

TARKISTUKSET 001-257

esittäjä(t): Teollisuus-, tutkimus- ja energiavaliokunta

Mietintö**Angelika Niebler**

EU:n kyberturvallisuusasetus

A8-0264/2018

Ehdotus asetukseksi (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

Tarkistus 1**Ehdotus asetukseksi
Johdanto-osan 1 kappale***Komission teksti*

(1) Verkko- ja tietojärjestelmillä ja televiestintäverkoilla ja -palveluilla on yhteiskunnassa elintärkeä rooli, ja niistä on tullut talouskasvun selkäranka. Tieto- ja viestintäteknikka luo pohjaa monimutkaisille järjestelmille, jotka tukevat yhteiskunnan toimintoja, pitävät talouden pyörät pyörimässä keskeisillä aloilla, kuten terveydenhuollossa, energia-alalla, rahoitusalailla ja liikenteessä, ja erityisesti tukevat sisämarkkinoiden toimintaa

Tarkistus

(1) Verkko- ja tietojärjestelmillä ja televiestintäverkoilla ja -palveluilla on yhteiskunnassa elintärkeä rooli, ja niistä on tullut talouskasvun selkäranka. Tieto- ja viestintäteknikka luo pohjaa monimutkaisille järjestelmille, jotka tukevat yhteiskunnan **päivittäisiä** toimintoja, pitävät talouden pyörät pyörimässä keskeisillä aloilla, kuten terveydenhuollossa, energia-alalla, rahoitusalailla ja liikenteessä, ja erityisesti tukevat sisämarkkinoiden toimintaa.

Tarkistus 2**Ehdotus asetukseksi
Johdanto-osan 2 kappale***Komission teksti*

(2) Verkko- ja tietojärjestelmien käyttö on nykyisin laajalla levinnyttä kansalaisten,

Tarkistus

(2) Verkko- ja tietojärjestelmien käyttö on nykyisin laajalla levinnyttä kansalaisten,

yrittäjien ja julkishallinnon piirissä kaikkialla unionissa. Digitoinnista ja verkkoyhteyksistä on tulossa keskeisiä ominaisuuksia yhä useammassa tuotteissa ja palveluissa, ja esineiden internetin myötä EU:ssa ennakoitaan otettavan käyttöön miljoonia, ellei miljardeja, verkkoon kytkettyjä digitaalisia laitteita seuraavan vuosikymmenen aikana. Yhä useammat laitteet liitetään internetiin huolehtimatta samalla siitä, että turvallisuus ja resilienssi ovat riittävällä tavalla sisäänrakennettuja, mikä johtaa puutteisiin kyberturvallisuudessa. Sertifioinnin vähäinen käyttö johtaa tässä yhteydessä siihen, että organisaatiot ja yksittäiset käyttäjät eivät saa riittävästi tietoa tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuusominaisuuksista, mikä heikentää luottamusta digitaalisiin ratkaisuihin.

yrittäjien ja julkishallinnon piirissä kaikkialla unionissa. Digitoinnista ja verkkoyhteyksistä on tulossa keskeisiä ominaisuuksia yhä useammassa tuotteissa ja palveluissa, ja esineiden internetin myötä EU:ssa ennakoitaan otettavan käyttöön miljoonia, ellei miljardeja, verkkoon kytkettyjä digitaalisia laitteita seuraavan vuosikymmenen aikana. Yhä useammat laitteet liitetään internetiin huolehtimatta samalla siitä, että turvallisuus ja resilienssi ovat riittävällä tavalla sisäänrakennettuja, mikä johtaa puutteisiin kyberturvallisuudessa. Sertifioinnin vähäinen käyttö johtaa tässä yhteydessä siihen, että organisaatiot ja yksittäiset käyttäjät eivät saa riittävästi tietoa tieto- ja viestintätekniikan tuotteiden, prosessien ja palvelujen kyberturvallisuusominaisuuksista, mikä heikentää luottamusta digitaalisiin ratkaisuihin. ***Juuri nämä asiat ovat keskeisiä Euroopan komission uudistusohjelmassa, jolla pyritään saamaan aikaan digitaaliset sisämarkkinat, sillä tieto- ja viestintätekniikan verkot muodostavat rungon digitaalisille tuotteille ja palveluille, joilla voidaan tukea kaikkia elämänaloja ja edistää talouskasvua Euroopassa. Jotta varmistetaan, että digitaalisten sisämarkkinoiden tavoitteet saavutetaan kaikilta osin, on huolehdittava siitä, että käytössä on välttämättömät teknologiset rakenneosat, joista ovat riippuvaisia sellaiset tärkeät alat kuin sähköiset terveyspalvelut, esineiden internet, tekoäly, kvanttitekniikka sekä älykkäät liikennejärjestelmät ja kehittyneet valmistus.***

Tarkistus 3

Ehdotus asetukseksi Johdanto-osan 3 kappale

Komission teksti

(3) Digitalisoinnin ja verkkoyhteyksien

Tarkistus

(3) Digitalisoinnin ja verkkoyhteyksien

yleistyminen lisää kyberturvallisuuteen liittyviä riskejä, jolloin koko yhteiskunta on haavoittuvampi kyberuhkille, ja pahentaa yksilöihin, myös heikommassa asemassa oleviin henkilöihin, kuten lapsiin, kohdistuvia vaaroja. Tämän yhteiskuntaan kohdistuvan riskin lieventämiseksi kyberturvallisuutta on tarpeen parantaa EU:ssa kaikin tarvittavin toimenpitein, jotta kansalaisten, hallintojen ja yritysten – pk-yrityksistä elintärkeiden infrastruktuureiden ylläpitäjiin – käyttämät verkko- ja tietojärjestelmät, televiestintäverkot, digitaaliset tuotteet, palvelut ja laitteet voidaan suojata paremmin kyberuhilta.

yleistyminen lisää kyberturvallisuuteen liittyviä riskejä, jolloin koko yhteiskunta on haavoittuvampi kyberuhkille, ja pahentaa yksilöihin, myös heikommassa asemassa oleviin henkilöihin, kuten lapsiin, kohdistuvia vaaroja. Tämän yhteiskuntaan kohdistuvan riskin lieventämiseksi kyberturvallisuutta on tarpeen parantaa EU:ssa kaikin tarvittavin toimenpitein, jotta kansalaisten, hallintojen ja yritysten – pk-yrityksistä elintärkeiden infrastruktuureiden ylläpitäjiin – käyttämät verkko- ja tietojärjestelmät, televiestintäverkot, digitaaliset tuotteet, palvelut ja laitteet voidaan suojata paremmin kyberuhilta. **Näin ollen**

Euroopan komission

17 päivänä tammikuuta 2018 julkaisema digitaalisen koulutuksen

toimintasuunnitelma, erityisesti

opettajille, oppilaiden vanhemmille ja

oppijoille kohdennettu EU:n laajuinen

tiedotuskampanja verkkoturvallisuuden,

kyberhygienian ja medialukutaidon

edistämiseksi sekä

kyberturvallisuusopetusta koskeva aloite,

joka pohjautuu kansalaisille tarkoitettuun

eurooppalaiseen digitaalisten taitojen

puitekehukseen, jonka tarkoituksena on

auttaa ihmisiä käyttämään teknologiaa

luottavaisin mielin ja vastuullisesti, on

askel oikeaan suuntaan.

Tarkistus 4

Ehdotus asetukseksi

Johdanto-osan 3 a kappale (uusi)

Komission teksti

Tarkistus

(3 a) ENISAn tavoitteita ja tehtäviä olisi

yhdenmukaistettava edelleen yhteisen

tiedonannon kanssa siltä osin kuin on

kyse kyberhygienian ja tietoisuuden

edistämisestä. Kyberresilienssi voidaan

saavuttaa panemalla täytäntöön

kyberhygienian peruseriaatteen.

Tarkistus 5

**Ehdotus asetukseksi
Johdanto-osan 3 b kappale (uusi)**

Komission teksti

Tarkistus

(3 b) ENISAn olisi annettava enemmän tietoon perustuvaa ja käytännön tukea unionin kyberturvallisuusosalalle, erityisesti pk- ja startup-yrityksille, jotka ovat tärkeitä innovatiivisten ratkaisujen kehittäjiä kyberpuolustusosalalla, ja edistettävä tiiviimpää yhteistyötä yliopistojen tutkimuslaitosten ja suurten toimijoiden kanssa, jotta voidaan vähentää riippuvuutta ulkoisista lähteistä peräisin olevista kyberturvallisuustuotteista ja luoda strateginen toimitusketju unionin sisälle.

Tarkistus 6

**Ehdotus asetukseksi
Johdanto-osan 4 kappale**

Komission teksti

Tarkistus

(4) Kyberhyökkäyksiä tapahtuu yhä enemmän, ja verkottunut talous ja yhteiskunta, jotka ovat alttiimpia kyberuhille ja -hyökkäyksille, edellyttävät vahvempaa puolustusvalmiutta. Vaikka kyberhyökkäykset ovat usein rajatylittäviä, kyberturvallisuusviranomaisten poliittiset vastatoimet ja lainvalvontavaltuudet ovat enimmäkseen kansallisia. Laajamittaiset kyberturvallisuuspoikkeamat voivat häiritä keskeisten palvelujen tarjoamista koko EU:ssa. Tämä edellyttää tehokasta EU-tason reagointia ja kriisinhallintaa, jossa nojaututaan kohdennettuihin politiikkoihin ja laaja-alaisempiin eurooppalaisen yhteisvastuun ja keskinäisen avunannon välineisiin. Poliitiikan laatijoille, toimialalle ja käyttäjille on tärkeää, että kyberturvallisuuden ja resilienssin tilaa unionissa arvioidaan säännöllisesti luotettavan unionin tiedon pohjalta ja että laaditaan järjestelmällisesti ennusteita tulevista kehityskuluista, haasteista ja uhkista sekä unionin tasolla että

(4) Kyberhyökkäyksiä tapahtuu yhä enemmän, ja verkottunut talous ja yhteiskunta, jotka ovat alttiimpia kyberuhille ja -hyökkäyksille, edellyttävät vahvempaa **ja turvatumpaa** puolustusvalmiutta. Vaikka kyberhyökkäykset ovat usein rajatylittäviä, kyberturvallisuusviranomaisten poliittiset vastatoimet ja lainvalvontavaltuudet ovat enimmäkseen kansallisia. Laajamittaiset kyberturvallisuuspoikkeamat voivat häiritä keskeisten palvelujen tarjoamista koko EU:ssa. Tämä edellyttää tehokasta EU-tason reagointia ja kriisinhallintaa, jossa nojaututaan kohdennettuihin politiikkoihin ja laaja-alaisempiin eurooppalaisen yhteisvastuun ja keskinäisen avunannon välineisiin. **Kyberpuolustusalan koulutustarpeet ovat suuret ja lisääntyvät koko ajan, ja niihin vastataan tehokkaimmin unionin tason yhteistoiminnalla.** Poliitiikan laatijoille, toimialalle ja käyttäjille on tärkeää, että kyberturvallisuuden ja resilienssin tilaa

maailmanlaajuisesti.

unionissa arvioidaan säännöllisesti luotettavan unionin tiedon pohjalta ja että laaditaan järjestelmällisesti ennusteita tulevista kehityskuluista, haasteista ja uhkista sekä unionin tasolla että maailmanlaajuisesti.

Tarkistus 7

Ehdotus asetukseksi Johdanto-osan 5 kappale

Komission teksti

(5) Unioniin kohdistuvien kyberturvallisuushaasteiden lisääntymisen vuoksi tarvitaan kattava joukko toimenpiteitä, jotka pohjautuvat aiempaan unionin toimintaan ja edistävät toisiaan vahvistavia tavoitteita. Tähän sisältyy tarve lisätä jäsenvaltioiden ja yritysten valmiuksia ja varautumiskykyä sekä parantaa yhteistyötä ja koordinoitua jäsenvaltioiden ja EU:n toimielinten, virastojen ja elinten välillä. Koska kyberuhkat ovat luonteeltaan rajattomia, on myös tarpeen lisätä valmiuksia unionin tasolla jäsenvaltioiden toimien täydentämiseksi erityisesti laajamittaisten rajatylittävien kyberturvallisuuspoikkeamien ja -kriisien tapauksessa. Tarvitaan myös lisätoimia kansalaisten ja yritysten tietoisuuden lisäämiseksi kyberturvallisuuteen liittyvistä kysymyksistä. **Lisäksi** digitaalisiin sisämarkkinoihin tunnettua luottamusta olisi edelleen parannettava tarjoamalla avointa tietoa tieto- ja viestintätekniikan tuotteiden ja palvelujen turvallisuustasosta. Tätä voidaan helpottaa EU:n laajuisella sertifiointilla, joka tuo käyttöön yhteiset kyberturvallisuusvaatimukset ja arviointiperusteet kansallisille markkinoille ja sektoreille.

Tarkistus

(5) Unioniin kohdistuvien kyberturvallisuushaasteiden lisääntymisen vuoksi tarvitaan kattava joukko toimenpiteitä, jotka pohjautuvat aiempaan unionin toimintaan ja edistävät toisiaan vahvistavia tavoitteita. Tähän sisältyy tarve lisätä jäsenvaltioiden ja yritysten valmiuksia ja varautumiskykyä sekä parantaa yhteistyötä, koordinoitua ja **tiedon jakamista** jäsenvaltioiden ja EU:n toimielinten, virastojen ja elinten välillä. Koska kyberuhkat ovat luonteeltaan rajattomia, on myös tarpeen lisätä valmiuksia unionin tasolla jäsenvaltioiden toimien täydentämiseksi erityisesti laajamittaisten rajatylittävien kyberturvallisuuspoikkeamien ja -kriisien tapauksessa **ja samalla korostaa, että on tärkeää ylläpitää ja vahvistaa edelleen kansallisia valmiuksia vastata kaikenkokoisiin kyberuhkiin**. Tarvitaan myös lisätoimia **koordinoidun EU:n tason vastatoimen toteuttamiseksi** sekä kansalaisten ja yritysten tietoisuuden lisäämiseksi kyberturvallisuuteen liittyvistä kysymyksistä. **Koska kyberpoikkeamat lisäksi vähentävät digitaalisten palveluiden tarjoajiin ja digitaalisiin sisämarkkinoihin tunnettua luottamusta etenkin kuluttajien keskuudessa, luottamusta** olisi edelleen parannettava tarjoamalla avointa tietoa tieto- ja viestintätekniikan tuotteiden, **prosessien ja palvelujen turvallisuustasosta painottamalla, että korkeatasoinen**

kyberturvallisuuden sertifiointi ei voi taata, että tieto- ja viestintätekniikan tuote tai palvelu olisi täysin turvallinen. Tätä voidaan helpottaa EU:n laajuisella sertifioinnilla, joka tuo käyttöön yhteiset kyberturvallisuusvaatimukset ja arviointiperusteet kansallisille markkinoille ja sektoreille, sekä edistämällä kyberlukutaitoa unionin laajuisen sertifiointin ohella, ja koska esineiden internetin laitteita on yhä enemmän saatavilla, yksityissektorin olisi toteutettava monia vapaaehtoisia toimenpiteitä, kuten salausta ja lohkoketjuteknologiaa, vahvistaakseen luottamusta tieto- ja viestintätekniikan tuotteiden, prosessien ja palveluiden turvallisuuteen. Kohdatut haasteet olisi otettava oikeasuhteisesti huomioon virastolle osoitetuissa määrärahoissa, jotta varmistetaan optimaalinen toimintakyky nykyisissä olosuhteissa.

Tarkistus 8

Ehdotus asetukseksi Johdanto-osan 5 a kappale (uusi)

Komission teksti

Tarkistus

(5 a) Euroopan turvallisuuden ja kyberpuolustuksen rakenteiden vahvistamiseksi on tärkeää ylläpitää ja kehittää jäsenvaltioiden valmiuksia vastata kattavasti kyberuhkiin, myös rajat ylittävien poikkeamien tapauksessa. Viraston harjoittama EU:n tason koordinointi ei saisi johtaa jäsenvaltioiden valmiuksien tai toimien vähenemiseen.

Tarkistus 9

Ehdotus asetukseksi Johdanto-osan 5 b kappale (uusi)

Komission teksti

Tarkistus

(5 b) Yrityksillä ja yksittäisillä kuluttajilla olisi oltava tarkat tiedot tieto- ja

viestintätekniiikan tuotteidensa turvallisuustasosta. Samalla on ymmärrettävä, että mikään tuote ei ole kyberturvallinen ja että kyberhygienian perussääntöjä olisi edistettävä ja ne olisi asetettava etusijalle.

Tarkistus 10

Ehdotus asetukseksi Johdanto-osan 7 kappale

Komission teksti

(7) Unioni on jo toteuttanut merkittäviä toimia kyberturvallisuuden varmistamiseksi ja luottamuksen lisäämiseksi digitaalitekniologioihin. Vuonna 2013 hyväksyttiin EU:n kyberturvallisuusstrategia ohjaamaan unionin poliittisia vastatoimia kyberturvallisuushyönteihin ja -riskeihin. Tarjotakseen eurooppalaisille paremman suojan verkkoympäristössä unioni hyväksyi vuonna 2016 ensimmäisenä kyberturvallisuusalan säädöksenä direktiivin (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa, jäljempänä 'verkko- ja tietoturvadirektiivi'. Verkko- ja **tietoturvadirektiivillä otettiin** käyttöön vaatimukset kansallisista valmiuksista kyberturvallisuuden alalla, ensimmäiset mekanismit jäsenvaltioiden strategisen ja operatiivisen yhteistyön tehostamiseksi sekä velvoitteet toteuttaa turvallisuustoimenpiteitä ja tehdä ilmoitukset poikkeamista talouden ja yhteiskunnan kannalta olennaisilla aloilla, kuten energia, liikenne, vesihuolto, pankkitoiminta, rahoitusmarkkinoiden infrastruktuurit, terveydenhuolto ja digitaalinen infrastruktuuri sekä keskeisten digitaalisten palvelujen (hakukoneet, pilvipalvelut ja verkossa toimivat markkinapaikat) tarjoajat. ENISAlle annettiin keskeinen rooli tukea direktiivin täytäntöönpanoa. Lisäksi kyberrikollisuuden tehokas torjunta on

Tarkistus

(7) Unioni on jo toteuttanut merkittäviä toimia kyberturvallisuuden varmistamiseksi ja luottamuksen lisäämiseksi digitaalitekniologioihin. Vuonna 2013 hyväksyttiin EU:n kyberturvallisuusstrategia ohjaamaan unionin poliittisia vastatoimia kyberturvallisuushyönteihin ja -riskeihin. Tarjotakseen eurooppalaisille paremman suojan verkkoympäristössä unioni hyväksyi vuonna 2016 ensimmäisenä kyberturvallisuusalan säädöksenä direktiivin (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa, jäljempänä 'verkko- ja tietoturvadirektiivi'. Verkko- ja **tietoturvadirektiivi, jonka onnistuminen riippuu suuresti täytäntöönpanon tehokkuudesta jäsenvaltioissa, joka on digitaalisten sisämarkkinoiden strategian mukainen ja jolla yhdessä muiden välineiden, kuten eurooppalaisesta sähköisen viestinnän säännöstöstä annetun direktiivin, asetuksen (EU) 2016/679 ja direktiivin 2002/58/EY, kanssa otetaan** käyttöön vaatimukset kansallisista valmiuksista kyberturvallisuuden alalla, ensimmäiset mekanismit jäsenvaltioiden strategisen ja operatiivisen yhteistyön tehostamiseksi sekä velvoitteet toteuttaa turvallisuustoimenpiteitä ja tehdä ilmoitukset poikkeamista talouden ja yhteiskunnan kannalta olennaisilla aloilla, kuten energia, liikenne, vesihuolto,

tärkeä prioriteetti Euroopan turvallisuusagendassa, joka tältä osin edistää yleistä tavoitetta saavuttaa kyberturvallisuuden korkea taso.

pankkitoiminta, rahoitusmarkkinoiden infrastruktuurit, terveydenhuolto ja digitaalinen infrastruktuuri sekä keskeisten digitaalisten palvelujen (hakukoneet, pilvipalvelut ja verkossa toimivat markkinapaikat) tarjoajat. ENISAlle annettiin keskeinen rooli tukea direktiivin täytäntöönpanoa. Lisäksi kyberrikollisuuden tehokas torjunta on tärkeä prioriteetti Euroopan turvallisuusagendassa, joka tältä osin edistää yleistä tavoitetta saavuttaa kyberturvallisuuden korkea taso.

Tarkistus 11

Ehdotus asetukseksi Johdanto-osan 8 kappale

Komission teksti

(8) Yleisesti tunnustetaan, että sen jälkeen, kun EU:n kyberturvallisuusstrategia hyväksyttiin vuonna 2013 ja viraston toimeksiantoa viimeksi tarkistettiin, yleinen poliittinen tilanne on muuttunut merkittävästi, myös epävarmemman ja vähemmän turvatus globaalien toimintaympäristön vuoksi. Tässä yhteydessä ja osana uutta unionin kyberturvallisuuspolitiikkaa on tarpeen tarkistaa ENISAn toimeksiantoa, jotta voidaan määritellä sen rooli muuttuneessa kyberturvallisuuden toimintaympäristössä ja varmistaa, että se auttaa tehokkaasti unionia vastaamaan tästä perusteellisesti muuttuneesta uhkaympäristöstä johtuviin kyberturvallisuushaasteisiin. Kuten viraston arvioinnissa todetaan, sen nykyinen toimeksianto ei ole riittävä näiden haasteiden kannalta.

Tarkistus

(8) Yleisesti tunnustetaan, että sen jälkeen, kun EU:n kyberturvallisuusstrategia hyväksyttiin vuonna 2013 ja viraston toimeksiantoa viimeksi tarkistettiin, yleinen poliittinen tilanne on muuttunut merkittävästi, myös epävarmemman ja vähemmän turvatus globaalien toimintaympäristön vuoksi. Tässä yhteydessä ja ***ottaen huomioon viraston vuosia jatkuneen myönteisen roolin asiantuntemuksen, koordinoinnin ja valmiuksien kehittämisen keskittämisessä, ja*** osana uutta unionin kyberturvallisuuspolitiikkaa on tarpeen tarkistaa ENISAn toimeksiantoa, jotta voidaan määritellä sen rooli muuttuneessa kyberturvallisuuden toimintaympäristössä ja varmistaa, että se auttaa tehokkaasti unionia vastaamaan tästä perusteellisesti muuttuneesta uhkaympäristöstä johtuviin kyberturvallisuushaasteisiin. Kuten viraston arvioinnissa todetaan, sen nykyinen toimeksianto ei ole riittävä näiden haasteiden kannalta.

Tarkistus 12

Ehdotus asetukseksi

Johdanto-osan 11 kappale

Komission teksti

(11) Unioniin kohdistuvien **kyberturvallisuushaasteiden** lisääntyessä viraston määrärahoja ja henkilöresursseja olisi lisättävä siten, että ne vastaavat sen uutta roolia ja tehtäviä sekä sen keskeistä asemaa eurooppalaista digitaalista toimintaympäristöä puolustavassa organisaatioiden ekosysteemissä.

Tarkistus

(11) Unioniin kohdistuvien **kyberturvallisuushkien ja -haasteiden** lisääntyessä viraston määrärahoja ja henkilöresursseja olisi lisättävä siten, että ne vastaavat sen uutta roolia ja tehtäviä sekä sen keskeistä asemaa eurooppalaista digitaalista toimintaympäristöä puolustavassa organisaatioiden ekosysteemissä, **mikä antaisi ENISAlle mahdollisuuden toteuttaa tehokkaasti sille tällä asetuksella annetut tehtävät.**

Tarkistus 13

Ehdotus asetukseksi Johdanto-osan 12 kappale

Komission teksti

(12) Viraston olisi kehitettävä ja ylläpidettävä korkealaatuista asiantuntemusta ja toimittava viitetahona, joka vahvistaa uskoa ja luottamusta sisämarkkinoihin riippumattomuutensa, antamansa neuvonnan ja levittämänsä tiedon laadun, menettelyjensä ja toimintatapojensa avoimuuden sekä tehtäviensä suorittamisessa osoittamansa huolellisuuden ansiosta. Viraston olisi aktiivisesti edistettävä kansallisia ja unionin toimia ja suoritettava tehtävänsä täydessä yhteistyössä unionin toimielinten, elinten, laitosten ja virastojen sekä jäsenvaltioiden kanssa. Lisäksi viraston olisi hyödynnettävä yksityisen sektorin ja muiden asiaankuuluvien sidosryhmien näkemyksiä ja niiden kanssa tehtävää yhteistyötä. **Viraston tehtävänannossa olisi vahvistettava, miten** viraston on määrä saavuttaa **tavoitteensa niin**, että **se pystyy toimimaan** joustavasti.

Tarkistus

(12) Viraston olisi kehitettävä ja ylläpidettävä korkealaatuista asiantuntemusta ja toimittava viitetahona, joka vahvistaa uskoa ja luottamusta sisämarkkinoihin riippumattomuutensa, antamansa neuvonnan ja levittämänsä tiedon laadun, menettelyjensä ja toimintatapojensa avoimuuden sekä tehtäviensä suorittamisessa osoittamansa huolellisuuden ansiosta. Viraston olisi aktiivisesti edistettävä kansallisia ja unionin toimia ja suoritettava tehtävänsä täydessä yhteistyössä unionin toimielinten, elinten, laitosten ja virastojen sekä jäsenvaltioiden kanssa, **vältettävä päällekkäistä työtä sekä edistettävä synergiaa ja täydentävyyttä ja siten huolehdittava koordinoitun toiminnan ja säästöjen aikaansaamisesta.** Lisäksi viraston olisi hyödynnettävä yksityisen ja **julkisen** sektorin ja muiden asiaankuuluvien sidosryhmien näkemyksiä ja niiden kanssa tehtävää yhteistyötä. **Selkeässä toimintasuunnitelmassa sekä tehtävissä ja tavoitteissa, jotka olisi määriteltävä selkeästi, olisi vahvistettava, miten** viraston on määrä saavuttaa

tavoitteensa niin, **että samalla otetaan asianmukaisesti huomioon**, että sen on toimittava tarvittaessa joustavasti. **Olisi pidettävä kiinni mahdollisimman korkeasta avoimuuden ja tietojen levittämisen tasosta silloin, kun se on mahdollista.**

Tarkistus 14

Ehdotus asetukseksi Johdanto-osan 12 a kappale (uusi)

Komission teksti

Tarkistus

(12 a) Viraston tehtäviä olisi arvioitava jatkuvasti ja tarkistettava oikea-aikaisesti, erityisesti sen koordinoititehtävää jäsenvaltioihin ja niiden kansallisiin viranomaisiin nähden, sekä mahdollisuutta toimia jäsenvaltioiden ja EU:n elinten ja toimielinten keskitettynä verkkoportaalina. Olisi arvioitava viraston tehtävää sisämarkkinoiden hajanaisuuden välttämiseksi sekä pakollisten kyberturvallisuuden sertifiointijärjestelmien mahdollisessa käyttöönotossa, mikäli tilanne tulevaisuudessa tällaista edellyttäisi, kuten myös viraston tehtävää EU:n markkinoille tulevien kolmansien maiden tuotteiden arvioinnissa sekä sellaisten yritysten, jotka eivät noudata EU:n vaatimuksia, mahdollisessa mustalle listalle asettamisessa.

Tarkistus 15

Ehdotus asetukseksi Johdanto-osan 12 b kappale (uusi)

Komission teksti

Tarkistus

(12 b) Jotta ENISA voisi tukea asianmukaisesti jäsenvaltioiden operatiivista yhteistyötä, sen olisi vahvistettava entisestään omia teknisiä

valmiuksiaan ja asiantuntemustaan. Siksi viraston olisi asteittain vahvistettava tätä tehtävää hoitavaa henkilöstöään, jotta se voisi kerätä ja analysoida itsenäisesti erityyppisiä ja monenlaisia kyberturvallisuusuhkia ja haittaohjelmia, tehdä rikosteknisiä analyyseja ja auttaa jäsenvaltioita vastaamaan laajamittaisiin turvallisuuspoikkeamiin. Jotta voidaan välttää mahdollisia päällekkäisyyksiä jäsenvaltioiden nykyisten valmiuksien kanssa, ENISAn olisi parannettava osaamistaan ja valmiuksiaan jäsenvaltioissa olevien resurssien pohjalta, erityisesti lähettämällä virastoon kansallisia asiantuntijoita, perustamalla asiantuntijapooleja, henkilöstön vaihto-ohjelmia jne. Viraston olisi tämän alan henkilöstöä valitessaan vaihteittain varmistettava, että he täyttävät asianmukaiset kriteerit riittävän tuen antamiseksi.

Tarkistus 16

Ehdotus asetukseksi Johdanto-osan 13 kappale

Komission teksti

(13) Viraston olisi avustettava komissiota antamalla neuvoja, lausuntoja ja analyysejä kaikista unionin asioista, jotka liittyvät kyberturvallisuusalan toimintapolitiikan ja lainsäädännön kehittämiseen, päivittämiseen ja uudelleentarkasteluun, mukaan lukien kriittisen infrastruktuurin suojaaminen ja kyberresilienssi. Viraston olisi toimittava neuvonnan ja asiantuntemuksen viitetahona unionin alakohtaisille toimintapoliittisille ja lainsäädännöllisille aloitteille, kun niihin liittyy kyberturvallisuuskysymyksiä.

Tarkistus

(13) Viraston olisi avustettava komissiota antamalla neuvoja, lausuntoja ja analyysejä kaikista unionin asioista, jotka liittyvät kyberturvallisuusalan toimintapolitiikan ja lainsäädännön kehittämiseen, päivittämiseen ja uudelleentarkasteluun, mukaan lukien kriittisen infrastruktuurin suojaaminen ja kyberresilienssi. Viraston olisi toimittava neuvonnan ja asiantuntemuksen viitetahona unionin alakohtaisille toimintapoliittisille ja lainsäädännöllisille aloitteille, kun niihin liittyy kyberturvallisuuskysymyksiä. ***Sen asiantuntemusta tarvitaan erityisesti, kun valmistellaan eurooppalaista kyberturvallisuuden sertifiointijärjestelmää koskevaa unionin monivuotista työohjelmaa. Viraston olisi toimitettava Euroopan parlamentille***

säännöllisesti kyberturvallisuusalan uutisia, analyysyjä ja tarkistuksia sekä kerrottava tehtäviensä edistymisestä.

Tarkistus 17

Ehdotus asetukseksi Johdanto-osan 14 kappale

Komission teksti

(14) Viraston lähtökohtaisena tehtävänä on edistää asianomaisen lainsäädännön johdonmukaista täytäntöönpanoa ja erityisesti verkko- ja tietoturvadirektiivin tehokasta täytäntöönpanoa, millä on olennainen merkitys kyberresilienssin lisäämisen kannalta. Koska kyberuhkaympäristö muuttuu nopeasti, on selvää, että jäsenvaltioita on tuettava omaksumalla kokonaisvaltaisempi, monialainen lähestymistapa kyberresilienssin rakentamiseen.

Tarkistus

(14) Viraston lähtökohtaisena tehtävänä on edistää asianomaisen lainsäädännön johdonmukaista täytäntöönpanoa ja erityisesti verkko- ja tietoturvadirektiivin, ***eurooppalaisesta sähköisen viestinnän säännöstöstä annetun direktiivin, asetuksen (EU) 2016/679 ja direktiivin 2002/58/EY*** tehokasta täytäntöönpanoa, millä on olennainen merkitys kyberresilienssin lisäämisen kannalta. Koska kyberuhkaympäristö muuttuu nopeasti, on selvää, että jäsenvaltioita on tuettava omaksumalla kokonaisvaltaisempi, monialainen lähestymistapa kyberresilienssin rakentamiseen.

Tarkistus 18

Ehdotus asetukseksi Johdanto-osan 15 kappale

Komission teksti

(15) Viraston olisi avustettava jäsenvaltioita sekä unionin toimielimiä, elimiä, laitoksia ja virastoja niiden pyrkimyksissä kehittää ja parantaa valmiuksia ja varautumiskykyä ehkäistä ja havaita kyberturvallisuusongelmia ja -poikkeamia ja reagoida niihin verkko- ja tietojärjestelmien turvallisuuden kannalta. Viraston olisi erityisesti tuettava kansallisten CSIRT-toimijoiden kehittämistä ja tehostamista, jotta niiden kypsyys olisi yhteisellä korkealla tasolla unionissa. Viraston olisi myös autettava kehittämään ja päivittämään unionin ja jäsenvaltioiden strategioita, jotka koskevat verkko- ja tietojärjestelmien turvallisuutta,

Tarkistus

(15) Viraston olisi avustettava jäsenvaltioita sekä unionin toimielimiä, elimiä, laitoksia ja virastoja niiden pyrkimyksissä kehittää ja parantaa valmiuksia ja varautumiskykyä ehkäistä ja havaita kyberturvallisuusongelmia ja -poikkeamia ja reagoida niihin verkko- ja tietojärjestelmien turvallisuuden kannalta. Viraston olisi erityisesti tuettava kansallisten CSIRT-toimijoiden kehittämistä ja tehostamista, jotta niiden kypsyys olisi yhteisellä korkealla tasolla unionissa. Viraston olisi myös autettava kehittämään ja päivittämään unionin ja jäsenvaltioiden strategioita, jotka koskevat verkko- ja tietojärjestelmien turvallisuutta,

erityisesti kyberturvallisuutta, sekä edistettävä niiden levittämistä ja seurattava niiden täytäntöönpanon edistymistä. Viraston olisi myös tarjottava koulutusta ja koulutusmateriaalia julkisille elimille ja **tarvittaessa** ”koulutettava kouluttajia”, jotta voidaan auttaa jäsenvaltioita kehittämään omia koulutusvalmiuksia.

erityisesti kyberturvallisuutta, sekä edistettävä niiden levittämistä ja seurattava niiden täytäntöönpanon edistymistä. **Koska inhimilliset virheet ovat merkittävimpiä kyberturvallisuusriskejä**, viraston olisi myös tarjottava koulutusta ja koulutusmateriaalia julkisille elimille ja ”koulutettava kouluttajia” **mahdollisimman laajasti**, jotta voidaan auttaa jäsenvaltioita **sekä unionin toimielimiä ja virastoja** kehittämään omia koulutusvalmiuksia. **Viraston olisi myös toimittava yhteyspisteenä jäsenvaltioille ja unionin toimielimille, joiden olisi voitava pyytää virastolta apua sen toimivallan ja tehtävien puitteissa.**

Tarkistus 19

Ehdotus asetukseksi Johdanto-osan 18 kappale

Komission teksti

(18) Viraston olisi koottava ja analysoitava CSIRT-toimijoilta ja CERT-EU:lta saatavat kansalliset raportit ja otettava käyttöön yhteiset säännöt, kieli ja terminologia tiedonvaihtoa varten. Viraston olisi myös otettava yksityinen sektori mukaan verkko- ja tietoturvadirektiivin kehukseen, jossa vahvistettiin perusta vapaaehtoiselle teknisten tietojen vaihdolle operatiivisella tasolla perustamalla CSIRT-verkosto.

