MUUDATUSETTEPANEKUD 001-257
Tööstuse, teadusuuringute ja energeetikakomisjon

Raport
Angelika Niebler **A8-0264/2018**
ELi küberturvalisust käsitlev õigusakt

Ettepanek võtta vastu määrus (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

Muudatusettepanek 1

Ettepanek võtta vastu määrus
Põhjendus 1

Komisjoni ettepanek	*Muudatusettepanek*
(1) Võrgu- ja infosüsteemidel ning telekommunikatsioonivõrkudel ja -teenustel on ühiskonnas elutähtis roll ning neist on saanud majanduskasvu tugisammas. Info- ja kommunikatsioonitehnoloogia on aluseks keerukatele süsteemidele, millele toetub ühiskondlik tegevus, mis tagavad majanduse toimimise võtmetähtsusega sektorites nagu tervishoid, energeetika, rahandus ja transport ning mis toetavad ennekõike siseturu toimimist.	(1) Võrgu- ja infosüsteemidel ning telekommunikatsioonivõrkudel ja -teenustel on ühiskonnas elutähtis roll ning neist on saanud majanduskasvu tugisammas. Info- ja kommunikatsioonitehnoloogia (IKT) on aluseks keerukatele süsteemidele, millele toetub ***ühiskonna igapäevane toimimine***, mis tagavad majanduse toimimise võtmetähtsusega sektorites nagu tervishoid, energeetika, rahandus ja transport ning mis toetavad ennekõike siseturu toimimist.

Muudatusettepanek 2

Ettepanek võtta vastu määrus
Põhjendus 2

Komisjoni ettepanek	*Muudatusettepanek*
(2) Võrgu- ja infosüsteemide kasutamine	(2) Võrgu- ja infosüsteemide kasutamine

kogu liidu kodanike, ettevõtjate ja valitsusasutuste seas on nüüd valdav. Digiteeritus ja ühenduvus on muutumas üha suurema hulga toodete ja teenuste põhitunnusteks ning asjade interneti kasutuselevõtuga võib eeldada, et järgmise kümne aasta jooksul võetakse kogu ELis kasutusele miljoneid kui mitte miljardeid ühendatud digitaalseid seadmeid. Kuigi internetti ühendatud seadmete arv kasvab, ei ole turvalisus ja vastupidavus neisse piisavalt sisse projekteeritud ning see toob kaasa ebapiisava küberturvalisuse. Sellises olukorras tähendab sertifitseerimise piiratud kasutamine, et organisatsioonidest ja eraisikutest kasutajatel ei ole IKT toodete ja teenuste küberturvalisuse omaduste kohta piisavalt teavet ning see vähendab usaldust digilahenduste vastu.	kogu liidu kodanike, ettevõtjate ja valitsusasutuste seas on nüüd valdav. Digiteeritus ja ühenduvus on muutumas üha suurema hulga toodete ja teenuste põhitunnusteks ning asjade interneti kasutuselevõtuga võib eeldada, et järgmise kümne aasta jooksul võetakse kogu ELis kasutusele miljoneid kui mitte miljardeid ühendatud digitaalseid seadmeid. Kuigi internetti ühendatud seadmete arv kasvab, ei ole turvalisus ja vastupidavus neisse piisavalt sisse projekteeritud ning see toob kaasa ebapiisava küberturvalisuse. Sellises olukorras tähendab sertifitseerimise piiratud kasutamine, et organisatsioonidest ja eraisikutest kasutajatel ei ole IKT toodete***, protsesside*** ja teenuste küberturvalisuse omaduste kohta piisavalt teavet ning see vähendab usaldust digilahenduste vastu. ***See püüdlus on digitaalse ühtse turu saavutamist käsitleva komisjoni reformikava keskmes, kuna IKT võrgud on aluseks digitaalsetele toodetele ja teenustele, mis võivad toetada meie elu kõiki aspekte ja edendada Euroopa majanduskasvu. Digitaalse ühtse turu eesmärkide täieliku saavutamise tagamiseks peavad paigas olema olulised tehnoloogilised ehitusplokid, millele tuginevad tähtsad valdkonnad, nagu e-tervis, asjade internet, tehisintellekt ja kvanttehnoloogia, samuti intelligentne transpordisüsteem ja kõrgtehnoloogilised tootmissüsteemid.***

Muudatusettepanek 3

Ettepanek võtta vastu määrus
Põhjendus 3

Komisjoni ettepanek	*Muudatusettepanek*
(3) Ulatuslikum digiteerimine ja ühenduvus toovad kaasa suuremad küberturvalisuse riskid, mille tõttu on kogu ühiskond küberohtude poolt lihtsamini haavatav ning üksikisikute, sh haavatavate isikute (nt laste) vastu suunatud ohud tulevad selgemalt esile. Et seda ühiskonna	(3) Ulatuslikum digiteerimine ja ühenduvus toovad kaasa suuremad küberturvalisuse riskid, mille tõttu on kogu ühiskond küberohtude poolt lihtsamini haavatav ning üksikisikute, sh haavatavate isikute (nt laste) vastu suunatud ohud tulevad selgemalt esile. Et seda ühiskonna

vastu suunatud riski leevendada, tuleb võtta kõik vajalikud meetmed, et parandada ELis küberturvalisust ning pakkuda küberohtude eest paremat kaitset võrgu- ja infosüsteemidele, telekommunikatsioonivõrkudele, digitaalsetele toodetele, teenustele ja seadmetele, mida kasutavad kodanikud, valitsused ja ettevõtjad alates VKEdest kuni elutähtsate taristute operaatoriteni.	vastu suunatud riski leevendada, tuleb võtta kõik vajalikud meetmed, et parandada ELis küberturvalisust ning pakkuda küberohtude eest paremat kaitset võrgu- ja infosüsteemidele, telekommunikatsioonivõrkudele, digitaalsetele toodetele, teenustele ja seadmetele, mida kasutavad kodanikud, valitsused ja ettevõtjad alates VKEdest kuni elutähtsate taristute operaatoriteni. ***Sellega seoses on 17. jaanuaril 2018 Euroopa Komisjoni poolt avaldatud digiõppe tegevuskava samm õiges suunas, eelkõige kogu ELi hõlmav õpetajatele, lapsevanematele ja õppuritele suunatud teadlikkuse suurendamise kampaania, et edendada võrgukeskkonna turvalisust, küberhügieeni ja meediapädevust, ning küberturvalisuse õpetamise algatus, mis lähtub Euroopa kodanike digipädevuse raamistikust, et võimaldada inimestel kasutada tehnoloogiat enesekindlalt ja vastutustundlikult.***

Muudatusettepanek 4

Ettepanek võtta vastu määrus
Põhjendus 3 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(3a) Usub, et ENISA eesmärgid ja ülesanded tuleks viia paremini kooskõlla ühisteatisega, võttes arvesse selles sisalduvat viidet küberhügieeni ja -teadlikkuse edendamisele; märgib, et kübervastupidavusvõimet on võimalik saavutada küberhügieeni aluspõhimõtete rakendamise abil;

Muudatusettepanek 5

Ettepanek võtta vastu määrus
Põhjendus 3 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(3b) ENISA peaks pakkuma rohkem teabepõhist ja praktilist tuge ELi küberjulgeolekutööstusele, eelkõige VKEdele ja idufirmadele, kes on küberkaitse valdkonnas peamised uuenduslike lahenduste loojad, ning peaks edendama tihedamat koostööd ülikoolide teadusorganisatsioonide ja suurte osalejatega, et vähendada sõltuvust liiduväliste tootjate küberjulgeolekutoodetest ja luua liidus strateegiline tarneahel.

