleisistä ja erityisistä kyberuhkista, haavoittuvuuksista ja mahdollisista vastatoimista. CERT-EU hakee IICB:ltä etukäteen hyväksynnän tällaisten kumppanien kanssa tehtävälle laajemmalle yhteistyölle. ***Tällaisessa yhteistyössä on kunnioitettava EU:n demokraattista integriteettiä.***

Tarkistus 60

Ehdotus asetukseksi
17 artikla – 3 kohta

Komission teksti	*Tarkistus*
3. CERT-EU voi vaikutuksen kohteena olevan unionin toimielimen, elimen tai viraston suostumuksella antaa poikkeamaan liittyviä tietoja kumppaneille, jotka voivat auttaa poikkeaman analysoinnissa.	*(Tarkistus ei vaikuta suomenkieliseen versioon.)*

Tarkistus 61

Ehdotus asetukseksi
19 artikla – -1 kohta (uusi)

Komission teksti	*Tarkistus*

	-1. Unionin toimielimet, elimet tai virastot voivat vapaaehtoisesti toimittaa CERT-EU:lle tietoja niihin vaikuttavista kyberuhkista, poikkeamista, läheltä piti -tilanteista ja haavoittuvuuksista. CERT-EU varmistaa, että on käytössä tehokkaita viestintävälineitä tietojenvaihdon helpottamiseksi unionin yksiköiden kanssa. CERT-EU voi asettaa etusijalle pakollisten ilmoitusten käsittelyn vapaaehtoisten ilmoitusten käsittelyyn nähden.

Tarkistus 62

Ehdotus asetukseksi
19 artikla – 1 kohta

Komission teksti	*Tarkistus*
1. Jotta CERT-EU ***kykenee koordinoimaan haavoittuvuuksien hallintaa ja poikkeamiin reagoimista***, se voi pyytää unionin toimielimiä, elimiä ja virastoja toimittamaan sille tietoa niiden ***tietoteknisiin*** järjestelmiin liittyvistä selvityksistä, jotka ***ovat merkityksellisiä CERT-EU:n tuen kannalta***. Pyynnön kohteena olevan ***toimielimen, elimen tai viraston*** on toimitettava pyydetyt tiedot ja niihin myöhemmin tehtävät muutokset ilman aiheetonta viivytystä.	1. Jotta CERT-EU ***voi suorittaa 12 artiklassa määritellyn toimeksiantonsa ja tehtävänsä***, se voi pyytää unionin toimielimiä, elimiä ja virastoja toimittamaan sille tietoa niiden ***tieto- ja viestintäteknisiin*** järjestelmiin liittyvistä selvityksistä, ***mukaan lukien tiedot kyberuhkista, läheltä piti -tilanteista, haavoittuvuuksista, vaarantumista kuvaavista indikaattoreista, kyberturvallisuushälytyksistä ja suosituksista,*** jotka ***koskevat kyberpoikkeamien havaitsemiseen käytettävien kyberturvallisuusvälineiden konfigurointia***. Pyynnön kohteena olevan ***yksikön*** on toimitettava pyydetyt tiedot ja niihin myöhemmin tehtävät muutokset ilman aiheetonta viivytystä.

Tarkistus 63

Ehdotus asetukseksi
19 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. Unionin toimielimet, elimet ja	*(Tarkistus ei vaikuta suomenkieliseen*

virastot toimittavat CERT-EU:n pyynnöstä ja ilman aiheetonta viivytystä digitaaliset tiedot, jotka niitä koskevissa poikkeamissa osallisina olleiden elektroniikkalaitteiden käyttö on luonut. CERT-EU voi selventää, minkä tyyppistä tällaista digitaalista tietoa se tarvitsee tilannekuvan muodostamista ja poikkeamiin reagoimista varten.	*versioon.)*

Tarkistus 64
Ehdotus asetukseksi
20 artikla – otsikko

Komission teksti	*Tarkistus*
Ilmoitusvelvoitteet	***Raportointivelvoitteet***

Tarkistus 65

Ehdotus asetukseksi
20 artikla – 1 kohta – 1 alakohta

Komission teksti	*Tarkistus*
Kaikki unionin toimielimet, elimet ja virastot antavat CERT-EU:lle ***ensimmäisen ilmoituksen*** merkittävistä kyberuhkista, haavoittuvuuksista ja poikkeamista ilman aiheetonta viivytystä ja joka tapauksessa viimeistään 24 tunnin kuluessa siitä, kun tällainen uhka, haavoittuvuus tai poikkeama on tullut niiden tietoon.	Kaikki unionin toimielimet, elimet ja virastot antavat CERT-EU:lle ***varhaisvaroituksen*** merkittävistä kyberuhkista, haavoittuvuuksista ja poikkeamista ilman aiheetonta viivytystä ja joka tapauksessa viimeistään 24 tunnin kuluessa siitä, kun tällainen uhka, haavoittuvuus tai poikkeama on tullut niiden tietoon. ***Varhaisvaroituksessa on tapauksen mukaan ilmoitettava, oletetaanko merkittävän poikkeaman johtuvan lainvastaisista tai vihamielisistä teoista ja voiko sillä olla rajatylittäviä vaikutuksia.***