Tarkistus 20

Ehdotus asetukseksi Johdanto-osan 19 kappale

Komission teksti

(19) Viraston olisi osallistuttava EU:n tason vastaukseen laajamittaisten rajatylittävien kyberturvallisuuspoikkeamien ja -kriisien tapauksessa. Tähän tehtävään olisi kuuluttava tarvittavan tiedon keruu ja

Tarkistus

(18) Viraston olisi koottava ja analysoitava CSIRT-toimijoilta ja CERT-EU:lta saatavat kansalliset raportit ja otettava käyttöön yhteiset säännöt, kieli ja terminologia tiedonvaihtoa varten. Viraston olisi myös otettava yksityinen **ja julkinen** sektori mukaan verkko- ja tietoturvadirektiivin kehukseen, jossa vahvistettiin perusta vapaaehtoiselle teknisten tietojen vaihdolle operatiivisella tasolla perustamalla CSIRT-verkosto.

Tarkistus

(19) Viraston olisi osallistuttava EU:n tason vastaukseen laajamittaisten rajatylittävien kyberturvallisuuspoikkeamien ja -kriisien tapauksessa. Tähän tehtävään olisi kuuluttava **jäsenvaltioiden viranomaisten**

toimiminen välittäjänä CSIRT-verkoston ja tekniikan alan toimijoiden sekä kriisinhallinnasta vastaavien päätöksentekijöiden välillä. Lisäksi virasto voisi tukea poikkeamien käsittelyä teknisestä näkökulmasta helpottamalla tarvittavien ratkaisujen teknistä vaihtoa jäsenvaltioiden välillä ja osallistumalla julkiseen viestintään. Viraston olisi tuettava tätä prosessia testaamalla tällaisen yhteistyön menettelyjä vuotuisissa kyberturvallisuusharjoituksissa.

koollekutsuminen ja auttaminen niiden vastatoimien koordinoinnissa, tarvittavan tiedon keruu ja toimiminen välittäjänä CSIRT-verkoston ja tekniikan alan toimijoiden sekä kriisinhallinnasta vastaavien päätöksentekijöiden välillä. Lisäksi virasto voisi tukea poikkeamien käsittelyä teknisestä näkökulmasta ***esimerkiksi*** helpottamalla tarvittavien ratkaisujen teknistä vaihtoa jäsenvaltioiden välillä ja osallistumalla julkiseen viestintään. Viraston olisi tuettava tätä prosessia testaamalla tällaisen yhteistyön menettelyjä vuotuisissa kyberturvallisuusharjoituksissa. ***Viraston olisi kunnioitettava kyberturvallisuutta koskevaa jäsenvaltioiden toimivaltaa ja erityisesti yleistä turvallisuutta, puolustusta ja kansallista turvallisuutta koskevaa toimivaltaa sekä yksittäisen valtion toimia rikosoikeuden alalla koskevaa toimivaltaa.***

Tarkistus 21

Ehdotus asetukseksi Johdanto-osan 25 kappale

Komission teksti

(25) Jäsenvaltiot voivat pyytää yrityksiä, joita poikkeama koskee, tekemään yhteistyötä antamalla tarvittavan tiedon ja avun virastolle, sanotun kuitenkin rajoittamatta niiden oikeutta suojata kaupallisesti arkaluonteiset tiedot.

Tarkistus

(25) Jäsenvaltiot voivat pyytää yrityksiä, joita poikkeama koskee, tekemään yhteistyötä antamalla tarvittavan tiedon ja avun virastolle, sanotun kuitenkin rajoittamatta niiden oikeutta suojata kaupallisesti arkaluonteiset tiedot ***ja yleisen turvallisuuden kannalta merkitykselliset tiedot.***

Tarkistus 22

Ehdotus asetukseksi Johdanto-osan 26 kappale

Komission teksti

(26) Ymmärtääkseen paremmin kyberturvallisuuteen liittyviä haasteita ja tarjotakseen strategista pitkän aikavälin

Tarkistus

(26) Ymmärtääkseen paremmin kyberturvallisuuteen liittyviä haasteita ja tarjotakseen strategista pitkän aikavälin

neuvontaa jäsenvaltioille ja unionin toimielimille viraston on tarpeen analysoida nykyisiä ja kehittymässä olevia riskejä. Tätä varten viraston olisi yhteistyössä jäsenvaltioiden ja tarvittaessa tilastokeskusten ja muiden elinten kanssa kerättävä tarvittavaa tietoa sekä tehtävä analyyskejä uusista teknologioista ja aihekohtaisia arviointeja teknologisten innovaatioiden odotettavissa olevista yhteiskunnallisista, oikeudellisista, taloudellisista ja sääntelyyn liittyvistä vaikutuksista verkko- ja tietoturvallisuuden ja erityisesti kyberturvallisuuden kannalta. Viraston olisi myös tuettava jäsenvaltioita ja unionin toimielimiä, virastoja ja elimiä kyberturvallisuuteen liittyvien uusien kehityssuuntausten kartoittamisessa ja kyberturvallisuuteen liittyvien ongelmien ehkäisyssä tekemällä analyyskejä uhkista ja poikkeamista.

Tarkistus 23

Ehdotus asetukseksi Johdanto-osan 27 kappale

Komission teksti

(27) Unionin resilienssin lisäämiseksi viraston olisi kehitettävä internetinfrastruktuurin ja elintärkeiden infrastruktuurien turvallisuuteen liittyvää huippuosaamista tarjoamalla neuvontaa, ohjeita ja parhaita käytäntöjä. Jotta kyberturvallisuusriskeistä ja mahdollisista suojakeinoista saataisiin tietoa helpommin ja paremmin jäsennellyssä muodossa, viraston olisi kehitettävä unionin ”tietokeskus” ja ylläpidettävä sitä. Kyseessä on keskitetty verkkoportaali, josta yleisö saa EU:n ja kansallisilta toimielimiltä, virastoilta ja laitoksilta peräisin olevaa tietoa kyberturvallisuudesta.

neuvontaa jäsenvaltioille ja unionin toimielimille viraston on tarpeen analysoida nykyisiä ja kehittymässä olevia riskejä, **poikkeamia, uhkia ja heikkouksia**. Tätä varten viraston olisi yhteistyössä jäsenvaltioiden ja tarvittaessa tilastokeskusten ja muiden elinten kanssa kerättävä tarvittavaa tietoa sekä tehtävä analyyskejä uusista teknologioista ja aihekohtaisia arviointeja teknologisten innovaatioiden odotettavissa olevista yhteiskunnallisista, oikeudellisista, taloudellisista ja sääntelyyn liittyvistä vaikutuksista verkko- ja tietoturvallisuuden ja erityisesti kyberturvallisuuden kannalta. Viraston olisi myös tuettava jäsenvaltioita ja unionin toimielimiä, virastoja ja elimiä kyberturvallisuuteen liittyvien uusien kehityssuuntausten kartoittamisessa ja kyberturvallisuuteen liittyvien ongelmien ehkäisyssä tekemällä analyyskejä uhkista, poikkeamista ja **heikkouksista**.

Tarkistus

(27) Unionin resilienssin lisäämiseksi viraston olisi kehitettävä internetinfrastruktuurin ja elintärkeiden infrastruktuurien turvallisuuteen liittyvää huippuosaamista tarjoamalla neuvontaa, ohjeita ja parhaita käytäntöjä. Jotta kyberturvallisuusriskeistä ja mahdollisista suojakeinoista saataisiin tietoa helpommin ja paremmin jäsennellyssä muodossa, viraston olisi kehitettävä unionin ”tietokeskus” ja ylläpidettävä sitä. Kyseessä on keskitetty verkkoportaali, josta yleisö saa EU:n ja kansallisilta toimielimiltä, virastoilta ja laitoksilta peräisin olevaa tietoa kyberturvallisuudesta.
Kyberturvallisuusriskejä ja mahdollisia suojakeinoja koskevien paremmin jäsennellyjen tietojen saannin helpottamisen olisi autettava

jäsenvaltioita kehittämään valmiuksiaan, yhdenmukaistamaan käytäntöjään ja siten parantamaan yleistä resilienssiään kyberhyökkäyksen aikana.

Tarkistus 24

Ehdotus asetukseksi Johdanto-osan 28 kappale

Komission teksti

(28) Viraston olisi autettava lisäämään yleisön tietoisuutta kyberturvallisuuteen liittyvistä riskeistä ja annettava yksittäisille käyttäjille ohjeita hyvistä toimintatavoista kansalaisten ja organisaatioiden käyttöön. Viraston pitäisi osaltaan edistää parhaita käytäntöjä ja ratkaisuja yksilöiden ja organisaatioiden tasolla keräämällä ja analysoimalla julkisesti saatavilla olevia tietoja merkittävistä poikkeamista ja kokoamalla raportteja ohjeistuksen antamiseksi yrityksille ja kansalaisille ja yleisen varautumis- ja resilienssitason parantamiseksi. Viraston olisi myös järjestettävä yhteistyössä jäsenvaltioiden sekä unionin toimielinten, elinten, virastojen ja laitosten kanssa säännöllisiä loppukäyttäjille suunnattuja tiedotus- ja valistuskampanjoita, joiden tarkoituksena on edistää turvallisempaa verkkokäyttäytymistä yksilötasolla ja lisätä tietoisuutta verkossa piilevistä mahdollisista uhkista, mukaan lukien verkkourkintayritysten, bottiverkkojen sekä talous- ja pankkipetosten kaltainen kyberrikollisuus, sekä edistää yleisluonteisen neuvonnan antamista aitouden todentamista ja tietosuojaa koskevissa kysymyksissä. Virastolla olisi oltava keskeinen rooli pyrittäessä lisäämään loppukäyttäjien tietoisuutta laitteiden turvallisuudesta.

Tarkistus

(28) Viraston olisi autettava lisäämään yleisön tietoisuutta, **myös edistämällä koulutusta** kyberturvallisuuteen liittyvistä riskeistä ja annettava yksittäisille käyttäjille ohjeita hyvistä toimintatavoista kansalaisten, organisaatioiden ja **yritysten** käyttöön. Viraston pitäisi osaltaan edistää **kyberhygienian** parhaita käytäntöjä, **joihin kuuluu useita käytäntöjä, jotka olisi pantava täytäntöön ja toteutettava säännöllisesti käyttäjien ja yritysten suojelemiseksi verkossa**, ja ratkaisuja yksilöiden, **organisaatioiden** ja **yritysten** tasolla keräämällä ja analysoimalla julkisesti saatavilla olevia tietoja merkittävistä poikkeamista ja kokoamalla **ja julkaisemalla** raportteja **ja oppaita** ohjeistuksen antamiseksi yrityksille ja kansalaisille ja yleisen varautumis- ja resilienssitason parantamiseksi. **ENISAn olisi myös pyrittävä tarjoamaan kuluttajille merkityksellistä tietoa sovellettavista sertifiointijärjestelmistä esimerkiksi tarjoamalla ohjeistusta ja suosituksia verkossa ja sen ulkopuolella toimiville markkinapaikoille.** Viraston olisi myös järjestettävä **digitaalisen koulutuksen toimintasuunnitelman mukaisesti ja** yhteistyössä jäsenvaltioiden sekä unionin toimielinten, elinten, virastojen ja laitosten kanssa säännöllisiä loppukäyttäjille suunnattuja tiedotus- ja valistuskampanjoita, joiden tarkoituksena on edistää turvallisempaa verkkokäyttäytymistä yksilötasolla **ja digitaalista lukutaitoa** ja lisätä tietoisuutta verkossa piilevistä mahdollisista uhkista,

mukaan lukien verkkourkintayritysten, bottiverkkojen sekä talous- ja pankkipetosten kaltainen kyberrikollisuus, sekä edistää yleisluonteisen neuvonnan antamista *monivaiheista* aitouden todentamista, *paikkausta, salaamista, anonymisointia* ja tietosuojaa koskevissa kysymyksissä. Virastolla olisi oltava keskeinen rooli pyrittäessä lisäämään loppukäyttäjien tietoisuutta laitteiden turvallisuudesta *ja palveluiden turvallisesta käytöstä, kun EU:n tasolla tehdään tunnetuksi sisäänrakennettua turvallisuutta, sisäänrakennettua yksityisyyttä sekä poikkeuksia ja niiden ratkaisuja. Tähän tavoitteeseen pyrkiessään viraston olisi hyödynnettävä mahdollisimman laajasti parhaita saatavilla olevia käytäntöjä ja asiantuntemusta, erityisesti akateemisten laitosten sekä tieto- ja viestintätekniikan tutkijoiden asiantuntemusta. Koska yksittäiset virheet ja tietämättömyys kyberturvallisuusriskeistä muodostavat kyberturvallisuuden merkittävimmän epävarmuustekijän, virastolle olisi osoitettava riittävät resurssit tämän tehtävän toteuttamiseksi mahdollisimman perusteellisesti.*

Tarkistus 25

Ehdotus asetukseksi Johdanto-osan 28 a kappale (uusi)

Komission teksti

Tarkistus

(28 a) Viraston olisi lisättävä yleisön tietoisuutta riskeistä, jotka liittyvät tietopetostapahtumiin ja tietovarkauksiin, joilla voi olla vakavia vaikutuksia yksilöiden perusoikeuksiin ja jotka voivat uhata oikeusvaltioperiaatetta ja vaarantaa demokraattisten yhteiskuntien ja myös jäsenvaltioiden demokraattisten prosessien vakauden.

Tarkistus 26

Ehdotus asetukseksi Johdanto-osan 30 kappale

Komission teksti

(30) Varmistaakseen tavoitteidensa täysimittaisen saavuttamisen viraston olisi oltava yhteydessä asiaankuuluviin toimielimiin, virastoihin ja elimiin, mukaan lukien CERT-EU, Europolissa toimiva Euroopan kyberrikostorjuntakeskus (EC3), Euroopan puolustusvirasto (EDA), laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaava eurooppalainen virasto (eu-LISA), Euroopan lentoturvallisuusvirasto (EASA) sekä muut kyberturvallisuuteen liittyviä kysymyksiä käsittelevät EU:n virastot. Sen olisi oltava yhteydessä myös tietosuoja-asioita käsitteleviin viranomaisiin, jotta voidaan vaihtaa tietotaitoa ja parhaita käytäntöjä ja antaa neuvontaa kyberturvallisuusnäkökohdista, joilla voi olla vaikutusta niiden toimintaan. Kansallisten ja unionin lainvalvonta- ja tietosuojaviranomaisten edustajien olisi voitava olla edustettuina **viraston pysyvässä sidosryhmässä**. Ollessaan yhteydessä lainvalvontaviranomaisiin sellaisissa verkko- ja tietoturvakysymyksissä, joilla voi olla vaikutusta niiden toimintaan, viraston olisi käytettävä olemassa olevia tiedonvaihtokanavia ja vakiintuneita verkostoja.

Tarkistus

(30) Varmistaakseen tavoitteidensa täysimittaisen saavuttamisen viraston olisi oltava yhteydessä asiaankuuluviin toimielimiin, **EU:n valvonta- ja muihin toimivaltaisiin viranomaisiin**, virastoihin ja elimiin, mukaan lukien CERT-EU, Europolissa toimiva Euroopan kyberrikostorjuntakeskus (EC3), Euroopan puolustusvirasto (EDA), **Euroopan GNSS-virasto (GSA), Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelin (BEREC)**, laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaava eurooppalainen virasto (eu-LISA), Euroopan **keskuspankki (EKP), Euroopan pankkiviranomainen (EPV), Euroopan tietosuojaneuvosto, Euroopan** lentoturvallisuusvirasto (EASA) sekä muut kyberturvallisuuteen liittyviä kysymyksiä käsittelevät EU:n virastot. Sen olisi oltava yhteydessä myös **eurooppalaisiin standardointiorganisaatioihin, asianomaisiin sidosryhmiin ja** tietosuoja-asioita käsitteleviin viranomaisiin, jotta voidaan vaihtaa tietotaitoa ja parhaita käytäntöjä ja antaa neuvontaa kyberturvallisuusnäkökohdista, joilla voi olla vaikutusta niiden toimintaan. Kansallisten ja unionin lainvalvonta- ja tietosuojaviranomaisten edustajien olisi voitava olla edustettuina **ENISAn neuvoantavassa ryhmässä**. Ollessaan yhteydessä lainvalvontaviranomaisiin sellaisissa verkko- ja tietoturvakysymyksissä, joilla voi olla vaikutusta niiden toimintaan, viraston olisi käytettävä olemassa olevia tiedonvaihtokanavia ja vakiintuneita verkostoja. **Olisi muodostettava kumppanuuksia sellaisten akateemisten laitosten kanssa, joilla on tutkimusaloitteita merkityksellisillä aloilla, ja kuluttajajärjestöiltä ja muilta järjestöiltä tuleville tiedoille olisi oltava sopivat kanavat ja tiedot olisi analysoitava**

aina.

Tarkistus 27

Ehdotus asetukseksi Johdanto-osan 31 kappale

Komission teksti

(31) Viraston olisi CSIRT-verkoston sihteeristönä toimivana jäsenenä tuettava jäsenvaltioiden CSIRT-toimijoita ja CERT-EU:ta operatiivisessa yhteistyössä kaikkien asiaankuuluvien CSIRT-verkoston tehtävien lisäksi, sellaisina kuin ne määritellään verkko- ja tietoturvadirektiivissä. Viraston olisi lisäksi edistettävä ja tuettava yhteistyötä asianomaisten CSIRT-toimijoiden välillä tapauksissa, joissa CSIRT-toimijoiden hallinnoimiin tai suojaamiin verkkoihin tai infrastruktuureihin kohdistuu poikkeamia, hyökkäyksiä tai häiriöitä, jotka koskevat tai mahdollisesti koskevat vähintään kahta CERT-toimijaa, ottaen asianmukaisesti huomioon CSIRT-verkoston menettelyohjeet.

Tarkistus

(31) Viraston olisi CSIRT-verkoston sihteeristönä toimivana jäsenenä tuettava jäsenvaltioiden CSIRT-toimijoita ja CERT-EU:ta operatiivisessa yhteistyössä kaikkien asiaankuuluvien CSIRT-verkoston tehtävien lisäksi, sellaisina kuin ne määritellään verkko- ja tietoturvadirektiivissä. Viraston olisi lisäksi edistettävä ja tuettava yhteistyötä asianomaisten CSIRT-toimijoiden välillä tapauksissa, joissa CSIRT-toimijoiden hallinnoimiin tai suojaamiin verkkoihin tai infrastruktuureihin kohdistuu poikkeamia, hyökkäyksiä tai häiriöitä, jotka koskevat tai mahdollisesti koskevat vähintään kahta CERT-toimijaa, ottaen asianmukaisesti huomioon CSIRT-verkoston menettelyohjeet. ***Virasto voi komission tai jäsenvaltion pyynnöstä suorittaa säännöllisiä kriittisten rajatylittävien infrastruktuurien tietoteknisen turvallisuuden tarkastuksia, joiden tarkoituksena on yksilöidä suosituksia niiden resilienssin parantamiseksi.***

Tarkistus 28

Ehdotus asetukseksi Johdanto-osan 33 kappale

Komission teksti

(33) Viraston olisi kehitettävä ja ylläpidettävä asiantuntemustaan kyberturvallisuussertifioinnissa, jotta voidaan tukea unionin politiikkaa tällä alalla. Viraston olisi edistettävä kyberturvallisuussertifioinnin käyttöä unionissa muun muassa osallistumalla kyberturvallisuuden sertifiointikehyksen

Tarkistus

(33) Viraston olisi kehitettävä ja ylläpidettävä asiantuntemustaan kyberturvallisuussertifioinnissa, jotta voidaan tukea unionin politiikkaa tällä alalla. Viraston olisi ***kehitettävä edelleen nykyisiä parhaita käytäntöjä ja*** edistettävä kyberturvallisuussertifioinnin käyttöä unionissa muun muassa osallistumalla

perustamiseen ja ylläpitoon unionin tasolla, jotta voidaan lisätä avoimuutta tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa ja tällä tavoin vahvistaa luottamusta digitaalisiin sisämarkkinoihin.

Tarkistus 29

Ehdotus asetukseksi Johdanto-osan 35 kappale

Komission teksti

(35) Viraston olisi kannustettava jäsenvaltioita ja palveluntarjoajia tiukentamaan yleisiä turvallisuusnormejaan, jotta kaikki internetin käyttäjät **voivat toteuttaa** tarvittavat toimenpiteet oman kyberturvallisuutensa varmistamiseksi. Erityisesti palveluntarjoajien ja tuotteiden valmistajien olisi poistettava tuotannosta tai kierrätettävä tuotteet ja palvelut, jotka eivät täytä **kyberturvallisuusnormeja**. ENISA voi yhteistyössä toimivaltaisten viranomaisten kanssa levittää tietoa sisämarkkinoilla tarjottavien tuotteiden ja palvelujen kyberturvallisuustasosta ja antaa varoituksia palveluntarjoajille ja valmistajille ja vaatia niitä parantamaan tuotteidensa ja palvelujensa turvallisuutta, mukaan lukien kyberturvallisuus.

kyberturvallisuuden sertifiointikehyksen perustamiseen ja ylläpitoon unionin tasolla, jotta voidaan lisätä avoimuutta tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa ja tällä tavoin vahvistaa luottamusta digitaalisiin sisämarkkinoihin.

Tarkistus

(35) Viraston olisi kannustettava jäsenvaltioita, **laitevalmistajia** ja palveluntarjoajia tiukentamaan yleisiä turvallisuusnormejaan, **jotka koskevat tieto- ja viestintätekniikan tuotteita, prosesseja, palveluja ja järjestelmiä, joiden olisi täytettävä turvallisuutta koskevat perusvaatimukset sisäänrakennettua ja oletusarvoista turvallisuutta koskevan periaatteen mukaisesti, erityisesti toimittamalla tarpeelliset päivitykset**, jotta **voidaan turvata** kaikki internetin käyttäjät **ja kannustaa näitä toteuttamaan** tarvittavat toimenpiteet oman kyberturvallisuutensa varmistamiseksi. Erityisesti palveluntarjoajien ja tuotteiden valmistajien olisi **järjestettävä palautusmenettely**, poistettava tuotannosta tai kierrätettävä tuotteet ja palvelut, jotka eivät täytä **kyberturvallisuuden perusvaatimuksia, kun taas maahantuojien ja jakelijoiden olisi varmistettava, että niiden EU:n markkinoille saattamat tieto- ja viestintätekniikan tuotteet, prosessit, palvelut ja järjestelmät täyttävät sovellettavat vaatimukset eivätkä aiheuta riskiä eurooppalaisille kuluttajille**. ENISA voi yhteistyössä toimivaltaisten viranomaisten kanssa levittää tietoa sisämarkkinoilla tarjottavien tuotteiden ja palvelujen kyberturvallisuustasosta ja antaa varoituksia palveluntarjoajille ja

valmistajille ja vaatia niitä parantamaan tuotteidensa, *prosessiensa*, palvelujensa ja *järjestelmiensä* turvallisuutta, mukaan lukien kyberturvallisuus. *Viraston olisi tehtävä sidosryhmien kanssa yhteistyötä koko EU:n laajuisen lähestymistavan määrittelemiseksi haavoittuvuuksien vastuulliseen julkistamiseen ja edistettävä asiaa koskevia parhaita käytäntöjä.*

Tarkistus 30

Ehdotus asetukseksi Johdanto-osan 36 kappale

Komission teksti

(36) Viraston olisi otettava täysimääräisesti huomioon meneillään olevat tutkimus-, kehittämis- ja teknologian arviointitoimet erityisesti unionin eri tutkimusaloitteissa antaakseen unionin toimielimille, elimille, virastoille ja laitoksille sekä tarvittaessa jäsenvaltioille pyynnöstä neuvoja verkko- ja tietoturva-alan tutkimustarpeista varsinkin kyberturvallisuuskysymyksissä.

Tarkistus

(36) Viraston olisi otettava täysimääräisesti huomioon meneillään olevat tutkimus-, kehittämis- ja teknologian arviointitoimet erityisesti unionin eri tutkimusaloitteissa antaakseen unionin toimielimille, elimille, virastoille ja laitoksille sekä tarvittaessa jäsenvaltioille pyynnöstä neuvoja verkko- ja tietoturva-alan tutkimustarpeista varsinkin kyberturvallisuuskysymyksissä. *Olisi erityisesti tehtävä yhteistyötä Euroopan tutkimusneuvoston (ERC) ja Euroopan innovaatio- ja teknologiainstituutin (EIT) kanssa, ja turvallisuustutkimus olisi sisällytettävä yhdeksänten tutkimuksen puiteohjelmaan ja Horisontti 2020 -puiteohjelmaan.*

Tarkistus 31

Ehdotus asetukseksi Johdanto-osan 36 a kappale (uusi)

Komission teksti

Tarkistus

(36 a) *Standardi on vapaaehtoinen ja markkinavetoinen väline, jolla annetaan teknisiä vaatimuksia ja ohjausta ja joka on luotu avoimessa, läpinäkyvässä ja osallistavassa prosessissa. Viraston olisi kuultava standardointiorganisaatioita säännöllisesti ja tehtävä tiiviisti*

yhteistyötä niiden kanssa erityisesti unionin kyberturvallisuuden sertifiointijärjestelmiä valmistellessaan.

Tarkistus 32

Ehdotus asetukseksi Johdanto-osan 37 kappale

Komission teksti

(37) Kyberturvallisuuteen liittyvät ongelmat ovat maailmanlaajuisia. Tarvitaan tiiviimpää kansainvälistä yhteistyötä turvallisuusstandardien parantamiseksi, mihin sisältyy myös yhteisten käyttäytymisnormien määrittely, sekä tiedonvaihtoa kansainvälisen yhteistoiminnan nopeuttamiseksi verkko- ja tietoturvakysymyksissä samoin kuin yhteistä maailmanlaajuisia lähestymistapaa näihin kysymyksiin. Tätä varten viraston olisi tuettava unionin osallistumista kolmansien maiden ja kansainvälisten organisaatioiden kanssa harjoitettavaan yhteistyöhön ja tämän yhteistyön lisäämistä tarjoamalla käyttöön asianomaisten unionin toimielinten, elinten, virastojen ja laitosten mahdollisesti tarvitsemaa asiantuntemusta ja analysointivalmiuksia.

Tarkistus

(37) Kyberturvallisuuteen liittyvät ongelmat ovat maailmanlaajuisia. Tarvitaan tiiviimpää kansainvälistä yhteistyötä turvallisuusstandardien parantamiseksi, mihin sisältyy myös yhteisten käyttäytymisnormien **ja käytännesääntöjen** määrittely **ja kansainvälisten standardien soveltaminen** sekä tiedonvaihtoa kansainvälisen yhteistoiminnan nopeuttamiseksi verkko- ja tietoturvakysymyksissä samoin kuin yhteistä maailmanlaajuisia lähestymistapaa näihin kysymyksiin. Tätä varten viraston olisi tuettava unionin osallistumista kolmansien maiden ja kansainvälisten organisaatioiden kanssa harjoitettavaan yhteistyöhön ja tämän yhteistyön lisäämistä tarjoamalla käyttöön asianomaisten unionin toimielinten, elinten, virastojen ja laitosten mahdollisesti tarvitsemaa asiantuntemusta ja analysointivalmiuksia.

Tarkistus 33

Ehdotus asetukseksi Johdanto-osan 40 kappale

Komission teksti

(40) Johtokunnan, jossa ovat edustettuna jäsenvaltiot ja komissio, olisi määriteltävä viraston toiminnan yleinen suunta ja varmistettava, että se hoitaa tehtäviään tämän asetuksen mukaisesti. Johtokunnalle olisi annettava tarvittavat valtuudet hyväksyä talousarvio, valvoa sen toteuttamista, vahvistaa tarvittavat varainhoitoa koskevat säännöt, luoda

Tarkistus

(40) Johtokunnan, jossa ovat edustettuna jäsenvaltiot ja komissio **sekä viraston tavoitteiden kannalta merkittävät sidosryhmät**, olisi määriteltävä viraston toiminnan yleinen suunta ja varmistettava, että se hoitaa tehtäviään tämän asetuksen mukaisesti. Johtokunnalle olisi annettava tarvittavat valtuudet hyväksyä talousarvio, valvoa sen toteuttamista, vahvistaa

avoimet menettelyt viraston päätöksentekoa varten, hyväksyä viraston yhtenäinen ohjelma-asiakirja, vahvistaa työjärjestyksensä, nimittää pääjohtaja sekä päättää tämän toimikauden jatkamisesta ja päättämisestä.

tarvittavat varainhoitoa koskevat säännöt, luoda avoimet menettelyt viraston päätöksentekoa varten, hyväksyä viraston yhtenäinen ohjelma-asiakirja, vahvistaa työjärjestyksensä, nimittää pääjohtaja sekä päättää tämän toimikauden jatkamisesta ja päättämisestä. ***Koska viraston tehtävät ovat hyvin teknisiä ja tieteellisiä, johtokunnan jäsenillä olisi oltava asianmukainen kokemus ja korkean tason asiantuntemusta viraston tehtäviin kuuluvista kysymyksistä.***

Tarkistus 34

Ehdotus asetukseksi Johdanto-osan 41 kappale

Komission teksti

(41) Viraston moitteettoman ja tehokkaan toiminnan takaamiseksi komission ja jäsenvaltioiden olisi varmistettava, että johtokunnan jäseniksi nimitettävillä henkilöillä on riittävä ammatillinen asiantuntemus ja kokemus toiminnallisilta aloilta. Johtokunnan työn jatkuvuuden varmistamiseksi komission ja jäsenvaltioiden olisi pyrittävä rajoittamaan johtokunnassa olevien edustajiensa vaihtuvuutta.

Tarkistus

(41) Viraston moitteettoman ja tehokkaan toiminnan takaamiseksi komission ja jäsenvaltioiden olisi varmistettava, että johtokunnan jäseniksi nimitettävillä henkilöillä on riittävä ammatillinen asiantuntemus ja kokemus toiminnallisilta aloilta. Johtokunnan työn jatkuvuuden varmistamiseksi komission ja jäsenvaltioiden olisi pyrittävä rajoittamaan johtokunnassa olevien edustajiensa vaihtuvuutta. ***Viraston työssä tarvittavien taitojen korkean markkina-arvon vuoksi on tärkeää varmistaa, että viraston henkilöstölle tarjottavat palkat ja sosiaalietuudet ovat kilpailukykyisiä ja varmistavat, että parhaat ammattilaiset voivat valita sen työpaikakseen.***

Perustelu

Riittävän asiantuntemuksen tason varmistamiseksi ENISAn on oltava kilpailukykyinen työnantaja erittäin kilpailluilla markkinoilla.

Tarkistus 35

Ehdotus asetukseksi Johdanto-osan 42 kappale

Komission teksti

Tarkistus

(42) Viraston moitteeton toiminta edellyttää, että sen pääjohtaja nimitetään ansioiden ja todistuksin osoitettujen hallinnollisten taitojen ja johtamistaitojen sekä kyberturvallisuuden kannalta merkityksellisen pätevyyden ja kokemuksen perusteella ja että pääjohtajan tehtäviä hoidetaan täysin riippumattomasti. Pääjohtajan olisi laadittava ehdotus viraston työohjelmaksi kuultuaan ensin komissiota ja toteutettava kaikki tarvittavat toimenpiteet varmistaakseen viraston työohjelman asianmukaisen toteuttamisen. Pääjohtajan olisi laadittava johtokunnalle esitettävä vuosikertomus sekä esitys viraston tuloja ja menoja koskevaksi ennakoarvioksi ja vastattava talousarvion toteuttamisesta. Pääjohtajan olisi voitava perustaa tilapäisiä työryhmiä erityisesti tieteellisiä, teknisiä, oikeudellisia tai sosioekonomisia erityiskysymyksiä varten. Pääjohtajan olisi varmistettava, että tilapäisten työryhmien jäsenet valitaan huippuasiantuntemuksen perusteella ja ottaen asianmukaisesti huomioon tarkasteltavan kysymyksen edellyttämällä tavalla edustuksellinen tasapaino jäsenvaltioiden julkishallintojen, unionin toimielinten ja yksityisen sektorin välillä, mukaan lukien toimiala, käyttäjät ja tiedeyhteisöä edustavat verkko- ja tietoturva-asiantuntijat.

Tarkistus 36

Ehdotus asetukseksi Johdanto-osan 44 kappale

Komission teksti

(44) Virastolla olisi oltava neuvoa-antavana elimenä **pysyvä sidosryhmä**, jotta voitaisiin varmistaa säännöllinen yhteydenpito yksityisen sektorin, kuluttajajärjestöjen ja muiden asianosaisten sidosryhmien kanssa. **Pysyvän sidosryhmän**, jonka johtokunta perustaa pääjohtajan ehdotuksesta, olisi keskityttävä sidosryhmiä koskeviin asioihin ja

(42) Viraston moitteeton toiminta edellyttää, että sen pääjohtaja nimitetään ansioiden ja todistuksin osoitettujen hallinnollisten taitojen ja johtamistaitojen sekä kyberturvallisuuden kannalta merkityksellisen pätevyyden ja kokemuksen perusteella ja että pääjohtajan tehtäviä hoidetaan täysin riippumattomasti. Pääjohtajan olisi laadittava ehdotus viraston työohjelmaksi kuultuaan ensin komissiota ja toteutettava kaikki tarvittavat toimenpiteet varmistaakseen viraston työohjelman asianmukaisen toteuttamisen. Pääjohtajan olisi laadittava johtokunnalle esitettävä vuosikertomus sekä esitys viraston tuloja ja menoja koskevaksi ennakoarvioksi ja vastattava talousarvion toteuttamisesta. Pääjohtajan olisi voitava perustaa tilapäisiä työryhmiä erityisesti tieteellisiä, teknisiä, oikeudellisia tai sosioekonomisia erityiskysymyksiä varten. Pääjohtajan olisi varmistettava, että tilapäisten työryhmien jäsenet valitaan huippuasiantuntemuksen perusteella ja ottaen asianmukaisesti huomioon tarkasteltavan kysymyksen edellyttämällä tavalla edustuksellinen **ja sukupuolten** tasapaino jäsenvaltioiden julkishallintojen, unionin toimielinten ja yksityisen sektorin välillä, mukaan lukien toimiala, käyttäjät ja tiedeyhteisöä edustavat verkko- ja tietoturva-asiantuntijat.