Muudatusettepanek 6

Ettepanek võtta vastu määrus
Põhjendus 4

Komisjoni ettepanek	*Muudatusettepanek*
(4) Küberründe id tuleb ette üha sagedamini ning küberohtude poolt lihtsamini haavatavat ühendatud majandust ja ühiskonda tuleb jõulisemalt kaitsta. Kuigi küberründed on sageli piiriülesed, on küberturvalisusega tegelevate ametiasutuste reageeringud ja õiguskaitseasutuste pädevus valdavalt riigipõhised. Mastaapsed küberintsidendid võivad katkestada elutähtsate teenuste pakkumise kogu ELis. See tähendab, et ELi tasandil on vaja tõhusat reageerimist ja kriisihaldust, mis tugineks sellekohastele põhimõtetele ning Euroopa solidaarsuse ja vastastikuse abi mitmekülgsetele vahenditele. Seepärast on usaldusväärsetel liidu andmetel põhinev liidu küberturvalisuse ja vastupidavuse olukorra regulaarne hindamine ning nii liidu kui ka maailma tasandi edasiste arengusuundade, väljakutsete ja ohtude süstemaatiline hindamine tähtis nii poliitikakujundajate ja	(4) Küberründe id tuleb ette üha sagedamini ning küberohtude poolt lihtsamini haavatavat ühendatud majandust ja ühiskonda tuleb jõulisemalt ***ja turvalisemalt*** kaitsta. Kuigi küberründed on sageli piiriülesed, on küberturvalisusega tegelevate ametiasutuste reageeringud ja õiguskaitseasutuste pädevus valdavalt riigipõhised. Mastaapsed küberintsidendid võivad katkestada elutähtsate teenuste pakkumise kogu ELis. See tähendab, et ELi tasandil on vaja tõhusat reageerimist ja kriisihaldust, mis tugineks sellekohastele põhimõtetele ning Euroopa solidaarsuse ja vastastikuse abi mitmekülgsetele vahenditele***. Vajadus koolituste järele on küberkaitse valdkonnas märkimisväärne ja suurenev ning kõige tõhusam viis selle rahuldamiseks on liidu tasandi koostöö.*** Seepärast on usaldusväärsetel liidu andmetel põhinev liidu küberturvalisuse ja vastupidavuse olukorra regulaarne

tööstuse kui ka kasutajate jaoks.

hindamine ning nii liidu kui ka maailma tasandi edasiste arengusuundade, väljakutsete ja ohtude süstemaatiline hindamine tähtis nii poliitikakujundajate ja tööstuse kui ka kasutajate jaoks.

Muudatusettepanek 7

Ettepanek võtta vastu määrus
Põhjendus 5

Komisjoni ettepanek	*Muudatusettepanek*
(5) Arvestades, et liitu ähvardavad küberturvalisuse probleemid kasvavad, on vaja igakülgset meetmete kogumit, mis toetuks liidu varasemale tegevusele ja edendaks üksteist vastastikku tugevdavaid eesmärke. Siia hulka kuulub vajadus veelgi suurendada liikmesriikide ja ettevõtjate suutlikkust ja valmisolekut ning parandada koostööd ja koordineerimist liikmesriikide ja ELi institutsioonide, asutuste ja organite vahel. Küberohud ei hooli riigipiiridest ja seepärast tuleb suurendada liidu tasandi suutlikkust, et see täiendaks liikmesriikide meetmeid eeskätt mastaapsete piiriüleste küberintsidentide ja -kriiside korral. Rohkem tuleb ära teha ka selleks, et suurendada kodanike ja ettevõtjate teadlikkust küberturvalisuse küsimustest. Ühtlasi tuleks veelgi suurendada usaldust digitaalse ühtse turu vastu ning pakkuda selleks läbipaistvat teavet IKT toodete ja teenuste turvalisuse tasemete kohta. Sellele saab kaasa aidata kogu ELi hõlmava sertifitseerimisega, mis tagab ühised küberturvalisuse nõuded ja hindamiskriteeriumid liikmesriikide turgudel ja sektorites.	(5) Arvestades, et liitu ähvardavad küberturvalisuse probleemid kasvavad, on vaja igakülgset meetmete kogumit, mis toetuks liidu varasemale tegevusele ja edendaks üksteist vastastikku tugevdavaid eesmärke. Siia hulka kuulub vajadus veelgi suurendada liikmesriikide ja ettevõtjate suutlikkust ja valmisolekut ning parandada koostööd, koordineerimist ***ja teabe jagamist*** liikmesriikide ja ELi institutsioonide, asutuste ja organite vahel. Küberohud ei hooli riigipiiridest ja sihipärased rünnakud on üha ulatuslikumad ja täpsemad ning seepärast tuleb suurendada liidu tasandi suutlikkust, et see täiendaks liikmesriikide meetmeid eeskätt mastaapsete piiriüleste küberintsidentide ja -kriiside korral***, rõhutades samas riikide suutlikkuse ja selle veelgi suurendamise olulisust igasugustele küberohtudele reageerimisel.*** Rohkem tuleb ära teha ka selleks, et ***ELi tasandil koordineeritult reageerida ning*** suurendada kodanike ja ettevõtjate teadlikkust küberturvalisuse küsimustest. Ühtlasi***, arvestades, et küberintsidendid õõnestavad usaldust digitaalsete teenuste osutajate ning*** digitaalse ühtse turu vastu, ***eelkõige tarbijate seas, tuleks usaldust suurendada*** ning pakkuda selleks läbipaistvat teavet IKT toodete***, protsesside*** ja teenuste turvalisuse tasemete kohta***, rõhutades, et isegi küberturvalisuse sertifitseerimise kõrge tase ei taga, et IKT toode või teenus on täiesti turvaline***. Sellele saab kaasa

aidata kogu ELi hõlmava sertifitseerimisega, mis tagab ühised küberturvalisuse nõuded ja hindamiskriteeriumid liikmesriikide turgudel ja sektorites, ***küberkirjaoskuse edendamisega kogu ELi hõlmava sertifitseerimise kõrval ning, arvestades asjade interneti seadmete üha suuremat kättesaadavust, on ka mitmeid vabatahtlikke meetmeid, mida erasektor peaks kasutama, et suurendada usaldust IKT toodete, protsesside ja teenuste turvalisuse vastu, näiteks krüpteerimine ja plokiahela tehnoloogia. Ähvardavad probleemid peaksid kajastuma proportsionaalselt ametile eraldatavas eelarves, et tagada praegustes tingimustes optimaalne toimimine.***

Muudatusettepanek 8

Ettepanek võtta vastu määrus
Põhjendus 5 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(5a) Euroopa julgeoleku- ja küberkaitsestruktuuride tugevdamise eesmärgil on oluline säilitada ja arendada liikmesriikide suutlikkust reageerida küberohtudele (sh piiriülestele intsidentidele) kõikehõlmavalt, seejuures ei tohiks ametipoolne koordineerimine ELi tasandil tuua kaasa suutlikkuse või jõupingutuste vähenemist liikmesriikides.

Muudatusettepanek 9

Ettepanek võtta vastu määrus
Põhjendus 5 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(5b) Ettevõtjatel ning üksikisikutest tarbijatel peaks olema täpne teave IKT toodete turvalisuse taseme kohta. Samal ajal tuleb mõista, et ükski toode ei ole küberturvaline ning et küberhügieeni

põhireegleid tuleb edendada ja seada need prioriteediks.

Muudatusettepanek 10

Ettepanek võtta vastu määrus
Põhjendus 7

Komisjoni ettepanek	*Muudatusettepanek*
(7) Euroopa Liit on juba astunud olulisi samme, et tagada küberturvalisus ja suurendada usaldust digitehnoloogia vastu. 2013. aastal võeti vastu ELi küberjulgeoleku strateegia, millest juhinduda liidu poliitilises reageerimises küberturvalisuse ohtudele ja riskidele. Et eurooplasi veebis paremini kaitsta, võttis liit 2016. aastal vastu küberturvalisuse valdkonna esimese õigusakti – direktiivi (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (edaspidi „võrgu- ja infoturbe direktiiv“). Võrgu- ja infoturbe direktiiviga pandi paika riikide suutlikkust puudutavad nõuded küberturvalisuse valdkonnas, kehtestati liikmesriikide vahelise strateegilise ja operatiivkoostöö edendamise esimesed mehhanismid ning juurutati turbemeetmete ja intsidentidest teatamise kohustused majanduse ja ühiskonna jaoks eluliselt tähtsates sektorites, nagu energeetika, transport, veevarustus, pangandus, finantsturutaristud, tervishoid, digitaristu, aga ka oluliste digitaalsete teenuste osutajate puhul (otsingumootorid, pilvandmetöötlusteenused ja internetipõhised kauplemiskohad). ENISA-le anti selle direktiivi rakendamise toetamisel põhiroll. Võitlus küberkuritegevusega on olulisel kohal ka Euroopa julgeoleku tegevuskavas, kus see aitab kaasa küberturvalisuse kõrge taseme saavutamise üldeesmärgile.	(7) Euroopa Liit on juba astunud olulisi samme, et tagada küberturvalisus ja suurendada usaldust digitehnoloogia vastu. 2013. aastal võeti vastu ELi küberjulgeoleku strateegia, millest juhinduda liidu poliitilises reageerimises küberturvalisuse ohtudele ja riskidele. Et eurooplasi veebis paremini kaitsta, võttis liit 2016. aastal vastu küberturvalisuse valdkonna esimese õigusakti – direktiivi (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (edaspidi „võrgu- ja infoturbe direktiiv“). Võrgu- ja infoturbe direktiiviga***, mille edukus sõltub otseselt direktiivi tulemuslikust rakendamisest liikmesriikides, viiakse ellu digitaalse ühtse turu strateegiat ning pannakse koos muude õigusaktidega, nagu direktiiv, millega kehtestatakse Euroopa elektroonilise side seadustik, määrus (EL) 2016/679 ja direktiiv 2002/58/EÜ,*** paika riikide suutlikkust puudutavad nõuded küberturvalisuse valdkonnas, kehtestati liikmesriikide vahelise strateegilise ja operatiivkoostöö edendamise esimesed mehhanismid ning juurutati turbemeetmete ja intsidentidest teatamise kohustused majanduse ja ühiskonna jaoks eluliselt tähtsates sektorites, nagu energeetika, transport, veevarustus, pangandus, finantsturutaristud, tervishoid, digitaristu, aga ka oluliste digitaalsete teenuste osutajate puhul (otsingumootorid, pilvandmetöötlusteenused ja internetipõhised kauplemiskohad). ENISA-le anti selle direktiivi rakendamise toetamisel põhiroll. Võitlus

	küberkuritegevusega on olulisel kohal ka Euroopa julgeoleku tegevuskavas, kus see aitab kaasa küberturvalisuse kõrge taseme saavutamise üldeesmärgile.