Tarkistus 66

Ehdotus asetukseksi
20 artikla – 1 kohta – 2 alakohta

Komission teksti	*Tarkistus*
Unionin asianomainen toimielin, elin tai virasto voi asianmukaisesti perustelluissa tapauksissa ja CERT-EU:n suostumuksella poiketa ***edellisessä kohdassa säädetystä*** määräajasta.	Unionin asianomainen toimielin, elin tai virasto voi asianmukaisesti perustelluissa tapauksissa ja CERT-EU:n suostumuksella poiketa ***tästä*** määräajasta.

Tarkistus 67

Ehdotus asetukseksi
20 artikla – 2 kohta – johdantokappale

Komission teksti	*Tarkistus*
2. Unionin toimielimet, elimet ja virastot ***ilmoittavat*** lisäksi CERT-EU:lle ilman aiheetonta viivytystä kyberuhkien, haavoittuvuuksien ja poikkeamien asianmukaiset tekniset tiedot, jotka mahdollistavat ongelmien havaitsemisen ennakolta, poikkeamiin reagoimisen tai lieventävien toimenpiteiden toteuttamisen. Ilmoituksen on sisällettävä seuraavat tiedot, jos ne ovat saatavilla:	2. Unionin toimielimet, elimet ja virastot ***lähettävät*** lisäksi ***ilmoituksen*** CERT-EU:lle ilman aiheetonta viivytystä ***ja joka tapauksessa 72 tunnin kuluessa siitä, kun merkittävä poikkeama on tullut niiden tietoon, päivittävät varhaisvaroituksen ja antavat merkittävästä poikkeamasta, sen vakavuudesta ja vaikutuksesta ensimmäisen arvion mukaan lukien*** kyberuhkien, haavoittuvuuksien ja poikkeamien asianmukaiset tekniset tiedot, jotka mahdollistavat ongelmien havaitsemisen ennakolta, poikkeamiin reagoimisen tai lieventävien toimenpiteiden toteuttamisen. Ilmoituksen on sisällettävä seuraavat tiedot, jos ne ovat saatavilla:

Tarkistus 68
Ehdotus asetukseksi
20 artikla – 2 kohta – 1 a alakohta (uusi)

Komission teksti	*Tarkistus*
	Unionin asianomainen toimielin, elin tai virasto voi asianmukaisesti perustelluissa tapauksissa ja CERT-EU:n suostumuksella poiketa tästä määräajasta.

Tarkistus 69

Ehdotus asetukseksi
20 artikla – 2 a kohta (uusi)

Komission teksti	*Tarkistus*
	2 a. Unionin toimielimet, elimet ja virastot toimittavat CERT-EU:lle viimeistään kuukauden kuluttua merkittävää poikkeamaa koskevasta ilmoituksesta loppuraportin, joka sisältää vähintään seuraavat tiedot:
	a) yksityiskohtainen kuvaus merkittävästä poikkeamasta, sen vakavuudesta ja vaikutuksista;
	b) merkittävän poikkeaman todennäköisesti aiheuttaneen uhan tai perimmäisen syyn tyyppi;
	c) toteutetut ja meneillään olevat toimenpiteet vaikutusten lieventämiseksi;
	d) soveltuvissa tapauksessa merkittävän poikkeaman rajatylittävät vaikutukset.
	Jos merkittävä poikkeama on edelleen meneillään ensimmäisessä alakohdassa tarkoitetun loppuraportin toimittamishetkellä, kyseisenä ajankohtana on toimitettava edistymisraportti ja kuukauden kuluessa loppuraportti.

Tarkistus 70

Ehdotus asetukseksi
20 artikla – 2 b kohta (uusi)

Komission teksti	*Tarkistus*
	2 b. Unionin asianomainen toimielin, elin tai virasto voi asianmukaisesti perustelluissa tapauksissa ja CERT-EU:n suostumuksella poiketa 2 a kohdassa säädetystä määräajasta.