Tarkistus

(44) Virastolla olisi oltava neuvoa-antavana elimenä **ENISAn neuvoa-antava ryhmä**, jotta voitaisiin varmistaa säännöllinen yhteydenpito yksityisen sektorin, kuluttajajärjestöjen, **tiedeyhteisön** ja muiden asianosaisten sidosryhmien kanssa. **ENISAn neuvoa-antavan ryhmän**, jonka johtokunta perustaa pääjohtajan ehdotuksesta, olisi keskityttävä

saatettava ne viraston tietoon. Pysyvän sidosryhmän kokoonpanossa ja tälle ryhmälle, jotka kuullaan erityisesti työohjelmaluonnoksesta, annettavissa tehtävissä olisi varmistettava sidosryhmien riittävä edustus viraston työskentelyssä.

sidosryhmiä koskeviin asioihin ja saatettava ne viraston tietoon. Pysyvän sidosryhmän kokoonpanossa ja tälle ryhmälle, jotka kuullaan erityisesti työohjelmaluonnoksesta, annettavissa tehtävissä olisi varmistettava sidosryhmien riittävä edustus viraston työskentelyssä.

Ottaen huomioon sertifiointivaatimusten merkityksen esineiden internetiä kohtaan tunnetun luottamuksen varmistamisessa komissio harkitsee erityisesti täytäntöönpanotoimenpiteitä EU:n laajuisen turvallisuusstandardien yhdenmukaistamisen varmistamiseksi esineiden internetin laitteiden osalta.

Tarkistus 37

Ehdotus asetukseksi Johdanto-osan 44 a kappale (uusi)

Komission teksti

Tarkistus

(44 a) Virastolla olisi oltava neuvoa-antavana elimenä sidosryhmien sertifiointiryhmä, jotta voitaisiin varmistaa säännöllinen yhteydenpito yksityisen sektorin, kuluttajajärjestöjen, tiedeyhteisön ja muiden asianosaisten sidosryhmien kanssa. Pääjohtajan perustaman sidosryhmien sertifiointiryhmän olisi koostuttava yleisestä neuvoa-antavasta komiteasta, joka antaa neuvoja siitä, mitkä tieto- ja viestintätekniiikan tuotteet ja palvelut tulevien eurooppalaisten tietotekniikkaturvallisuuden sertifiointijärjestelmien olisi katettava, ja tilapäisistä komiteoista, jotka antavat pyydettyä neuvoja ehdolla olevia eurooppalaisia kyberturvallisuusjärjestelmiä koskevista ehdotuksista, niiden kehittämisestä ja hyväksymisestä.

Tarkistus 38

Ehdotus asetukseksi Johdanto-osan 46 kappale

Komission teksti

(46) Jotta voidaan varmistaa viraston täydellinen itsemääräämisoikeus ja riippumattomuus ja jotta virasto pystyy suorittamaan uusia ja täydentäviä tehtäviä, myös ennakoimattomia tehtäviä hätätilanteissa, virastolle olisi annettava riittävä ja itsenäinen talousarvio, jonka tulot koostuvat ensisijaisesti unionin rahoitusosuudesta ja viraston työhön osallistuvien kolmansien maiden rahoitusosuuksista. Viraston henkilöstön enemmistön työtehtävien olisi liityttävä suoraan viraston toimeksiannon operatiiviseen täytäntöönpanoon. Viraston isäntäjäsenvaltion tai minkä tahansa muun jäsenvaltion olisi voitava maksaa vapaaehtoisia rahoitusosuuksia virastolle. Unionin talousarviomenettelyä olisi sovellettava edelleen unionin yleisestä talousarviosta maksettaviin tukiin. Lisäksi tilintarkastustuomioistuimen olisi tarkastettava viraston tilit avoimuuden ja vastuuvollisuuden varmistamiseksi.

Tarkistus 39

Ehdotus asetukseksi Johdanto-osan 47 kappale

Komission teksti

(47) Vaatimustenmukaisuuden arviointi on menettely sen osoittamiseksi, täyttyvätkö tuotteelle, prosessille, palvelulle, järjestelmälle, henkilölle tai elimelle asetetut erityiset vaatimukset. Tätä asetusta sovellettaessa sertifiointi olisi katsottava vaatimustenmukaisuuden arvioinnin tyypiksi, joka koskee tuotteen, prosessin, palvelun, järjestelmän tai näiden yhdistelmän, jäljempänä 'tieto- ja viestintäteknikan tuotteet ja palvelut',

Tarkistus

(46) Jotta voidaan varmistaa viraston täydellinen itsemääräämisoikeus ja riippumattomuus ja jotta virasto pystyy suorittamaan uusia ja täydentäviä tehtäviä, myös ennakoimattomia tehtäviä hätätilanteissa, virastolle olisi annettava riittävä ja itsenäinen talousarvio, jonka tulot koostuvat ensisijaisesti unionin rahoitusosuudesta ja viraston työhön osallistuvien kolmansien maiden rahoitusosuuksista. ***Asianmukaiset määrärahat ovat äärimmäisen tärkeät sen varmistamiseksi, että virastolla on riittävät valmiudet toteuttaa kaikki lisääntyvät tehtävänsä ja tavoitteensa.*** Viraston henkilöstön enemmistön työtehtävien olisi liityttävä suoraan viraston toimeksiannon operatiiviseen täytäntöönpanoon. Viraston isäntäjäsenvaltion tai minkä tahansa muun jäsenvaltion olisi voitava maksaa vapaaehtoisia rahoitusosuuksia virastolle. Unionin talousarviomenettelyä olisi sovellettava edelleen unionin yleisestä talousarviosta maksettaviin tukiin. Lisäksi tilintarkastustuomioistuimen olisi tarkastettava viraston tilit avoimuuden, vastuuvollisuuden ja ***varojen tehokkaan käytön*** varmistamiseksi.

Tarkistus

(47) Vaatimustenmukaisuuden arviointi on menettely sen osoittamiseksi, täyttyvätkö tuotteelle, prosessille, palvelulle, järjestelmälle, henkilölle tai elimelle asetetut erityiset vaatimukset. Tätä asetusta sovellettaessa sertifiointi olisi katsottava vaatimustenmukaisuuden arvioinnin tyypiksi, joka koskee tuotteen, prosessin, palvelun, järjestelmän tai näiden yhdistelmän, jäljempänä 'tieto- ja viestintäteknikan tuotteet, ***prosessit*** ja

kyberturvallisuusominaisuuksia ja jonka suorittaa riippumaton kolmas osapuoli, **joka ei ole** tuotteen valmistaja tai palvelun tarjoaja. Sertifiointi ei sinänsä takaa, että sertifioidut tieto- ja viestintätekniikan tuotteet ja palvelut ovat kyberturvallisia. Se on pikemminkin menettely ja tekninen menetelmä todistaa, että tieto- ja viestintätekniikan tuotteet ja palvelut on testattu ja että ne täyttävät tietyt kyberturvallisuusvaatimukset, jotka on vahvistettu muualla, esimerkiksi teknisissä standardeissa.

palvelut’, kyberturvallisuusominaisuuksia ja jonka suorittaa riippumaton kolmas osapuoli **tai, jos se on sallittua, tuotteen valmistaja tai palvelun tarjoaja itsearviointina. Itsearviointiin voivat suorittaa tuotteen valmistaja, pk-yritykset tai palvelun tarjoaja, kuten tässä asetuksessa on määritetty, ja soveltuvin osin uuden lainsäädäntökehyksen säädösten mukaisesti. Lisäksi sen voi suorittaa tuotteen valmistaja tai muu toimija, kun kyberturvallisuuspoikkeaman todennäköisyys ja/tai sen todennäköisyys, että tällaisesta poikkeamasta olisi merkittävää haittaa yhteiskunnalle tai sen suurelle osalle, ei odoteta olevan suuri tai merkittävä, ottaen huomioon valmistajan tai palveluntarjoajan kyseisen tuotteen tai palvelun suunniteltu käyttötarkoitus.** Sertifiointi ei sinänsä takaa, että sertifioidut tieto- ja viestintätekniikan tuotteet, **prosessit** ja palvelut ovat kyberturvallisia, **ja siitä olisi tiedotettava kuluttajille ja yrityksillä asianmukaisesti.** Se on pikemminkin menettely ja tekninen menetelmä todistaa, että tieto- ja viestintätekniikan tuotteet, **prosessit** ja palvelut on testattu ja että ne täyttävät tietyt kyberturvallisuusvaatimukset, jotka on vahvistettu muualla, esimerkiksi teknisissä standardeissa. **Näihin teknisiin standardeihin kuuluu ilmoitus siitä, voiko tieto- ja viestintätekniikan tuote, prosessi ja palvelu täyttää tehtävänsä silloin, kun se ei ole yhteydessä internetiin.**

Tarkistus 40

Ehdotus asetukseksi Johdanto-osan 48 kappale

Komission teksti

(48) **Kyberturvallisuussertifiointilla on tärkeä** rooli lisättäessä tieto- ja viestintätekniikan tuotteiden ja palvelujen turvallisuutta ja niihin tunnettua luottamusta. Digitaaliset sisämarkkinat ja erityisesti datatalous ja esineiden internet

Tarkistus

(48) **Eurooppalaisella kyberturvallisuussertifiointilla on olennainen** rooli lisättäessä tieto- ja viestintätekniikan tuotteiden, **prosessien** ja palvelujen turvallisuutta ja niihin tunnettua luottamusta. Digitaaliset sisämarkkinat ja

voivat menestyä vain, jos vallitsee yleinen julkinen luottamus siihen, että tuotteissa ja palveluissa varmistetaan kyberturvallisuus **tietyllä** tasolla. Verkkoyhteyksillä varustetut ja automatisoidut autot, sähköiset terveyspalvelut, teollisuusautomaation ohjausjärjestelmät ja älykkäät verkot ovat joitakin esimerkkejä aloista, joilla sertifiointi on jo laajalti käytössä tai tulee todennäköisesti käyttöön lähitulevaisuudessa. Verko- ja tietoturvadirektiivillä säännellyt alat ovat samalla aloja, joilla kyberturvallisuussertifiointilla on ratkaiseva merkitys.

Tarkistus 41

Ehdotus asetukseksi Johdanto-osan 49 kappale

Komission teksti

(49) Vuonna 2016 antamassaan tiedonannossa ”Euroopan kyberresilienssijärjestelmän vahvistaminen sekä kilpailukykyisen ja innovatiivisen kyberturvallisuustoimialan tukeminen” komissio linjasi tarpeen ottaa käyttöön laadukkaita, kohtuuhintaisia ja yhteentoimivia kyberturvallisuustuotteita ja -ratkaisuja. Tieto- ja viestintäteknikan tuotteiden ja -palvelujen tarjonta sisämarkkinoilla on edelleen maantieteellisesti hyvin hajanaista. Tämä johtuu siitä, että Euroopan kyberturvallisuusala on kehittynyt suurelta osin kansallisista valtiollisen kysynnän lähtökohdista. Kyberturvallisuuden sisämarkkinoiden toimintapuuhteisiin kuuluu lisäksi yhteentoimivien ratkaisujen (teknisten standardien), toimintatapojen ja EU:n laajuisten sertifiointimekanismien puuttuminen. Tämä yhtäältä vaikeuttaa eurooppalaisten yritysten kilpailua niin kansallisella kuin Euroopan ja maailmanlaajuisellakin tasolla ja toisaalta vähentää yksilöiden ja yritysten saatavilla

erityisesti datatalous ja esineiden internet voivat menestyä vain, jos vallitsee yleinen julkinen luottamus siihen, että tuotteissa ja palveluissa varmistetaan kyberturvallisuus **korkealla** tasolla. Verkkoyhteyksillä varustetut ja automatisoidut autot, sähköiset terveyspalvelut, teollisuusautomaation ohjausjärjestelmät ja älykkäät verkot ovat joitakin esimerkkejä aloista, joilla sertifiointi on jo laajalti käytössä tai tulee todennäköisesti käyttöön lähitulevaisuudessa. Verko- ja tietoturvadirektiivillä säännellyt alat ovat samalla aloja, joilla kyberturvallisuussertifiointilla on ratkaiseva merkitys.

Tarkistus

(49) Vuonna 2016 antamassaan tiedonannossa ”Euroopan kyberresilienssijärjestelmän vahvistaminen sekä kilpailukykyisen ja innovatiivisen kyberturvallisuustoimialan tukeminen” komissio linjasi tarpeen ottaa käyttöön laadukkaita, kohtuuhintaisia ja yhteentoimivia kyberturvallisuustuotteita ja -ratkaisuja. Tieto- ja viestintäteknikan tuotteiden, **prosessien** ja -palvelujen tarjonta sisämarkkinoilla on edelleen maantieteellisesti hyvin hajanaista. Tämä johtuu siitä, että Euroopan kyberturvallisuusala on kehittynyt suurelta osin kansallisista valtiollisen kysynnän lähtökohdista. Kyberturvallisuuden sisämarkkinoiden toimintapuuhteisiin kuuluu lisäksi yhteentoimivien ratkaisujen (teknisten standardien), toimintatapojen ja EU:n laajuisten sertifiointimekanismien puuttuminen. Tämä yhtäältä vaikeuttaa eurooppalaisten yritysten kilpailua niin kansallisella kuin Euroopan ja maailmanlaajuisellakin tasolla ja toisaalta vähentää yksilöiden ja yritysten saatavilla

olevan hyödyllisen ja käyttökelpoisen kyberturvallisuusteknologian valinnanvaraa. Samoin myös digitaalisten sisämarkkinoiden strategian täytäntöönpanon väliarvioinnissa komissio korosti tarvetta huolehtia verkkoon liitettyjen tuotteiden ja järjestelmien turvallisuudesta ja totesi, että luomalla tieto- ja viestintätekniiikan turvallisuudelle eurooppalaiset puitteet, joissa annetaan säännöt tieto- ja viestintäteknologian turvallisuussertifiointin järjestämisestä unionissa, voitaisiin sekä ylläpitää luottamusta internetiin ja puuttua kyberturvallisuuden markkinoiden nykyiseen hajanaisuuteen.

Tarkistus 42

Ehdotus asetukseksi Johdanto-osan 50 kappale

Komission teksti

(50) Tieto- ja viestintätekniiikan tuotteiden ja palvelujen kyberturvallisuussertifiointia käytetään tällä hetkellä vain vähäisessä määrin. Kun sitä käytetään, käyttö rajoittuu enimmäkseen jäsenvaltioiden tasolle tai teollisuuslähtöisten järjestelmien piiriin. Tässä yhteydessä yhden kansallisen kyberturvallisuusviranomaisen myöntämää sertifiointia ei periaatteessa tunnusteta muissa jäsenvaltioissa. Yritykset voivat näin ollen joutua sertifiimaan tuotteensa ja palvelunsa useissa jäsenvaltioissa, joissa ne toimivat, esimerkiksi voidakseen osallistua kansallisiin hankintamenettelyihin. Syntymässä on uusia järjestelmiä, mutta vaikuttaa siltä, ettei ole olemassa johdonmukaista ja kokonaisvaltaista lähestymistapaa laaja-alaisiin kyberturvallisuuskysymyksiin esimerkiksi esineiden internetin alalla. Nykyisissä järjestelmissä on merkittäviä puutteita ja eroja, jotka liittyvät niiden tuotekatteeseen, varmuustasoihin, aineellisiin edellytyksiin ja tosiasialliseen käyttöön.

olevan hyödyllisen ja käyttökelpoisen kyberturvallisuusteknologian valinnanvaraa. Samoin myös digitaalisten sisämarkkinoiden strategian täytäntöönpanon väliarvioinnissa komissio korosti tarvetta huolehtia verkkoon liitettyjen tuotteiden ja järjestelmien turvallisuudesta ja totesi, että luomalla tieto- ja viestintätekniiikan turvallisuudelle eurooppalaiset puitteet, joissa annetaan säännöt tieto- ja viestintäteknologian turvallisuussertifiointin järjestämisestä unionissa, voitaisiin sekä ylläpitää luottamusta internetiin ja puuttua kyberturvallisuuden markkinoiden nykyiseen hajanaisuuteen.

Tarkistus

(50) Tieto- ja viestintätekniiikan tuotteiden, **prosessien** ja palvelujen kyberturvallisuussertifiointia käytetään tällä hetkellä vain vähäisessä määrin. Kun sitä käytetään, käyttö rajoittuu enimmäkseen jäsenvaltioiden tasolle tai teollisuuslähtöisten järjestelmien piiriin. Tässä yhteydessä yhden kansallisen kyberturvallisuusviranomaisen myöntämää sertifiointia ei periaatteessa tunnusteta muissa jäsenvaltioissa. Yritykset voivat näin ollen joutua sertifiimaan tuotteensa, **prosessinsa** ja palvelunsa useissa jäsenvaltioissa, joissa ne toimivat, esimerkiksi voidakseen osallistua kansallisiin hankintamenettelyihin, **mikä aiheuttaa yrityksille lisäkustannuksia**. Syntymässä on uusia järjestelmiä, mutta vaikuttaa siltä, ettei ole olemassa johdonmukaista ja kokonaisvaltaista lähestymistapaa laaja-alaisiin kyberturvallisuuskysymyksiin esimerkiksi esineiden internetin alalla. Nykyisissä järjestelmissä on merkittäviä puutteita ja eroja, jotka liittyvät niiden tuotekatteeseen, **riskiperusteisiin** varmuustasoihin,

aineellisiin edellytyksiin ja tosiasialliseen käyttöön. *Tämän osalta keskeinen tekijä on jäsenvaltioiden välinen vastavuoroinen tunnustaminen ja luottamus. ENISAn tärkeänä tehtävänä on auttaa jäsenvaltioita kehittämään vankka institutionaalinen rakenne ja asiantuntemus suojaautumisessa mahdollisia kyberhyökkäyksiä vastaan. Tarvitaan tapauskohtaista lähestymistapaa sen varmistamiseksi, että palveluihin, prosesseihin ja tuotteisiin sovelletaan asianmukaisia sertifiointijärjestelmiä. Lisäksi tarvitaan riskipainotteista lähestymistapaa riskien tehokasta tunnistamista ja lieventämistä varten, joskin samalla on tunnustettava, ettei ole mahdollista saada järjestelmää, jossa yhden ratkaisun oletetaan sopivan kaikille.*

Tarkistus 43

Ehdotus asetukseksi Johdanto-osan 52 kappale

Komission teksti

(52) Edellä esitetyn perusteella on tarpeen perustaa eurooppalainen kyberturvallisuuden sertifiointikehys, jossa vahvistetaan tärkeimmät horisontaaliset vaatimukset kehitettäville eurooppalaisille kyberturvallisuuden sertifiointijärjestelmille ja jonka ansiosta tieto- ja viestintätekniikan tuotteita ja palveluja koskevat sertifikaatit voidaan tunnustaa ja ottaa käyttöön kaikissa jäsenvaltioissa. Eurooppalaisen sertifiointikehysten tulisi palvella kahta tarkoitusta. Yhtäältä sen pitäisi lisätä luottamusta tieto- ja viestintätekniikan tuotteisiin ja palveluihin, jotka on sertifioitu tällaisten järjestelmien mukaisesti. Toisaalta sen avulla pitäisi välttää tilanne, jossa käytössä on monia keskenään ristiriitaisia tai päällekkäisiä kansallisia kyberturvallisuussertifiointeja, ja vähentää siten digitaalisilla

Tarkistus

(52) Edellä esitetyn perusteella on tarpeen **omaksua yhteinen lähestymistapa ja** perustaa eurooppalainen kyberturvallisuuden sertifiointikehys, jossa vahvistetaan tärkeimmät horisontaaliset vaatimukset kehitettäville eurooppalaisille kyberturvallisuuden sertifiointijärjestelmille ja jonka ansiosta tieto- ja viestintätekniikan tuotteita, **prosesseja** ja palveluja koskevat sertifikaatit voidaan tunnustaa ja ottaa käyttöön kaikissa jäsenvaltioissa. **Tässä yhteydessä on olennaista käyttää perustana nykyisiä kansallisia ja kansainvälisiä järjestelmiä sekä vastavuoroisen tunnustamisen järjestelmiä, erityisesti SOGIS-järjestelmää, sekä mahdollistaa sujuva siirtyminen tällaisten järjestelmien piiriin kuuluvista nykyisistä järjestelmistä eurooppalaisen kehysten mukaisiin**

sisämarkkinoilla yrityksille aiheutuvia kustannuksia. Järjestelmien olisi oltava syrjimättömiä ja kansainvälisiin ja/tai unionin standardeihin perustuvia, paitsi jos kyseiset standardit ovat tehottomia tai epäasianmukaisia EU:n oikeutettujen tavoitteiden saavuttamiseksi.

uusiin järjestelmiin. Eurooppalaisen sertifiointikehyksen tulisi palvella kahta tarkoitusta. Yhtäältä sen pitäisi lisätä luottamusta tieto- ja viestintätekniikan tuotteisiin, **prosesseihin** ja palveluihin, jotka on sertifioitu tällaisten järjestelmien mukaisesti. Toisaalta sen avulla pitäisi välttää tilanne, jossa käytössä on monia keskenään ristiriitaisia tai päällekkäisiä kansallisia kyberturvallisuussertifiointeja, ja vähentää siten digitaalisilla sisämarkkinoilla yrityksille aiheutuvia kustannuksia. **Jos kansallinen järjestelmä on korvattu eurooppalaisella kyberturvallisuussertifioinnilla, eurooppalaisen järjestelmän mukaan annetut sertifikaatit olisi hyväksyttävä päteviksi tapauksissa, joissa on edellytetty kansallisen järjestelmän mukaista sertifikaattia.** Järjestelmien olisi **perustuttava sisäänrakennetun turvallisuuden periaatteeseen ja asetuksessa (EU) 2016/679 tarkoitettuihin periaatteisiin.** Niiden olisi myös oltava syrjimättömiä ja kansainvälisiin ja/tai unionin standardeihin perustuvia, paitsi jos kyseiset standardit ovat tehottomia tai epäasianmukaisia EU:n oikeutettujen tavoitteiden saavuttamiseksi.

Tarkistus 44

Ehdotus asetukseksi
Johdanto-osan 52 a kappale (uusi)

Komission teksti

Tarkistus

(52 a) Eurooppalaisen kyberturvallisuuden sertifiointikehyksen on oltava yhdenmukainen kaikissa jäsenvaltioissa, jotta vältetään ”sertifiointihoppailu” jäsenvaltioiden erilaisten kustannusten tai vaatimustasojen vuoksi.

Tarkistus 45

Ehdotus asetukseksi
Johdanto-osan 52 b kappale (uusi)

Komission teksti

Tarkistus

(52 b) *Sertifiointijärjestelmien olisi perustuttava siihen, mikä on jo käytössä kansallisella ja kansainvälisellä tasolla, hyödynnettävä nykyisiä vahvuuksia sekä arvioitava ja korjattava heikkouksia.*

Tarkistus 46

Ehdotus asetukseksi Johdanto-osan 52 c kappale (uusi)

Komission teksti

Tarkistus

(52 c) *Tarvitaan joustavia kyberturvallisuusratkaisuja, jotta toimialalla olisi etumatkaa pahantahtoisiin hyökkäyksiin ja uhkiin nähden, joten sertifiointijärjestelmien olisi vältettävä nopean vanhentumisen riskit.*

Tarkistus 47

Ehdotus asetukseksi Johdanto-osan 53 kappale

Komission teksti

Tarkistus

(53) Komissiolle olisi siirrettävä valta hyväksyä eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät yksittäisille tieto- ja viestintätekniiikan tuotteiden ja palvelujen ryhmille. Kansallisten sertifioinnin valvontaviranomaisten olisi vastattava näiden järjestelmien täytäntöönpanosta ja valvonnasta, ja näissä järjestelmissä myönnettyjen sertifikaattien olisi oltava voimassa ja tunnustettuja kaikkialla unionissa. Toimialan tai muiden yksityisten organisaatioiden ylläpitämien sertifiointijärjestelmien ei tulisi kuulua tämän asetuksen soveltamisalaan. Tällaisia järjestelmiä ylläpitävät elimet voivat kuitenkin ehdottaa, että komissio ottaa tällaiset järjestelmät lähtökohdaksi niiden hyväksymiseksi eurooppalaisena

(53) Komissiolle olisi siirrettävä valta hyväksyä eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät yksittäisille tieto- ja viestintätekniiikan tuotteiden, **prosessien** ja palvelujen ryhmille. Kansallisten sertifioinnin valvontaviranomaisten olisi vastattava näiden järjestelmien täytäntöönpanosta ja valvonnasta, ja näissä järjestelmissä myönnettyjen sertifikaattien olisi oltava voimassa ja tunnustettuja kaikkialla unionissa. Toimialan tai muiden yksityisten organisaatioiden ylläpitämien sertifiointijärjestelmien ei tulisi kuulua tämän asetuksen soveltamisalaan. Tällaisia järjestelmiä ylläpitävät elimet voivat kuitenkin ehdottaa, että komissio ottaa tällaiset järjestelmät lähtökohdaksi niiden hyväksymiseksi eurooppalaisena

järjestelmänä.

järjestelmänä. *Viraston olisi yksilöitävä ja arvioitava toimialan tai yksityisten organisaatioiden ylläpitämiä järjestelmiä, jotta voidaan valita parhaat käytännöt, jotka voitaisiin ottaa osaksi eurooppalaista järjestelmää. Alan toimijat voivat suorittaa tuotteidensa tai palvelujensa itsearvioinnin ennen sertifiointia ja osoittaa näin, että niiden tuotteet tai palvelut ovat pyydettyessä tai tarvittaessa valmiita sertifiointiprosessiin.*

Tarkistus 48

Ehdotus asetukseksi Johdanto-osan 53 a kappale (uusi)

Komission teksti

Tarkistus

(53 a) Viraston ja komission olisi hyödynnettävä mahdollisimman laajasti EU:ssa ja/tai kansainvälisellä tasolla jo käytössä olevia sertifiointijärjestelmiä. ENISAn olisi voitava arvioida, mitkä jo käytössä olevat järjestelmät olisivat tarkoitukseen soveltuvia ja voitaisiin sisällyttää unionin lainsäädäntöön yhteistyössä EU:n standardointijärjestöjen kanssa ja olisivat mahdollisimman laajasti kansainvälisesti tunnustettuja. Jäsenvaltioiden olisi kerättävä nykyisiä hyviä käytäntöjä ja jaettava ne keskenään.

Tarkistus 49

Ehdotus asetukseksi Johdanto-osan 54 kappale

Komission teksti

Tarkistus

(54) Tämän asetuksen säännökset eivät saisi vaikuttaa unionin lainsäädäntöön, jossa annetaan erityiset säännöt tieto- ja viestintätekniikan tuotteiden ja palvelujen sertifioinnista. Erityisesti yleisessä tietosuoja-asetuksessa säädetään sertifiointimekanismeista sekä tietosuojasineteistä ja -merkeistä, joiden tarkoituksena on osoittaa, että

(54) Tämän asetuksen säännökset eivät saisi vaikuttaa unionin lainsäädäntöön, jossa annetaan erityiset säännöt tieto- ja viestintätekniikan tuotteiden, **prosessien** ja palvelujen sertifioinnista. Erityisesti yleisessä tietosuoja-asetuksessa säädetään sertifiointimekanismeista sekä tietosuojasineteistä ja -merkeistä, joiden tarkoituksena on osoittaa, että

rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat kyseistä asetusta käsittelytoimia suorittaessaan. Rekisteröityjen olisi tällaisten sertifiointimekanismien ja tietosuojasinettien ja -merkkien avulla voitava nopeasti arvioida asianomaisten tuotteiden ja palvelujen tietosuojataso. Tämä asetusta ei rajoita tietojenkäsittelytoimintojen sertifiointia yleisen tietosuojasetuksen mukaisesti, ei myöskään silloin, kun nämä toimet on sisällytetty tuotteisiin ja palveluihin.

Tarkistus 50

Ehdotus asetukseksi Johdanto-osan 55 kappale

Komission teksti

(55) Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien tarkoituksena olisi oltava varmistaa, että tällaisessa järjestelmässä sertifioidut tieto- ja viestintätekniikan tuotteet ja palvelut täyttävät määritellyt vaatimukset. Nämä vaatimukset koskevat kykyä suojautua tietyllä **varmuustasolla** toimilta, joiden tarkoituksena on vaarantaa tallennettujen, siirrettävien tai käsiteltävien tietojen tai niihin liittyvien kyseisissä tuotteissa, prosesseissa, palveluissa ja järjestelmissä tarjottavien tai välitettävien toimintojen tai palvelujen käytettävyys, aitous, eheys ja luottamuksellisuus tässä asetuksessa tarkoitettussa merkityksessä. Tässä asetuksessa ei ole mahdollista määrittellä yksityiskohtaisesti kyberturvallisuusvaatimuksia kaikille tieto- ja viestintätekniikan tuotteille ja palveluille. Tieto- ja viestintätekniikan tuotteet ja palvelut ja niihin liittyvät kyberturvallisuustarpeet ovat niin moninaiset, että on hyvin vaikeaa määrittellä yleisiä kyberturvallisuusvaatimuksia, jotka olisivat voimassa kaikkialla. Siksi kyberturvallisuus olisi määriteltävä laajasti ja yleisesti sertifiointitarkoituksia varten ja

rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat kyseistä asetusta käsittelytoimia suorittaessaan. Rekisteröityjen olisi tällaisten sertifiointimekanismien ja tietosuojasinettien ja -merkkien avulla voitava nopeasti arvioida asianomaisten tuotteiden ja palvelujen tietosuojataso. Tämä asetusta ei rajoita tietojenkäsittelytoimintojen sertifiointia yleisen tietosuojasetuksen mukaisesti, ei myöskään silloin, kun nämä toimet on sisällytetty tuotteisiin ja palveluihin.

Tarkistus

(55) Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien tarkoituksena olisi oltava varmistaa, että tällaisessa järjestelmässä sertifioidut tieto- ja viestintätekniikan tuotteet, palvelut ja **prosessit** täyttävät määritellyt vaatimukset. Nämä vaatimukset koskevat kykyä suojautua tietyllä **riskitasolla** toimilta, joiden tarkoituksena on vaarantaa tallennettujen, siirrettävien tai käsiteltävien tietojen tai niihin liittyvien kyseisissä tuotteissa, prosesseissa, palveluissa ja järjestelmissä tarjottavien tai välitettävien toimintojen tai palvelujen käytettävyys, aitous, eheys ja luottamuksellisuus tässä asetuksessa tarkoitettussa merkityksessä. Tässä asetuksessa ei ole mahdollista määrittellä yksityiskohtaisesti kyberturvallisuusvaatimuksia kaikille tieto- ja viestintätekniikan tuotteille, palveluille ja **prosesseille**. Tieto- ja viestintätekniikan tuotteet, palvelut ja **prosessit** ja niihin liittyvät kyberturvallisuustarpeet ovat niin moninaiset, että on hyvin vaikeaa määrittellä yleisiä kyberturvallisuusvaatimuksia, jotka olisivat voimassa kaikkialla. Siksi kyberturvallisuus olisi määriteltävä laajasti ja yleisesti sertifiointitarkoituksia varten ja

sitä olisi täydennettävä erityisillä kyberturvallisuustavoitteilla, jotka on tarpeen ottaa huomioon suunniteltaessa eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä. Se, miten tällaiset tavoitteet saavutetaan yksittäisissä tieto- ja viestintätekniikan tuotteissa ja palveluissa, olisi täsmennettävä yksityiskohtaisemmin komission hyväksymien yksittäisten sertifiointijärjestelmien tasolla, esimerkiksi viittaamalla standardeihin tai teknisiin eritelmiin.

sitä olisi täydennettävä erityisillä kyberturvallisuustavoitteilla, jotka on tarpeen ottaa huomioon suunniteltaessa eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä. Se, miten tällaiset tavoitteet saavutetaan yksittäisissä tieto- ja viestintätekniikan tuotteissa, palveluissa ja **prosesseissa**, olisi täsmennettävä yksityiskohtaisemmin komission hyväksymien yksittäisten sertifiointijärjestelmien tasolla, esimerkiksi viittaamalla standardeihin tai teknisiin eritelmiin. ***Kaikkia tietyn toimitusketjun toimijoita olisi rohkaistava kehittämään ja ottamaan käyttöön turvallisuusnormeja, teknisiä normeja sekä sisäänrakennetun turvallisuuden periaatteita kaikissa tuotteen, palvelun tai prosessin linkaaren vaiheissa. Kukin eurooppalainen kyberturvallisuuden sertifiointijärjestelmä olisi suunniteltava tämän mukaisesti.***

Tarkistus 51

Ehdotus asetukseksi Johdanto-osan 56 kappale

Komission teksti

(56) Komissiolle olisi annettava valtuudet pyytää ENISAA valmistelemaan yksittäisiä tieto- ja viestintätekniikan tuotteita tai palveluja varten ehdolla olevat järjestelmät. ***Edelleen komissiolle olisi annettava valtuudet hyväksyä ENISAn valmisteleman ehdolla olevan järjestelmän pohjalta eurooppalainen kyberturvallisuuden sertifiointijärjestelmä täytäntöönpanosäädöksillä.*** Kun otetaan huomioon tämän asetuksen yleinen tarkoitus ja siinä määritellyt turvallisuustavoitteet, ***komission hyväksymissä*** eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä olisi määriteltävä tietyt vähimmäistekijät yksittäisen järjestelmän kohteen, soveltamisalan ja toiminnan osalta. Näihin olisi sisällyttävä muun muassa

Tarkistus

(56) Komissiolle olisi annettava valtuudet pyytää ENISAA valmistelemaan yksittäisiä tieto- ja viestintätekniikan tuotteita, ***prosesseja*** tai palveluja varten ehdolla olevat järjestelmät ***perusteltujen syiden pohjalta, erityisesti kun on kyse sisämarkkinoita pirstaloivista kansallisista kyberturvallisuuden sertifiointijärjestelmistä, olemassa olevasta tai ennakoitavasta tarpeesta tukea unionin lainsäädäntöä tai jäsenvaltioiden sertifiointiryhmän tai sidosryhmien sertifiointiryhmän lausunnosta. Sen jälkeen kun komissio on arvioinut ENISAn komission pyynnöstä valmisteleman ehdolla olevat sertifiointijärjestelmät, komissiolle olisi annettava valtuudet hyväksyä eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät delegoiduilla***

kyberturvallisuussertifiointin soveltamisala ja kohde, mukaan lukien sertifiointin kattamat tieto- ja viestintätekniiikan tuotteiden ja palvelujen luokat, yksityiskohtainen eritelmä kyberturvallisuusvaatimuksista esimerkiksi viittaamalla standardeihin tai teknisiin eritelmiin, yksittäiset arviointiperusteet ja -menetelmät sekä aiottu varmuustaso: perustaso, korotettu ja/tai korkea.

säädöksillä. Kun otetaan huomioon tämän asetuksen yleinen tarkoitus ja siinä määritellyt turvallisuustavoitteet, **kyseisissä** eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä olisi määriteltävä tietyt vähimmäistekijät yksittäisen järjestelmän kohteen, soveltamisalan ja toiminnan osalta. Näihin olisi sisällyttävä muun muassa kyberturvallisuussertifiointin soveltamisala ja kohde, mukaan lukien sertifiointin kattamat tieto- ja viestintätekniiikan tuotteiden ja palvelujen luokat, yksityiskohtainen eritelmä kyberturvallisuusvaatimuksista esimerkiksi viittaamalla standardeihin tai teknisiin eritelmiin, yksittäiset arviointiperusteet ja -menetelmät sekä aiottu varmuustaso: perustaso, korotettu ja/tai korkea.