Muudatusettepanek 11

Ettepanek võtta vastu määrus
Põhjendus 8

Komisjoni ettepanek	*Muudatusettepanek*
(8) Tuleb tõdeda, et 2013. aasta küberjulgeoleku strateegia vastuvõtmisest ja ameti mandaadi viimasest läbivaatamisest möödunud aja jooksul on üldine poliitiline kontekst oluliselt muutunud, seda ka seoses ebakindlama ja vähem turvalise üldise õhustikuga maailmas. Sellist olukorda arvestades on vaja liidu uue küberturvalisuse poliitika raames läbi vaadata ENISA mandaat, et määrata kindlaks ameti roll muutunud küberturvalisuse tingimustes ning tagada, et see annab tulemusliku panuse sellesse, kuidas liit reageerib põhjalikult muutnud ohtude maastikul esile kerkivatele küberturvalisuse probleemidele, millega toimetulemiseks ei ole praegune mandaat ameti hinnangul piisav.	(8) Tuleb tõdeda, et 2013. aasta küberjulgeoleku strateegia vastuvõtmisest ja ameti mandaadi viimasest läbivaatamisest möödunud aja jooksul on üldine poliitiline kontekst oluliselt muutunud, seda ka seoses ebakindlama ja vähem turvalise üldise õhustikuga maailmas. Sellist olukorda ***ja ameti eelnevate aastate positiivset rolli erialateadmiste koondamisel, koordineerimisel ja suutlikkuse arendamisel arvesse võttes*** on vaja liidu uue küberturvalisuse poliitika raames läbi vaadata ENISA mandaat, et määrata kindlaks ameti roll muutunud küberturvalisuse tingimustes ning tagada, et see annab tulemusliku panuse sellesse, kuidas liit reageerib põhjalikult muutnud ohtude maastikul esile kerkivatele küberturvalisuse probleemidele, millega toimetulemiseks ei ole praegune mandaat ameti hinnangul piisav.

Muudatusettepanek 12

Ettepanek võtta vastu määrus
Põhjendus 11

Komisjoni ettepanek	*Muudatusettepanek*
(11) Arvestades liidu ees seisvate küberturvalisusega seotud probleemide kasvu, tuleks suurendada ametile eraldatavaid finants- ja inimressursse, et need vastaksid ameti tõhustatud rollile ja ülesannetele ning ameti tähtsale	(11) Arvestades liidu ees seisvate küberturvalisusega seotud ***ohtude ja*** probleemide kasvu, tuleks suurendada ametile eraldatavaid finants- ja inimressursse, et need vastaksid ameti tõhustatud rollile ja ülesannetele ning ameti

positsioonile Euroopa digitaalse ökosüsteemi kaitsmisel.

tähtsale positsioonile Euroopa digitaalse ökosüsteemi kaitsmisel, ***võimaldades ENISA-l täita tõhusalt talle käesoleva määrusega pandud ülesandeid***.

Muudatusettepanek 13

Ettepanek võtta vastu määrus
Põhjendus 12

Komisjoni ettepanek	*Muudatusettepanek*
(12) Amet peaks välja kujundama oskusteabe kõrge taseme ja seda hoidma ning tegutsema kontaktüksusena, mis tekitab ühtsel turul usaldust ja kindlustunnet tänu oma sõltumatusele, antud nõu ja levitatava teabe kvaliteedile, menetluste ja töömeetodite läbipaistvusele ning oma ülesannete hoolikale täitmisele. Täites oma ülesandeid täielikus koostöös liidu institutsioonide, organite ja asutuste, aga ka liikmesriikidega, peaks amet andma ennetava panuse riikide ja liidu tegevusse. Lisaks peaks amet arendama edasi erasektorilt saadud sisendit, lähtudes erasektori ja muude asjaomaste sidusrühmadega tehtavast koostööst. Ameti ülesannete kogumiga tuleks paika panna, kuidas amet peab oma eesmärgid saavutama, tagades talle samas tööks vajaliku paindlikkuse.	(12) Amet peaks välja kujundama oskusteabe kõrge taseme ja seda hoidma ning tegutsema kontaktüksusena, mis tekitab ühtsel turul usaldust ja kindlustunnet tänu oma sõltumatusele, antud nõu ja levitatava teabe kvaliteedile, menetluste ja töömeetodite läbipaistvusele ning oma ülesannete hoolikale täitmisele. Täites oma ülesandeid täielikus koostöös liidu institutsioonide, organite ja asutuste, aga ka liikmesriikidega, peaks amet andma ennetava panuse riikide ja liidu tegevusse, ***vältides topelttööd, edendades sünergiat ja täiendavust ning saavutades sellega koordineerimise ja eelarvesäästu***. Lisaks peaks amet arendama edasi ***era- ja avalikult sektorilt*** saadud sisendit, lähtudes erasektori ja muude asjaomaste sidusrühmadega tehtavast koostööst. ***Selge tegevuskava ning selgelt kindlaks määratud*** ameti ülesannete ***ja eesmärkide*** kogumiga tuleks paika panna, kuidas amet peab oma eesmärgid saavutama***, pöörates samas nõuetekohast tähelepanu ameti*** tööks ***vajalikule paindlikkusele***. ***Võimaluse korral tuleks säilitada kõrgeim läbipaistvuse ja teabe levitamise tase.***

Muudatusettepanek 14

Ettepanek võtta vastu määrus
Põhjendus 12 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(12a) Ameti rolli tuleks pidevalt hinnata ja õigeaegselt läbi vaadata, eelkõige selle koordineerivat rolli liikmesriikide ja nende riiklike ametiasutuste suhtes ning võimalust tegutseda liikmesriikide ning ELi organite ja institutsioonide ühtse kontaktpunktina. Samuti tuleks hinnata ameti rolli siseturu killustumise vältimisel ja kohustuslike küberturvalisuse sertifitseerimise kavade võimalikul kasutuselevõtmisel, kui tulevikus peaks olukord sellist muutust nõudma, ning lisaks tuleks hinnata ameti rolli seoses ELi turule sisenevate kolmandatest riikidest pärit toodete hindamisega ja ELi kriteeriumidele mittevastavate ettevõtete võimaliku musta nimekirja lisamisega.

Muudatusettepanek 15

Ettepanek võtta vastu määrus
Põhjendus 12 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(12b) Et pakkuda liikmesriikidele asjakohast tuge operatiivses koostöös, peaks Euroopa Liidu Võrgu- ja Infoturbeamet (ENISA) veelgi tugevdama oma tehnilist suutlikkust ja eksperditeadmisi. Selleks peaks amet järk-järgult tugevdama nimetatud ülesannetega tegelevat töötajaskonda, et olla suuteline koguma ja autonoomselt analüüsima eri liiki küberohte ja pahavara, tegema kohtuekspertiisi ja aitama liikmesriike ulatuslikele intsidentidele reageerimisel. Et vältida liikmesriikides olemasoleva suutlikkuse dubleerimist, peaks ENISA suurendama oma oskusteavet ja liikmesriikides olemasolevatel vahenditel põhinevat

	suutlikkust, sealhulgas lähetades ametisse riiklikke eksperte, moodustades ekspertide rühmi, kasutades töötajate vahetusprogramme jne. Kõnealuse valdkonna töötajate valimisel peaks amet järk-järgult tagama, et nad vastavad asjakohase toe pakkumiseks vajalikele kriteeriumitele.