Tarkistus 71

Ehdotus asetukseksi
20 artikla – 3 kohta

Komission teksti	*Tarkistus*
3. CERT-EU toimittaa Euroopan unionin kyberturvallisuusvirastolle kuukausittain tiivistelmän, joka sisältää anonymisoidut koontitiedot merkittävistä kyberuhkista, haavoittuvuuksista ja poikkeamista, joista on ilmoitettu 1 kohdan mukaisesti.	3. CERT-EU toimittaa Euroopan unionin kyberturvallisuusvirastolle kuukausittain tiivistelmän, joka sisältää anonymisoidut koontitiedot merkittävistä kyberuhkista, haavoittuvuuksista ja poikkeamista, joista on ilmoitettu 1 kohdan mukaisesti. ***Tiivistelmä sisällytetään kahden vuoden välein julkaistavaan kertomukseen kyberturvallisuuden tilasta unionissa direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 18 artiklan mukaisesti.***

Tarkistus 72

Ehdotus asetukseksi
20 artikla – 4 kohta

Komission teksti	*Tarkistus*
4. IICB ***voi*** antaa ohjeasiakirjoja tai suosituksia ilmoitusta koskevista säännöistä ja sen sisällöstä. CERT-EU levittää asianmukaiset tekniset tiedot, jotta unionin toimielimet, elimet ja virastot voivat havaita ongelmat ennakolta, reagoida poikkeamiin tai toteuttaa lieventäviä toimenpiteitä.	4. IICB antaa ohjeasiakirjoja tai suosituksia ilmoitusta koskevista säännöistä ja sen sisällöstä. CERT-EU levittää asianmukaiset tekniset tiedot, jotta unionin toimielimet, elimet ja virastot voivat havaita ongelmat ennakolta, reagoida poikkeamiin tai toteuttaa lieventäviä toimenpiteitä.

Tarkistus 73

Ehdotus asetukseksi
20 artikla – 5 kohta

Komission teksti	*Tarkistus*
5. Ilmoitusvelvoitteet eivät koske EU:n turvallisuusluokiteltuja tietoja	***Poistetaan.***

eivätkä tietoja, jotka unionin toimielin, elin tai virasto on saanut jäsenvaltion turvallisuus- tai tiedustelupalvelulta tai lainvalvontaviranomaiselta nimenomaisesti sillä ehdolla, ettei tietoja jaeta CERT-EU:n kanssa.

Tarkistus 74

Ehdotus asetukseksi
24 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. Komissio antaa Euroopan parlamentille ja neuvostolle kertomuksen tämän asetuksen täytäntöönpanosta viimeistään ***48*** kuukauden kuluttua tämän asetuksen voimaantulosta ja sen jälkeen ***kolmen*** vuoden välein.	2. Komissio antaa Euroopan parlamentille ja neuvostolle kertomuksen tämän asetuksen täytäntöönpanosta viimeistään ***36*** kuukauden kuluttua tämän asetuksen voimaantulosta ja sen jälkeen ***kahden*** vuoden välein.

Tarkistus 75

Ehdotus asetukseksi
24 artikla – 3 kohta

Komission teksti	*Tarkistus*
3. Komissio arvioi tämän asetuksen toimivuutta ja antaa siitä kertomuksen Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle aikaisintaan ***viiden*** vuoden kuluttua asetuksen voimaantulopäivästä.	3. Komissio arvioi tämän asetuksen toimivuutta ja antaa siitä kertomuksen Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle aikaisintaan ***kolmen*** vuoden kuluttua asetuksen voimaantulopäivästä***, koska kyberuhkaympäristö kehittyy nopeasti***.

Tarkistus 76

Ehdotus asetukseksi
Liite I – 1 kohta – johdantokappale

Komission teksti	*Tarkistus*
Kyberturvallisuuden perustasossa otetaan	Kyberturvallisuuden perustasossa otetaan

huomioon seuraavat osa-alueet:	huomioon ***vähintään*** seuraavat osa-alueet:

Tarkistus 77

Ehdotus asetukseksi
Liite I – 1 kohta – 1 a alakohta (uusi)

Komission teksti	*Tarkistus*
	1 a) henkilöstön kyberturvallisuuskoulutus;

Tarkistus 78

Ehdotus asetukseksi
Liite I – 1 kohta – 3 alakohta

Komission teksti	*Tarkistus*
3) resurssien hallinta, mukaan lukien ***tietoteknisten resurssien*** inventointi ja ***tietoverkkojen*** kartoitus;	3) resurssien ***hankinta ja*** hallinta, mukaan lukien ***tieto- ja viestintäteknisten resurssien*** inventointi ja ***tieto- ja viestintäverkkojen*** kartoitus;

Tarkistus 79

Ehdotus asetukseksi
Liite I – 1 kohta – 7 alakohta

Komission teksti	*Tarkistus*
7) järjestelmien hankinta, kehittäminen ja ylläpito;	7) järjestelmien hankinta, kehittäminen ja ylläpito***, mukaan lukien sisäisten avoimen lähdekoodin ohjelmistojen kehittäminen***;