Tarkistus 52

Ehdotus asetukseksi Johdanto-osan 56 a kappale (uusi)

Komission teksti

Tarkistus

(56 a) Viraston olisi oltava eurooppalaisia kyberturvallisuusjärjestelmiä koskevan tiedon viitekeskus. Sen olisi ylläpidettävä verkkosivustoa, jossa on kaikki asiaankuuluvat tiedot, myös peruutetuista ja vanhentuneista sertifikaateista ja sertifiointijärjestelmän kattamista kansallisista sertifioinneista. Viraston olisi varmistettava, että riittävä osa sen verkkosivuston sisällöstä on tavallisten kuluttajien ymmärrettävissä.

Tarkistus 53

Ehdotus asetukseksi Johdanto-osan 56 b kappale (uusi)

Komission teksti

Tarkistus

(56 b) Varmuustason määrittely sertifikaateissa on tarpeen, jotta

loppukäyttäjää saa viitteen siitä, minkätyyppisiä odotettuja kyberuhkia tuotteen, prosessin tai palvelun kyberturvallisuustoimenpiteillä pyritään estämään. Kyberuhat on määriteltävä ottaen huomioon odotettavissa oleva riski sekä hyökkäyksen tekijän tai tekijöiden valmiudet sertifiointin kattamien tieto- ja viestintätekniikan tuotteiden, prosessien ja palvelujen oletetun käytön yhteydessä. Varmuustasolla ”perustaso” tarkoitetaan valmiuksia suojautua hyökkäyksiltä, jotka voidaan välttää perustason kyberturvallisuustoimenpiteillä ja jotka voidaan tarkistaa vaivattomasti tarkastelemalla teknisiä asiakirjoja. Varmuustasolla ”korotettu” tarkoitetaan valmiuksia suojautua tunnetuilta hyökkäyksiltä, joiden tekijän taso on melko kehittynyt mutta jonka resurssit ovat rajalliset. Varmuustasolla ”korkea” tarkoitetaan valmiuksia suojautua ennalta tuntemattomilta haavoittuvuuksilta ja pitkälle kehitetyiltä hyökkäyksiltä, joihin liittyy uusinta teknologiaa ja huomattavat resurssit, kuten rahoitusta saavia monialaisia ryhmiä.

Tarkistus 54

Ehdotus asetukseksi Johdanto-osan 56 c kappale (uusi)

Komission teksti

Tarkistus

(56 c) Jotta voidaan välttää kansallisista kyberturvallisuusjärjestelmistä johtuvaa sisämarkkinoiden hajanaisuutta, tukea tulevaa lainsäädäntöä sekä lisätä luottamusta ja turvallisuutta, komissiolle olisi siirrettävä valta hyväksyä Euroopan unionin toiminnasta tehdyn sopimuksen 290 artiklan mukaisesti säädöksiä, jotka koskevat eurooppalaisten kyberturvallisuussertifiointin painopisteiden vahvistamista, jatkuvan ohjelman hyväksymistä ja eurooppalaisten sertifiointijärjestelmien hyväksymistä. On erityisen tärkeää, että

komissio asiaa valmistellessaan toteuttaa asianmukaiset kuulemiset, myös asiantuntijatasolla, ja että nämä kuulemiset toteutetaan paremmasta lainsäädännöstä 13 päivänä huhtikuuta 2016 tehdyssä toimitusten sopimuksessa vahvistettujen periaatteiden mukaisesti. Jotta voitaisiin erityisesti varmistaa tasavertainen osallistuminen delegoitujen säädösten valmisteluun, Euroopan parlamentille ja neuvostolle toimitetaan kaikki asiakirjat samaan aikaan kuin jäsenvaltioiden asiantuntijoille, ja Euroopan parlamentin ja neuvoston asiantuntijoilla on järjestelmällisesti oikeus osallistua komission asiantuntijaryhmien kokouksiin, joissa valmistellaan delegoituja säädöksiä.

Tarkistus 55

Ehdotus asetukseksi Johdanto-osan 56 d kappale (uusi)

Komission teksti

Tarkistus

(56 d) Kuhunkin eurooppalaiseen kyberturvallisuuden sertifiointijärjestelmään liittyvissä arviointimenetelmissä ja -menettelyissä olisi edistettävä unionin tasolla eettistä hakkerointia, jonka tavoitteena on paikantaa laitteiden ja tietojärjestelmien heikkoudet ja haavoittuvuudet ennakoimalla pahantahtoisten hakkereiden aikomat toimet ja taidot.

Tarkistus 56

Ehdotus asetukseksi Johdanto-osan 57 kappale

Komission teksti

Tarkistus

(57) Eurooppalaisen kyberturvallisuussertifiointin käytön tulisi edelleen olla vapaaehtoista, jollei toisin säädetä unionin tai kansallisessa

(57) Eurooppalaisen kyberturvallisuussertifiointin käytön tulisi edelleen olla vapaaehtoista, jollei toisin säädetä unionin tai kansallisessa

lainsäädännössä. Jotta voitaisiin kuitenkin saavuttaa tämän asetuksen tavoitteet ja välttää hajanaisuus sisämarkkinoilla, sellaisten kansallisten kyberturvallisuuden sertifiointijärjestelmien tai -menettelyjen, joiden kattamat tieto- ja viestintätekniikan tuotteet ja palvelut kuuluvat jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, olisi lakattava tuottamasta oikeusvaikutuksia alkaen päivästä, jonka komissio vahvistaa **täytäntöönpanosäädöksessä**. Jäsenvaltiot eivät myöskään saisi ottaa käyttöön uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä tieto- ja viestintätekniikan tuotteille ja palveluille, jotka kuuluvat jo jonkin olemassa olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan.

Tarkistus 57

Ehdotus asetukseksi Johdanto-osan 57 a kappale (uusi)

Komission teksti

lainsäädännössä. Jotta voitaisiin kuitenkin saavuttaa tämän asetuksen tavoitteet ja välttää hajanaisuus sisämarkkinoilla, sellaisten kansallisten kyberturvallisuuden sertifiointijärjestelmien tai -menettelyjen, joiden kattamat tieto- ja viestintätekniikan tuotteet, **prosessit** ja palvelut kuuluvat jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, olisi lakattava tuottamasta oikeusvaikutuksia alkaen päivästä, jonka komissio vahvistaa **delegoidussa säädöksessä**. Jäsenvaltiot eivät myöskään saisi ottaa käyttöön uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä tieto- ja viestintätekniikan tuotteille ja palveluille, jotka kuuluvat jo jonkin olemassa olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan. **Tämä asetus ei kuitenkaan saisi vaikuttaa kansallisiin järjestelmiin, jotka kattavat tieto- ja viestintätekniikan tuotteet, prosessit ja palvelut, joita käytetään jäsenvaltioiden tarpeisiin aloilla, joista ne ovat yksin vastuussa.**

Tarkistus

(57 a) Velvollisuus antaa tuotetta koskeva ilmoitus, joka sisältää jäsenneiltyä tietoa tuotteen, prosessin tai palvelun sertifioinnista, otetaan käyttöön, jotta kuluttajat saisivat enemmän tietoa ja voisivat tehdä perustellun valinnan.

Tarkistus 58

Ehdotus asetukseksi Johdanto-osan 57 b kappale (uusi)

Komission teksti

Tarkistus

(57 b) Uusia eurooppalaisia

kyberturvallisuusjärjestelmiä ehdottaessaan ENISAn ja muiden asiaankuuluvien elinten olisi kiinnitettävä asianmukaista huomiota ehdotuksen kilpailudynamiikkaan ja varmistettava erityisesti, että kun kyseisellä alalla on paljon pieniä ja keskisuuria yrityksiä, esimerkiksi ohjelmistokehittämisen alalla, sertifiointijärjestelmät eivät muodosta estettä uusille yrityksille ja innovoinnille.

Tarkistus 59

Ehdotus asetukseksi Johdanto-osan 57 c kappale (uusi)

Komission teksti

Tarkistus

(57 c) Eurooppalaiset kyberturvallisuusjärjestelmät auttavat yhdenmukaistamaan ja yhdentämään kyberturvallisuuskäytäntöjä unionissa. Niistä ei kuitenkaan pidä tulla kyberturvallisuuden vähimmäistasoa. Eurooppalaisten kyberturvallisuusjärjestelmien suunnittelussa olisi otettava huomioon myös kyberturvallisuusalan uusien innovaatioiden kehittäminen ja mahdollistettava ne.

Tarkistus 60

Ehdotus asetukseksi Johdanto-osan 58 kappale

Komission teksti

Tarkistus

(58) Kun eurooppalainen kyberturvallisuuden sertifiointijärjestelmä on hyväksytty, tieto- ja viestintätekniikan tuotteiden valmistajien tai tieto- ja viestintätekniikan palvelujen tarjoajien olisi voitava jättää tuotteidensa tai palvelujensa sertifiointia koskeva hakemus valitsemalleen vaatimustenmukaisuuden arviointilaitokselle. Vaatimustenmukaisuuden arviointilaitosten olisi saatava akkreditointi

(58) Kun eurooppalainen kyberturvallisuuden sertifiointijärjestelmä on hyväksytty, tieto- ja viestintätekniikan tuotteiden valmistajien tai tieto- ja viestintätekniikan *prosessien tai* palvelujen tarjoajien olisi voitava jättää tuotteidensa tai palvelujensa sertifiointia koskeva hakemus valitsemalleen vaatimustenmukaisuuden arviointilaitokselle *kaikkialla unionissa*. Vaatimustenmukaisuuden arviointilaitosten

akkreditointielimeltä, jos ne täyttävät tässä asetuksessa vahvistetut tietyt erityiset vaatimukset. Akkreditointi olisi myönnettävä enintään viideksi vuodeksi, ja se voidaan uusida samoin edellytyksin, jos vaatimustenmukaisuuden arviointilaitos täyttää vaatimukset. Akkreditointielimen olisi peruutettava vaatimustenmukaisuuden arviointilaitoksen akkreditointi, jos akkreditoinnin edellytykset eivät täyty tai eivät enää täyty tai jos vaatimustenmukaisuuden arviointilaitoksen toiminta rikkoo tämän asetuksen säännöksiä.

olisi saatava akkreditointi akkreditointielimeltä, jos ne täyttävät tässä asetuksessa vahvistetut tietyt erityiset vaatimukset. Akkreditointi olisi myönnettävä enintään viideksi vuodeksi, ja se voidaan uusida samoin edellytyksin, jos vaatimustenmukaisuuden arviointilaitos täyttää vaatimukset. Akkreditointielimen olisi peruutettava vaatimustenmukaisuuden arviointilaitoksen akkreditointi, jos akkreditoinnin edellytykset eivät täyty tai eivät enää täyty tai jos vaatimustenmukaisuuden arviointilaitoksen toiminta rikkoo tämän asetuksen säännöksiä. ***Viraston olisi toteutettava tarkastuksia vaatimustenmukaisuuden arviointilaitosten yhtäläisen laatu- ja tarkkuustason varmistamiseksi, jotta voidaan välttää sääntelyerojen hyväksikäyttö. Tulokset olisi ilmoitettava virastolle, komissiolle ja parlamentille ja asetettava julkisesti saataville.***

Tarkistus 61

Ehdotus asetukseksi Johdanto-osan 58 a kappale (uusi)

Komission teksti

Tarkistus

(58 a) Eurooppalaisen kyberturvallisuussertifiointin pakollinen käyttö olisi rajoitettava tapauksiin, joissa toimialalle, kansalaisille ja kuluttajille aiheutuvat kustannukset voidaan perustella riskianalyysillä. Keskeisiä palveluja häiritsevät poikkeamat voivat haitata taloudellisen toiminnan harjoittamista, aiheuttaa huomattavia taloudellisia tappioita, heikentää käyttäjien luottamusta ja aiheuttaa merkittävää vahinkoa unionin taloudelle. Keskeisten palvelujen tarjoajia koskeva eurooppalaisen kyberturvallisuussertifiointin pakollinen käyttö olisi rajoitettava niihin tekijöihin, jotka ovat niiden toiminnan kannalta ratkaisevan tärkeitä, eikä sitä saisi ulottaa yleisluonteisiin tuotteisiin, prosesseihin ja

palveluihin, mikä aiheuttaisi perusteettomia kustannuksia toimialalle ja kuluttajille. Komission olisi tehtävä yhteistyötä direktiivin (EU) 2016/1148 11 artiklan mukaisesti perustetun yhteistyöryhmän kanssa, jotta voidaan määrittää luettelo sellaisten tuotteiden, prosessien ja palvelujen luokista, jotka on nimenomaisesti tarkoitettu keskeisten palvelujen tarjoajien käyttöön ja joiden toimintahäiriöt turvallisuuspoikkeamien aikana voivat vaikuttaa erittäin haitallisesti keskeiseen palveluun. Kyseinen luettelo olisi laadittava asteittain ja sitä olisi päivitettävä tarpeen vaatiessa. Ainoastaan tässä luettelossa olevien tuotteiden, prosessien ja palveluiden olisi oltava pakollisia keskeisten palveluiden tarjoajille.

Tarkistus 62

**Ehdotus asetukseksi
Johdanto-osan 58 b kappale (uusi)**

Komission teksti

Tarkistus

(58 b) Kansallisessa lainsäädännössä olevat viittaukset kansallisiin standardeihin, joiden oikeusvaikutukset ovat lakanneet eurooppalaisen sertifiointijärjestelmän tultua voimaan, voivat mahdollisesti aiheuttaa sekaannusta valmistajien ja loppukäyttäjien keskuudessa. Jotta voidaan välttää se, että valmistajat jatkavat lakkautettujen kansallisten sertifikaattien mukaisten eritelmiä soveltamista, jäsenvaltioiden olisi perussopimusten mukaisten velvoitteiden mukaan mukautettava kansallista lainsäädäntöään vastaamaan eurooppalaista sertifiointijärjestelmää.

Tarkistus 63

**Ehdotus asetukseksi
Johdanto-osan 59 kappale**

(59) On tarpeen velvoittaa kaikki jäsenvaltiot nimeämään yksi kyberturvallisuussertifiointin valvontaviranomainen valvomaan sitä, ovatko niiden alueelle sijoittautuneet vaatimustenmukaisuuden arviointilaitokset ja niiden myöntämät sertifikaatit tämän asetuksen vaatimusten ja asianomaisten kyberturvallisuuden sertifiointijärjestelmien vaatimusten mukaisia. Kansallisten sertifiointin valvontaviranomaisten olisi käsiteltävä luonnollisten tai oikeushenkilöiden tekemät valitukset, jotka liittyvät niiden alueelle sijoittautuneiden vaatimustenmukaisuuden arviointilaitosten myöntämiin sertifikaatteihin, tutkittava asianmukaisessa määrin valituksen kohde ja ilmoitettava valituksen tekijälle tutkinnan etenemisestä ja tuloksesta kohtuullisessa ajassa. Lisäksi niiden olisi tehtävä yhteistyötä muiden kansallisten sertifiointin valvontaviranomaisten tai muiden viranomaisten kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniikan tuotteet ja palvelut eivät vastaa tämän asetuksen tai yksittäisten **kyberturvallisuusjärjestelmien** vaatimuksia.

(59) On tarpeen velvoittaa kaikki jäsenvaltiot nimeämään yksi kyberturvallisuussertifiointin valvontaviranomainen valvomaan sitä, ovatko niiden alueelle sijoittautuneet vaatimustenmukaisuuden arviointilaitokset ja niiden myöntämät sertifikaatit tämän asetuksen vaatimusten ja asianomaisten kyberturvallisuuden sertifiointijärjestelmien vaatimusten mukaisia, **ja varmistamaan, että eurooppalaiset kyberturvallisuussertifikaatit tunnustetaan niiden alueilla.** Kansallisten sertifiointin valvontaviranomaisten olisi käsiteltävä luonnollisten tai oikeushenkilöiden tekemät valitukset, jotka liittyvät niiden alueelle sijoittautuneiden vaatimustenmukaisuuden arviointilaitosten myöntämiin sertifikaatteihin **tai väitettyihin sertifikaattien tunnustamatta jättämisiin alueellaan,** tutkittava asianmukaisessa määrin valituksen kohde ja ilmoitettava valituksen tekijälle tutkinnan etenemisestä ja tuloksesta kohtuullisessa ajassa. Lisäksi niiden olisi tehtävä yhteistyötä muiden kansallisten sertifiointin valvontaviranomaisten tai muiden viranomaisten kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniikan tuotteet, **prosessit** ja palvelut eivät vastaa tämän asetuksen tai yksittäisten **kyberturvallisuusjärjestelmien** vaatimuksia **tai joissa eurooppalaisia kyberturvallisuussertifikaatteja ei tunnusteta. Näiden olisi myös valvottava ja tarkistettava, että itse annetut vaatimustenmukaisuusvakuutukset ovat vaatimusten mukaisia ja että vaatimustenmukaisuuden arviointilaitosten myöntämät eurooppalaiset kyberturvallisuussertifikaatit ovat tässä asetuksessa esitettyjen vaatimusten mukaisia sekä Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien sääntöjen ja vastaavan**

eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimusten mukaisia. Kansallisten sertifiointin valvontaviranomaisten tehokas yhteistyö on olennaista eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien sekä tieto- ja viestintäteknikan tuotteiden ja palvelujen kyberturvallisuutta koskevien teknisten seikkojen asianmukaisen täytäntöönpanon kannalta. Komission olisi helpotettava tätä tietojen vaihtoa asettamalla saataville yleinen sähköinen tietotukijärjestelmä, esimerkiksi markkinavalvontaa koskeva tieto- ja viestintäjärjestelmä (ICSMS) tai tuoteturvallisuutta koskeva EU:n nopea tiedonvaihtojärjestelmä (RAPEX), joita markkinavalvontaviranomaiset jo käyttävät asetuksen (EY) N:o 765/2008 mukaisesti.

Tarkistus 64

Ehdotus asetukseksi Johdanto-osan 60 kappale

Komission teksti

(60) Eurooppalaisen kyberturvallisuuden sertifiointikehyksen johdonmukaisen soveltamisen varmistamiseksi olisi perustettava **Euroopan kyberturvallisuuden** sertifiointiryhmä, **jäljempänä 'sertifiointiryhmä'**, joka koostuu kansallisista sertifiointin valvontaviranomaisista. Ryhmän päätehtävinä tulisi olla neuvoa ja avustaa komissiota sen pyrkiessä varmistamaan eurooppalaisen kyberturvallisuuden sertifiointikehyksen yhdenmukaisen täytäntöönpanon ja soveltamisen, avustaa virastoa ehdolla olevien kyberturvallisuuden sertifiointijärjestelmien valmistelussa tiiviissä yhteistyössä sen kanssa, suosittaa, että komissio pyytää virastoa valmistelevaan ehdolla olevan eurooppalaisen kyberturvallisuuden

Tarkistus

(60) Eurooppalaisen kyberturvallisuuden sertifiointikehyksen johdonmukaisen soveltamisen varmistamiseksi olisi perustettava **jäsenvaltioiden** sertifiointiryhmä, joka koostuu kansallisista sertifiointin valvontaviranomaisista. Ryhmän päätehtävinä tulisi olla neuvoa ja avustaa komissiota sen pyrkiessä varmistamaan eurooppalaisen kyberturvallisuuden sertifiointikehyksen yhdenmukaisen täytäntöönpanon ja soveltamisen, avustaa virastoa ehdolla olevien kyberturvallisuuden sertifiointijärjestelmien valmistelussa tiiviissä yhteistyössä sen kanssa, suosittaa, että komissio pyytää virastoa valmistelevaan ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän, sekä antaa

sertifiointijärjestelmän, sekä antaa komissiolle osoitettuja lausuntoja voimassa olevien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien ylläpitämisestä ja tarkistamisesta.

Tarkistus 65

Ehdotus asetukseksi Johdanto-osan 60 a kappale (uusi)

Komission teksti

komissiolle osoitettuja lausuntoja voimassa olevien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien ylläpitämisestä ja tarkistamisesta.

Tarkistus

(60 a) Vaatimustenmukaisuuden arviointilaitosten pätevyyden samantasoisuuden varmistamiseksi, vastavuoroisen tunnustamisen helpottamiseksi sekä vaatimustenmukaisuuden arviointilaitosten antamien sertifikaattien ja vaatimustenmukaisuuden arviointitulosten yleisen tunnustamisen edistämiseksi kansallisilla sertifioinnin valvontaviranomaisilla on oltava käytössä perusteellinen ja avoin vertaisarviointijärjestelmä ja niiden on oltava arvioinnin kohteena säännöllisesti.

Tarkistus 66

Ehdotus asetukseksi Johdanto-osan 60 b kappale (uusi)

Komission teksti

Tarkistus

(60 b) Kansallisten sertifioinnin valvontaviranomaisten välinen tehokas yhteistyö on oleellista vertaisarvioinnin asianmukaisen toiminnan kannalta sekä silloin, kun on kyse rajatylittävästä akkreditoinnista. Avoimuuden varmistamiseksi on tarpeen säätää kansallisten sertifioinnin valvontaviranomaisten velvollisuudesta vaihtaa tietoja keskenään ja toimittaa asiaankuuluvat tiedot kansallisille viranomaisille ja komissiolle. Kansallisten akkreditointielinten hoitamien

akkreditointipalvelujen saatavuutta koskevat päivitetty ja paikkansapitävät tiedot olisi myös saatettava yleisesti saataville ja niiden olisi siksi oltava etenkin vaatimuksenmukaisuuden arviointilaitosten käytettävissä.

Tarkistus 67

Ehdotus asetukseksi Johdanto-osan 61 kappale

Komission teksti

(61) Tietoisuuden lisäämiseksi ja tulevien EU:n kyberturvallisuusjärjestelmien hyväksymisen helpottamiseksi Euroopan komissio voi antaa yleisiä tai alakohtaisia kyberturvallisuutta koskevia suuntaviivoja esimerkiksi hyvistä kyberturvallisuuskäytännöistä tai vastuullisesta kyberturvallisuuskäyttäytymisestä korostaen sertifioitujen tieto- ja viestintätekniikan tuotteiden ja palvelujen käytön myönteistä vaikutusta.

Tarkistus

(61) Tietoisuuden lisäämiseksi ja tulevien EU:n kyberturvallisuusjärjestelmien hyväksymisen helpottamiseksi Euroopan komissio voi antaa yleisiä tai alakohtaisia kyberturvallisuutta koskevia suuntaviivoja esimerkiksi hyvistä kyberturvallisuuskäytännöistä tai vastuullisesta kyberturvallisuuskäyttäytymisestä korostaen sertifioitujen tieto- ja viestintätekniikan tuotteiden, ***prosessien*** ja palvelujen käytön myönteistä vaikutusta.

Tarkistus 68

Ehdotus asetukseksi Johdanto-osan 63 kappale

Komission teksti

(63) Jotta voidaan täsmentää tarkemmin kriteerit vaatimustenmukaisuuden arviointilaitosten akkreditointia varten, komissiolle olisi siirrettävä valta hyväksyä säädösvalan siirron nojalla annettavia delegoituja säädöksiä Euroopan unionin toiminnasta tehdyn sopimuksen 290 artiklan mukaisesti. Komissio järjestää valmistelutyönsä aikana asianmukaisia kuulemisia, myös asiantuntijatasolla. Nämä kuulemiset toteutetaan paremmasta lainsäädännöstä 13 päivänä huhtikuuta 2016 tehdyssä toimielinten välisessä sopimuksessa vahvistettujen periaatteiden mukaisesti. Jotta voitaisiin erityisesti

Tarkistus

(63) Jotta voidaan täsmentää tarkemmin kriteerit vaatimustenmukaisuuden arviointilaitosten akkreditointia varten, komissiolle olisi siirrettävä valta hyväksyä säädösvalan siirron nojalla annettavia delegoituja säädöksiä Euroopan unionin toiminnasta tehdyn sopimuksen 290 artiklan mukaisesti. Komissio järjestää valmistelutyönsä aikana asianmukaisia kuulemisia, myös asiantuntijatasolla ***ja tarvittaessa asianomaisten sidosryhmien kanssa***. Nämä kuulemiset toteutetaan paremmasta lainsäädännöstä 13 päivänä huhtikuuta 2016 tehdyssä toimielinten välisessä sopimuksessa vahvistettujen

varmistaa tasavertainen osallistuminen delegoitujen säädösten valmisteluun, Euroopan parlamentille ja neuvostolle toimitetaan kaikki asiakirjat samaan aikaan kuin jäsenvaltioiden asiantuntijoille, ja Euroopan parlamentin ja neuvoston asiantuntijoilla on järjestelmällisesti oikeus osallistua komission asiantuntijaryhmien kokouksiin, joissa valmistellaan delegoituja säädöksiä.

periaatteiden mukaisesti. Jotta voitaisiin erityisesti varmistaa tasavertainen osallistuminen delegoitujen säädösten valmisteluun, Euroopan parlamentille ja neuvostolle toimitetaan kaikki asiakirjat samaan aikaan kuin jäsenvaltioiden asiantuntijoille, ja Euroopan parlamentin ja neuvoston asiantuntijoilla on järjestelmällisesti oikeus osallistua komission asiantuntijaryhmien kokouksiin, joissa valmistellaan delegoituja säädöksiä.

Tarkistus 69

Ehdotus asetukseksi Johdanto-osan 65 kappale

Komission teksti

(65) *Olisi sovellettava tarkastusmenettelyä hyväksyttäessä täytäntöönpanosäädöksiä*, jotka koskevat tieto- ja viestintätekniikan tuotteiden ja palvelujen eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä, viraston tutkimusten toteuttamista koskevia yksityiskohtaisia sääntöjä sekä kansallisten sertifiointin valvontaviranomaisten komissiolle tekemien, akkreditoitujen vaatimustenmukaisuuden arviointilaitoksia koskevien ilmoitusten olosuhteita, muutoseikkoja ja menettelyjä.

Tarkistus

(65) *Lisäksi voidaan hyväksyä delegoituja säädöksiä*, jotka koskevat tieto- ja viestintätekniikan tuotteiden, *prosessien* ja palvelujen eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä, viraston tutkimusten toteuttamista koskevia yksityiskohtaisia sääntöjä sekä kansallisten sertifiointin valvontaviranomaisten komissiolle tekemien, akkreditoitujen vaatimustenmukaisuuden arviointilaitoksia koskevien ilmoitusten olosuhteita, muutoseikkoja ja menettelyjä.

Tarkistus 70

Ehdotus asetukseksi Johdanto-osan 66 kappale

Komission teksti

(66) Viraston toimintaa olisi arvioitava riippumattomasti. Arvioinnissa olisi otettava huomioon viraston tavoitteiden saavuttaminen, sen toimintatavat ja sen tehtävien merkityksellisyys. *Arvioinnissa olisi myös arvioitava eurooppalaisen kyberturvallisuuden sertifiointikehyksen vaikutusta, vaikuttavuutta ja tehokkuutta.*

Tarkistus

(66) Viraston toimintaa olisi arvioitava *jatkuvasti ja* riippumattomasti. Arvioinnissa olisi otettava huomioon viraston tavoitteiden saavuttaminen, sen toimintatavat ja sen tehtävien merkityksellisyys, *erityisesti sen koordinoititehtävä jäsenvaltioihin ja niiden kansallisiin viranomaisiin nähden. Uudelleentarkastelun yhteydessä*

komission olisi arvioitava viraston mahdollisuutta toimia jäsenvaltioiden sekä EU:n toimielinten ja elinten keskitettynä verkkoportaalina.

Tarkistus 71

Ehdotus asetukseksi Johdanto-osan 66 a kappale (uusi)

Komission teksti

Tarkistus

(66 a) Arvioinnissa olisi myös arvioitava eurooppalaisen kyberturvallisuuden sertifiointikehyksen vaikutusta, vaikuttavuutta ja tehokkuutta. Uudelleentarkastelun yhteydessä komissio voisi arvioida viraston roolia unionin markkinoille tulevien kolmansien maiden tuotteiden ja palveluiden arvioinnissa ja mahdollisuutta asettaa mustalle listalle yrityksiä, jotka eivät noudata unionin sääntöjä.

Tarkistus 72

Ehdotus asetukseksi Johdanto-osan 66 b kappale (uusi)

Komission teksti

Tarkistus

(66 b) Arvioinnissa olisi analysoitava unionissa myytävien tuotteiden ja palveluiden kyberturvallisuuden tasoa. Uudelleentarkastelun yhteydessä komission olisi arvioitava, asetetaanko kyberturvallisuuden keskeiset vaatimukset ehdoksi sisämarkkinoille pääsulle.

Tarkistus 73

Ehdotus asetukseksi 1 artikla – 1 kohta – a alakohta

Komission teksti

Tarkistus

a) vahvistetaan ”*EU:n kyberturvallisuusviraston*” *ENISAn*, jäljempänä ’virasto’, tavoitteet, tehtävät ja

a) vahvistetaan ”*Euroopan unionin verkko- ja tietoturaviraston*”, jäljempänä ’virasto’, tavoitteet, tehtävät ja

organisatoriset näkökohdat **ja**

organisatoriset näkökohdat ja

Tarkistus 74

Ehdotus asetukseksi 1 artikla – 1 kohta – b alakohta

Komission teksti

b) vahvistetaan kehys eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perustamiselle, jotta voidaan varmistaa riittävántasoinen kyberturvallisuus tieto- ja viestintäteknikan tuotteille ja palveluille unionissa. Tämän kehyksen soveltaminen ei rajoita niiden erityisten säännösten soveltamista, jotka koskevat vapaaehtoista ***tai*** pakollista sertifiointia ***muiden unionin säädösten nojalla.***

Tarkistus

b) vahvistetaan kehys eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perustamiselle, jotta voidaan ***välttää sertifiointijärjestelmien hajanaisuus unionissa ja*** varmistaa riittävántasoinen kyberturvallisuus tieto- ja viestintäteknikan tuotteille, ***prosesseille*** ja palveluille unionissa. Tämän kehyksen soveltaminen ei rajoita niiden erityisten säännösten soveltamista, jotka koskevat vapaaehtoista ***ja tarvittaessa*** pakollista sertifiointia, ***siltä osin kuin tässä asetuksessa niin säädetään*** tai muiden unionin säädösten nojalla.

Tarkistus 75

Ehdotus asetukseksi 1 artikla – 1 a kohta (uusi)

Komission teksti

Virasto hoitaa tehtävänsä siten, että se ei rajoita kyberturvallisuutta koskevaa jäsenvaltioiden toimivaltaa eikä varsinkaan jäsenvaltioiden toimivaltaa, joka koskee yleistä turvallisuutta, puolustusta, kansallista turvallisuutta ja rikosoikeutta.

Tarkistus

Tarkistus 76

Ehdotus asetukseksi 2 artikla – 1 kohta – 1 alakohta

Komission teksti

1) 'kyberturvallisuudella' kaikkia toimia, joita tarvitaan verkko- ja

Tarkistus

(Tarkistus ei vaikuta suomenkieliseen

tietojärjestelmien, niiden käyttäjien ja asianosaisten henkilöiden suojaamiseksi kyberuhilta;

versioon.)

Tarkistus 77

Ehdotus asetukseksi 2 artikla – 1 kohta – 2 alakohta

Komission teksti

2) ’verkko- ja tietojärjestelmällä’ direktiivin (EU) 2016/1148 4 artiklan 1 kohdassa **tarkoitettua järjestelmää**;

Tarkistus

2) ’verkko- ja tietojärjestelmällä’ direktiivin (EU) 2016/1148 4 artiklan 1 kohdassa **määriteltyä verkko- ja tietojärjestelmää**;

Tarkistus 78

Ehdotus asetukseksi 2 artikla – 1 kohta – 3 alakohta

Komission teksti

3) ’verkko- ja tietojärjestelmien turvallisuutta koskevalla kansallisella strategialla’ direktiivin (EU) 2016/1148 4 artiklan 3 kohdassa **tarkoitettua kehystä**;

Tarkistus

3) ’verkko- ja tietojärjestelmien turvallisuutta koskevalla kansallisella strategialla’ direktiivin (EU) 2016/1148 4 artiklan 3 kohdassa **määriteltyä verkko- ja tietojärjestelmien turvallisuutta koskevaa kansallista strategiaa**;

Tarkistus 79

Ehdotus asetukseksi 2 artikla – 1 kohta – 4 alakohta

Komission teksti

4) ’keskeisten palvelujen tarjoajalla’ direktiivin (EU) N:o 2016/1148 4 artiklan 4 kohdassa määriteltyä **julkista tai yksityistä toimijaa**;

Tarkistus

4) ’keskeisten palvelujen tarjoajalla’ direktiivin (EU) N:o 2016/1148 4 artiklan 4 kohdassa määriteltyä **keskeisten palvelujen tarjoajaa**;

Tarkistus 80

Ehdotus asetukseksi 2 artikla – 1 kohta – 5 alakohta

Komission teksti

5) 'digitaalisen palvelun tarjoajalla' direktiivin (EU) N:o 2016/1148 4 artiklan 6 kohdassa määriteltyä digitaalisen palvelun **tarjoavaa oikeushenkilöä**;

Tarkistus 81

Ehdotus asetukseksi
2 artikla – 1 kohta – 6 alakohta

Komission teksti

6) 'poikkeamalla' direktiivin (EU) N:o 2016/1148 4 artiklan 7 kohdassa määriteltyä tapahtumaa;

Tarkistus 82

Ehdotus asetukseksi
2 artikla – 1 kohta – 7 alakohta

Komission teksti

7) 'poikkeamien käsittelyllä' direktiivin (EU) N:o 2016/1148 4 artiklan 8 kohdassa määriteltyä **menettelyä**;

Tarkistus 83

Ehdotus asetukseksi
2 artikla – 1 kohta – 8 alakohta

Komission teksti

8) 'kyberuhalla' potentiaalista tilannetta tai tapahtumaa, joka voi vaikuttaa haitallisesti verkko- ja tietojärjestelmiin, niiden käyttäjiin ja asianosaisiin henkilöihin;

Tarkistus 84

Ehdotus asetukseksi
2 artikla – 1 kohta – 8 a alakohta (uusi)

Tarkistus

5) 'digitaalisen palvelun tarjoajalla' direktiivin (EU) N:o 2016/1148 4 artiklan 6 kohdassa määriteltyä digitaalisen palvelun **tarjoajaa**;

Tarkistus

(6) 'poikkeamalla' direktiivin (EU) N:o 2016/1148 4 artiklan 7 kohdassa määriteltyä poikkeamaa;

Tarkistus

7) 'poikkeamien käsittelyllä' direktiivin (EU) N:o 2016/1148 4 artiklan 8 kohdassa määriteltyä **poikkeaman käsittelyä**;

Tarkistus

8) 'kyberuhalla' potentiaalista tilannetta, tapahtumaa tai **tahallista toimintaa, myös automaattista käskyä**, joka voi **vahingoittaa, häiritä tai muutoin** vaikuttaa haitallisesti verkko- ja tietojärjestelmiin, niiden käyttäjiin ja asianosaisiin henkilöihin;

8 a) 'kyberhygienialla' yksinkertaisia rutiinitoimenpiteitä, jotka säännöllisesti toimeenpantuina ja toteutettuina minimoivat käyttäjien ja yritysten altistumisen verkossa kyberuhkien riskeille.