Muudatusettepanek 16

Ettepanek võtta vastu määrus
Põhjendus 13

Komisjoni ettepanek	*Muudatusettepanek*
(13) Amet peaks abistama komisjoni nõuannete, arvamuste ja analüüsidega kõigis liidu küsimustes, mis on seotud küberturvalisuse valdkonna, sealhulgas elutähtsa sideinfrastruktuuri kaitse ja kübervastupidavusvõime alase poliitika ja õigusaktide väljatöötamisega. Amet peaks tegutsema nõuandva ja oskusteavet pakkuva kontaktüksusena selliste liidu sektorispetsiifilise poliitika ja õigusalaste algatuste jaoks, mis puudutavad küberturvalisust.	(13) Amet peaks abistama komisjoni nõuannete, arvamuste ja analüüsidega kõigis liidu küsimustes, mis on seotud küberturvalisuse valdkonna, sealhulgas elutähtsa sideinfrastruktuuri kaitse ja kübervastupidavusvõime alase poliitika ja õigusaktide väljatöötamisega. Amet peaks tegutsema nõuandva ja oskusteavet pakkuva kontaktüksusena selliste liidu sektorispetsiifilise poliitika ja õigusalaste algatuste jaoks, mis puudutavad küberturvalisust. ***Ameti eksperditeadmisi on eriti vaja Euroopa küberturvalisuse sertifitseerimise kavade liidu mitmeaastase tööprogrammi koostamisel. Amet peaks esitama parlamendile regulaarselt ajakohastatud teabe, analüüsid ja ülevaate küberturvalisuse valdkonna ja ameti ülesannete muutumise kohta.***

Muudatusettepanek 17

Ettepanek võtta vastu määrus
Põhjendus 14

Komisjoni ettepanek	*Muudatusettepanek*
(14) Ameti põhiülesanne on toetada asjakohase õigusraamistiku järjepidevat rakendamist, eelkõige võrgu- ja infoturbe	(14) Ameti põhiülesanne on toetada asjakohase õigusraamistiku järjepidevat rakendamist, eelkõige võrgu- ja infoturbe

direktiivi tulemuslikku rakendamist, mis on kübervastupidavusvõime suurendamise jaoks eluliselt tähtis. Arvestades seda, kui kiiresti küberturvalisuse ohud muutuvad, on selge, et liikmesriike tuleb toetada igakülgsema ja eri valdkondi hõlmava poliitilise lähenemisega kübervastupidavusvõime loomisele.	direktiivi***, Euroopa elektroonilise side seadustiku kehtestamise direktiivi, määruse (EL) 2016/679 ja direktiivi 2002/58/EÜ*** tulemuslikku rakendamist, mis on kübervastupidavusvõime suurendamise jaoks eluliselt tähtis. Arvestades seda, kui kiiresti küberturvalisuse ohud muutuvad, on selge, et liikmesriike tuleb toetada igakülgsema ja eri valdkondi hõlmava poliitilise lähenemisega kübervastupidavusvõime loomisele.

Muudatusettepanek 18

Ettepanek võtta vastu määrus
Põhjendus 15

Komisjoni ettepanek	*Muudatusettepanek*
(15) Amet peaks abistama liikmesriike ja liidu institutsioone, organeid ja asutusi töös, mida nad teevad, et luua ja suurendada suutlikkust ja valmisolekut ennetada ja avastada küberturvalisuse intsidente ja neile reageerida, ning seoses võrgu- ja infosüsteemide turvalisusega. Eeskätt peaks amet toetama riiklike CSIRTide arendamist ja tõhustamist, et neil oleks kogu liidus ühtemoodi kõrge küpsuse aste. Samuti peaks amet abistama liidu ja liikmesriikide võrgu- ja infosüsteemide turvalisuse strateegiate väljatöötamist ja uuendamist, edendama nende levitamist ja hoidma silma peal nende rakendamisel. Lisaks peaks amet pakkuma koolitusi ja koolitusmaterjali avalikele asutustele ning koolitama vajaduse korral koolitajaid, et aidata liikmesriikidel välja kujundada nende endi koolitussuutlikkus.	(15) Amet peaks abistama liikmesriike ja liidu institutsioone, organeid ja asutusi töös, mida nad teevad, et luua ja suurendada suutlikkust ja valmisolekut ennetada ja avastada küberturvalisuse intsidente ja neile reageerida, ning seoses võrgu- ja infosüsteemide turvalisusega. Eeskätt peaks amet toetama riiklike CSIRTide arendamist ja tõhustamist, et neil oleks kogu liidus ühtemoodi kõrge küpsuse aste. Samuti peaks amet abistama liidu ja liikmesriikide võrgu- ja infosüsteemide turvalisuse strateegiate väljatöötamist ja uuendamist, edendama nende levitamist ja hoidma silma peal nende rakendamisel. Arvestades, et inimvigade puhul on tegemiste ühe kõige asjakohasema küberturvalisuse ohuga, peaks amet pakkuma lisaks koolitusi ja koolitusmaterjali avalikele asutustele ning koolitama võimalikult suures ulatuses koolitajaid, et aidata liikmesriikidel ning liidu institutsioonidel ja asutustel välja kujundada nende endi koolitussuutlikkus. ***Samuti peaks amet olema liikmesriikide ja liidu institutsioonide kontaktpunkt, kellel peaks olema võimalus taotleda ametilt abi talle määratud pädevuste ja rollide***

raames.

Muudatusettepanek 19

Ettepanek võtta vastu määrus
Põhjendus 18

Komisjoni ettepanek	*Muudatusettepanek*
(18) Amet peaks koondama ja analüüsima riikide CSIRTide ja CERT-EU aruandeid ning koostama teabevahetuse jaoks ühised eeskirjad, keele ja terminoloogia. Võrgu- ja infoturbe direktiiviga loodud CSIRTide võrgustikuga loodi alus vabatahtlikuks tehnilise teabe vahetamiseks operatiivtasandil – selle raames peaks amet kaasama ka ***erasektori***.	(18) Amet peaks koondama ja analüüsima riikide CSIRTide ja CERT-EU aruandeid ning koostama teabevahetuse jaoks ühised eeskirjad, keele ja terminoloogia. Võrgu- ja infoturbe direktiiviga loodud CSIRTide võrgustikuga loodi alus vabatahtlikuks tehnilise teabe vahetamiseks operatiivtasandil – selle raames peaks amet kaasama ka ***era- ja avaliku sektori***.

Muudatusettepanek 20

Ettepanek võtta vastu määrus
Põhjendus 19

Komisjoni ettepanek	*Muudatusettepanek*
(19) Amet peaks andma oma panuse sellesse, kuidas ELi tasandil reageeritakse mastaapsetele piiriülestele küberturvalisuse intsidentidele ja kriisidele. See funktsioon peaks hõlmama asjaomase teabe kogumist ning vahendajarolli CSIRTide võrgustiku ja tehnilise kogukonna, aga ka kriisi haldamise eest vastutavate otsusetegijate vahel. Lisaks võiks amet toetada intsidendikäsitlust tehnilise külje pealt, hõlbustades vajalike lahenduste tehnilist vahetamist liikmesriikide vahel ja pakkudes sisendit avaliku teabevahetuse jaoks. Amet peaks seda protsessi toetama sellise koostöö aspektide testimisega iga-aastaste küberturvalisuse õppuste käigus.	(19) Amet peaks andma oma panuse sellesse, kuidas ELi tasandil reageeritakse mastaapsetele piiriülestele küberturvalisuse intsidentidele ja kriisidele. See funktsioon peaks hõlmama ***liikmesriikide asutuste kokku kutsumist ja nende reageerimise koordineerimisel abistamist,*** asjaomase teabe kogumist ning vahendajarolli CSIRTide võrgustiku ja tehnilise kogukonna, aga ka kriisi haldamise eest vastutavate otsusetegijate vahel. Lisaks võiks amet toetada intsidendikäsitlust tehnilise külje pealt, ***näiteks*** hõlbustades vajalike lahenduste tehnilist vahetamist liikmesriikide vahel ja pakkudes sisendit avaliku teabevahetuse jaoks. Amet peaks seda protsessi toetama sellise koostöö aspektide testimisega iga-aastaste küberturvalisuse õppuste käigus. ***Amet peaks austama liikmesriikide küberturvalisuse alast pädevust, eriti***

	pädevust, mis on seotud avaliku julgeoleku, riigikaitse, riikliku julgeoleku ja riigi tegevusega kriminaalõiguse valdkonnas.

Muudatusettepanek 21

Ettepanek võtta vastu määrus
Põhjendus 25

Komisjoni ettepanek	*Muudatusettepanek*
(25) Liikmesriigid võivad paluda, et intsidendist mõjutatud ettevõtjad teeksid koostööd ning pakuksid ametile vajalikku teavet ja abi, ilma et see piiraks nende õigust kaitsta tundlikku äriteavet.	(25) Liikmesriigid võivad paluda, et intsidendist mõjutatud ettevõtjad teeksid koostööd ning pakuksid ametile vajalikku teavet ja abi, ilma et see piiraks nende õigust kaitsta tundlikku äriteavet ***ja avaliku julgeoleku seisukohast olulist teavet***.