Tarkistus 80

Ehdotus asetukseksi
Liite I – 1 kohta – 7 a alakohta (uusi)

Komission teksti	*Tarkistus*
	7 a) kyberturvallisuustarkastukset;

Tarkistus 81

Ehdotus asetukseksi
Liite I – 1 kohta – 9 alakohta

Komission teksti	*Tarkistus*
9) poikkeamien hallinta, mukaan lukien toimintamallit, joilla parannetaan poikkeamiin varautumista ja reagoimista ja niistä toipumista sekä yhteistyötä CERT-EU:n kanssa, kuten turvallisuuden seurannan ja kirjaamisen ylläpito;	9) poikkeamien hallinta, mukaan lukien toimintamallit, joilla parannetaan poikkeamiin varautumista ja reagoimista ja niistä toipumista***, raportointivelvoitteiden noudattamista ja raportoinnin nopeuttamista*** sekä yhteistyötä CERT-EU:n kanssa, kuten turvallisuuden seurannan ja kirjaamisen ylläpito;

Tarkistus 82

Ehdotus asetukseksi
Liite II – 1 kohta – 3 a alakohta (uusi)

Komission teksti	*Tarkistus*
	3 a) henkilöstön säännöllinen kyberturvallisuuskoulutus;

Tarkistus 83

Ehdotus asetukseksi
Liite II – 1 kohta – 4 alakohta – a alakohta

Komission teksti	*Tarkistus*
a) sellaisten sopimuksista johtuvien esteiden poistaminen, jotka rajoittavat ***tietotekniikan palveluntarjoajien*** mahdollisuuksia jakaa tietoja poikkeamista, haavoittuvuuksista ja kyberuhkista CERT-EU:n kanssa;	a) sellaisten sopimuksista johtuvien esteiden poistaminen, jotka rajoittavat ***tieto- ja viestintäteknisten palvelujen tarjoajien*** mahdollisuuksia jakaa tietoja poikkeamista, haavoittuvuuksista ja kyberuhkista CERT-EU:n kanssa;

ASIAN KÄSITTELY
LAUSUNNON ANTAVASSA VALIOKUNNASSA

Otsikko	Toimenpiteet yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa
Viiteasiakirjat	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Asiasta vastaava valiokunta Ilmoitettu istunnossa (pvä)	ITRE 4.4.2022
Lausunnon antanut valiokunta Ilmoitettu istunnossa (pvä)	AFCO 4.4.2022
Valmistelija Nimitetty (pvä)	Markéta Gregorová 20.6.2022
Valiokuntakäsittely	26.10.2022 1.12.2022
Hyväksytty (pvä)	25.1.2023
Lopullisen äänestyksen tulos	+: 24 –: 0 0: 0
Lopullisessa äänestyksessä läsnä olleet jäsenet	Gerolf Annemans, Gabriele Bischoff, Damian Boeselager, Gwendoline Delbos-Corfield, Salvatore De Meo, Daniel Freund, Charles Goerens, Esteban González Pons, Laura Huhtasaari, Victor Negrescu, Max Orville, Domènec Ruiz Devesa, Helmut Scholz, Pedro Silva Pereira, Sven Simon, Guy Verhofstadt, Loránt Vincze, Rainer Wieland
Lopullisessa äänestyksessä läsnä olleet varajäsenet	Nathalie Colin-Oesterlé, Pascal Durand, Seán Kelly, Jaak Madison, Maite Pagazaurtundúa
Lopullisessa äänestyksessä läsnä olleet sijaiset (209 art. 7 kohta)	Leszek Miller

LOPULLINEN ÄÄNESTYS NIMENHUUTOÄÄNESTYKSENÄ LAUSUNNON ANTAVASSA VALIOKUNNASSA

24	+
ID	Gerolf Annemans, Laura Huhtasaari, Jaak Madison
PPE	Nathalie Colin-Oesterlé, Salvatore De Meo, Esteban González Pons, Seán Kelly, Sven Simon, Loránt Vincze, Rainer Wieland
Renew	Charles Goerens, Max Orville, Maite Pagazaurtundúa, Guy Verhofstadt
S&D	Gabriele Bischoff, Pascal Durand, Leszek Miller, Victor Negrescu, Domènec Ruiz Devesa, Pedro Silva Pereira
The Left	Helmut Scholz
Verts/ALE	Damian Boeselager, Gwendoline Delbos-Corfield, Daniel Freund

0	-

0	0

Symbolien selitys:
+ : puolesta
- : vastaan
0 : tyhjää