Tarkistus 85

Ehdotus asetukseksi 2 artikla – 1 kohta – 9 alakohta

Komission teksti

9) 'eurooppalaisella kyberturvallisuuden sertifiointijärjestelmällä' unionin tasolla määriteltyjä kattavia sääntöjä, teknisiä vaatimuksia, standardeja ja menettelyjä, joita sovelletaan kyseisen erityisen järjestelmän kattamien tieto- ja viestintätekniikan tuotteiden ja palvelujen sertifiointiin;

Tarkistus

9) 'eurooppalaisella kyberturvallisuuden sertifiointijärjestelmällä' unionin tasolla määriteltyjä **ja viraston yksilöimien kansainvälisten ja eurooppalaisten standardien ja tieto- ja viestintätekniikan eritelmien mukaisia** kattavia sääntöjä, teknisiä vaatimuksia, standardeja ja menettelyjä, joita sovelletaan kyseisen erityisen järjestelmän kattamien tieto- ja viestintätekniikan tuotteiden, **prosessien** ja palvelujen sertifiointiin;

Tarkistus 86

Ehdotus asetukseksi 2 artikla – 1 kohta – 10 alakohta

Komission teksti

10) 'eurooppalaisella kyberturvallisuussertifikaatilla' vaatimustenmukaisuuden arviointilaitoksen antamaa asiakirjaa, jolla todistetaan, että tietty tieto- ja viestintätekniikan tuote tai palvelu täyttää eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä vahvistetut erityiset vaatimukset;

Tarkistus

10) 'eurooppalaisella kyberturvallisuussertifikaatilla' vaatimustenmukaisuuden arviointilaitoksen antamaa asiakirjaa, jolla todistetaan, että tietty tieto- ja viestintätekniikan tuote tai palvelu **tai prosessi** täyttää eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä vahvistetut erityiset vaatimukset;

Tarkistus 87

Ehdotus asetukseksi
2 artikla – 1 kohta – 11 a alakohta (uusi)

Komission teksti

Tarkistus

(11 a) **'tieto- ja viestintäteknii­kan prosessilla' toimintaa, jonka tarkoituksena on suunnitella, kehittää, ylläpitää ja tarjota tieto- ja viestintäteknii­kan tuote tai palvelu;**

Tarkistus 88

Ehdotus asetukseksi
2 artikla – 1 kohta – 11 b alakohta (uusi)

Komission teksti

Tarkistus

(11 b)
'kuluttajaelektronii­kkalaitteella' laitteita, jotka koostuvat laitteista tai ohjelmistoista, jotka käsittelevät henkilö­­tietoja tai liitetään internetiin domotiikan ja kotitalouden valvontalaitteiden, toimistolaitteiden, reitityslaitteiden ja verkkoon liitettävien laitteiden, kuten älytelevisioiden, lelujen ja pelikonsolien, virtuaalisten tai henkilökohtaisten avustajien, verkkoon liitettävien suoratoistolaitteiden, puettavien laitteiden, ääniohjattavien ja virtuaalitodellisuuslaitteiden toimintaa varten;

Tarkistus 89

Ehdotus asetukseksi
2 artikla – 1 kohta – 16 alakohta

Komission teksti

Tarkistus

16) 'standardilla' asetuksen (EU) N:o 1025/2012 2 artiklan 1 kohdassa määriteltyä standardia.

16) 'standardilla, **teknisellä eritelmällä ja tieto- ja viestintäteknii­kan teknisellä eritelmällä**' asetuksen (EU) N:o 1025/2012 2 artiklan 1, **4 ja 5** kohdassa määriteltyä standardia, **teknistä eritelmää tai tieto- ja viestintäteknii­kan teknistä eritelmää.**

Tarkistus 90

Ehdotus asetukseksi
2 artikla – 1 kohta – 16 a alakohta (uusi)

Komission teksti

Tarkistus

16 a) 'kansallisella sertifiointin valvontaviranomaisella' kunkin jäsenvaltion tämän asetuksen 50 artiklan mukaisesti nimittämää elintä;

Tarkistus 91

Ehdotus asetukseksi
2 artikla – 1 kohta – 16 b alakohta (uusi)

Komission teksti

Tarkistus

16 b) 'itsearviointilla' vaatimustenmukaisuuslausumaa, jossa valmistaja ilmoittaa, että sertifiointijärjestelmässä vahvistetut tuotteita, prosesseja tai palveluita koskevat täsmälliset vaatimukset täyttyvät;

Tarkistus 92

Ehdotus asetukseksi
2 artikla – 1 kohta – 16 c alakohta (uusi)

Komission teksti

Tarkistus

16 c) 'oletusarvoisella turvallisuudella' tilannetta, jossa jos tuote, ohjelmisto tai prosessi voidaan asentaa tavalla, joka varmistaa korkeamman turvallisuuden tason, ensimmäisen käyttäjän olisi saatava oletuskonfiguraatio, jossa on mahdollisimman turvalliset asetukset. Jos riski- ja käytettävyyshanalyysin perusteella voidaan tapauskohtaisesti päätellä, että tällainen asetus ei ole toteutettavissa, käyttäjiä olisi pyydettävä valitsemaan kaikkein turvallisin asetus.

Tarkistus 93

Ehdotus asetukseksi
2 artikla – 1 kohta – 16 d alakohta (uusi)

Komission teksti

Tarkistus

16 d) 'keskeisten palvelujen tarjoajilla' direktiivin (EU) N:o 2016/1148 4 artiklan 4 kohdassa määriteltyjä keskeisten palvelujen tarjoajia.

Tarkistus 94

Ehdotus asetukseksi
3 artikla – 1 kohta

Komission teksti

Tarkistus

1. Virasto hoitaa sille tämän asetuksen mukaisesti kuuluvia tehtäviä kyberturvallisuuden korkean tason **edistämiseksi** unionissa.

1. Virasto hoitaa sille tämän asetuksen mukaisesti kuuluvia tehtäviä **ja sitä vahvistetaan** kyberturvallisuuden korkean yleisen tason **saavuttamiseksi-, jotta unionissa voidaan torjua kyberhyökkäyksiä, vähentää sisämarkkinoiden hajanaisuutta ja parantaa niiden toimintaa ja varmistaa yhdenmukaisuus ottamalla huomioon jäsenvaltioiden kyberturvallisuusedirektiivin mukaiset yhteistyösaavutukset.**

Tarkistus 95

Ehdotus asetukseksi
4 artikla – 1 kohta

Komission teksti

Tarkistus

1. Virasto on kyberturvallisuuden **osaamiskeskus** riippumattomuutensa, antamansa neuvonnan ja avun ja tarjoamansa tiedon tieteellisen ja teknisen laadun, toimintatapojensa ja -menettelyjensä avoimuuden sekä tehtäviensä suorittamisessa osoittamansa huolellisuuden ansiosta.

1. Virasto on kyberturvallisuuden **teoreettisen ja käytännön osaamisen keskus** riippumattomuutensa, antamansa neuvonnan ja avun ja tarjoamansa tiedon tieteellisen ja teknisen laadun, toimintatapojensa ja -menettelyjensä avoimuuden sekä tehtäviensä suorittamisessa osoittamansa huolellisuuden ansiosta.

Tarkistus 96

Ehdotus asetukseksi
4 artikla – 2 kohta

Komission teksti

2. Virasto auttaa unionin toimielimiä, virastoja ja elimiä sekä jäsenvaltioita kehittämään ja panemaan täytäntöön kyberturvallisuutta koskevat toimintapolitiikat.

Tarkistus

2. Virasto auttaa unionin toimielimiä, virastoja ja elimiä sekä jäsenvaltioita kehittämään ja panemaan täytäntöön kyberturvallisuutta koskevat toimintapolitiikat **sekä lisäämään kansalaisten ja yritysten tietoisuutta.**

Tarkistus 97

Ehdotus asetukseksi
4 artikla – 3 kohta

Komission teksti

3. Virasto tukee valmiuksien kehittämistä ja varautumista **kaikkialla unionissa** avustamalla unionia, jäsenvaltioita sekä julkisia ja yksityisiä sidosryhmiä niiden verkko- ja tietojärjestelmien suojelun lisäämiseksi, ammattitaidon ja osaamisen kehittämiseksi kyberturvallisuuden alalla ja kyberresilienssin saavuttamiseksi.

Tarkistus

3. Virasto tukee valmiuksien kehittämistä ja varautumista **kaikissa unionin toimielimissä, virastoissa ja elimissä** avustamalla unionia, jäsenvaltioita sekä julkisia ja yksityisiä sidosryhmiä niiden verkko- ja tietojärjestelmien suojelun lisäämiseksi, **kyberresilienssin ja toimintavalmiuksien kehittämiseksi ja parantamiseksi, tietoisuuden lisäämiseksi** sekä ammattitaidon ja osaamisen kehittämiseksi kyberturvallisuuden alalla ja kyberresilienssin saavuttamiseksi.

Tarkistus 98

Ehdotus asetukseksi
4 artikla – 4 kohta

Komission teksti

4. Virasto edistää yhteistyötä ja koordinointia unionin tasolla jäsenvaltioiden, unionin toimielinten, virastojen ja elinten sekä asiaankuuluvien sidosryhmien välillä, **mukaan lukien yksityinen sektori**, kyberturvallisuuteen liittyvissä kysymyksissä.

Tarkistus

4. Virasto edistää yhteistyötä, koordinointia ja **tietojen jakamista** unionin tasolla jäsenvaltioiden, unionin toimielinten, virastojen ja elinten sekä asiaankuuluvien sidosryhmien välillä kyberturvallisuuteen liittyvissä kysymyksissä.

Tarkistus 99

Ehdotus asetukseksi
4 artikla – 5 kohta

Komission teksti

5. Virasto lisää kyberturvallisuusvalmiuksia unionin tasolla jäsenvaltioiden toimien täydentämiseksi kyberuhkien ehkäisemisessä ja niihin vastaamisessa erityisesti rajat ylittävien poikkeamien tapauksessa.

Tarkistus

5. Virasto lisää **osaltaan** kyberturvallisuusvalmiuksia unionin tasolla jäsenvaltioiden toimien täydentämiseksi kyberuhkien ehkäisemisessä ja niihin vastaamisessa erityisesti rajat ylittävien poikkeamien tapauksessa **sekä suorittaakseen tehtävänsä unionin toimielinten avustamiseksi kyberturvallisuuteen liittyvien toimintapolitiikkojen kehittämisessä.**

Tarkistus 100

Ehdotus asetukseksi
4 artikla – 6 kohta

Komission teksti

6. Virasto edistää sertifiointin käyttöä muun muassa osallistumalla kyberturvallisuuden sertifiointikehyksen perustamiseen ja ylläpitoon unionin tasolla tämän asetuksen III osaston mukaisesti, jotta voidaan lisätä avoimuutta tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa ja tällä tavoin vahvistaa luottamusta digitaalisiin sisämarkkinoihin.

Tarkistus

6. Virasto edistää sertifiointin käyttöä, **jotta voidaan välttää sisämarkkinoiden hajanaisuutta ja parantaa niiden toimintaa**, muun muassa osallistumalla kyberturvallisuuden sertifiointikehyksen perustamiseen ja ylläpitoon unionin tasolla tämän asetuksen III osaston mukaisesti, jotta voidaan lisätä avoimuutta tieto- ja viestintätekniikan tuotteiden, palvelujen ja **prosessien** kyberturvallisuuden varmistuksessa ja tällä tavoin vahvistaa luottamusta digitaalisiin sisämarkkinoihin **sekä parantaa yhteensopivuutta nykyisten kansallisten ja kansainvälisten sertifiointijärjestelmien välillä.**

Tarkistus 101

Ehdotus asetukseksi
4 artikla – 7 kohta

Komission teksti

7. Virasto edistää tietoisuuden korkeaa tasoa kansalaisten ja yritysten keskuudessa

Tarkistus

7. Virasto edistää **ja tukee hankkeita, joilla edistetään** tietoisuuden,

kyberturvallisuuteen liittyvissä kysymyksissä.

kyberhygienian ja kyberlukutaidon korkeaa tasoa kansalaisten ja yritysten keskuudessa kyberturvallisuuteen liittyvissä kysymyksissä.

Tarkistus 102

Ehdotus asetukseksi 5 artikla – 1 kohta

Komission teksti

1. avustaa ja neuvoa erityisesti antamalla riippumattomia lausuntoja ja tekemällä valmistelutyötä unionin politiikan ja lainsäädännön kehittämisessä ja tarkistamisessa kyberturvallisuuden alalla sekä alakohtaisissa toimintapoliittisissa ja lainsäädännöllisissä aloitteissa, kun niihin liittyy kyberturvallisuuskysymyksiä;

Tarkistus

1. avustaa ja neuvoa erityisesti antamalla riippumattomia lausuntoja ja **analyyseja asiankuuluvista toiminnoista kyberympäristössä ja** tekemällä valmistelutyötä unionin politiikan ja lainsäädännön kehittämisessä ja tarkistamisessa kyberturvallisuuden alalla sekä alakohtaisissa toimintapoliittisissa ja lainsäädännöllisissä aloitteissa, kun niihin liittyy kyberturvallisuuskysymyksiä;

Tarkistus 103

Ehdotus asetukseksi 5 artikla – 2 kohta

Komission teksti

2. auttaa jäsenvaltioita panemaan johdonmukaisesti täytäntöön erityisesti direktiiviin (EU) 2016/1148 liittyvää unionin kyberturvallisuuspolitiikkaa ja -lainsäädäntöä muun muassa antamalla lausuntoja, ohjeita ja neuvoja ja laatimalla parhaita käytäntöjä riskinhallinnan, poikkeamista raportoinnin ja tietojen jakamisen kaltaisista aiheista sekä helpottamalla parhaiden käytäntöjen vaihtoa toimivaltaisten viranomaisten välillä tältä osin;

Tarkistus

2. auttaa jäsenvaltioita panemaan johdonmukaisesti täytäntöön erityisesti direktiiviin (EU) 2016/1148, **eurooppalaisesta sähköisen viestinnän säännöstöstä annettuun direktiiviin, asetukseen (EU) 2016/678 ja direktiiviin 2002/58/EY** liittyvää unionin kyberturvallisuuspolitiikkaa ja -lainsäädäntöä muun muassa antamalla lausuntoja, ohjeita ja neuvoja ja laatimalla parhaita käytäntöjä **turvallisen ohjelmisto- ja järjestelmäkehittämisen,** riskinhallinnan, poikkeamista raportoinnin ja tietojen jakamisen, **teknisten ja organisatoristen toimenpiteiden** kaltaisista aiheista, **erityisesti ottamalla käyttöön koordinoituja haavoittuvuuksien havaitsemisohjelmia** sekä helpottamalla parhaiden käytäntöjen vaihtoa

toimivaltaisten viranomaisten välillä tältä osin;

Tarkistus 104

Ehdotus asetukseksi 5 artikla – 2 a kohta (uusi)

Komission teksti

Tarkistus

2 a. kehittää ja edistää toimintapolitiikkoja, joilla tuetaan avoimen internetin julkisen ytimen yleistä saatavuutta tai eheyttä, joilla tarjotaan koko internetille sen keskeiset toiminnot ja joilla tuetaan sen normaalia toimintaa, muun muassa keskeisten protokollien (erityisesti DNS:n, BGP:n ja IPv6:n) turvallisuutta ja vakautta, verkkotunnusjärjestelmän toimintaa (mukaan lukien kaikki aluetunnukset) sekä juurialueen toimintaa;

Tarkistus 105

Ehdotus asetukseksi 5 artikla – 4 kohta – 2 alakohta

Komission teksti

Tarkistus

2) sähköisen viestinnän turvallisuuden parantamista muun muassa tarjoamalla asiantuntemusta ja neuvontaa sekä helpottamalla parhaiden käytäntöjen vaihtoa toimivaltaisten viranomaisten välillä;

2) sähköisen viestinnän, **tiedon varastoinnin ja käsittelyn** turvallisuuden parantamista muun muassa tarjoamalla asiantuntemusta ja neuvontaa sekä helpottamalla parhaiden käytäntöjen vaihtoa toimivaltaisten viranomaisten välillä;

Tarkistus 106

Ehdotus asetukseksi 5 artikla – 5 a kohta (uusi)

Komission teksti

Tarkistus

5 a. auttaa jäsenvaltioita panemaan johdonmukaisesti täytäntöön unionin tietosuojaa koskevaa politiikkaa ja lainsäädäntöä, erityisesti asetukset (EU)

2016/679, sekä auttaa Euroopan tietosuojaneuvostoa suuntaviivojen kehittämisessä asetuksen (EU) 2016/679 täytäntöön panemiseksi kyberturvallisuuden osalta. Euroopan tietosuojaneuvosto kuulee virastoa aina kun se antaa lausunnon tai päätöksen yleisen tietosuoja-asetuksen täytäntöönpanosta ja kyberturvallisuudesta, muun muassa yksityisyyden suojaa koskeviin vaikutustenarviointeihin, tietoturvaloukkausilmoituksiin, käsittelyn turvallisuuteen, turvallisuusvaatimuksiin ja sisäänrakennettuun yksityisyyteen liittyvistä kysymyksistä.

Tarkistus 107

**Ehdotus asetukseksi
6 artikla – 1 kohta – a a alakohta (uusi)**

Komission teksti

Tarkistus

a a) jäsenvaltioita ja unionin toimielimiä niiden ottaessa käyttöön ja soveltaessa haavoittuvuuksista ilmoittamista koskevia koordinoituja toimintaperiaatteita ja haavoittuvuuksista ilmoittamista koskevia viranomaisten tarkastusprosesseja, joiden käytäntöjen ja määritysten olisi oltava avoimia ja riippumattomasti valvottuja;

Tarkistus 108

**Ehdotus asetukseksi
6 artikla – 1 kohta – a b alakohta (uusi)**

Komission teksti

Tarkistus

a b) Virasto edistää pitkän aikavälin eurooppalaisen tietotekniikan turvallisuushankkeen kehittämistä ja käynnistämistä, jotta voidaan edelleen edistää kyberturvallisuutta koskevaa tutkimusta unionissa ja jäsenvaltioissa, yhteistyössä Euroopan tutkimusneuvoston ja Euroopan innovaatio- ja teknologiainstituutin kanssa ja ottaen

Tarkistus 109

Ehdotus asetukseksi 6 artikla – 1 kohta – g alakohta

Komission teksti

g) jäsenvaltioita järjestämällä vuosittain 7 artiklan 6 kohdassa tarkoitettuja laajamittaisia kyberturvallisuusharjoituksia unionin tasolla ja antamalla poliittisia suosituksia harjoitusten arviointiprosessin ja niistä saatavien kokemusten pohjalta;

Tarkistus

g) jäsenvaltioita järjestämällä **säännöllisesti ja vähintään** vuosittain 7 artiklan 6 kohdassa tarkoitettuja laajamittaisia kyberturvallisuusharjoituksia unionin tasolla ja antamalla poliittisia suosituksia **ja jakamalla parhaita käytäntöjä** harjoitusten arviointiprosessin ja niistä saatavien kokemusten pohjalta;

Tarkistus 110

Ehdotus asetukseksi 6 artikla – 2 kohta

Komission teksti

2. Virasto helpottaa tietojen jakamisen ja analysoinnin alakohtaisten keskusten (ISAC) perustamista ja antaa niille jatkuvaa tukea erityisesti direktiivin (EU) 2016/1148 liitteessä II mainituilla aloilla tarjoamalla käyttöön parhaita käytäntöjä ja ohjeita käytettävissä olevista välineistä ja menettelyistä sekä ohjeita tietojen jakamiseen liittyvien sääntelykysymysten ratkaisemiseksi.

Tarkistus

2. Virasto helpottaa tietojen jakamisen ja analysoinnin alakohtaisten keskusten (ISAC) perustamista ja antaa niille jatkuvaa tukea erityisesti direktiivin (EU) 2016/1148 liitteessä II mainituilla aloilla tarjoamalla käyttöön parhaita käytäntöjä ja ohjeita käytettävissä olevista välineistä ja menettelyistä, **kyberhygienian periaatteista** sekä ohjeita tietojen jakamiseen liittyvien sääntelykysymysten ratkaisemiseksi.

Tarkistus 111

Ehdotus asetukseksi 7 artikla – 1 kohta

Komission teksti

1. Virasto tukee operatiivista yhteistyötä **toimivaltaisten julkisten** elinten välillä sekä sidosryhmien välillä.

Tarkistus

1. Virasto tukee operatiivista yhteistyötä **jäsenvaltioiden, unionin toimielinten, virastojen ja** elinten välillä sekä sidosryhmien välillä, **jotta saadaan aikaan yhteistyötä analysoimalla ja**

arvioimalla nykyisiä kansallisia järjestelmiä, kehittämällä ja panemalla täytäntöön suunnitelma sekä käyttämällä asianmukaisia välineitä mahdollisimman korkeatasoisen kyberturvallisuussertifiointin saavuttamiseksi unionissa ja jäsenvaltioissa.

Tarkistus 112

Ehdotus asetukseksi

7 artikla – 4 kohta – 1 alakohta – b alakohta

Komission teksti

b) tarjoamalla pyynnöstä teknistä apua sellaisten poikkeamien yhteydessä, joilla on merkittävä vaikutus;

Tarkistus

b) tarjoamalla pyynnöstä teknistä apua, **joka annetaan tiedonvaihdon ja asiantuntemuksen muodossa**, sellaisten poikkeamien yhteydessä, joilla on merkittävä vaikutus;

Tarkistus 113

Ehdotus asetukseksi

7 artikla – 4 kohta – 1 alakohta – b a alakohta (uusi)

Komission teksti

Tarkistus

b a) Jos tilanne edellyttää kiireellisiä toimia, koska poikkeaman vaikutus on erittäin haitallinen, jäsenvaltio voi pyytää apua viraston asiantuntijoilta tilanteen arvioimiseksi. Pyyntöön on sisällyttävä kuvaus tilanteesta, mahdolliset tavoitteet ja arvioidut tarpeet.

Tarkistus 114

Ehdotus asetukseksi

7 artikla – 5 kohta – 1 alakohta

Komission teksti

Kahden tai useamman sellaisen jäsenvaltion pyynnöstä, jota asia koskee, ja pelkästään neuvonnan **tarjoamiseksi** uusien poikkeamien ehkäisemistä varten virasto antaa tukea jälkikäteen tehtävälle tekniselle

Tarkistus

Yhden tai useamman sellaisen jäsenvaltion pyynnöstä, jota asia koskee, ja pelkästään **avun tarjoamiseksi** neuvonnan **muodossa** uusien poikkeamien ehkäisemistä **tai avun muodossa nykyisiin laajamittaisiin**

tutkimukselle tai suorittaa tällaisen tutkimuksen sen jälkeen, kun vaikutukseltaan merkittävistä poikkeamista saadaan direktiivin (EU) 2016/1148 mukaisesti ilmoituksia yrityksiltä, joihin nämä poikkeamat ovat vaikuttaneet. Lisäksi virasto suorittaa tällaisen tutkimuksen asianmukaisesti perustellusta pyynnöstä, jonka komissio tekee yhteisymmärryksessä asianomaisten jäsenvaltioiden kanssa tapauksissa, joissa tällaiset poikkeamat vaikuttavat useampaan kuin *kahteen* jäsenvaltioon.

poikkeamiin reagoimista varten virasto antaa tukea jälkikäteen tehtävälle tekniselle tutkimukselle tai suorittaa tällaisen tutkimuksen sen jälkeen, kun vaikutukseltaan merkittävistä poikkeamista saadaan direktiivin (EU) 2016/1148 mukaisesti ilmoituksia yrityksiltä, joihin nämä poikkeamat ovat vaikuttaneet. ***Virasto toteuttaa edellä mainitut toimet saatuaan asiaa koskevat tiedot jäsenvaltioita, joihin nämä poikkeamat ovat vaikuttaneet, ja käyttäen uhka-analyysiin omia resurssejaan sekä turvallisuuspoikkeamiin reagoimiseen tarkoitettuja resursseja.*** Lisäksi virasto suorittaa tällaisen tutkimuksen asianmukaisesti perustellusta pyynnöstä, jonka komissio tekee yhteisymmärryksessä asianomaisten jäsenvaltioiden kanssa tapauksissa, joissa tällaiset poikkeamat vaikuttavat useampaan kuin *yhteen* jäsenvaltioon. ***Toimiessaan näin virasto varmistaa, ettei se paljasta jäsenvaltioiden keskeisten valtion tehtävien turvaamiseksi toteuttamia, erityisesti kansallista turvallisuutta koskevia toimia.***

Tarkistus 115

Ehdotus asetukseksi 7 artikla – 6 kohta

Komission teksti

6. Virasto järjestää vuosittain kyberturvallisuusharjoituksia unionin tasolla ja tukee jäsenvaltioita ja EU:n toimielimiä, virastoja ja elimiä harjoitusten järjestämisessä niiden pyynnöstä. Unionin tasolla järjestettävät vuotuiset harjoitukset sisältävät teknisiä, operatiivisia ja strategisia osatekijöitä ja auttavat valmistelemaan yhteistyöhön perustuvan vastauksen unionin tasolla laajamittaisiin rajatylittäviin kyberturvallisuuspoikkeamiin. Virasto myös edistää ja auttaa tarvittaessa järjestämään alakohtaisia kyberturvallisuusharjoituksia yhdessä

Tarkistus

6. Virasto järjestää ***säännöllisesti ja joka tapauksessa vähintään*** vuosittain kyberturvallisuusharjoituksia unionin tasolla ja tukee jäsenvaltioita ja EU:n toimielimiä, virastoja ja elimiä harjoitusten järjestämisessä niiden pyynnöstä. Unionin tasolla järjestettävät vuotuiset harjoitukset sisältävät teknisiä, operatiivisia ja strategisia osatekijöitä ja auttavat valmistelemaan yhteistyöhön perustuvan vastauksen unionin tasolla laajamittaisiin rajatylittäviin kyberturvallisuuspoikkeamiin. Virasto myös edistää ja auttaa tarvittaessa järjestämään alakohtaisia

ISAC-keskusten kanssa ja sallii ISAC-keskusten osallistumisen myös unionin tasolla järjestettäviin kyberturvallisuusharjoituksiin.

kyberturvallisuusharjoituksia yhdessä ISAC-keskusten kanssa ja sallii ISAC-keskusten osallistumisen myös unionin tasolla järjestettäviin kyberturvallisuusharjoituksiin.

Tarkistus 116

Ehdotus asetukseksi 7 artikla – 7 kohta

Komission teksti

7. Virasto laatii poikkeamista ja uhista säännöllisesti EU:n kyberturvallisuuden teknisen tilanneraportin, joka perustuu julkisiin tietolähteisiin, sen omaan analyysiin ja raportteihin, jotka on saatu muun muassa CSIRT-toimijoilta (vapaaehtoisuuden pohjalta) tai verkko- ja tietoturvadirektiivillä perustetuilta keskitetyiltä yhteyspisteiltä (verkko- ja tietoturvadirektiivin 14 artiklan 5 kohdan mukaisesti), Europolissa toimivalta Euroopan kyberrikostorjuntakeskukselta (EC3) sekä CERT-EU:lta.

Tarkistus

7. Virasto laatii poikkeamista ja uhista säännöllisesti **perusteellisen** EU:n kyberturvallisuuden teknisen tilanneraportin, joka perustuu julkisiin tietolähteisiin, sen omaan analyysiin ja raportteihin, jotka on saatu muun muassa CSIRT-toimijoilta (vapaaehtoisuuden pohjalta) tai verkko- ja tietoturvadirektiivillä perustetuilta keskitetyiltä yhteyspisteiltä (verkko- ja tietoturvadirektiivin 14 artiklan 5 kohdan mukaisesti), Europolissa toimivalta Euroopan kyberrikostorjuntakeskukselta (EC3) sekä CERT-EU:lta. **Pääjohtaja esittää julkiset havainnot Euroopan parlamentille tarvittaessa.**

Tarkistus 117

Ehdotus asetukseksi 7 artikla – 7 a kohta (uusi)

Komission teksti

Tarkistus

7 a. Virasto edistää osaltaan tarvittaessa ja saatuaan komissiolta ennakkoon hyväksynnän kyberyhteistyötä Naton kyberpuolustuksen osaamiskeskuksen ja viestintä- ja tiedotusakatemian kanssa.

Tarkistus 118

Ehdotus asetukseksi 7 artikla – 8 kohta – a alakohta

Komission teksti

a) kokoamalla raportteja kansallisista lähteistä, jotta voidaan edistää yhteistä tilannetietoisuutta;

Tarkistus

a) ***analysoimalla ja*** kokoamalla raportteja kansallisista lähteistä, jotta voidaan edistää yhteistä tilannetietoisuutta;

Tarkistus 119

**Ehdotus asetukseksi
7 artikla – 8 kohta – c alakohta**

Komission teksti

c) tukemalla poikkeaman tai kriisin teknistä käsittelyä, muun muassa helpottamalla teknisten ratkaisujen jakamista jäsenvaltioiden välillä;

Tarkistus

c) tukemalla ***oman riippumattoman asiantuntemuksensa ja resurssiensa pohjalta*** poikkeaman tai kriisin teknistä käsittelyä, muun muassa helpottamalla teknisten ratkaisujen ***vapaaehtoista*** jakamista jäsenvaltioiden välillä;

Tarkistus 120

**Ehdotus asetukseksi
7 artikla – 8 a kohta (uusi)**

Komission teksti

Tarkistus

8 a. Virasto järjestää tarvittaessa keskusteluja ja avustaa jäsenvaltioiden viranomaisia vastatoimiensa koordinoinnissa toissijaisuus- ja suhteellisuusperiaatteiden mukaisesti.