Muudatusettepanek 22

Ettepanek võtta vastu määrus
Põhjendus 26

Komisjoni ettepanek	*Muudatusettepanek*
(26) Et küberturvalisuse valdkonna probleemidest paremini aru saada ning liikmesriikidele ja liidu institutsioonidele pikaajalist strateegilist nõu anda, peab amet analüüsima praeguseid ja kujunemisjärgus riske. Sel eesmärgil peaks amet koostöös liikmesriikidega ja vajaduse korral ka statistikaasutuste ja muude asutustega koguma asjakohast teavet ning analüüsima kujunemisjärgus tehnoloogiaid ja andma teemakohaseid hinnanguid võrgu- ja infoturbe, eeskätt küberturvalisuse tehnoloogiliste uuenduste eeldatavale ühiskondlikule, õiguslikule, majanduslikule ja regulatiivsele mõjule. Peale selle peaks amet toetama ohtude ja ***intsidentide*** analüüsimise kaudu liikmesriike ja liidu institutsioone, organeid ja asutusi esilekerkivate suundumuste kindlakstegemisel ja küberturvalisusega seotud probleemide vältimisel.	(26) Et küberturvalisuse valdkonna probleemidest paremini aru saada ning liikmesriikidele ja liidu institutsioonidele pikaajalist strateegilist nõu anda, peab amet analüüsima praeguseid ja kujunemisjärgus riske***, intsidente, ohte ja nõrku kohti***. Sel eesmärgil peaks amet koostöös liikmesriikidega ja vajaduse korral ka statistikaasutuste ja muude asutustega koguma asjakohast teavet ning analüüsima kujunemisjärgus tehnoloogiaid ja andma teemakohaseid hinnanguid võrgu- ja infoturbe, eeskätt küberturvalisuse tehnoloogiliste uuenduste eeldatavale ühiskondlikule, õiguslikule, majanduslikule ja regulatiivsele mõjule. Peale selle peaks amet toetama ohtude***,*** ***intsidentide*** ja ***turvanõrkuste*** analüüsimise kaudu liikmesriike ja liidu institutsioone, organeid ja asutusi esilekerkivate suundumuste kindlakstegemisel ja

küberturvalisusega seotud probleemide vältimisel.

Muudatusettepanek 23

Ettepanek võtta vastu määrus
Põhjendus 27

Komisjoni ettepanek	*Muudatusettepanek*
(27) Amet peaks liidu vastupidavuse suurendamiseks arendama internetitaristu ja elutähtsate infrastruktuuride turvalisuse alaseid teadmisi, pakkudes nõuandeid, juhiseid ja parimaid tavasid. Et tagada hõlpsam juurdepääs paremini struktureeritud teabele küberturvalisuse riskide ja võimalike lahenduste kohta, peaks amet arendama välja liidu teabekeskuse ja hoidma seda käigus. Teabekeskus oleks universaalne portaal, mis jagaks üldsusele küberturvalisuse kohta teavet, mis on saadud ELi ja riikide institutsioonidelt, organitelt ja asutustelt.	(27) Amet peaks liidu vastupidavuse suurendamiseks arendama internetitaristu ja elutähtsate infrastruktuuride turvalisuse alaseid teadmisi, pakkudes nõuandeid, juhiseid ja parimaid tavasid. Et tagada hõlpsam juurdepääs paremini struktureeritud teabele küberturvalisuse riskide ja võimalike lahenduste kohta, peaks amet arendama välja liidu teabekeskuse ja hoidma seda käigus. Teabekeskus oleks universaalne portaal, mis jagaks üldsusele küberturvalisuse kohta teavet, mis on saadud ELi ja riikide institutsioonidelt, organitelt ja asutustelt. ***Küberjulgeolekuohte ja võimalikke vastumeetmeid käsitlevale paremini struktureeritud teabele juurdepääsu võimaldamine peaks aitama liikmesriikidel suutlikkust parandada ja tavasid ühtlustada ning suurendada seega oma üldist vastupidavusvõimet küberrünnete suhtes.***

Muudatusettepanek 24

Ettepanek võtta vastu määrus
Põhjendus 28

Komisjoni ettepanek	*Muudatusettepanek*
(28) Amet peaks aitama suurendada üldsuse teadlikkust küberturvalisusega seotud riskidest ja jagama kodanikele ja ***organisatsioonidele*** mõeldud juhiseid individuaalsete kasutajate heade tavade kohta; Amet peaks aitama kaasa ka parimate tavade ja lahenduste	(28) Amet peaks aitama suurendada üldsuse teadlikkust***, sealhulgas harimise abil,*** küberturvalisusega seotud riskidest ja jagama kodanikele***, organisatsioonidele*** ja ***ettevõtjatele*** mõeldud juhiseid individuaalsete kasutajate heade tavade kohta; Amet peaks aitama kaasa ka

propageerimisele üksikisikute ja ***organisatsioonide*** tasandil; selleks tuleks koguda ja analüüsida avalikult kättesaadavat teavet oluliste intsidentide kohta ning koostada aruanded, et pakkuda ettevõtjatele ja kodanikele juhiseid ning parandada valmisoleku ja vastupidavuse üldist taset. Amet peaks korraldama koostöös liikmesriikide ja liidu institutsioonide, organite, asutuste ja ametitega korrapäraseid lõppkasutajatele suunatud üldsuse harimise ja teavituskampaaniaid, mille eesmärk on propageerida üksikisikute ohutumat veebikäitumist ja suurendada teadlikkust küberkeskkonnas varitseda võivatest ohtudest, sealhulgas sellistest küberkuritegudest nagu andmepüügi rünnakud, robotvõrgud, finants- ja pangapettused, ning tutvustada autentimise ja andmekaitse alaseid elementaarseid nõuandeid. Ametil peaks olema keskne roll selles, et lõppkasutajad saaksid kiiremini teadlikuks seadmete turvalisusest.

küberhügieeni parimate tavade ***propageerimisele, mis hõlmavad mitmeid meetmeid, mida tuleks korrapäraselt rakendada ja ellu viia, et kaitsta kasutajaid ja ettevõtjaid veebis,*** ja lahenduste propageerimisele üksikisikute***,*** ***organisatsioonide*** ja ***ettevõtjate*** tasandil; selleks tuleks koguda ja analüüsida avalikult kättesaadavat teavet oluliste intsidentide kohta ning koostada ***ja avaldada*** aruanded ***ja juhendid***, et pakkuda ettevõtjatele ja kodanikele juhiseid ning parandada valmisoleku ja vastupidavuse üldist taset. ***ENISA peaks ka püüdma pakkuda tarbijatele asjakohast teavet kohaldatavate sertifitseerimise kavade kohta, näiteks andes suuniseid ja soovitusi internetipõhistele ja internetivälistele kauplemiskohtadele.*** Amet peaks korraldama ***kooskõlas digihariduse tegevuskavaga ja*** koostöös liikmesriikide ja liidu institutsioonide, organite, asutuste ja ametitega korrapäraseid lõppkasutajatele suunatud üldsuse harimise ja teavituskampaaniaid, mille eesmärk on propageerida üksikisikute ohutumat veebikäitumist***, digikirjaoskust*** ja suurendada teadlikkust küberkeskkonnas varitseda võivatest ohtudest, sealhulgas sellistest küberkuritegudest nagu andmepüügi rünnakud, robotvõrgud, finants- ja pangapettused, ning tutvustada ***mitmeteguriline*** autentimise***, paikamise, krüptimise, andmete anonüümseks muutmise*** ja andmekaitse alaseid elementaarseid nõuandeid. Ametil peaks olema keskne roll selles, et lõppkasutajad saaksid kiiremini teadlikuks seadmete turvalisusest ***ja teenuste turvalisest kasutamisest, ning samuti sisseprojekteeritud turbe, lõimprivaatsuse, intsidentide ja nende lahenduste populariseerimises ELi tasandil. Selle eesmärgi saavutamiseks peaks amet kasutama maksimaalselt olemasolevaid parimaid tavasid ja kogemusi, eriti neid, mis on pärit teadusasutustelt ja IT-turvalisusega tegelevatelt teadlastelt. Ametile tuleks anda piisavad vahendid***

	selle ülesande võimalikult hästi täitmiseks, arvestades, et isiklikud vead ja küberohtude mitte teadmine on küberturvalisuse valdkonnas ebakindluse põhitegur.

Muudatusettepanek 25

Ettepanek võtta vastu määrus
Põhjendus 28 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(28a) Amet peaks suurendama üldsuse teadlikkust andmetega seotud pettuste ja varguste riskidest, mis võivad oluliselt kahjustada isiku põhiõigusi, ohustada õigusriiki ja demokraatlike ühiskondade stabiilsust, sealhulgas demokraatlikke protsesse liikmesriikides,

Muudatusettepanek 26

Ettepanek võtta vastu määrus
Põhjendus 30

Komisjoni ettepanek	*Muudatusettepanek*
(30) Tagamaks, et amet saavutab oma eesmärgid täies ulatuses, peaks ta suhtlema asjaomaste institutsioonide, organite ja asutustega, kelle hulgas on CERT-EU, Europoli juures tegutsev küberkuritegevuse vastase võitluse Euroopa keskus (EC3), Euroopa Kaitseagentuur (EDA), Vabadusel, Turvalisusel ja Õigusel Rajaneva Ala Suuremahuliste IT-süsteemide Operatiivjuhtimise Euroopa Amet (eu-LISA), Euroopa Lennundusohutusamet (EASA) ja mistahes muud ELi ametid, kes tegelevad küberturvalisusega. Peale selle peaks ta suhtlema veel andmekaitsega tegelevate ametiasutustega, et vahetada oskusteavet ja parimaid tavasid ning anda nõu küberturvalisuse aspektide kohta, mis võiksid mõjutada nende tööd. Riikide ja	(30) Tagamaks, et amet saavutab oma eesmärgid täies ulatuses, peaks ta suhtlema asjaomaste institutsioonide, ***ELi järelevalve- ja muude pädevate ametite,*** organite ja asutustega, kelle hulgas on CERT-EU, Europoli juures tegutsev küberkuritegevuse vastase võitluse Euroopa keskus (EC3), Euroopa Kaitseagentuur (EDA), ***Euroopa GNSSi Agentuur (GSA), Elektroonilise Side Euroopa Reguleerivate Asutuste Ühendatud Amet (BEREC),*** Vabadusel, Turvalisusel ja Õigusel Rajaneva Ala Suuremahuliste IT-süsteemide Operatiivjuhtimise Euroopa Amet (eu-LISA), Euroopa ***Keskpank (EKP), Euroopa Pangandusjärelevalve (EBA), Euroopa Andmekaitsenõukogu, Euroopa*** Lennundusohutusamet (EASA) ja mistahes

liidu õiguskaitseasutuste ja andmekaitseasutuste esindajad peaksid olema esindatud ***ameti alalises sidusrühmas***. Õiguskaitseasutustega koostöö tegemisel võrgu- ja infoturbe küsimustes, mis võivad nende tööd mõjutada, peaks amet arvestama olemasolevate teabekanalite ja rajatud võrgustikega.	muud ELi ametid, kes tegelevad küberturvalisusega. Peale selle peaks ta suhtlema veel ***Euroopa standardiorganisatsioonide, asjaomaste sidusrühmade ja*** andmekaitsega tegelevate ametiasutustega, et vahetada oskusteavet ja parimaid tavasid ning anda nõu küberturvalisuse aspektide kohta, mis võiksid mõjutada nende tööd. Riikide ja liidu õiguskaitseasutuste ja andmekaitseasutuste esindajad peaksid olema esindatud ***ENISA nõuanderühmas***. Õiguskaitseasutustega koostöö tegemisel võrgu- ja infoturbe küsimustes, mis võivad nende tööd mõjutada, peaks amet arvestama olemasolevate teabekanalite ja rajatud võrgustikega. ***Selliste teadusasutustega, kes on käivitanud asjaomastes valdkondades teadusalgatusi, tuleks luua partnerlussuhted, ning tarbija- ja teiste organisatsioonide panustamiseks tuleks tagada asjakohased võimalused ja nende panust tuleks alati analüüsida.***

Muudatusettepanek 27

Ettepanek võtta vastu määrus
Põhjendus 31

Komisjoni ettepanek	*Muudatusettepanek*
(31) Amet on CSIRTide võrgustiku liige ja pakub neile ka sekretariaaditeenuseid ning peaks toetama liikmesriikide CSIRTe ja CERT-EUd operatiivkoostöös, mis lisandub CSIRTide võrgustiku kõigile asjaomastele ülesannetele, mis on kindlaks määratud võrgu- ja infotrube direktiivis. Veelgi enam, amet peaks edendama ja toetama ka asjaomaste CSIRTide koostööd, kui toimuvad intsidendid, ründed või häired CSIRTide hallatavates või kaitstavates võrkudes või taristutes, mis hõlmavad või võivad hõlmata vähemalt kahte CSIRTi, võttes sealjuures nõuetekohaselt arvesse CSIRTide võrgustiku standardset töökorda.	(31) Amet on CSIRTide võrgustiku liige ja pakub neile ka sekretariaaditeenuseid ning peaks toetama liikmesriikide CSIRTe ja CERT-EUd operatiivkoostöös, mis lisandub CSIRTide võrgustiku kõigile asjaomastele ülesannetele, mis on kindlaks määratud võrgu- ja infotrube direktiivis. Veelgi enam, amet peaks edendama ja toetama ka asjaomaste CSIRTide koostööd, kui toimuvad intsidendid, ründed või häired CSIRTide hallatavates või kaitstavates võrkudes või taristutes, mis hõlmavad või võivad hõlmata vähemalt kahte CSIRTi, võttes sealjuures nõuetekohaselt arvesse CSIRTide võrgustiku standardset töökorda. ***Amet viib***

	komisjoni või liikmesriigi taotluse korral läbi elutähtsate piiriüleste taristute korrapäraseid sõltumatuid IT-turvalisuse auditeid eesmärgiga teha kindlaks võimalikud kübertutvalisuse riskid ja anda soovitusi taristute vastupanuvõime tugevdamiseks.

Muudatusettepanek 28

Ettepanek võtta vastu määrus
Põhjendus 33

Komisjoni ettepanek	*Muudatusettepanek*
(33) Lisaks peaks amet arendama ja säilitama oma oskusteavet küberturvalisuse sertifitseerimise kohta, et toetada liidu poliitikat selles valdkonnas. Amet peaks edendama küberturvalisuse sertifitseerimise kasutuselevõttu liidus muu hulgas sellega, et aitab kehtestada liidu tasandil küberturvalisuse sertifitseerimise raamistiku ja seda hallata, et suurendada IKT toodete ja teenuste küberturvalisuse alase usaldusväärsuse läbipaistvust ning tugevdada seeläbi usaldust digitaalse siseturu vastu.	(33) Lisaks peaks amet arendama ja säilitama oma oskusteavet küberturvalisuse sertifitseerimise kohta, et toetada liidu poliitikat selles valdkonnas. Amet peaks ***tuginema olemasolevatele parimatele tavadele ja*** edendama küberturvalisuse sertifitseerimise kasutuselevõttu liidus muu hulgas sellega, et aitab kehtestada liidu tasandil küberturvalisuse sertifitseerimise raamistiku ja seda hallata, et suurendada IKT toodete ja teenuste küberturvalisuse alase usaldusväärsuse läbipaistvust ning tugevdada seeläbi usaldust digitaalse siseturu vastu.

Muudatusettepanek 29

Ettepanek võtta vastu määrus
Põhjendus 35

Komisjoni ettepanek	*Muudatusettepanek*
(35) Amet peaks innustama liikmesriike ja teenusepakkujaid tõstma oma üldisi turbestandardeid, et kõik internetikasutajad ***saaksid võtta*** vajalikud meetmed oma isikliku küberturvalisuse tagamiseks. Eelkõige peaksid tootjad ja teenuseosutajad võtma tagasi või taaskasutusse tooted ja teenused, mis ei vasta küberturvalisuse ***standarditele***. Koostöös pädevate asutustega võib ENISA jagada teavet	(35) Amet peaks innustama liikmesriike***, tootjaid*** ja teenusepakkujaid tõstma oma üldisi turbestandardeid ***seoses IKT toodete, protsesside, teenuste ja süsteemidega, mis peaksid vastama põhilistele julgeolekualastele kohustustele, mis on kooskõlas sisseprojekteeritud turbe ja vaikimisi turbe põhimõttega, eelkõige pakkudes vajalikke ajakohastusi***, et kõik internetikasutajad ***oleksid kaitstud ja***

siseturul pakutavate toodete ja teenuste küberturvalisuse taseme kohta ning avaldada teenusepakkujatele ***ja*** tootjatele suunatud hoiatusi, milles nõutakse nende toodete ***ja*** teenuste turvalisuse, sealhulgas küberturvalisuse parandamist.

motiveeritud võtma vajalikud meetmed oma isikliku küberturvalisuse tagamiseks. Eelkõige peaksid tootjad ja teenuseosutajad ***tagasi nõudma,*** võtma tagasi või taaskasutusse tooted ja teenused, mis ei vasta ***põhilistele*** küberturvalisuse ***kohustustele, samas kui importijad ja turustajad peaksid tagama, et nende poolt ELi turule lastud IKT tooted, protsessid, teenused ja süsteemid vastavad kohaldatavatele nõuetele ning ei kujuta endast ohtu Euroopa tarbijatele***. Koostöös pädevate asutustega võib ENISA jagada teavet siseturul pakutavate toodete ja teenuste küberturvalisuse taseme kohta ning avaldada teenusepakkujatele***,*** tootjatele suunatud hoiatusi, milles nõutakse nende toodete***, protsesside,*** teenuste ***ja süsteemide*** turvalisuse, sealhulgas küberturvalisuse parandamist. ***Amet peaks tegema sidusrühmadega koostööd, et töötada vastutustundliku turvanõrkustest teatamise kohta välja ELi-ülene lähenemisviis, ning edendama parimaid tavasid selles valdkonnas.***