Tarkistus 121

**Ehdotus asetukseksi
7 a artikla (uusi)**

Komission teksti

Tarkistus

7 a artikla

Viraston tekniset valmiudet

1. Edellä 7 artiklassa kuvattujen tavoitteiden saavuttamiseksi ja viraston työohjelman mukaisesti virasto kehittää muun muassa seuraavat tekniset valmiudet ja taidot:

- a) *kyky kerätä tietoa kyberturvallisuusuuhkista julkisista lähteistä ja*
- b) *kyky käyttää teknisiä laitteita, välineitä ja asiantuntemusta etänä.*
2. *Tämän artiklan 1 kohdassa tarkoitettujen teknisten valmiuksien täyttämiseksi ja asianmukaisten taitojen kehittämiseksi virasto*
- a) *varmistaa, että sen palvelukseenottoprosesseissa otetaan huomioon tarvittavat moninaiset tekniset taidot ja*
- b) *tekee yhteistyötä CERT-EU:n ja Europolin kanssa tämän asetuksen 7 artiklan 2 kohdan mukaisesti.*

Tarkistus 122

Ehdotus asetukseksi 8 artikla – 1 kohta – a alakohta – johdantokappale

Komission teksti

a) tukee ja edistää tieto- ja viestintäteknii­kan tuotteiden ja palvelujen kyberturvallisuussertifiointiin liittyvän, tämän asetuksen III osastolla käyttöön otettavan unionin politiikan kehittämistä ja täytäntöönpanoa tehtävänään

Tarkistus

a) tukee ja edistää tieto- ja viestintäteknii­kan tuotteiden, palvelujen ja **prosessien** kyberturvallisuussertifiointiin liittyvän, tämän asetuksen III osastolla käyttöön otettavan unionin politiikan kehittämistä ja täytäntöönpanoa tehtävänään

Tarkistus 123

Ehdotus asetukseksi 8 artikla – 1 kohta – a alakohta – -1 alakohta (uusi)

Komission teksti

Tarkistus

-1) määrittää jatkuvasti standardeja, teknisiä eritelmiä sekä tieto- ja viestintäteknii­kkaa koskevia teknisiä eritelmiä;

Tarkistus 124

Ehdotus asetukseksi
8 artikla – 1 kohta – a alakohta – 1 alakohta

Komission teksti

1) valmistella ehdolla olevat eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät tieto- ja viestintäteknikan tuotteille ja **palveluille** tämän asetuksen 44 artiklan mukaisesti;

Tarkistus

1) valmistella ehdolla olevat eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät tieto- ja viestintäteknikan tuotteille, **palveluille ja prosesseille** tämän asetuksen 44 artiklan mukaisesti **yhteistyössä alan sidosryhmien ja standardointiorganisaatioiden kanssa virallisessa, standardoidussa ja avoimessa prosessissa**;

Tarkistus 125

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

Komission teksti

Tarkistus

1 a) arvioida yhteistyössä tämän asetuksen 53 artiklan mukaisen jäsenvaltioiden sertifiointiryhmän kanssa menettelyjä, joita tämän asetuksen 51 artiklassa tarkoitetut vaatimustenmukaisuuden arviointilaitokset ovat ottaneet käyttöön eurooppalaisten kyberturvallisuussertifikaattien myöntämistä varten, tarkoituksenaan varmistaa, että vaatimustenmukaisuuden arviointilaitokset soveltavat tätä asetusta yhdenmukaisesti myöntäessään sertifikaatteja;

Tarkistus 126

Ehdotus asetukseksi
8 artikla – 1 kohta – a alakohta – 1 b alakohta (uusi)

Komission teksti

Tarkistus

1 b) toteuttaa sertifioidujen tieto- ja viestintäteknikan tuotteiden, prosessien ja palvelujen säännöllisiä riippumattomia jälkitarkastuksia eurooppalaisten kyberturvallisuuden

*sertifiointijärjestelmien
vaatimustenmukaisuuden osalta;*

Tarkistus 127

Ehdotus asetukseksi

8 artikla – 1 kohta – a alakohta – 2 alakohta

Komission teksti

2) avustaa komissiota toimimalla ***Euroopan kyberturvallisuuden*** sertifiointiryhmän sihteeristönä tämän asetuksen 53 artiklan mukaisesti;

Tarkistus

2) avustaa komissiota toimimalla ***jäsenvaltioiden*** sertifiointiryhmän sihteeristönä tämän asetuksen 53 artiklan mukaisesti;

Tarkistus 128

Ehdotus asetukseksi

8 artikla – 1 kohta – a alakohta – 3 alakohta

Komission teksti

3) koota ja julkaista ohjeita ja laatia hyviä käytäntöjä, jotka koskevat tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuusvaatimuksia, yhteistyössä kansallisten sertifiointin valvontaviranomaisten ja toimialan kanssa;

Tarkistus

3) koota ja julkaista ohjeita ja laatia hyviä käytäntöjä, ***myös kyberhygienian periaatteista***, jotka koskevat tieto- ja viestintätekniikan tuotteiden, ***prosessien*** ja palvelujen kyberturvallisuusvaatimuksia, yhteistyössä kansallisten sertifiointin valvontaviranomaisten ja toimialan kanssa ***virallisessa, standardoidussa ja avoimessa prosessissa***;

Tarkistus 129

Ehdotus asetukseksi

8 artikla – 1 kohta – b alakohta

Komission teksti

b) helpottaa tieto- ja viestintätekniisten tuotteiden ja palvelujen riskinhallintaan ja turvallisuuteen liittyvien eurooppalaisten ja kansainvälisten standardien laatimista ja käyttöönottoa sekä antaa yhteistyössä jäsenvaltioiden kanssa neuvoja ja suuntaviivoja keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia koskeviin turvallisuusvaatimuksiin liittyvistä teknisistä aloista sekä jo

Tarkistus

b) helpottaa tieto- ja viestintätekniisten tuotteiden, ***prosessien*** ja palvelujen riskinhallintaan ja turvallisuuteen liittyvien eurooppalaisten ja kansainvälisten standardien laatimista ja käyttöönottoa sekä antaa yhteistyössä jäsenvaltioiden ***ja toimialan*** kanssa neuvoja ja suuntaviivoja keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia koskeviin turvallisuusvaatimuksiin liittyvistä

olemassa olevista standardeista, mukaan lukien jäsenvaltioiden kansalliset standardit, direktiivin (EU) 2016/1148 19 artiklan 2 kohdan mukaisesti;

teknisistä aloista sekä jo olemassa olevista standardeista, mukaan lukien jäsenvaltioiden kansalliset standardit, direktiivin (EU) 2016/1148 19 artiklan 2 kohdan mukaisesti, **ja jakaa nämä tiedot jäsenvaltioiden kanssa;**

Tarkistus 130

Ehdotus asetukseksi 9 artikla – 1 kohta – c alakohta

Komission teksti

c) tarjoaa yhteistyössä jäsenvaltioiden viranomaisten asiantuntijoiden kanssa neuvoja, ohjeita ja parhaita käytäntöjä, jotka koskevat verkko- ja tietojärjestelmien turvallisuutta ja erityisesti internetinfrastruktuurin ja direktiivin (EU) 2016/1148 liitteessä II mainittuja aloja tukevien infrastruktuurien turvallisuutta;

Tarkistus

c) tarjoaa yhteistyössä jäsenvaltioiden viranomaisten **ja asianomaisten sidosryhmien** asiantuntijoiden kanssa neuvoja, ohjeita ja parhaita käytäntöjä, jotka koskevat verkko- ja tietojärjestelmien turvallisuutta ja erityisesti internetinfrastruktuurin ja direktiivin (EU) 2016/1148 liitteessä II mainittuja aloja tukevien infrastruktuurien turvallisuutta;

Tarkistus 131

Ehdotus asetukseksi 9 artikla – 1 kohta – e alakohta

Komission teksti

e) lisää suuren yleisön tietoisuutta kyberturvallisuuteen liittyvistä riskeistä ja antaa yksittäisille käyttäjille ohjeita hyvistä käytännöistä kansalaisten ja organisaatioiden käyttöön;

Tarkistus

e) lisää **jatkuvasti** suuren yleisön tietoisuutta kyberturvallisuuteen liittyvistä riskeistä ja antaa yksittäisille käyttäjille **koulutusta ja** ohjeita hyvistä käytännöistä kansalaisten ja organisaatioiden käyttöön **ja edistää ennaltaehkäisevien tietotekniikan turvallisuuteen liittyvien vahvojen toimenpiteiden sekä luotettavien tietoturva- ja yksityisyydensuojatoimien käyttöönottoa;**

Tarkistus 132

Ehdotus asetukseksi 9 artikla – 1 kohta – g alakohta

Komission teksti

g) järjestää yhteistyössä jäsenvaltioiden ja unionin toimielinten, elinten, laitosten ja virastojen kanssa säännöllisiä tiedotuskampanjoita **kyberturvallisuuden ja sen näkyvyyden parantamiseksi unionissa.**

Tarkistus 133

**Ehdotus asetukseksi
9 artikla – 1 kohta – g a alakohta (uusi)**

Komission teksti

Tarkistus 134

**Ehdotus asetukseksi
10 artikla – 1 kohta – a alakohta**

Komission teksti

a) **antaa** unionille ja jäsenvaltioille neuvoja **kyberturvallisuusalan** tutkimustarpeista ja -painopisteistä, jotta nykyisiin ja kehittyviin riskeihin ja uhkiin, myös jos ne liittyvät uusiin ja kehittyviin tieto- ja viestintäteknologioihin, voitaisiin löytää toimivia ratkaisuja ja jotta riskinehkäisytekniikoita voitaisiin käyttää tehokkaasti;

Tarkistus 135

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

Tarkistus

g) järjestää yhteistyössä jäsenvaltioiden ja unionin toimielinten, elinten, laitosten ja virastojen kanssa säännöllisiä tiedotuskampanjoita **laajan julkisen keskustelun aikaansaamiseksi.**

Tarkistus

g a) tukee jäsenvaltioiden välistä tiiviimpää koordinointia ja parhaiden käytäntöjen vaihtoa kyberturvallisuutta koskevan koulutuksen ja lukutaidon, kyberhygienian ja tietoisuuden lisäämisen osalta;

Tarkistus

a) **varmistaa asianomaisten käyttäjäryhmien kuulemisen etukäteen ja antaa** unionille ja jäsenvaltioille neuvoja **kyberturvallisuuden, tietosuojan ja yksityisyydensuojan alojen** tutkimustarpeista ja -painopisteistä, jotta nykyisiin ja kehittyviin riskeihin ja uhkiin, myös jos ne liittyvät uusiin ja kehittyviin tieto- ja viestintäteknologioihin, voitaisiin löytää toimivia ratkaisuja ja jotta riskinehkäisytekniikoita voitaisiin käyttää tehokkaasti;

Komission teksti

Tarkistus

b a) toteuttaa omaa tutkimustoimintaansa sellaisilla aloilla, joita unionin nykyiset tutkimusohjelmat eivät vielä kata, mutta jotka tuovat selvää eurooppalaista lisäarvoa.

Tarkistus 136

**Ehdotus asetukseksi
11 artikla – 1 kohta – c a alakohta (uusi)**

Komission teksti

Tarkistus

c a) tarjota neuvoja ja tukea komissiolle yhteistyössä 53 artiklan nojalla perustetun jäsenvaltioiden sertifiointiryhmän kanssa kysymyksissä, jotka liittyvät kolmansien maiden kanssa tehtäviin kyberturvallisuussertifikaattien vastavuoroista tunnustamista koskeviin sopimuksiin.

Tarkistus 137

**Ehdotus asetukseksi
12 artikla – 1 kohta – d alakohta**

Komission teksti

Tarkistus

d) ***pysyvä sidosryhmä***, jonka tehtävät vahvistetaan 20 artiklassa.

d) ***ENISAn neuvoa-antava ryhmä***, jonka tehtävät vahvistetaan 20 artiklassa;

Tarkistus 138

**Ehdotus asetukseksi
14 artikla – 1 kohta – e alakohta**

Komission teksti

Tarkistus

e) arvioi ja hyväksyy viraston toimintaa koskevan vuotuisen konsolidoidun toimintakertomuksen ja toimittaa sen yhdessä arviointinsa kanssa seuraavan vuoden heinäkuun 1 päivään mennessä Euroopan parlamentille, neuvostolle, komissiolle ja

e) arvioi ja hyväksyy viraston toimintaa koskevan vuotuisen konsolidoidun toimintakertomuksen ja toimittaa sen yhdessä arviointinsa kanssa seuraavan vuoden heinäkuun 1 päivään mennessä Euroopan parlamentille, neuvostolle, komissiolle ja

tilintarkastustuomioistuimelle.
Toimintakertomus sisältää tilinpäätöksen ja kuvauksen siitä, **kuinka virasto** on saavuttanut tulosindikaattorinsa.
Toimintakertomus julkistetaan;

tilintarkastustuomioistuimelle.
Toimintakertomus sisältää tilinpäätöksen, kuvauksen **varainkäytön vaikuttavuudesta** ja **arvion viraston tehokkuudesta sekä** siitä, **missä määrin se** on saavuttanut tulosindikaattorinsa. Toimintakertomus julkistetaan;

Tarkistus 139

Ehdotus asetukseksi 14 artikla – 1 kohta – m alakohta

Komission teksti

m) nimittää pääjohtajan ja jatkaa tarvittaessa tämän toimikautta tai erottaa tämän asetuksen 33 artiklan mukaisesti;

Tarkistus

m) nimittää pääjohtajan **ammattillisiin kriteereihin perustuvan valintamenettelyn kautta** ja jatkaa tarvittaessa tämän toimikautta tai erottaa tämän asetuksen 33 artiklan mukaisesti;

Tarkistus 140

Ehdotus asetukseksi 14 artikla – 1 kohta – o alakohta

Komission teksti

o) tekee kaikki päätökset viraston sisäisistä rakenteista ja tarvittaessa niiden muuttamisesta ottaen huomioon viraston toimintatarpeet ja moitteettoman varainhoidon;

Tarkistus

o) tekee kaikki päätökset viraston sisäisistä rakenteista ja tarvittaessa niiden muuttamisesta ottaen huomioon viraston **tässä asetuksessa luetellut** toimintatarpeet ja moitteettoman varainhoidon;

Tarkistus 141

Ehdotus asetukseksi 16 artikla – 4 kohta

Komission teksti

4. **Pysyvän sidosryhmän** jäsenet voivat osallistua puheenjohtajan kutsusta johtokunnan kokouksiin ilman äänioikeutta.

Tarkistus

4. **ENISAn neuvoa-antavan ryhmän** jäsenet voivat osallistua puheenjohtajan kutsusta johtokunnan kokouksiin ilman äänioikeutta.

Tarkistus 142

Ehdotus asetukseksi

18 artikla – 3 kohta

Komission teksti

3. Hallitukseen kuuluu viisi jäsentä, jotka nimitetään johtokunnan jäsenten keskuudesta ja joista yksi on johtokunnan puheenjohtaja, joka voi myös toimia hallituksen puheenjohtajana, ja yksi on komission edustaja. Pääjohtaja osallistuu hallituksen kokouksiin ilman äänioikeutta.

Tarkistus

3. Hallitukseen kuuluu viisi jäsentä, jotka nimitetään johtokunnan jäsenten keskuudesta ja joista yksi on johtokunnan puheenjohtaja, joka voi myös toimia hallituksen puheenjohtajana, ja yksi on komission edustaja. Pääjohtaja osallistuu hallituksen kokouksiin ilman äänioikeutta. ***Nimityksissä on pyrittävä sukupuolten tasapuoliseen edustukseen hallituksessa.***

Perustelu

Hallituksen nimityksissä on pyrittävä sukupuolten tasapuoliseen edustukseen johtokuntaa koskevan 13 artiklan 3 kohdan säännösten mukaisesti.

Tarkistus 143

Ehdotus asetukseksi 19 artikla – 2 kohta

Komission teksti

2. Pääjohtaja raportoi pyydettyä Euroopan parlamentille tehtäviensä hoidosta. Neuvosto voi pyytää pääjohtajaa raportoimaan tehtäviensä hoidosta.

Tarkistus

2. Pääjohtaja raportoi ***vuosittain tai*** pyydettyä Euroopan parlamentille tehtäviensä hoidosta. Neuvosto voi pyytää pääjohtajaa raportoimaan tehtäviensä hoidosta.

Tarkistus 144

Ehdotus asetukseksi 19 artikla – 5 a kohta (uusi)

Komission teksti

Tarkistus

5 a. Pääjohtajan on myös toimittava Euroopan komission puheenjohtajan kyberturvallisuuspolitiikan institutionaalisen erityisneuvonantajana, jonka toimivaltuudet on määritelty 6 päivänä helmikuuta 2014 annetussa komission päätöksessä C(2014) 541.

Tarkistus 145

**Ehdotus asetukseksi
20 artikla – otsikko**

Komission teksti

Pysyvä sidosryhmä

Tarkistus 146

**Ehdotus asetukseksi
20 artikla – 1 kohta**

Komission teksti

1. Johtokunta perustaa pääjohtajan esityksestä ***pysyvän sidosryhmän***, joka koostuu asiaan liittyviä sidosryhmiä, kuten tieto- ja viestintätekniiikan alaa, sähköisten viestintäverkkojen tai yleisön saatavilla olevien palvelujen tarjoajia ja kuluttajajärjestöjä, edustavista tunnustetuista ***asiantuntijoista***, tiedeyhteisöä edustavista kyberturvallisuusasiantuntijoista sekä [eurooppalaisesta sähköisen viestinnän säännöstöstä annetun direktiivin] mukaisesti ilmoitettujen toimivaltaisten viranomaisten sekä lainvalvonta- ja tietosuojaviranomaisten edustajista.

Tarkistus 147

**Ehdotus asetukseksi
20 artikla – 2 kohta**

Komission teksti

2. ***Pysyvän sidosryhmän*** menettelyt,

Tarkistus

ENISAn neuvoa-antava ryhmä;

(Vastaava muutos tehdään kaikkialle tekstiin. Jos tarkistus hyväksytään, koko tekstiin on tehtävä teknisiä muutoksia.)

Tarkistus

1. Johtokunta perustaa ***avoimella tavalla*** pääjohtajan esityksestä ***ENISAn neuvoa-antavan ryhmän***, joka koostuu asiaan liittyviä sidosryhmiä, kuten tieto- ja viestintätekniiikan alaa, ***muun muassa pk-yrityksiä, kyberturvallisuusdirektiivin mukaisten keskeisten palvelujen tarjoajia***, sähköisten viestintäverkkojen tai yleisön saatavilla olevien palvelujen tarjoajia ja kuluttajajärjestöjä, edustavista tunnustetuista ***turvallisuusasiantuntijoista***, tiedeyhteisöä edustavista kyberturvallisuusasiantuntijoista, ***eurooppalaisten standardointiorganisaatioiden ja EU:n virastojen edustajista*** sekä [eurooppalaisesta sähköisen viestinnän säännöstöstä annetun direktiivin] mukaisesti ilmoitettujen toimivaltaisten viranomaisten sekä lainvalvonta- ja tietosuojaviranomaisten edustajista. ***Johtokunta varmistaa eri sidosryhmien asianmukaisen tasapainoisen edustuksen.***

Tarkistus

2. ***ENISAn neuvoa-antavan ryhmän***

jotka koskevat erityisesti ryhmän jäsenten lukumäärää, sen kokoonpanoa, johtokunnan suorittamaa ryhmän jäsenten nimeämistä, pääjohtajan tekemää esitystä sekä ryhmän toimintaa, määritellään viraston sisäisissä toimintasäännöissä ja julkaistaan.

Tarkistus 148

Ehdotus asetukseksi 20 artikla – 3 kohta

Komission teksti

3. ***Pysyvän sidosryhmän*** puheenjohtajana toimii pääjohtaja tai pääjohtajan tähän tehtävään tapauskohtaisesti nimeämä henkilö.

Tarkistus 149

Ehdotus asetukseksi 20 artikla – 4 kohta

Komission teksti

4. ***Pysyvän sidosryhmän*** jäsenten toimikausi on kaksi ja puoli vuotta. Johtokunnan jäsenet eivät saa olla ***pysyvän sidosryhmän*** jäseniä. Komission ja jäsenvaltioiden asiantuntijoilla on oikeus olla läsnä ***pysyvän sidosryhmän*** kokouksissa ja osallistua sen työhön. Muiden pääjohtajan tärkeiksi katsomien elinten edustajia, jotka eivät ole ***pysyvän sidosryhmän*** jäseniä, voidaan pyytää saapuville ***pysyvän sidosryhmän*** kokouksiin ja osallistumaan sen työhön.

Tarkistus 150

Ehdotus asetukseksi 20 artikla – 4 a kohta (uusi)

menettelyt, jotka koskevat erityisesti ryhmän jäsenten lukumäärää, sen kokoonpanoa, johtokunnan suorittamaa ryhmän jäsenten nimeämistä, pääjohtajan tekemää esitystä sekä ryhmän toimintaa, määritellään viraston sisäisissä toimintasäännöissä ja julkaistaan.

Tarkistus

3. ***ENISAn neuvoa-antavan ryhmän*** puheenjohtajana toimii pääjohtaja tai pääjohtajan tähän tehtävään tapauskohtaisesti nimeämä henkilö.

Tarkistus

4. ***ENISAn neuvoa-antavan ryhmän*** jäsenten toimikausi on kaksi ja puoli vuotta. Johtokunnan jäsenet eivät saa olla ***ENISAn neuvoa-antavan ryhmän*** jäseniä. Komission ja jäsenvaltioiden asiantuntijoilla on oikeus olla läsnä ***ENISAn neuvoa-antavan ryhmän*** kokouksissa ja osallistua sen työhön. Muiden pääjohtajan tärkeiksi katsomien elinten edustajia, jotka eivät ole ***ENISAn neuvoa-antavan ryhmän*** jäseniä, voidaan pyytää saapuville ***ENISAn neuvoa-antavan ryhmän*** kokouksiin ja osallistumaan sen työhön.

4 a. *ENISAn neuvoa-antava ryhmä esittää säännöllisesti vuoden mittaan suunnitelmiensa päivityksiä ja esittää tavoitteensa työohjelmassaan, joka julkaistaan kuuden kuukauden välein avoimuuden varmistamiseksi.*

Tarkistus 151

Ehdotus asetukseksi 20 artikla – 5 kohta

5. ***Pysyvä sidosryhmä*** neuvoo virastoa sen tehtävien hoidossa. Erityisesti se neuvoo pääjohtajaa tämän laatiessa esitystä viraston työohjelmaksi sekä yhteydenpidossa asianmukaisten sidosryhmien kanssa ***kaikissa*** työohjelmaan liittyvissä kysymyksissä.

5. ***ENISAn neuvoa-antava ryhmä*** neuvoo virastoa sen tehtävien hoidossa ***paitsi tämän asetuksen III osaston soveltamisessa***. Erityisesti se neuvoo pääjohtajaa tämän laatiessa esitystä viraston työohjelmaksi sekä yhteydenpidossa asianmukaisten sidosryhmien kanssa työohjelmaan liittyvissä kysymyksissä.

Tarkistus 152

Ehdotus asetukseksi 20 a artikla (uusi)

20 a artikla

Sidosryhmien sertifiointiryhmä

1. ***Pääjohtaja perustaa sidosryhmien sertifiointiryhmän, joka koostuu yleisestä neuvoa-antavasta komiteasta, joka antaa yleisiä neuvoja tämän asetuksen III osaston soveltamista ja perustaa tilapäisiä komiteoita kunkin ehdolla olevan järjestelmän valmistelemista, kehittämistä ja hyväksymistä varten. Tämän ryhmän jäsenet valitaan asiaan liittyviä sidosryhmiä, kuten tieto- ja viestintätekniikan alaa, muun muassa pk-yrityksiä, kyberturvallisuusdirektiivin***

mukaisten keskeisten palvelujen tarjoajia, sähköisten viestintäverkkojen tai yleisön saatavilla olevien palvelujen tarjoajia ja kuluttajajärjestöjä, edustavista tunnustetuista turvallisuusasiantuntijoista, tiedeyhteisöä edustavista kyberturvallisuusasiantuntijoista ja eurooppalaisten standardointiorganisaatioiden edustajista sekä [eurooppalaisesta sähköisen viestinnän säännöstöstä annetun direktiivin] mukaisesti ilmoitettujen toimivaltaisten viranomaisten sekä lainvalvonta- ja tietosuojaviranomaisten edustajista.

2. Sidosryhmien sertifiointiryhmän menettelyt, jotka koskevat erityisesti ryhmän jäsenten lukumäärää, sen kokoonpanoa ja pääjohtajan suorittamaa ryhmän jäsenten nimeämistä, määrittellään viraston sisäisissä toimintasäännöissä, niissä noudatetaan parhaita käytäntöjä kaikkien sidosryhmien oikeudenmukaisen edustuksen ja yhtäläisten oikeuksien varmistamiseksi ja ne julkaistaan.

3. Johtokunnan jäsenet eivät saa olla sidosryhmien sertifiointiryhmän jäseniä. ENISAn neuvoo-antavan ryhmän jäsenet saavat olla myös sidosryhmien sertifiointiryhmän jäseniä. Komission ja jäsenvaltioiden asiantuntijoilla on oikeus olla läsnä sidosryhmien sertifiointiryhmän kokouksissa kutsuttuna. Muiden pääjohtajan tärkeiksi katsomien elinten edustajia voidaan pyytää sidosryhmien sertifiointiryhmän kokouksiin ja osallistumaan sen työhön.

4. Sidosryhmien sertifiointiryhmä neuvoo virastoa sen tehtävien hoidossa tämän asetuksen III osaston osalta. Sillä on erityisesti oikeus ehdottaa komissiolle tämän asetuksen 44 artiklassa tarkoitettua ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän valmistelemista sekä osallistua tämän asetuksen 43–48 ja

53 artiklassa kuvattuihin menettelyihin tällaisten järjestelmien hyväksymiseksi.

Tarkistus 153

Ehdotus asetukseksi 21 a artikla (uusi)

Komission teksti

Tarkistus

21 a artikla

Virastolle esitettävät pyynnöt

- 1. Viraston olisi perustettava yhteyspiste, jonka kautta viraston tavoitteisiin ja tehtäviin kuuluvat neuvonta- ja avustamispyyntöt voidaan esittää. Pyyntöihin on liitettävä taustatiedot käsiteltävästä asiasta. Viraston olisi arvioitava pyyntöjen mahdolliset vaikutukset resursseihin ja määritettävä myöhemmin pyyntöjen johdosta toteutettavat toimenpiteet. Jos virasto torjuu pyynnön, sen on perusteltava päätöksensä.***
- 2. Edellä 1 kohdassa tarkoitettuja pyyntöjä voivat esittää:***
 - a) Euroopan parlamentti***
 - b) neuvosto***
 - c) komissio ja***
 - d) kaikki jäsenvaltioiden nimeämät toimivaltaiset elimet, kuten direktiivin 2002/21/EY 2 artiklassa määritellyt kansalliset sääntelyviranomaiset.***
- 3. Johtokunta vahvistaa viraston sisäisissä toimintasäännöissä 1 ja 2 kohdan soveltamista koskevat käytännön järjestelyt erityisesti virastolle osoitettujen pyyntöjen esittämisen, tärkeysjärjestykseen asettamisen ja seurannan sekä tiedottamisen osalta.***

Tarkistus 154

Ehdotus asetukseksi 24 artikla – 2 kohta

Komission teksti

2. Johtokunnan jäsenten, pääjohtajan, ***pysyvän sidosryhmän*** jäsenten, tilapäisiin työryhmiin osallistuvien ulkopuolisten asiantuntijoiden sekä viraston henkilöstön, mukaan lukien ne toimihenkilöt, jotka on otettu palvelukseen jäsenvaltioiden tilapäisesti lähettäminä virkamiehinä, on myös tehtäviensä päätyttyä noudatettava Euroopan unionin toiminnasta tehdyn sopimuksen 339 artiklan mukaista salassapitovelvollisuutta.

Tarkistus 155

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

Komission teksti

Tarkistus 156

Ehdotus asetukseksi
30 artikla – 2 kohta

Komission teksti

2. Tilintarkastustuomioistuimella on valtuudet tehdä kaikkien virastolta unionin rahoitusta saaneiden avustuksensaajien, toimeksisaajien ja alihankkijoiden osalta asiakirjoihin perustuvia ja paikan päällä suoritettavia tarkastuksia.

Tarkistus 157

Ehdotus asetukseksi

Tarkistus

2. Johtokunnan jäsenten, pääjohtajan, ***ENISAn neuvo-antavan ryhmän*** jäsenten, tilapäisiin työryhmiin osallistuvien ulkopuolisten asiantuntijoiden sekä viraston henkilöstön, mukaan lukien ne toimihenkilöt, jotka on otettu palvelukseen jäsenvaltioiden tilapäisesti lähettäminä virkamiehinä, on myös tehtäviensä päätyttyä noudatettava Euroopan unionin toiminnasta tehdyn sopimuksen 339 artiklan mukaista salassapitovelvollisuutta.

Tarkistus

Alustavan ennakoarvioesityksen on perustuttava tämän asetuksen 21 artiklan 1 kohdassa tarkoitetun yhtenäisen ohjelma-asiakirjan tavoitteisiin ja odotettuihin tuloksiin, ja siinä on otettava huomioon näiden tavoitteiden ja odotettujen tulosten saavuttamiseksi tarvittavat taloudelliset resurssit tulosbudjetoinnin periaatteen mukaisesti.

Tarkistus

2. Tilintarkastustuomioistuimella on valtuudet tehdä kaikkien virastolta unionin rahoitusta saaneiden avustuksensaajien, toimeksisaajien ja alihankkijoiden osalta asiakirjoihin perustuvia ***tarkastuksia*** ja paikan päällä suoritettavia tarkastuksia.

36 artikla – 5 kohta

Komission teksti

5. Viraston toimihenkilöiden henkilökohtaista vastuuta virastoa kohtaan säännellään sen henkilöstöön sovellettavissa asiaa koskevilla määräyksissä.

Tarkistus

5. Viraston toimihenkilöiden henkilökohtaista vastuuta virastoa kohtaan säännellään sen henkilöstöön sovellettavissa asiaa koskevilla määräyksissä. ***On varmistettava henkilöstön tehokas palvelukseenotto.***

Tarkistus 158

Ehdotus asetukseksi 37 artikla – 2 kohta

Komission teksti

2. Euroopan unionin elinten käännöskeskus huolehtii viraston toiminnan edellyttämistä käännöspalveluista.

Tarkistus

2. Euroopan unionin elinten käännöskeskus ***tai muu käännöspalvelujen tarjoaja*** huolehtii viraston toiminnan edellyttämistä käännöspalveluista ***julkisia hankintoja koskevien sääntöjen mukaisesti ja asiaa koskevien varainhoitosääntöjen rajoissa.***

Tarkistus 159

Ehdotus asetukseksi 39 artikla – 1 kohta

Komission teksti

1. Siltä osin kuin on tarpeen tämän asetuksen tavoitteiden saavuttamiseksi virasto voi tehdä yhteistyötä kolmansien maiden toimivaltaisten viranomaisten ja/tai kansainvälisten järjestöjen kanssa. Virasto voi tätä varten vahvistaa työjärjestelyt näiden kolmansien maiden viranomaisten ja kansainvälisten järjestöjen kanssa, edellyttäen että komissio antaa tähän ennakkohyväksynnän. Näistä järjestelyistä ei seuraa oikeudellisia velvoitteita unionille ja sen jäsenvaltioille.

Tarkistus

1. Siltä osin kuin on tarpeen tämän asetuksen tavoitteiden saavuttamiseksi virasto voi tehdä yhteistyötä kolmansien maiden toimivaltaisten viranomaisten ja/tai kansainvälisten järjestöjen kanssa. Virasto voi tätä varten vahvistaa työjärjestelyt näiden kolmansien maiden viranomaisten ja kansainvälisten järjestöjen kanssa, edellyttäen että komissio antaa tähän ennakkohyväksynnän. ***Mahdolliseen yhteistyöhön Naton kanssa voi sisältyä yhteisiä kyberturvallisuusharjoituksia ja yhteistä kyberturvallisuuspoikkeamiin reagoimisen koordinointia.*** Näistä järjestelyistä ei seuraa oikeudellisia velvoitteita unionille ja sen jäsenvaltioille.

Perustelu

Ottaen huomioon kyberpoikkeamien rajatylittävän luonteen ENISAn olisi tarvittaessa tehtävä yhteistyötä muiden Euroopan kyberturvallisuusalan toimijoiden kuten Naton kanssa. Tämä on erityisen tärkeää, koska NATOlla voi olla kybervalmiuksia, joita ENISAlla ei ole, ja päinvastoin. Tapauksessa, jossa valtioita kohtaan kohdistuisi suuri määrä kyberhyökkäyksiä, Euroopan turvallisuuden kannalta on ehdottoman tärkeää, että ENISA tekee yhteistyötä Naton kaltaisten kansainvälisten järjestöjen kanssa kansainvälisellä tasolla.

Tarkistus 160

Ehdotus asetukseksi 41 artikla – 2 kohta

Komission teksti

2. Viraston isäntäjäsenvaltion on tarjottava parhaat mahdolliset edellytykset viraston moitteettomalle toiminnalle, mukaan lukien toimivat liikenneyhteydet sijaintipaikalle, henkilöstön jäsenten lapsille soveltuvat koulunkäyntimahdollisuudet, puolisoiden mahdollisuudet päästä työmarkkinoille sekä riittävä sosiaaliturvan ja terveydenhuoltopalvelujen saatavuus lapsille ja puolisoille.

Tarkistus

2. Viraston isäntäjäsenvaltion on tarjottava parhaat mahdolliset edellytykset viraston moitteettomalle toiminnalle, mukaan lukien **koko viraston sijoittaminen samaan paikkaan**, toimivat liikenneyhteydet sijaintipaikalle, henkilöstön jäsenten lapsille soveltuvat koulunkäyntimahdollisuudet, puolisoiden mahdollisuudet päästä työmarkkinoille sekä riittävä sosiaaliturvan ja terveydenhuoltopalvelujen saatavuus lapsille ja puolisoille.

Perustelu

Viraston nykyinen järjestely, jossa sen hallinto toimii Iráklionissa ja ydintoiminnot hoidetaan Ateenassa, on osoittautunut tehottomaksi ja kalliiksi. ENISAn koko henkilöstön olisi siksi työskenneltävä samassa kaupungissa. Tässä kohdassa mainitut perusteet huomioon ottaen sijaintipaikan olisi oltava Ateena.

Tarkistus 161

Ehdotus asetukseksi 43 artikla – 1 kohta

Komission teksti

Eurooppalaisella kyberturvallisuuden sertifiointijärjestelmällä todistetaan, että **tällaisen järjestelmän mukaisesti sertifioidut tieto- ja viestintätekniikan tuotteet** ja **palvelut** täyttävät määritellyt vaatimukset, jotka koskevat niiden kykyä suojautua tietyllä varmuustasolla toimilta,

Tarkistus

Eurooppalaisella kyberturvallisuuden sertifiointijärjestelmällä todistetaan, että **sertifiointin kattamissa tieto- ja viestintätekniikan tuotteissa, prosesseissa ja palveluissa ei sertifiointin aikana ole tunnettuja haavoittuvuuksia** ja ne täyttävät määritellyt vaatimukset, jotka

joiden tarkoituksena on vaarantaa tallennettujen, siirrettävien tai käsiteltävien tietojen tai kyseisissä tuotteissa, prosesseissa, palveluissa ja järjestelmissä tarjottavien tai välitettävien toimintojen tai palvelujen käytettävyys, aitous, eheys ja luottamuksellisuus.

Tarkistus 162

Ehdotus asetukseksi 44 artikla – -1 kohta (uusi)

Komission teksti

voivat viitata eurooppalaisiin ja kansainvälisiin standardeihin, teknisiin eritelmiin ja tieto- ja viestintätekniiikan teknisiin eritelmiin ja jotka koskevat niiden kykyä suojautua ***koko elinkaarensa ajan*** tietyllä varmuustasolla toimilta, joiden tarkoituksena on vaarantaa tallennettujen, siirrettävien tai käsiteltävien tietojen tai kyseisissä tuotteissa, prosesseissa, palveluissa ja järjestelmissä tarjottavien tai välitettävien toimintojen tai palvelujen käytettävyys, aitous, eheys ja luottamuksellisuus, ***ja ne täyttävät eritellyt turvallisuustavoitteet.***

Tarkistus

-1. Komissio antaa tämän asetuksen täydentämiseksi 55 a artiklan mukaisesti delegoituja säädöksiä unionin jatkuvan työohjelman perustamiseksi eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä varten. Näissä delegoiduissa säädöksissä määritetään unionin tasolla toteutettavat yhteiset toimet ja strategiset painopisteet. Unionin jatkuvaan työohjelmaan on sisällyttävä erityisesti eurooppalaiseen kyberturvallisuuden sertifiointijärjestelmään soveltuvien tieto- ja viestintätekniiikan tuotteiden, prosessien ja palvelujen prioriteettiluettelo sekä analyysi siitä, onko vaatimustenmukaisuuden arviointilaitosten ja kansallisten sertifiointin valvontaviranomaisten keskuudessa olemassa vastaavantasoisia laatua, osaamista ja asiantuntemusta, ja tarvittaessa ehdotus toimenpiteistä, joilla tällainen vastaavuuden taso voidaan saavuttaa.

Ensimmäinen unionin jatkuva työohjelma laaditaan viimeistään ... [kuuden kuukauden kuluttua tämän asetuksen

voimaantulosta], ja päivitetään tarpeen vaatiessa mutta siitä lähtien joka tapauksessa ainakin kahden vuoden välein. Unionin jatkuva työohjelma julkistetaan.

Ennen unionin jatkuvan työohjelman hyväksymistä tai päivittämistä komissio kuulee jäsenvaltioiden sertifiointiryhmää, virastoa ja sidosryhmien sertifiointiryhmää avoimella, läpinäkyvällä ja osallistavalla kuulemisella.

Tarkistus 163

**Ehdotus asetukseksi
44 artikla – -1 a kohta (uusi)**

Komission teksti

Tarkistus

-1 a. Jos se on perusteltua, komissio pyytää virastoa laatimaan ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän. Pyyntö perustuu unionin jatkuvaan työohjelmaan.

Tarkistus 164

**Ehdotus asetukseksi
44 artikla – 1 kohta**

Komission teksti

Tarkistus

1. Kun komissio on esittänyt asiaa koskevan pyynnön, ENISA valmistelee ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän, joka täyttää tämän asetuksen 45, 46 ja 47 artiklassa esitetyt vaatimukset. Jäsenvaltiot tai 53 artiklalla perustettu Euroopan kyberturvallisuuden sertifiointiryhmä, jäljempänä 'sertifiointiryhmä', voivat esittää komissiolle ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän valmistelemista.

1. Ehdolla olevaa eurooppalaista kyberturvallisuuden sertifiointijärjestelmää koskeva pyyntö sisältää soveltamisalan, 45 artiklassa tarkoitetut sovellettavat turvallisuustavoitteet, 47 artiklassa tarkoitetut sovellettavat osatekijät ja määrääjän, johon mennessä tietyn ehdolla olevan järjestelmän on tultava voimaan. Komissio voi pyyntöä laatiessaan kuulla virastoa, jäsenvaltioiden sertifiointiryhmää ja sidosryhmien sertifiointiryhmää.

Tarkistus 165

Ehdotus asetukseksi 44 artikla – 2 kohta

Komission teksti

2. Valmistellessaan 1 kohdassa tarkoitettuja ehdolla olevia järjestelmiä **ENISA** kuulee kaikkia asiaankuuluvia sidosryhmiä ja tekee tiivistä yhteistyötä sertifiointiryhmän kanssa. **Sertifiointiryhmä antaa ENISAlle** apua ja asiantuntijaneuvontaa, jota **ENISA** tarvitsee ehdolla olevan järjestelmän valmistelussa, tarvittaessa myös antamalla lausuntoja.

Tarkistus

2. Valmistellessaan –1 kohdassa (**uusi**) tarkoitettuja ehdolla olevia järjestelmiä **virasto** kuulee kaikkia asiaankuuluvia sidosryhmiä **virallisessa, avoimessa ja osallistavassa kuulemisprosessissa** ja tekee **tämän asetuksen 20 a artiklan mukaisesti** tiivistä yhteistyötä **jäsenvaltioiden** sertifiointiryhmän, **sidosryhmien sertifiointiryhmän, tämän asetuksen 20 a artiklan mukaisten tilapäisten komiteoiden ja eurooppalaisten standardointielinten** kanssa. **Ne antavat virastolle** apua ja asiantuntijaneuvontaa, jota **virasto** tarvitsee ehdolla olevan järjestelmän valmistelussa, tarvittaessa myös antamalla lausuntoja.

Tarkistus 166

Ehdotus asetukseksi 44 artikla – 3 kohta

Komission teksti

3. **ENISA** toimittaa tämän artiklan 2 kohdan mukaisesti valmistellun ehdolla olevan **eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän** komissiolle.

Tarkistus

3. **Virasto** toimittaa tämän artiklan **1 ja** 2 kohdan mukaisesti valmistellun ehdolla olevan **järjestelmän** komissiolle.

Tarkistus 167

Ehdotus asetukseksi 44 artikla – 4 kohta

Komission teksti

4. Komissio voi **ENISA:n** valmisteleman ehdolla olevan järjestelmän pohjalta hyväksyä 55 artiklan **1 kohdan** mukaisesti **täytäntöönpanosäädöksiä** tieto- ja viestintätekniiikan tuotteiden ja

Tarkistus

4. Komissio voi **viraston** valmisteleman ehdolla olevan järjestelmän pohjalta hyväksyä 55 **a** artiklan mukaisesti **delegoituja säädöksiä tämän asetuksen täydentämiseksi** tieto- ja viestintätekniiikan

palvelujen eurooppalaisista kyberturvallisuuden sertifiointijärjestelmistä, jotka täyttävät **tämän asetuksen** 45, 46 ja 47 artiklan vaatimukset.

Tarkistus 168

Ehdotus asetukseksi 44 artikla – 5 kohta

Komission teksti

5. **ENISA** ylläpitää erityistä verkkosivustoa, joka tarjoaa eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä koskevaa tiedotusta ja julkisuutta.

tuotteiden, **prosessien** ja palvelujen eurooppalaisista kyberturvallisuuden sertifiointijärjestelmistä, jotka täyttävät 45, 46 ja 47 artiklan vaatimukset.

Tarkistus

5. **Virasto** ylläpitää erityistä verkkosivustoa, joka tarjoaa eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä koskevaa tiedotusta ja julkisuutta, **mukaan lukien peruutetut ja vanhentuneet sertifiikaatit sekä sertifiointin kattamat kansalliset sertifiikaatit.**

Jos eurooppalainen kyberturvallisuuden sertifiointijärjestelmä täyttää vaatimukset, joita sen on tarkoitus noudattaa ja joista säädetään sovellettavassa unionin yhdenmukaistamislainsäädännössä, komissio julkaisee viipymättä sen viitetiedot Euroopan unionin virallisessa lehdessä ja muita keinoja käyttäen sovellettavassa unionin yhdenmukaistamissäädöksessä säädettyjen edellytysten mukaisesti.

Tarkistus 169

Ehdotus asetukseksi 44 artikla – 5 a kohta (uusi)

Komission teksti

Tarkistus

5 a. Virasto tarkastelee hyväksytyjä järjestelmiä tässä asetuksessa vahvistetun rakenteen mukaisesti niiden voimassaolon päätyttyä 47 artiklan 1 kohdan a c alakohdan mukaisesti tai komission pyynnöstä ja ottaen huomioon asianomaisilta sidosryhmiltä saadun palautteen.

Tarkistus 170

Ehdotus asetukseksi 45 artikla – 1 kohta – johdantokappale

Komission teksti

Eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän suunnittelussa on otettava huomioon soveltuvin osin *seuraavat* turvallisuustavoitteet:

Tarkistus

Eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän suunnittelussa on otettava huomioon soveltuvin osin turvallisuustavoitteet, *joilla varmistetaan*:

Tarkistus 171

Ehdotus asetukseksi 45 artikla – 1 kohta – a alakohta

Komission teksti

a) *suojata tallennetut, siirretyt tai muulla tavoin käsitellyt tiedot vahingossa tapahtuvalta tai luvattomalta tallentamiselta, käsittelyltä, käytöltä tai luovuttamiselta;*

Tarkistus

a) *palvelujen, toimintojen ja tietojen luottamuksellisuus, eheys, saatavuus ja yksityisyys;*

Tarkistus 172

Ehdotus asetukseksi 45 artikla – 1 kohta – b alakohta

Komission teksti

b) *suojata tallennetut, siirretyt tai muulla tavoin käsitellyt tiedot vahingossa tapahtuvalta tai luvattomalta tuhoamiselta, tahattomalta katoamiselta tai muuttamiselta;*

Tarkistus

b) *että palveluihin, toimintoihin ja tietoihin pääsevät ja niitä voivat käyttää vain valtuutetut henkilöt ja/tai järjestelmät ja ohjelmat;*

Tarkistus 173

Ehdotus asetukseksi 45 artikla – 1 kohta – c alakohta

Komission teksti

c) *varmistaa, että valtuutettujen henkilöiden, ohjelmien tai koneiden saatavilla on ainoastaan ne tiedot, palvelut tai toiminnot, joihin näillä on*

Tarkistus

c) *että käytössä on prosessi, jolla tunnistetaan ja dokumentoidaan kaikki tieto- ja viestintätekniikan tuotteissa, prosesseissa ja palveluissa olevat*

käyttöoikeudet;

riippuvuudet ja tunnetut haavoittuvuudet;

Tarkistus 174

Ehdotus asetukseksi
45 artikla – 1 kohta – d alakohta

Komission teksti

d) *tallentaa tieto siitä, mitkä tiedot, toiminnot tai palvelut on ilmoitettu, sekä ilmoituksen ajankohta ja tekijä;*

Tarkistus

d) *että tieto- ja viestintätekniikan tuotteet, prosessit ja palvelut eivät sisällä tunnettuja haavoittuvuuksia;*

Tarkistus 175

Ehdotus asetukseksi
45 artikla – 1 kohta – e alakohta

Komission teksti

e) *varmistaa, että on mahdollista tarkastaa, mitä tietoja, palveluja tai toimintoja on käytetty, sekä käytön ajankohta ja käyttäjä;*

Tarkistus

e) *että käytössä on prosessi, jolla puututaan tieto- ja viestintätekniikan tuotteissa, prosesseissa ja palveluissa äskettäin havaittuihin haavoittuvuuksiin;*

Tarkistus 176

Ehdotus asetukseksi
45 artikla – 1 kohta – f alakohta

Komission teksti

f) *palauttaa tietojen, palvelujen ja toimintojen saatavuus ja käytettävyys mahdollisimman pian fyysisen tai teknisen vian sattuessa;*

Tarkistus

f) *että tieto- ja viestintätekniikan tuotteiden, prosessien ja palveluiden suojaus on oletusarvoista ja sisäänrakennettua;*

Tarkistus 177

Ehdotus asetukseksi
45 artikla – 1 kohta – g alakohta

Komission teksti

g) *varmistaa tieto- ja viestintätekniikan tuotteille ja palveluille ajantasainen ohjelmisto, joka ei sisällä tunnettuja haavoittuvuuksia, ja mekanismit, joilla varmistetaan ohjelmistojen turvalliset*

Tarkistus

g) *että tieto- ja viestintätekniikan tuotteilla ja palveluilla on ajantasainen ohjelmisto, joka ei sisällä tunnettuja haavoittuvuuksia, ja mekanismit, joilla varmistetaan ohjelmistojen turvalliset*

päivitykset.

päivitykset.

Tarkistus 178

Ehdotus asetukseksi 45 artikla – 1 kohta – g a alakohta (uusi)

Komission teksti

Tarkistus

g a) että kyberpoikkeamiin liittyvät muut riskit, kuten henkeen, terveyteen, ympäristöön ja muihin merkittäviin oikeudellisiin etuihin kohdistuvat riskit minimoidaan.

Tarkistus 179

Ehdotus asetukseksi 46 artikla – 1 kohta

Komission teksti

Tarkistus

1. Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määritellä yksi tai useampi varmuustaso – perustaso, korotettu ja/tai korkea – kyseisessä järjestelmässä sertifioiduille tieto- ja viestintätekniikan tuotteille ja palveluille.

1. Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määritellä yksi tai useampi **riskiin perustuva** varmuustaso **tieto- ja viestintätekniikan tuotteiden, prosessien ja palveluiden asiayhteyden ja aiotun käytön mukaan** – perustaso, korotettu ja/tai korkea – kyseisessä järjestelmässä sertifioiduille tieto- ja viestintätekniikan tuotteille, **prosesseille** ja palveluille.

Tarkistus 180

Ehdotus asetukseksi 46 artikla – 2 kohta – a alakohta

Komission teksti

Tarkistus

a) perustasolla oleva varmuustaso **viittaa eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän yhteydessä myönnettyyn sertifikaattiin, joka antaa rajallisen luottamustason** tieto- ja viestintätekniikan **tuotteen tai palvelun vältetyille** tai esitetyille

a) perustasolla oleva varmuustaso **vastaa** tieto- ja viestintätekniikan **tuotteeseen, prosessiin** tai **palveluun liittyvää alhaista riskiä yhdistetyn todennäköisyyden ja vahingon osalta ja ottaen huomioon niiden aiotun käytön ja asiayhteyden; perustasolla oleva varmuustaso tuo varmuuden siitä, että**

kyberturvallisuusominaisuuksille ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on vähentää kyberturvallisuuspoikkeamien riskiä;

tunnetuilta kyberpoikkeamien perustason riskeiltä voidaan suojautua;

Tarkistus 181

Ehdotus asetukseksi
46 artikla – 2 kohta – b alakohta

Komission teksti

b) korotettu varmuustaso *viittaa eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän yhteydessä myönnettyyn sertifiikaattiin, joka antaa korotetun luottamustason* tieto- ja viestintätekniikan *tuotteen* tai *palvelun* *väitetyille tai esitetyille kyberturvallisuusominaisuuksille ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on vähentää merkittävästi kyberturvallisuuspoikkeamien riskiä;*

Tarkistus

b) korotettu varmuustaso *vastaa* tieto- ja viestintätekniikan *tuotteeseen, prosessiin* tai *palveluun liittyvää korkeampaa riskiä yhdistetyn todennäköisyyden ja vahingon osalta; korotettu varmuustaso tuo varmuuden siitä, että tunnetut kyberpoikkeamien riskit voidaan estää ja on myös olemassa valmiudet suojautua kyberhyökkäyksiltä, joilla on rajalliset resurssit;*

Tarkistus 182

Ehdotus asetukseksi
46 artikla – 2 kohta – c alakohta

Komission teksti

c) korkea varmuustaso *viittaa eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän yhteydessä myönnettyyn sertifiikaattiin, joka antaa korotettua varmuustasoa korkeamman luottamustason* tieto- ja viestintätekniikan *tuotteen* tai *palvelun* *väitetyille tai esitetyille kyberturvallisuusominaisuuksille ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on ehkäistä*

Tarkistus

c) korkea varmuustaso *vastaa tieto- ja viestintätekniikan tuotteeseen, prosessiin tai palveluun liittyvää vahinkoa koskevaa korkeaa riskiä. Korkea varmuustaso tuo varmuuden siitä, että kyberpoikkeamien riskit voidaan estää ja on myös olemassa valmiudet suojautua kyberhyökkäyksiltä, joihin liittyy uusinta teknologiaa ja huomattavat resurssit;*

kyberturvallisuuspoikkeamat.

Tarkistus 183

**Ehdotus asetukseksi
46 a artikla (uusi)**

Komission teksti

Tarkistus

46 a artikla

***Eurooppalaisten kyberturvallisuuden
sertifiointijärjestelmien varmuustasojen
arviointi***

- 1. Perustasolla olevalla varmuustasolla tieto- ja viestintätekniikan tuotteen, prosessin tai palvelun valmistaja tai tarjoaja voi tehdä itsearviointin omalla vastuullaan.***
- 2. Korotetulla varmuustasolla arviointi on tehtävä vähintään tarkistamalla, vastaavatko tuotteen, prosessin tai palvelun turvallisuustoiminnot sen teknisiä asiakirjoja.***
- 3. Korkealla varmuustasolla arviointimenetelmään on kuuluttava ainakin tehokkuustestaus, jossa arvioidaan turvallisuustoimintojen kykyä suojautua hyökkäjiltä, joilla on huomattavat resurssit.***

Tarkistus 184

**Ehdotus asetukseksi
47 artikla – 1 kohta – a alakohta**

Komission teksti

Tarkistus

a) sertifiointin kohde ja soveltamisala, mukaan lukien sen kattamien tieto- ja viestintätekniikan tuotteiden ja palvelujen tyyppi tai luokat;

a) sertifiointin kohde ja soveltamisala, mukaan lukien sen kattamien tieto- ja viestintätekniikan tuotteiden, **prosessien** ja palvelujen tyyppi tai luokat;

Tarkistus 185

**Ehdotus asetukseksi
47 artikla – 1 kohta – a a alakohta (uusi)**

Komission teksti

Tarkistus

a a) soveltamisala ja kyberturvallisuusvaatimukset, ja soveltamisalan ja vaatimusten on tarvittaessa vastattava niiden kansallisten kyberturvallisuussertifiointien soveltamisalaa ja vaatimuksia, jotka se korvaa tai joista on annettu säädöksiä;

Tarkistus 186

**Ehdotus asetukseksi
47 artikla – 1 kohta – a b alakohta (uusi)**

Komission teksti

Tarkistus

a b) sertifiointijärjestelmien voimassaoloaika;

Tarkistus 187

**Ehdotus asetukseksi
47 artikla – 1 kohta – b alakohta**

Komission teksti

Tarkistus

b) yksityiskohtainen erittely kyberturvallisuusvaatimuksista, joihin nähden erityiset tieto- ja viestintätekniikan tuotteet ja palvelut arvioidaan, esimerkiksi viittaamalla **unionin** tai kansainvälisiin standardeihin tai teknisiin eritelmiin;

b) yksityiskohtainen erittely kyberturvallisuusvaatimuksista, joihin nähden erityiset tieto- ja viestintätekniikan tuotteet, **prosessit** ja palvelut arvioidaan, esimerkiksi viittaamalla **eurooppalaisiin** tai kansainvälisiin standardeihin, teknisiin eritelmiin tai **tieto- ja viestintätekniikan** teknisiin eritelmiin, **jotka on määritelty siten, että sertifiointi voidaan sisällyttää tai se voi perustua tuottajan systemaattisiin turvallisuusprosesseihin, joita noudatetaan kyseisentuotteen tai palvelun kehityksen ja elinkaaren aikana;**

Tarkistus 188

**Ehdotus asetukseksi
47 artikla – 1 kohta – b a alakohta (uusi)**

Komission teksti

Tarkistus

b a) tiedot tunnetuista kyberuhkista, joita sertifiointi eivät kata, ja ohjeet niiden käsittelemiseksi;

Tarkistus 189

**Ehdotus asetukseksi
47 artikla – 1 kohta – c alakohta**

Komission teksti

Tarkistus

c) soveltuvin osin yksi tai useampi varmuustaso;

c) soveltuvin osin yksi tai useampi varmuustaso ***ottaen huomioon muun muassa riskiperusteisen lähestymistavan;***

Tarkistus 190

**Ehdotus asetukseksi
47 artikla – 1 kohta – c a alakohta (uusi)**

Komission teksti

Tarkistus

c a) maininta siitä, onko itse annettu vaatimustenmukaisuusvakuutus sallittu järjestelmässä, ja menettely, jota sovelletaan vaatimustenmukaisuuden arviointiin tai itse annettuun vaatimustenmukaisuusvakuutukseen tai molempiin;

Tarkistus 191

**Ehdotus asetukseksi
47 artikla – 1 kohta – d alakohta**

Komission teksti

Tarkistus

d) yksittäiset ***arvioinnissa käytettävät perusteet*** ja menetelmät, ***mukaan lukien*** arvioinnin tyypit, jotta voidaan osoittaa, että 45 artiklassa tarkoitetut erityiset tavoitteet saavutetaan;

d) yksittäiset ***arviointiperusteet, vaatimustenmukaisuuden*** arvioinnin tyypit ja menetelmät, jotta voidaan osoittaa, että 45 artiklassa tarkoitetut erityiset tavoitteet saavutetaan;

Tarkistus 192

Ehdotus asetukseksi
47 artikla – 1 kohta – e alakohta

Komission teksti

e) sertifiointiin edellyttämät tiedot, jotka hakijan on toimitettava vaatimustenmukaisuuden arviointilaitoksille;

Tarkistus

e) sertifiointiin edellyttämät tiedot, jotka hakijan on toimitettava vaatimustenmukaisuuden arviointilaitoksille;

Tarkistus 193

Ehdotus asetukseksi
47 artikla – 1 kohta – f alakohta

Komission teksti

f) *jos järjestelmä tarjoaa käyttöön merkkejä tai merkintöjä, näiden merkkien tai merkintöjen käytön edellytykset;*

Tarkistus

f) *tämän asetuksen 47 a artiklan mukaiset kyberturvallisuustiedot;*

Tarkistus 194

Ehdotus asetukseksi
47 artikla – 1 kohta – g alakohta

Komission teksti

g) *jos järjestelmään kuuluu valvonta, säännöt sertifiointien vaatimusten noudattamisen seurantaan varten, mukaan lukien mekanismit sen osoittamiseksi, että määritellyt kyberturvallisuusvaatimuksia noudatetaan jatkuvasti;*

Tarkistus

g) säännöt sertifiointien vaatimusten noudattamisen seurantaan varten, mukaan lukien mekanismit sen osoittamiseksi, että määritellyt kyberturvallisuusvaatimuksia noudatetaan jatkuvasti;

Tarkistus 195

Ehdotus asetukseksi
47 artikla – 1 kohta – h alakohta

Komission teksti

h) ehdot *sertifiointiin* myöntämiselle, voimassa pitämiseksi ja jatkamiseksi sekä sen soveltamisalan laajentamiselle ja supistamiselle;

Tarkistus

h) ehdot *sertifikaatin* myöntämiselle, voimassa pitämiseksi, jatkamiseksi ja *tarkistamiselle* sekä sen soveltamisalan *ja voimassaoloajan* laajentamiselle ja supistamiselle;

Tarkistus 196

Ehdotus asetukseksi 47 artikla – 1 kohta – h a alakohta (uusi)

Komission teksti

Tarkistus

h a) säännöt, jotka koskevat sertifiointin jälkeen mahdollisesti ilmenevien haavoittuvuuksien käsittelyä sellaisen dynaamisen ja jatkuvan organisatorisen prosessin avulla, johon osallistuvat tarjoajat ja käyttäjät;

Tarkistus 197

Ehdotus asetukseksi 47 artikla – 1 kohta – i alakohta

Komission teksti

Tarkistus

i) säännöt seurauksista tapauksissa, joissa sertifioidut tieto- ja viestintätekniikan tuotteet ja palvelut eivät vastaa sertifiointivaatimuksia;

i) säännöt seurauksista tapauksissa, joissa ***itsearvioidut ja*** sertifioidut tieto- ja viestintätekniikan tuotteet ja palvelut eivät vastaa sertifiointivaatimuksia;

Tarkistus 198

Ehdotus asetukseksi 47 artikla – 1 kohta – j alakohta

Komission teksti

Tarkistus

j) säännöt siitä, miten ***aiemmin tuntemattomat*** tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberhaavoittuvuudet on määrä raportoida ja käsitellä;

j) säännöt siitä, miten tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberhaavoittuvuudet, ***jotka eivät olleet julkisessa tiedossa,*** on määrä raportoida ja käsitellä ***sen jälkeen, kun ne on havaittu;***

Tarkistus 199

Ehdotus asetukseksi 47 artikla – 1 kohta – l alakohta

Komission teksti

Tarkistus

l) sellaisten kansallisten kyberturvallisuuden sertifiointijärjestelmien yksilöinti, jotka

l) sellaisten kansallisten ***tai kansainvälisten*** kyberturvallisuuden sertifiointijärjestelmien yksilöinti, jotka

kattavat saman tyyppin tai samojen luokkien tieto- ja viestintäteknii­kan tuotteita ja palveluja;

kattavat saman tyyppin tai samojen luokkien tieto- ja viestintäteknii­kan tuotteita, **prosesseja** ja palveluja, **turvallisuusvaatimuksia ja arviointikriteerejä ja -menetelmiä**;

Tarkistus 200

Ehdotus asetukseksi
47 artikla – 1 kohta – m a alakohta (uusi)

Komission teksti

Tarkistus

m a) kolmansien maiden kanssa suoritettavan sertifiointijärjestelmien vastavuoroisen tunnustamisen edellytykset;

Tarkistus 201

Ehdotus asetukseksi
47 artikla – 1 a kohta (uusi)

Komission teksti

Tarkistus

1 a. Päivityksiä sisältävät ylläpitoprosessit eivät saa johtaa sertifiointin pätemättömyyteen, paitsi jos kyseisillä muutoksilla on huomattava haitallinen vaikutus tieto- ja viestintäteknii­kan tuotteen, palvelun ja prosessin turvallisuuteen.

Tarkistus 202

Ehdotus asetukseksi
47 a artikla (uusi)

Komission teksti

Tarkistus

47 a artikla

Sertifioituja tuotteita, prosesseja ja palveluja koskevat kyberturvallisuustiedot

1. Tämän asetuksen mukaiseen sertifiointijärjestelmään kuuluvien tieto- ja viestintäteknii­kan tuotteiden, prosessien ja palvelujen valmistaja tai tarjoaja toimittaa loppukäyttäjälle

sähköisen tai paperimuodossa olevan asiakirjan, joka sisältää seuraavat tiedot: tieto- ja viestintätekniiikan tuotteen, prosessin ja palvelun aiottuun käyttöön liittyvän sertifiointin varmuustaso; kuvaus riskeistä, joilta suojautumiselta sertifiointin on tarkoitus antaa varmuus; suosituksia siitä, kuinka käyttäjät voivat edelleen edistää tuotteen, prosessin tai palvelun kyberturvallisuutta, säännönmukaisuutta ja tukijaksoa päivitysten jälkeen; soveltuvin osin tietoa siitä, kuinka käyttäjät voivat säilyttää tuotteen, prosessin tai palvelun pääominaisuudet hyökkäyksen tapahtuessa.

2. Tämän artiklan 1 kohdassa tarkoitettuna asiakirjana on oltava saatavilla tuotteen, prosessin tai palvelun koko elinkaaren ajan, kunnes se poistetaan markkinoilta ja vähintään viiden vuoden ajan.

3. Komissio antaa täytäntöönpanosäädöksiä, joilla vahvistetaan malli asiakirjaa varten. Komissio voi pyytää virastoa valmistelemaan malliehdotuksen. Kyseinen täytäntöönpanosäädös hyväksytään tämän asetuksen 55 artiklassa tarkoitettua tarkastelumenettelyä noudattaen.

Tarkistus 203

Ehdotus asetukseksi 48 artikla – 1 kohta

Komission teksti

1. Tieto- ja viestintätekniiikan tuotteet ja palvelut, jotka on sertifioitu jossain 44 artiklan mukaisesti hyväksytyssä eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä, katsotaan kyseisen järjestelmän vaatimusten mukaisiksi.

Tarkistus 204

Tarkistus

1. Tieto- ja viestintätekniiikan tuotteet, **prosessit** ja palvelut, jotka on sertifioitu jossain 44 artiklan mukaisesti hyväksytyssä eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä, katsotaan kyseisen järjestelmän vaatimusten mukaisiksi.

Ehdotus asetukseksi
48 artikla – 4 kohta – johdantokappale

Komission teksti

4. Poiketen siitä, mitä 3 kohdassa säädetään, asianmukaisesti perustelluissa tapauksissa yksittäisessä eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määrätä, että järjestelmästä saatavan eurooppalaisen kyberturvallisuussertifikaatin voi myöntää vain julkinen elin. Tämän julkisen elimen on oltava **joko**

Tarkistus

4. Poiketen siitä, mitä 3 kohdassa säädetään, **ja vain** asianmukaisesti perustelluissa tapauksissa, **kuten kansalliseen turvallisuuteen liittyvistä syistä**, yksittäisessä eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määrätä, että järjestelmästä saatavan eurooppalaisen kyberturvallisuussertifikaatin voi myöntää vain julkinen elin. Tämän julkisen elimen on oltava **tämän asetuksen 51 artiklan 1 kohdan nojalla vaatimustenmukaisuuden arviointilaitoksena akkreditoitu elin. Luonnollisen henkilön tai oikeushenkilön, joka jättää tieto- ja viestintätekniikan tuotteensa tai palvelunsa sertifiotaviksi, on esitettävä 51 artiklassa tarkoitetulle vaatimustenmukaisuuden arviointilaitokselle kaikki sertifiointimenettelyn suorittamiseen tarvittavat tiedot.**

Tarkistus 205

Ehdotus asetukseksi
48 artikla – 5 kohta

Komission teksti

5. Luonnollisen tai oikeushenkilön, joka jättää tieto- ja viestintätekniikan tuotteensa tai palvelunsa sertifiotaviksi, on toimitettava 51 artiklassa tarkoitetulle vaatimustenmukaisuuden arviointilaitokselle kaikki sertifiointimenettelyn suorittamiseen tarvittavat tiedot.

Tarkistus

5. Luonnollisen tai oikeushenkilön, joka jättää tieto- ja viestintätekniikan tuotteensa, palvelunsa tai **prosessinsa** sertifiotaviksi, on toimitettava 51 artiklassa tarkoitetulle vaatimustenmukaisuuden arviointilaitokselle kaikki sertifiointimenettelyn suorittamiseen tarvittavat tiedot, **mukaan luettuina tiedot kaikista tunnetuista turvallisuushaavoittuvuuksista. Sertifiotavaksi jättäminen voi tapahtua mille tahansa 51 artiklassa tarkoitetulle vaatimustenmukaisuuden**

arviointilaitokselle.

Tarkistus 206

Ehdotus asetukseksi 48 artikla – 6 kohta

Komission teksti

6. Sertifikaatit voidaan myöntää **enintään kolmeksi vuodeksi**, ja ne voidaan uusia samoin edellytyksin, jos sovellettavat vaatimukset täyttävät edelleen.

Tarkistus

6. Sertifikaatit voidaan myöntää **kutakin sertifiointijärjestelmää varten tapauskohtaisesti määritetyksi enimmäisajanjaksoksi, joka ei kuitenkaan saa ylittää viittä vuotta**, ja ne voidaan uusia samoin edellytyksin, jos sovellettavat vaatimukset täyttävät edelleen.

Perustelu

Näin varmistetaan joustavuus, jotta voimassaoloaika voidaan mukauttaa käyttötarkoituksen mukaan.

Tarkistus 207

Ehdotus asetukseksi 48 artikla – 7 kohta

Komission teksti

7. Tämän artiklan mukaisesti myönnetty eurooppalainen kyberturvallisuussertifikaatti on tunnustettava kaikissa jäsenvaltioissa.

Tarkistus

7. Tämän artiklan mukaisesti myönnetty eurooppalainen kyberturvallisuussertifikaatti on tunnustettava **kyseisen sertifikaatin kattamia tieto- ja viestintäteknikan tuotteita ja prosesseja sekä kuluttajaelektronikkalaitteita koskevat paikalliset kyberturvallisuusvaatimukset täyttäväksi** kaikissa jäsenvaltioissa **ottaen huomioon 46 artiklassa tarkoitetut määritellyt varmuustasot, eikä tällaisia sertifikaatteja saa syrjiä alkuperäjäsenvaltion tai 51 artiklassa tarkoitetun sertifikaatin antaneen vaatimustenmukaisuuden arviointilaitoksen perusteella.**

Perustelu

Hajanaisuuden välttämiseksi EU:n kyberturvallisuuden sertifiointijärjestelmien

tunnustamisessa ja/tai vaatimustenmukaisuudessa artiklassa on painotettava, että syrjintä sertifiointin myöntämipaikan perusteella ei ole sallittua.

Tarkistus 208

Ehdotus asetukseksi 48 a artikla (uusi)

Komission teksti

Tarkistus

48 a artikla

Keskeisten palvelujen tarjoajille tarkoitettut sertifiointijärjestelmät

- 1. Kun eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät on hyväksytty tämän artiklan 2 kohdan mukaisesti, keskeisten palvelujen tarjoajien on direktiivin (EU) 2016/1148 14 artiklan turvallisuusvaatimusten täyttämiseksi käytettävä kyseisten sertifiointijärjestelmien kattamia tuotteita, prosesseja ja palveluita.***
- 2. Kuultuaan direktiivin (EU) 2016/1148 11 artiklassa tarkoitettua yhteistyöryhmää komissio antaa [vuoden kuluttua tämän asetuksen voimaantulosta] 55 a artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tätä asetusta luettelemalla sellaisten tuotteiden, prosessien ja palvelujen luokat, jotka täyttävät molemmat seuraavista kriteereistä:***
 - a) ne on tarkoitettu keskeisten palvelujen tarjoajien käyttöön ja***
 - b) niiden toimintahäiriöillä olisi erittäin haitallinen vaikutus keskeisen palvelun tarjoamiseen.***
- 3. Komissio antaa 55 a artiklan mukaisesti delegoituja säädöksiä, joilla muutetaan tätä asetusta päivittämällä tarpeen mukaan tämän artiklan 3 kohdassa tarkoitettua tuotteiden, prosessien ja palveluiden luokkien luetteloa.***
- 4. Komissio pyytää virastoa valmistelemaan tämän asetuksen***

44 artiklan -1 kohdan mukaisesti ehdolla olevat eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät tämän artiklan 2 ja 3 kohdassa tarkoitetun tuotteiden, prosessien ja palveluiden luokkien luetteloa varten heti kun kyseinen luettelo on hyväksytty tai päivitetty. Tällaisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti myönnettyjen sertifikaattien on oltava korkealla varmuustasolla.

Tarkistus 209

Ehdotus asetukseksi 48 b artikla (uusi)

Komission teksti

Tarkistus

48 b artikla

Eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä koskevat vastalauseet

- 1. Jos jäsenvaltio katsoo, että eurooppalainen kyberturvallisuuden sertifiointijärjestelmä ei täysin täytä niitä vaatimuksia, jotka sen on tarkoitus kattaa ja joista säädetään soveltuvassa unionin yhdenmukaistamislainsäädännössä, sen on ilmoitettava asiasta komissiolle ja toimitettava asiasta yksityiskohtainen selvitys. Kuultuaan asiaa koskevan unionin yhdenmukaistamislainsäädännön mukaisesti perustettua komiteaa tarpeen vaatiessa tai kuultuaan muulla tavalla alan asiantuntijoita, komissio päättää*
 - a) eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän viitetietojen julkaisemisesta tai julkaisematta jättämisestä taikka julkaisemisesta rajoituksin Euroopan unionin virallisessa lehdessä;*
 - b) eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän viitetietojen säilyttämisestä tai säilyttämisestä rajoituksin Euroopan unionin virallisessa lehdessä taikka niiden poistamisesta*

Euroopan unionin virallisesta lehdestä.

2. Komissio julkaisee verkkosivustollaan tietoa niistä eurooppalaisista kyberturvallisuuden sertifiointijärjestelmistä, joihin on sovellettu tämän artiklan 1 kohdassa tarkoitettua päätöstä.

3. Komissio ilmoittaa virastolle tämän artiklan 1 kohdassa tarkoitettua päätöksestä ja pyytää tarpeen vaatiessa tarkistamaan kyseessä olevaa eurooppalaista kyberturvallisuuden sertifiointijärjestelmää.

4. Tämän artiklan 1 kohdan a alakohdassa tarkoitettu päätös hyväksytään tämän asetuksen 55 artiklan 2 kohdassa tarkoitettua neuvoo-antavaa menettelyä noudattaen.

5. Tämän artiklan 1 kohdan b alakohdassa tarkoitettu päätös hyväksytään tämän asetuksen 55 artiklan 2 a (uusi) kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

Tarkistus 210

Ehdotus asetukseksi 49 artikla – 1 kohta

Komission teksti

1. Sellaisia tieto- ja viestintätekniiikan tuotteita ja palveluja varten voimassa olevat kansalliset kyberturvallisuuden sertifiointijärjestelmät ja niihin liittyvät menettelyt, jotka kuuluvat jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, lakkaavat tuottamasta oikeusvaikutuksia alkaen päivästä, joka vahvistetaan 44 artiklan 4 kohdan nojalla hyväksytyssä täytäntöönpanosäädöksessä, sanotun kuitenkin rajoittamatta 3 kohdan soveltamista. Sellaisia tieto- ja viestintätekniiikan tuotteita ja palveluja varten voimassa olevat kansalliset kyberturvallisuuden sertifiointijärjestelmät ja niihin liittyvät menettelyt, jotka eivät

Tarkistus

1. Sellaisia tieto- ja viestintätekniiikan tuotteita, **prosesseja** ja palveluja varten voimassa olevat kansalliset kyberturvallisuuden sertifiointijärjestelmät ja niihin liittyvät menettelyt, jotka kuuluvat jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, lakkaavat tuottamasta oikeusvaikutuksia alkaen päivästä, joka vahvistetaan 44 artiklan 4 kohdan nojalla hyväksytyssä täytäntöönpanosäädöksessä, sanotun kuitenkin rajoittamatta 3 kohdan soveltamista. Sellaisia tieto- ja viestintätekniiikan tuotteita, **prosesseja** ja palveluja varten voimassa olevat kansalliset kyberturvallisuuden sertifiointijärjestelmät ja niihin liittyvät

kuulu jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, pysyvät edelleen voimassa.

menettelyt, jotka eivät kuulu jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, pysyvät edelleen voimassa.

Tarkistus 211

Ehdotus asetukseksi 49 artikla – 2 kohta

Komission teksti

2. Jäsenvaltiot eivät saa ottaa käyttöön uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä tieto- ja viestintätekniikan tuotteille ja palveluille, jotka kuuluvat jonkin voimassa olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan.

Tarkistus

2. Jäsenvaltiot eivät saa ottaa käyttöön uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä tieto- ja viestintätekniikan tuotteille, *prosesseille* ja palveluille, jotka kuuluvat jonkin voimassa olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan.

Tarkistus 212

Ehdotus asetukseksi 49 artikla – 3 a kohta (uusi)

Komission teksti

Tarkistus

3 a. Jäsenvaltioiden on toimitettava komissiolle kaikki kansallisen kyberturvallisuuden sertifiointijärjestelmien laatimista koskevat pyynnöt ja ilmoitettava syyt niiden hyväksymiselle.