Muudatusettepanek 30

Ettepanek võtta vastu määrus
Põhjendus 36

Komisjoni ettepanek	*Muudatusettepanek*
(36) Amet peaks täies ulatuses võtma arvesse tehtavaid teadusuuringuid, arendustegevust ja tehnoloogilisi hindamisi, eelkõige neid, mida tehakse mitmesuguste Euroopa Liidu teadusalgatuste raames, et nõustada liidu institutsioone, organeid ja asutusi ning kui see on asjakohane, liikmesriike nende taotlusel seoses vajadusega teadusuuringute järele võrgu- ja infoturbe, eelkõige küberturvalisuse valdkonnas.	(36) Amet peaks täies ulatuses võtma arvesse tehtavaid teadusuuringuid, arendustegevust ja tehnoloogilisi hindamisi, eelkõige neid, mida tehakse mitmesuguste Euroopa Liidu teadusalgatuste raames, et nõustada liidu institutsioone, organeid ja asutusi ning kui see on asjakohane, liikmesriike nende taotlusel seoses vajadusega teadusuuringute järele võrgu- ja infoturbe, eelkõige küberturvalisuse valdkonnas. ***Konkreetsemalt tuleks sisse seada koostöö Euroopa Teadusnõukogu (ERC) ja Euroopa Innovatsiooni- ja Tehnoloogiainstituudiga (EIT) ning***

	üheksandasse teadusuuringute raamprogrammi (FP9) ja programmi „Horisont 2020“ tuleks lisada turvalisusuuringud.

Muudatusettepanek 31

Ettepanek võtta vastu määrus
Põhjendus 36 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(36a) Standardid on vabatahtlikud ja turupõhised vahendid, mis pakuvad tehnilisi nõudeid ja suuniseid, ning avatud, läbipaistva ja kaasava protsessi tulemus. Amet peaks regulaarselt pidama nõu ja tegema tihedat koostööd standardiorganisatsioonidega, eriti Euroopa küberturvalisuse sertifitseerimise kavade koostamisel.

Muudatusettepanek 32

Ettepanek võtta vastu määrus
Põhjendus 37

Komisjoni ettepanek	*Muudatusettepanek*
(37) Küberturvalisusega seotud probleemid on ülemaailmsed. Vaja on teha tihedamat rahvusvahelist koostööd, et parandada turbestandardeid, (sealhulgas määratleda ühised käitumisnormid) ja teabe jagamist, millega edendatakse nii kiiremat rahvusvahelist koostööd reageerimise valdkonnas kui ka ühtset ülemaailmset lähenemisviisi võrgu- ja infoturbele. Selleks peaks amet toetama liidu tihedamat kaasamist ning koostööd kolmandate riikide ja rahvusvaheliste organisatsioonidega, pakkudes vajaduse korral asjaomastele liidu institutsioonidele, organitele ja asutustele vajalikku oskusteavet ja analüüsi.	(37) Küberturvalisusega seotud probleemid on ülemaailmsed. Vaja on teha tihedamat rahvusvahelist koostööd, et parandada turbestandardeid, (sealhulgas määratleda ühised käitumisnormid ***ja tegevusjuhendid*****), rahvusvaheliste standardite kasutamist** ja teabe jagamist, millega edendatakse nii kiiremat rahvusvahelist koostööd reageerimise valdkonnas kui ka ühtset ülemaailmset lähenemisviisi võrgu- ja infoturbele. Selleks peaks amet toetama liidu tihedamat kaasamist ning koostööd kolmandate riikide ja rahvusvaheliste organisatsioonidega, pakkudes vajaduse korral asjaomastele liidu institutsioonidele, organitele ja asutustele vajalikku oskusteavet ja analüüsi.

Muudatusettepanek 33

Ettepanek võtta vastu määrus
Põhjendus 40

Komisjoni ettepanek	*Muudatusettepanek*
(40) Liikmesriikide ja komisjoni esindajatest koosnev haldusnõukogu peaks kindlaks määrama ameti tegevuse üldsuuna ning tagama, et amet täidab oma ülesandeid vastavalt käesolevale määrusele. Haldusnõukogule tuleks anda õigus koostada ameti eelarve ja kontrollida selle täitmist, võtta vastu kohased finantseeskirjad, kehtestada ameti otsuste tegemiseks läbipaistev kord, võtta vastu ameti ühtne programmdokument, võtta vastu ameti töökord, nimetada ametisse tegevdirektor ning otsustada tegevdirektori ametiaja pikendamise ja tema ametiaja lõpetamise üle.	(40) Liikmesriikide ja komisjoni ***ning ameti eesmärkide jaoks asjaomaste sidusrühmade*** esindajatest koosnev haldusnõukogu peaks kindlaks määrama ameti tegevuse üldsuuna ning tagama, et amet täidab oma ülesandeid vastavalt käesolevale määrusele. Haldusnõukogule tuleks anda õigus koostada ameti eelarve ja kontrollida selle täitmist, võtta vastu kohased finantseeskirjad, kehtestada ameti otsuste tegemiseks läbipaistev kord, võtta vastu ameti ühtne programmdokument, võtta vastu ameti töökord, nimetada ametisse tegevdirektor ning otsustada tegevdirektori ametiaja pikendamise ja tema ametiaja lõpetamise üle. ***Ameti ülimalt tehnilisi ja teaduslikke ülesandeid silmas pidades peaksid haldusnõukokku kuuluma liikmed, kes on asjakohase kogemusega kõrgetasemeliste eksperditeadmistega ameti tegevusvaldkonda kuuluvates küsimustes.***

Muudatusettepanek 34

Ettepanek võtta vastu määrus
Põhjendus 41

Komisjoni ettepanek	*Muudatusettepanek*
(41) Ameti nõuetekohaseks ja tulemuslikuks toimimiseks peaksid komisjon ja liikmesriigid tagama, et haldusnõukogu liikmeteks nimetatavatel isikutel on vajalikud erialateadmised ja kogemused. Komisjon ja liikmesriigid peaksid püüdma piirata oma esindajate vahetumist haldusnõukogus, et tagada selle töö järjepidevus.	(41) Ameti nõuetekohaseks ja tulemuslikuks toimimiseks peaksid komisjon ja liikmesriigid tagama, et haldusnõukogu liikmeteks nimetatavatel isikutel on vajalikud erialateadmised ja kogemused. Komisjon ja liikmesriigid peaksid püüdma piirata oma esindajate vahetumist haldusnõukogus, et tagada selle töö järjepidevus. ***Kuna ameti tööks vajalikud oskused on suure***

turuväärtusega, tuleb tagada, et kõikidele ameti töötajatele pakutav palk ja sotsiaalsed tingimused oleksid konkurentsivõimelised ning et ametis töötamise kasuks saaksid otsustada parimad eksperdid.

Selgitus

Piisaval tasemel asjatundlikkuse tagamiseks peab ENISA olema äärmiselt tiheda konkurentsiga turul konkurentsivõimeline tööandja.

Muudatusettepanek 35

Ettepanek võtta vastu määrus
Põhjendus 42

Komisjoni ettepanek	*Muudatusettepanek*
(42) Ameti sujuvaks toimimiseks on tarvis, et tegevdirektor nimetataks ametisse silmas pidades tema teeneid, dokumenteeritud haldamis- ja juhtimisoskust ning küberturvalisuse alaseid teadmisi ja kogemusi ning et tegevdirektori ülesandeid täidetaks täiesti sõltumatult. Tegevdirektor peaks pärast komisjoniga konsulteerimist koostama ettepaneku ameti tööprogrammi kohta ning võtma kõik vajalikud meetmed ameti tööprogrammi nõuetekohase täitmise tagamiseks. Tegevdirektor peaks koostama igal aastal haldusnõukogule esitatava aruande, koostama ameti tulude ja kulude kalkulatsiooni eelnõu ning vastutama eelarve täitmise eest. Lisaks peaks tegevdirektoril olema võimalus luua ajutisi töörühmi selleks, et käsitleda eelkõige teaduslikke, tehnilisi, juriidilisi või sotsiaal-majanduslikke küsimusi. Tegevdirektor peaks tagama, et ajutistesse töörühmadesse valitakse liikmed kõige põhjalikumate erialateadmiste põhjal, võttes nõuetekohaselt arvesse, et seal oleksid (lähtuvalt sellest, kuidas see on konkreetset küsimust arvestades asjakohane) tasakaalustatult esindatud liikmesriikide riiklikud haldusorganid, liidu institutsioonid ja erasektor, sealhulgas	(42) Ameti sujuvaks toimimiseks on tarvis, et tegevdirektor nimetataks ametisse silmas pidades tema teeneid, dokumenteeritud haldamis- ja juhtimisoskust ning küberturvalisuse alaseid teadmisi ja kogemusi ning et tegevdirektori ülesandeid täidetaks täiesti sõltumatult. Tegevdirektor peaks pärast komisjoniga konsulteerimist koostama ettepaneku ameti tööprogrammi kohta ning võtma kõik vajalikud meetmed ameti tööprogrammi nõuetekohase täitmise tagamiseks. Tegevdirektor peaks koostama igal aastal haldusnõukogule esitatava aruande, koostama ameti tulude ja kulude kalkulatsiooni eelnõu ning vastutama eelarve täitmise eest. Lisaks peaks tegevdirektoril olema võimalus luua ajutisi töörühmi selleks, et käsitleda eelkõige teaduslikke, tehnilisi, juriidilisi või sotsiaal-majanduslikke küsimusi. Tegevdirektor peaks tagama, et ajutistesse töörühmadesse valitakse liikmed kõige põhjalikumate erialateadmiste põhjal, võttes nõuetekohaselt arvesse, et seal oleksid (lähtuvalt sellest, kuidas see on konkreetset küsimust arvestades asjakohane) tasakaalustatult ***ja ka soolises tasakaalus*** esindatud liikmesriikide riiklikud haldusorganid, liidu