Tarkistus 213

Ehdotus asetukseksi 49 artikla – 3 b kohta (uusi)

Komission teksti

Tarkistus

3 b. Jäsenvaltioiden on pyynnöstä toimitettava muille jäsenvaltioille, virastolle tai komissiolle vähintäänkin sähköisessä muodossa luonnokset kansallisiksi kyberturvallisuuden sertifiointijärjestelmiksi.

Tarkistus 214

Ehdotus asetukseksi 49 artikla – 3 c kohta (uusi)

Komission teksti

Tarkistus

3 c. Jäsenvaltioiden on vastattava kolmen kuukauden kuluessa muilta jäsenvaltioilta, virastolta tai komissiolta mahdollisesti saamiinsa huomautuksiin tämän artiklan 3 b kohdassa tarkoitettua luonnoksesta ja otettava ne asiamukaisesti huomioon, sanotun kuitenkaan rajoittamatta direktiivin (EU) 2015/1535 soveltamista.

Tarkistus 215

Ehdotus asetukseksi 49 artikla – 3 d kohta (uusi)

Komission teksti

Tarkistus

3 d. Jos tämän artiklan 3 kohdan c alakohdan mukaisesti saaduista huomautuksista käy ilmi, että kansallisen kyberturvallisuuden sertifiointijärjestelmän luonnoksella on todennäköisesti kielteinen vaikutus sisämarkkinoiden moitteettomaan toimintaan, huomautuksen saanut jäsenvaltio kuulee virastoa ja komissiota ja ottaa niiden huomautukset tarkasti huomioon ennen järjestelmäluonnoksen hyväksymistä.

Tarkistus 216

Ehdotus asetukseksi 50 artikla – 5 kohta

Komission teksti

Tarkistus

5. Tämän asetuksen tehokkaan täytäntöönpanon varmistamiseksi on aiheellista, että kyseiset viranomaiset osallistuvat 53 artiklan nojalla perustettuun ***Euroopan kyberturvallisuuden***

5. Tämän asetuksen tehokkaan täytäntöönpanon varmistamiseksi on aiheellista, että kyseiset viranomaiset osallistuvat 53 artiklan nojalla perustettuun ***jäsenmaiden*** sertifiointiryhmään

sertifiointiryhmään aktiivisella, tehokkaalla ja turvallisella tavalla.

aktiivisella, tehokkaalla ja turvallisella tavalla.

Tarkistus 217

Ehdotus asetukseksi 50 artikla – 6 kohta – a alakohta

Komission teksti

a) valvottava tämän osaston säännösten soveltamista ja huolehdittava niiden täytäntöönpanosta kansallisella tasolla sekä **valvottava sitä**, ovatko niiden alueelle sijoittautuneiden vaatimustenmukaisuuden arviointilaitosten myöntämät sertifikaatit tämän osaston vaatimusten ja vastaavan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimusten mukaisia;

Tarkistus

a) valvottava tämän osaston säännösten soveltamista ja huolehdittava niiden täytäntöönpanosta kansallisella tasolla sekä **tarkistettava vaatimustenmukaisuus Euroopan kyberturvallisuuden sertifiointiryhmän 53 artiklan 3 kohdan d a alakohdan nojalla hyväksymien sääntöjen mukaisesti**

i) sitä, ovatko niiden alueelle sijoittautuneiden vaatimustenmukaisuuden arviointilaitosten myöntämät sertifikaatit tämän osaston vaatimusten ja vastaavan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimusten mukaisia; **ja**

ii) **sitä, ovatko tieto- ja viestintätekniikan prosessia, tuotetta tai palvelua koskevat jonkin järjestelmän mukaiset itse annetut vaatimustenmukaisuusvakuutukset vaatimusten mukaisia;**

Tarkistus 218

Ehdotus asetukseksi 50 artikla – 6 kohta – b alakohta

Komission teksti

b) seurattava ja valvottava vaatimustenmukaisuuden arviointilaitosten toimintaa tämän asetuksen soveltamiseksi, mukaan lukien vaatimustenmukaisuuden arviointilaitoksista ilmoittaminen ja siihen liittyvät tehtävät tämän asetuksen 52 artiklan mukaisesti;

Tarkistus

b) seurattava ja valvottava **ja vähintään joka toinen vuosi arvioitava** vaatimustenmukaisuuden arviointilaitosten toimintaa tämän asetuksen soveltamiseksi, mukaan lukien vaatimustenmukaisuuden arviointilaitoksista ilmoittaminen ja siihen liittyvät tehtävät tämän asetuksen

52 artiklan mukaisesti;

Tarkistus 219

Ehdotus asetukseksi 50 artikla – 6 kohta – b a alakohta (uusi)

Komission teksti

Tarkistus

***b a) suoritettava tarkastuksia
varmistaakseen, että unionissa
sovelletaan vastaavia vaatimuksia, ja
raportoitava tuloksista virastolle ja
sertifiointiryhmälle;***

Perustelu

Näin voidaan varmistaa, että kaikkialla unionissa sovelletaan samantasoista palvelua ja laatuja, sekä estää mahdollinen ”sertifiointishoppailu”.

Tarkistus 220

Ehdotus asetukseksi 50 artikla – 6 kohta – c alakohta

Komission teksti

Tarkistus

c) käsiteltävä luonnollisten tai oikeushenkilöiden tekemät valitukset, jotka liittyvät niiden alueelle sijoittautuneiden vaatimustenmukaisuuden arviointilaitosten myöntämiin sertifikaatteihin, tutkittava asianmukaisessa määrin valituksen kohde ja ilmoitettava valituksen tekijälle tutkinnan etenemisestä ja tuloksesta kohtuullisessa ajassa;

c) käsiteltävä luonnollisten tai oikeushenkilöiden tekemät valitukset, jotka liittyvät niiden alueelle sijoittautuneiden vaatimustenmukaisuuden arviointilaitosten myöntämiin sertifikaatteihin ***tai vaatimustenmukaisuuden itsearviointeihin***, tutkittava asianmukaisessa määrin valituksen kohde ja ilmoitettava valituksen tekijälle tutkinnan etenemisestä ja tuloksesta kohtuullisessa ajassa;

Tarkistus 221

Ehdotus asetukseksi 50 artikla – 6 kohta – c a alakohta (uusi)

Komission teksti

Tarkistus

c a) raportoitava a alakohdan mukaisten tarkistusten ja b alakohdan mukaisten arviointien tuloksista virastolle ja Euroopan kyberturvallisuuden

sertifiointiryhmälle;

Tarkistus 222

Ehdotus asetukseksi 50 artikla – 6 kohta – d alakohta

Komission teksti

d) tehtävä yhteistyötä muiden kansallisten sertifiointin valvontaviranomaisten tai muiden viranomaisten kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniiikan tuotteet ja palvelut eivät vastaa tämän asetuksen tai yksittäisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien vaatimuksia;

Tarkistus

d) tehtävä yhteistyötä muiden kansallisten sertifiointin valvontaviranomaisten tai muiden viranomaisten, **kuten kansallisten tietosuojan valvontaviranomaisten**, kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniiikan tuotteet, **prosessit** ja palvelut eivät vastaa tämän asetuksen tai yksittäisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien vaatimuksia;

Tarkistus 223

Ehdotus asetukseksi 50 artikla – 6 kohta – d alakohta

Komission teksti

d) tehtävä yhteistyötä muiden kansallisten sertifiointin valvontaviranomaisten tai muiden viranomaisten kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniiikan tuotteet ja palvelut eivät vastaa tämän asetuksen tai yksittäisten eurooppalaisten **kyberturvallisuuden** sertifiointijärjestelmien vaatimuksia;

Tarkistus

d) tehtävä yhteistyötä muiden kansallisten sertifiointin valvontaviranomaisten tai muiden viranomaisten, **kuten kansallisten tietosuojan valvontaviranomaisten**, kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniiikan tuotteet ja palvelut eivät vastaa tämän asetuksen tai yksittäisten eurooppalaisten **tietoteknisen turvallisuuden** sertifiointijärjestelmien vaatimuksia;

Perustelu

Tämä on otettu Euroopan tietosuojavaltuutetun lausunnosta.

Tarkistus 224

Ehdotus asetukseksi
50 artikla – 7 kohta – c a alakohta (uusi)

Komission teksti

Tarkistus

c a) peruuttaa sellaisten kansallisten vaatimustenmukaisuuden arviointilaitosten akkreditointi, jotka eivät ole tämän asetuksen mukaisia;

Tarkistus 225

Ehdotus asetukseksi
50 artikla – 7 kohta – e alakohta

Komission teksti

Tarkistus

e) peruuttaa kansallisen lainsäädännön mukaisesti sertifikaatit, jotka eivät täytä tämän asetuksen tai eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimuksia;

e) peruuttaa kansallisen lainsäädännön mukaisesti sertifikaatit, jotka eivät täytä tämän asetuksen tai eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimuksia, **ja tiedottaa asiasta vastaavasti kansallisille akkreditointielimille;**

Tarkistus 226

Ehdotus asetukseksi
50 artikla – 8 kohta

Komission teksti

Tarkistus

8. Kansallisten sertifiointin valvontaviranomaisten on tehtävä yhteistyötä keskenään ja komission kanssa ja erityisesti vaihdettava tietoja, kokemuksia ja hyviä käytäntöjä tieto- ja viestintätekniiikan tuotteiden ja palvelujen kyberturvallisuussertifiointista ja niiden kyberturvallisuuteen liittyvistä teknisistä kysymyksistä.

8. Kansallisten sertifiointin valvontaviranomaisten on tehtävä yhteistyötä keskenään ja komission kanssa ja erityisesti vaihdettava tietoja, kokemuksia ja hyviä käytäntöjä tieto- ja viestintätekniiikan tuotteiden, **prosessien** ja palvelujen kyberturvallisuussertifiointista ja niiden kyberturvallisuuteen liittyvistä teknisistä kysymyksistä.

Tarkistus 227

Ehdotus asetukseksi
50 artikla – 8 a kohta (uusi)

Komission teksti

Tarkistus

8 a. Kunkin kansallisen sertifiointin valvontaviranomaisen ja kunkin kansallisen sertifiointin valvontaviranomaisen jäsenen ja henkilöstön on unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti pidettävä salassa sekä toimikautensa aikana että sen jälkeen kaikki luottamukselliset tiedot, jotka ovat tulleet heidän tietoonsa heidän suorittaessaan tehtäviään tai käyttäessään valtuuksiaan.

Tarkistus 228

**Ehdotus asetukseksi
50 a artikla (uusi)**

Komission teksti

Tarkistus

50 a artikla

Vertaisarviointi

- 1. Kansallisista sertifiointin valvontaviranomaisista on tehtävä vertaisarviointi kaikkien niiden viraston järjestämien toimintojen osalta, joita ne suorittavat 50 artiklan mukaisesti.**
- 2. Vertaisarvioinnissa käytetään luotettavia ja avoimia arviointiperusteita ja -menettelyjä, erityisesti kun on kyse rakenteista, henkilöresursseista ja prosesseista koskevista vaatimuksista, luottamuksellisuudesta ja valituksista. On säädettävä tällaisen arvioinnin perusteella tehtäviä päätöksiä koskevista asianmukaisista muutoksenhakumenettelyistä.**
- 3. Vertaisarvioinnissa on arvioitava kansallisten sertifiointin valvontaviranomaisten käyttöön ottamia menettelyjä, erityisesti menettelyjä, joilla tarkastetaan, että sertifikaatit, vaatimustenmukaisuuden arviointilaitosten toiminnan seuranta ja valvontaa koskevat menettelyt, henkilöstön pätevyys, tarkastusten ja tarkastus menetelmien oikeellisuus sekä tulosten paikkansapitävyys ovat vaatimusten mukaisia.**

Vertaisarvioinnissa on myös arvioitava, onko kyseisillä kansallisilla sertifiointin valvontaviranomaisilla riittävät resurssit tehtäviensä asianmukaiseen hoitamiseen, kuten 50 artiklan 4 kohdassa edellytetään.

4. Kansallisten sertifiointin valvontaviranomaisten vertaisarvioinnin toteuttavat kaksi muiden jäsenvaltioiden kansallista sertifiointin valvontaviranomaista ja komissio, ja se toteutetaan vähintään kerran viidessä vuodessa. Virasto voi osallistua vertaisarviointiin ja se päättää osallistumisestaan riskinarviointianalyysin perusteella.

5. Komissio voi antaa 55 a artiklan mukaisesti tätä asetusta täydentäviä delegoituja säädöksiä, joilla vahvistetaan vähintään viideksi vuodeksi vertaisarviointeja varten suunnitelma, jossa esitetään perusteet vertaisarviointiryhmän kokoonpanolle, vertaisarvioinnissa käytetyt menetelmät, aikataulu, arviointien suoritusihteys ja muut arviointiin liittyvät tehtävät. Tällaisia delegoituja säädöksiä antaessaan komissio ottaa asianmukaisesti huomioon jäsenvaltioiden sertifiointiryhmän huomautukset.

6. Jäsenvaltioiden sertifiointiryhmä tarkastelee vertaisarviointien tuloksia. Virasto laatii tuloksista yhteenvedon ja antaa tarvittaessa ohjeita ja parhaita käytäntöjä koskevia asiakirjoja ja julkistaa ne.

Tarkistus 229

**Ehdotus asetukseksi
51 artikla – 1 a kohta (uusi)**

Komission teksti

Tarkistus

1 a. Kun on kyse korkeasta varmuustasosta, vaatimustenmukaisuuden arviointilaitoksen on akkreditoinnin

lisäksi saatava kansallisen sertifiointin valvontaviranomaisen ilmoitus kyberturvallisuuden arviointiin liittyvästä pätevyydestään ja asiantuntemuksestaan. Kansallisen sertifiointin valvontaviranomaisen on tehtävä säännöllisesti tarkastuksia ilmoitettujen vaatimustenmukaisuuden arviointilaitosten pätevyydestä ja asiantuntemuksesta.

Perustelu

Korkeat varmuustasot edellyttävät tehokkuustestausta. Tehokkuustestejä suorittavien vaatimustenmukaisuuden arviointilaitosten pätevyys ja asiantuntemus on tarkastettava säännöllisesti, jotta saadaan varmuus testien laadusta.

Tarkistus 230

**Ehdotus asetukseksi
51 artikla – 2 a kohta (uusi)**

Komission teksti

Tarkistus

2 a. On tehtävä tarkastuksia, jotta voidaan varmistaa, että unionissa sovelletaan vastaavanlaisia vaatimuksia, ja tuloksista on raportoitava virastolle ja sertifiointiryhmälle.

Tarkistus 231

**Ehdotus asetukseksi
51 artikla – 2 b kohta (uusi)**

Komission teksti

Tarkistus

2 b. Jos valmistajat valitsevat tämän asetuksen 48 artiklan 3 kohdan mukaisen itse annettavan vaatimustenmukaisuusvakuutuksen, vaatimustenmukaisuuden arviointilaitokset ryhtyvät lisätoimiin niiden sisäisten menettelyjen varmentamiseksi, joihin valmistaja on ryhtynyt sen varmistamiseksi, että sen tuotteet ja/tai palvelut ovat eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimusten

mukaisia.

Tarkistus 232

Ehdotus asetukseksi 52 artikla – 5 kohta

Komission teksti

5. Komissio voi **täytäntöönpanosäädöksillä** määritellä olosuhteet, muutoseikat ja menettelyt tämän artiklan 1 kohdassa tarkoitetuille ilmoituksille. Nämä **täytäntöönpanosäädökset** hyväksytään 55 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

Tarkistus

5. Komissio voi **delegoiduilla säädöksillä** määritellä olosuhteet, muutoseikat ja menettelyt tämän artiklan 1 kohdassa tarkoitetuille ilmoituksille. Nämä **delegoidut säädökset** hyväksytään 55 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

Tarkistus 233

Ehdotus asetukseksi 53 artikla – otsikko

Komission teksti

Euroopan kyberturvallisuuden sertifiointiryhmä

Tarkistus

Jäsenvaltioiden sertifiointiryhmä

(Vastaava muutos tehdään kaikkialle tekstiin. Jos tarkistus hyväksytään, koko tekstiin on tehtävä teknisiä muutoksia.)

Tarkistus 234

Ehdotus asetukseksi 53 artikla – 1 kohta

Komission teksti

1. Perustetaan **Euroopan kyberturvallisuuden** sertifiointiryhmä, jäljempänä 'sertifiointiryhmä'.

Tarkistus

1. Perustetaan **jäsenmaiden** sertifiointiryhmä, jäljempänä 'sertifiointiryhmä'.

Tarkistus 235

Ehdotus asetukseksi 53 artikla – 2 kohta

Komission teksti

2. **Ryhmä** koostuu kansallisista sertifiointin valvontaviranomaisista. Kansallisten sertifiointin valvontaviranomaisten on oltava edustettuina johtajatasolla tai muulla korkealla tasolla.

Tarkistus

2. **Jäsenvaltioiden sertifiointiryhmä** koostuu **kunkin jäsenvaltion** kansallisista sertifiointin valvontaviranomaisista. Kansallisten sertifiointin valvontaviranomaisten on oltava edustettuina johtajatasolla tai muulla korkealla tasolla. **Sidosryhmien sertifiointiryhmän jäsenet voidaan kutsua ryhmän kokouksiin ja osallistumaan sen työhön.**

Tarkistus 236

Ehdotus asetukseksi
53 artikla – 3 kohta – johdantokappale

Komission teksti

3. **Sertifiointiryhmän** tehtävänä on

Tarkistus

3. **Jäsenmaiden sertifiointiryhmän** tehtävänä on

Tarkistus 237

Ehdotus asetukseksi
53 artikla – 3 kohta – b alakohta

Komission teksti

b) avustaa ja neuvoa **ENISAa** ja tehdä sen kanssa yhteistyötä ehdolla olevan järjestelmän valmistelemisessä tämän asetuksen 44 artiklan mukaisesti;

Tarkistus

b) avustaa ja neuvoa **virastoa** ja tehdä sen kanssa yhteistyötä ehdolla olevan järjestelmän valmistelemisessä tämän asetuksen 44 artiklan mukaisesti;

Tarkistus 238

Ehdotus asetukseksi
53 artikla – 3 kohta – d a alakohta (uusi)

Komission teksti

Tarkistus

d a) hyväksyä suosituksia, joissa määritetään, kuinka usein kansallisten sertifiointin valvontaviranomaisten on suoritettava sertifiointien ja vaatimustenmukaisuuden itsearviointien varmentamisia, sekä näiden

varmennusten kriteerit, laajuus ja soveltamisala, ja hyväksyä yhteiset säännöt ja standardit raportoinnille 50 artiklan 6 kohdan mukaisesti.

Tarkistus 239

Ehdotus asetukseksi 53 artikla – 3 kohta – e alakohta

Komission teksti

e) tarkastella merkityksellistä kehitystä kyberturvallisuussertifiointin alalla ja vaihtaa hyviä käytäntöjä kyberturvallisuuden sertifiointijärjestelmistä;

Tarkistus

e) tarkastella merkityksellistä kehitystä kyberturvallisuussertifiointin alalla ja vaihtaa **tietoa ja** hyviä käytäntöjä kyberturvallisuuden sertifiointijärjestelmistä;

Tarkistus 240

Ehdotus asetukseksi 53 artikla – 3 kohta – f a alakohta (uusi)

Komission teksti

Tarkistus

f a) helpottaa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukauttamista kansainvälisesti tunnustettuihin standardeihin muun muassa tarkastamalla nykyisiä eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä ja antamalla tarvittaessa virastolle suosituksia aloista, joilla sen olisi puututtava yhdessä asiaankuuluvien kansainvälisten standardointiorganisaatioiden kanssa saatavilla olevien kansainvälisesti tunnustettujen standardien puutteisiin tai aukkoihin;

Tarkistus 241

Ehdotus asetukseksi 53 artikla – 3 kohta – f b alakohta (uusi)

Komission teksti

Tarkistus

f b) ottaa käyttöön vertaisarviointiprosessi. Prosessi koskee erityisesti kansallisia sertifiointin valvontaviranomaisia niiden 48 ja 50 artiklassa tarkoitettujen tehtävien toteuttamisen osalta, ja siihen sisältyy tarvittaessa ohjeiden ja parhaita käytäntöjä koskevien asiakirjojen laatiminen, jotta kansalliset sertifiointin valvontaviranomaiset noudattaisivat paremmin tätä asetusta.

Tarkistus 242

**Ehdotus asetukseksi
53 artikla – 3 kohta – f c alakohta (uusi)**

Komission teksti

Tarkistus

f c) valvoa sertifiikaatin seurantaa ja ylläpitämistä.

Tarkistus 243

**Ehdotus asetukseksi
53 artikla – 3 kohta – f d alakohta (uusi)**

Komission teksti

Tarkistus

f d) ottaa huomioon ehdolla olevan järjestelmän valmistelun yhteydessä toteutetun sidosryhmien kuulemisen tulokset 44 artiklan mukaisesti;

Tarkistus 244

**Ehdotus asetukseksi
53 artikla – 4 kohta**

Komission teksti

Tarkistus

4. ***Sertifiointiryhmän*** puheenjohtajana ja sihteeristönä toimii komissio ***ENISAn*** avustuksella siten kuin 8 artiklan a alakohdassa säädetään.

4. ***Jäsenvaltioiden sertifiointiryhmän*** puheenjohtajana ja sihteeristönä toimii komissio ***viraston*** avustuksella siten kuin 8 artiklan a alakohdassa säädetään.

Tarkistus 245

Ehdotus asetukseksi 53 a artikla (uusi)

Komission teksti

Tarkistus

53a artikla

***Oikeus tehokkaisiin oikeussuojakeinoihin
valvontaviranomaista tai
vaatimustenmukaisuuden arviointilaitosta
vastaan***

***1. Rajoittamatta muita hallinnollisia
muutoksenhakukeinoja tai muita kuin
oikeudellisia oikeussuojakeinoja
jokaisella luonnollisella henkilöllä tai
oikeushenkilöllä on oikeus tehokkaisiin
oikeussuojakeinoihin***

***a) sitä koskevaa
vaatimustenmukaisuuden
arviointilaitoksen tai kansallisen
sertifioinnin valvontaviranomaisen
päätöstä vastaan, mukaan lukien
soveltuvien osien päätös myöntää, olla
myöntämättä tai tunnustamatta henkilön
hallussa olevaa eurooppalaista
kyberturvallisuussertifikaattia, ja***

***b) kun kansallinen sertifioinnin
valvontaviranomainen ei käsittele sen
toimivaltaan kuuluvaa valitusta.***

***2. Oikeustoimet
vaatimustenmukaisuuden arviointilaitosta
tai kansallista sertifioinnin
valvontaviranomaista vastaan on
nostettava sen jäsenvaltion
tuomioistuimessa, johon
vaatimustenmukaisuuden arviointilaitos
tai kansallinen sertifioinnin
valvontaviranomainen on sijoittautunut.***

Tarkistus 246

Ehdotus asetukseksi 55 artikla – 2 a kohta (uusi)

Komission teksti

Tarkistus

2 a. Kun viitataan tähän kohtaan, sovelletaan asetuksen (EU) N:o 182/2011 5 artiklaa.

Tarkistus 247

**Ehdotus asetukseksi
55 a artikla (uusi)**

Komission teksti

Tarkistus

55 a artikla

Siirretyn säädösvallan käyttäminen

- 1. Siirretään komissiolle valta antaa delegoituja säädöksiä tässä artiklassa säädetyin edellytyksin.**
- 2. Siirretään komissiolle ... päivästä ...kuuta ... [perussäädöksen voimaantulopäivä] määräämättömäksi ajaksi 44 ja 48 a artiklassa tarkoitettu valta antaa delegoituja säädöksiä.**
- 3. Euroopan parlamentti tai neuvosto voi milloin tahansa peruuttaa 44 ja 48 a artiklassa tarkoitettun säädösvallan siirron. Peruuttamispäätöksellä lopetetaan tuossa päätöksessä mainittu säädösvallan siirto. Peruuttaminen tulee voimaan sitä päivää seuraavana päivänä, jona sitä koskeva päätös julkaistaan Euroopan unionin virallisessa lehdessä, tai jonakin myöhempänä, kyseisessä päätöksessä mainittuna päivänä. Peruuttamispäätös ei vaikuta jo voimassa olevien delegoitujen säädösten pätevyYTEEN.**
- 4. Ennen kuin komissio hyväksyy delegoidun säädöksen, se kuulee kunkin jäsenvaltion nimeämiä asiantuntijoita paremmasta lainsäädännöstä 13 päivänä huhtikuuta 2016 tehdyssä toimielinten sopimuksessa vahvistettujen periaatteiden mukaisesti.**
- 5. Heti kun komissio on antanut delegoidun säädöksen, komissio antaa sen**

tiedoksi yhtäaikaisesti Euroopan parlamentille ja neuvostolle.

6. Edellä olevan 44 ja 48 a artiklan nojalla annettu delegoitu säädös tulee voimaan ainoastaan, jos Euroopan parlamentti tai neuvosto ei ole kahden kuukauden kuluessa siitä, kun asianomainen säädös on annettu tiedoksi Euroopan parlamentille ja neuvostolle, ilmaissut vastustavansa sitä tai jos sekä Euroopan parlamentti että neuvosto ovat ennen mainitun määräajan päättymistä ilmoittaneet komissiolle, että ne eivät vastusta säädöstä. Euroopan parlamentin tai neuvoston aloitteesta tätä määräaikaa jatketaan kahdella kuukaudella.

Tarkistus 248

Ehdotus asetukseksi 56 artikla – 1 kohta

Komission teksti

1. Komissio arvioi viimeistään **viiden** vuoden kuluttua 58 artiklassa tarkoitettua päivämäärästä ja sen jälkeen **viiden** vuoden välein viraston ja sen työtapojen vaikutuksen, tehokkuuden ja tuloksellisuuden sekä mahdollisen tarpeen muuttaa viraston toimeksiantoa ja tällaisten muutosten taloudelliset vaikutukset. Arvioinnissa otetaan huomioon viraston toiminnastaan mahdollisesti saama palaute. Jos komissio katsoo, ettei viraston toiminnan jatkaminen ole enää perusteltua sille asetettuihin tavoitteisiin, toimeksiantoon ja tehtäviin nähden, se voi ehdottaa, että tätä asetusta muutetaan virastoa koskevien säännösten osalta.

Tarkistus 249

Ehdotus asetukseksi 56 artikla – 2 kohta

Komission teksti

2. Arvioinnissa arvioidaan myös

Tarkistus

1. Komissio arvioi viimeistään **kahden** vuoden kuluttua 58 artiklassa tarkoitettua päivämäärästä ja sen jälkeen **kahden** vuoden välein viraston ja sen työtapojen vaikutuksen, tehokkuuden ja tuloksellisuuden sekä mahdollisen tarpeen muuttaa viraston toimeksiantoa ja tällaisten muutosten taloudelliset vaikutukset. Arvioinnissa otetaan huomioon viraston toiminnastaan mahdollisesti saama palaute. Jos komissio katsoo, ettei viraston toiminnan jatkaminen ole enää perusteltua sille asetettuihin tavoitteisiin, toimeksiantoon ja tehtäviin nähden, se voi ehdottaa, että tätä asetusta muutetaan virastoa koskevien säännösten osalta.

2. Arvioinnissa arvioidaan myös

III osaston säännösten vaikutusta, tehokkuutta ja tuloksellisuutta suhteessa tavoitteisiin varmistaa tieto- ja viestintäteknikan tuotteiden ja palvelujen kyberturvallisuuden riittävä taso unionissa ja parantaa sisämarkkinoiden toimintaa.

Tarkistus 250

Ehdotus asetukseksi 56 artikla – 2 a kohta (uusi)

Komission teksti

III osaston säännösten vaikutusta, tehokkuutta ja tuloksellisuutta suhteessa tavoitteisiin varmistaa tieto- ja viestintäteknikan tuotteiden, *prosessien* ja palvelujen kyberturvallisuuden riittävä taso unionissa ja parantaa sisämarkkinoiden toimintaa.

Tarkistus

2 a. *Arvioinnissa arvioidaan, ovatko sisämarkkinoille pääsyä koskevat keskeiset kyberturvallisuusvaatimukset tarpeen, jotta voidaan estää sellaisten tuotteiden, palveluiden ja prosessien pääsy unionin markkinoille, jotka eivät täytä kyberturvallisuuden perusvaatimuksia.*

Tarkistus 251

Ehdotus asetukseksi Liite -I (uusi)

Komission teksti

Tarkistus

LIITE -I

On todennäköistä, että Euroopan kyberturvallisuuden sertifiointikehystä käyttöön otettaessa huomio kiinnittyy välittömästi merkittäviin aloihin uusien teknologioiden haasteisiin vastaamiseksi. Erityisesti esineiden internet on mielenkiinnon kohteena, sillä se koskee sekä kuluttajien että teollisuuden vaatimuksia. Sertifiointikehyksen osalta ehdotetaan seuraavaa prioriteettiluetteloa:

- 1) Pilvipalvelun tarjonnan sertifiointi.**
- 2) Esineiden internetin laitteiden sertifiointi, mukaan lukien:**
 - a. yksilötason laitteet, kuten puettavat**

älylaitteet;

b. yhteisötason laitteet, kuten älyautot, älykodit, terveydenhoitolaitteet;

c. yhteiskunnan tason laitteet, kuten älykkäät kaupungit ja älykkäät verkot.

3) Teollisuus 4.0, joka käsittää älykkäät, toisiinsa yhdistetyt kyberfyysiset järjestelmät, joilla automatisoidaan kaikki teollisen toiminnan vaiheet suunnittelusta ja valmistuksesta toimintaan, toimitusketjuun ja palvelujen ylläpitoon;

4) Arkielämässä käytettävän teknologian ja tuotteiden sertifiointi. Esimerkkejä tällaisista voisivat olla verkkolaitteet, kuten kotitalouksien verkkoreitittimet.

Tarkistus 252

Ehdotus asetukseksi

Liite I – 1 kohta – 5 a alakohta (uusi)

Komission teksti

Tarkistus

5 a. Jos vaatimustenmukaisuuden arviointilaitoksen omistaa tai sen toimintaa harjoittaa julkinen taho tai laitos, riippumattomuus ja eturistiriitojen pois sulkeminen on varmistettava ja dokumentoitava sertifiointiin valvontaviranomaisen ja vaatimustenmukaisuuden arviointilaitoksen välillä.

Tarkistus 253

Ehdotus asetukseksi

Liite I – 1 kohta – 8 alakohta

Komission teksti

Tarkistus

8. Vaatimustenmukaisuuden arviointilaitoksen on kyettävä suorittamaan kaikki vaatimustenmukaisuuden arviointitehtävät, jotka sille on tässä asetuksessa osoitettu, siitä riippumatta, suorittaako vaatimustenmukaisuuden arviointilaitos kyseiset tehtävät itse vai

8. Vaatimustenmukaisuuden arviointilaitoksen on kyettävä suorittamaan kaikki vaatimustenmukaisuuden arviointitehtävät, jotka sille on tässä asetuksessa osoitettu, siitä riippumatta, suorittaako vaatimustenmukaisuuden arviointilaitos kyseiset tehtävät itse vai

suoritetaanko ne sen puolesta ja sen vastuulla.

suoritetaanko ne sen puolesta ja sen vastuulla. ***Kaikki alihankinta tai ulkopuolisen henkilöstön kuuleminen on dokumentoitava asianmukaisesti, siihen ei saa osallistua välittäjiä, ja siitä on laadittava kirjallinen sopimus, jossa sovitaan muun muassa luottamuksellisuudesta ja eturistiriidoista. Kyseisen vaatimustenmukaisuuden arviointilaitoksen on kannettava täysi vastuu suoritetuista tehtävistä.***

Tarkistus 254

Ehdotus asetukseksi Liite I – 1 kohta – 12 alakohta

Komission teksti

12. Vaatimustenmukaisuuden arviointilaitosten, niiden ylimmän johdon ja arviointihenkilöstön puolueettomuus on taattava.

Tarkistus

12. Vaatimustenmukaisuuden arviointilaitosten, niiden ylimmän johdon ja arviointihenkilöstön ***ja alihankkijoiden*** puolueettomuus on taattava.

Tarkistus 255

Ehdotus asetukseksi Liite I – 1 kohta – 15 alakohta

Komission teksti

15. Vaatimustenmukaisuuden ***arviointilaitosten henkilöstöllä*** on vaitiolovelvollisuus kaikkien niiden tietojen suhteen, joita ***se saa*** suorittaessaan tehtäviään tämän asetuksen tai sen täytäntöön panemiseksi annetun kansallisen lainsäädännön säännösten mukaisesti, paitsi niiden jäsenvaltioiden ***toimivaltaisiin viranomaisiin nähden***, joissa laitoksen toimet suoritetaan.

Tarkistus

15. Vaatimustenmukaisuuden ***arviointilaitoksen ja sen henkilöstön, komiteoiden, tytäryhtiöiden, alihankkijoiden ja laitokseen yhteydessä olevien elinten tai ulkoisten elinten henkilöstön on ylläpidettävä luottamuksellisuutta ja niillä*** on vaitiolovelvollisuus kaikkien niiden tietojen suhteen, joita ***ne saavat*** suorittaessaan tehtäviään tämän asetuksen tai sen täytäntöön panemiseksi annetun kansallisen lainsäädännön säännösten mukaisesti, paitsi ***kun näihin sovelletaan unionin tai jäsenvaltion lainsäädäntöä, jossa edellytetään niiden julkistamista, lukuun ottamatta*** niiden jäsenvaltioiden ***toimivaltaisten viranomaisten osalta***, joissa laitoksen toimet suoritetaan.

***Omistusoikeudet on suojattava.
Vaatimustenmukaisuuden
arviointilaitoksella on oltava käytössä
tämän jakson 15 vaatimusten mukaiset
dokumentoidut menettelyt.***

Tarkistus 256

**Ehdotus asetukseksi
Liite I – 1 kohta – 15 a alakohta (uusi)**

Komission teksti

Tarkistus

***15 a. Jaksoa 15 lukuun ottamatta tämän
liitteen vaatimukset eivät estä millään
tavalla teknisten tietojen ja
sääntelyohjeistuksen vaihtoa
vaatimustenmukaisuuden
arviointilaitoksen ja sertifiointia hakevan
tai sitä harkitsevan henkilön välillä.***

Tarkistus 257

**Ehdotus asetukseksi
Liite I – 1 kohta – 15 b alakohta (uusi)**

Komission teksti

Tarkistus

***15 b. Vaatimustenmukaisuuden
arviointilaitosten on toimittava
johdonmukaisilla, oikeudenmukaisilla ja
kohtuullisilla ehdoilla ja edellytyksillä ja
otettava huomioon suosituksessa
2003/361/EY tarkoitettujen pienten ja
keskisuurten yritysten maksuihin liittyvät
edut.***