majandusringkonnad, kasutajad ning võrgu- ja infoturbe alal pädevad teaduseksperdid.	institutsioonid ja erasektor, sealhulgas majandusringkonnad, kasutajad ning võrgu- ja infoturbe alal pädevad teaduseksperdid.

Muudatusettepanek 36

Ettepanek võtta vastu määrus
Põhjendus 44

Komisjoni ettepanek	*Muudatusettepanek*
(44) Ametil peaks olema nõuandva organina ***alaline sidusrühm***, mis tagaks regulaarse dialoogi erasektori, tarbijate organisatsioonide ja teiste asjaomaste sidusrühmadega. Tegevdirektori ettepanekul haldusnõukogu asutatud ***alaline sidusrühm*** peaks keskenduma sidusrühmade jaoks olulistele küsimustele ja juhtima neile ameti tähelepanu. Alalise sidusrühma koosseis ja ülesanded (eelkõige tuleb rühmaga konsulteerida tööprogrammi projekti üle) peaksid tagama sidusrühmade piisava esindatuse ameti töös.	(44) Ametil peaks olema nõuandva organina ***ENISA nõuanderühm***, mis tagaks regulaarse dialoogi erasektori, tarbijate organisatsioonide***, teadusasutuste*** ja teiste asjaomaste sidusrühmadega. Tegevdirektori ettepanekul haldusnõukogu asutatud ***ENISA nõuanderühm*** peaks keskenduma sidusrühmade jaoks olulistele küsimustele ja juhtima neile ameti tähelepanu. Alalise sidusrühma koosseis ja ülesanded (eelkõige tuleb rühmaga konsulteerida tööprogrammi projekti üle) peaksid tagama sidusrühmade piisava esindatuse ameti töös. ***Arvestades, kui olulised on sertifitseerimisnõuded asjade interneti usaldusväärsuse tagamiseks, kaalub komisjon konkreetsete rakendusmeetmete võtmist, millega tagatakse asjade interneti seadmete turvastandardite ühtlustamine kogu ELis.***

Muudatusettepanek 37

Ettepanek võtta vastu määrus
Põhjendus 44 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(44a) Ametil peaks olema nõuandva organina sidusrühmade sertifitseerimisrühm, et tagada regulaarne dialoog erasektori, tarbijate organisatsioonide, teadusasutuste ja teiste asjaomaste sidusrühmadega. Tegevdirektori loodud sidusrühmade

	sertifitseerimisrühm peaks koosnema üldisest nõuandekomiteest, kes esitab ettepanekuid selle kohta, millised IKT tooted ja teenused tuleks tulevikus hõlmata Euroopa IT-turvalisuse sertifitseerimise kavadega, ning ajutised komiteed, kes esitavad ettepanekuid Euroopa küberturvalisuse sertifitseerimise ettevalmistavate kavade esildamiseks, koostamiseks ja vastuvõtmiseks.

Muudatusettepanek 38

Ettepanek võtta vastu määrus
Põhjendus 46

Komisjoni ettepanek	*Muudatusettepanek*
(46) Et tagada ameti täielik autonoomia ja sõltumatus ning võimaldada tal täita uusi ja lisaülesandeid, sealhulgas kiireloomulisi erakorralisi ülesandeid, tuleks ametile eraldada piisav ja autonoomne eelarve, mille peamine tulu tuleb liidu osamaksest ja ameti töös osalevate kolmandate riikide sissemaksetest. Enamik ameti töötajaid peaks olema otseselt tegev ameti manaadi rakendamises. Asukohaliikmesriigil või mis tahes muul liikmesriigil peaks olema lubatud teha ameti tuludesse vabatahtlikult sissemakseid. Liidu eelarvemenetluse kohaldamist tuleks jätkata mis tahes subsiidiumide suhtes, mida makstakse Euroopa Liidu üldeelarvest. Lisaks sellele peaks ameti raamatupidamisarvestust läbipaistvuse ja vastutuse tagamiseks auditeerima kontrollikoda.	(46) Et tagada ameti täielik autonoomia ja sõltumatus ning võimaldada tal täita uusi ja lisaülesandeid, sealhulgas kiireloomulisi erakorralisi ülesandeid, tuleks ametile eraldada piisav ja autonoomne eelarve, mille peamine tulu tuleb liidu osamaksest ja ameti töös osalevate kolmandate riikide sissemaksetest. ***Piisav eelarve on ülioluline tagamaks, et ametil on kõigi oma kasvavate ülesannete ja eesmärkide täitmiseks vajalik suutlikkus.*** Enamik ameti töötajaid peaks olema otseselt tegev ameti manaadi rakendamises. Asukohaliikmesriigil või mis tahes muul liikmesriigil peaks olema lubatud teha ameti tuludesse vabatahtlikult sissemakseid. Liidu eelarvemenetluse kohaldamist tuleks jätkata mis tahes subsiidiumide suhtes, mida makstakse Euroopa Liidu üldeelarvest. Lisaks sellele peaks ameti raamatupidamisarvestust läbipaistvuse***,*** vastutuse ja ***kulude tasuvuse*** tagamiseks auditeerima kontrollikoda.

Muudatusettepanek 39

Ettepanek võtta vastu määrus
Põhjendus 47

Komisjoni ettepanek	*Muudatusettepanek*
(47) Vastavushindamine on hindamisprotsess, mille käigus hinnatakse, kas toote, protsessi, teenuse, süsteemi, isiku või asutusega seotud erinõuded on täidetud. Käesoleva määruse kohaldamisel tuleks sertifitseerimist käsitada teatavat liiki vastavushindamisena, mis puudutab toote, protsessi, teenuse, süsteemi või nende kombinatsiooni (edaspidi „IKT tooted ja teenused“) küberturvalisuse elemente ja mida teostab sõltumatu kolmas isik, mitte tootja või teenusepakkuja. Sertifitseerimine iseenesest ei taga, et sertifitseeritud IKT tooted ja teenused on küberturvalised. Pigem on see menetlus ja tehniline metoodika tõendamaks, et IKT tooteid ja teenuseid on kontrollitud ja et need vastavad teatavatele küberturvalisuse nõuetele, mis on sätestatud mujal, näiteks tehnilistes standardites.	(47) Vastavushindamine on hindamisprotsess, mille käigus hinnatakse, kas toote, protsessi, teenuse, süsteemi, isiku või asutusega seotud erinõuded on täidetud. Käesoleva määruse kohaldamisel tuleks sertifitseerimist käsitada teatavat liiki vastavushindamisena, mis puudutab toote, protsessi, teenuse, süsteemi või nende kombinatsiooni (edaspidi „IKT tooted***, protsessid*** ja teenused“) küberturvalisuse elemente ja mida teostab sõltumatu kolmas isik***, või juhul, kui see on lubatud,*** tootja või teenusepakkuja ***enesehindamise teel***. ***Enesehindamise võib läbi viia käesolevas määruses täpsustatud tootja, VKE või teenuseosutaja ning, kui see on asjakohane, nii nagu on ette nähtud uues õigusraamistikus ja selle kohaselt. Enesehindamise võib korraldada tootja või käitaja, kui küberturvalisuse intsidendi toimumise tõenäosus ja/või tõenäosus, et taoline intsident tekitab olulist kahju ühiskonnale või selle suurele osale, ei ole eeldatavalt suur ega märkimisväärne, võttes arvesse tootja või teenuseosutaja poolt kõnealusele tootele või teenusele ette nähtud kasutusotstarvet.*** Sertifitseerimine iseenesest ei taga, et sertifitseeritud IKT tooted***, protsessid*** ja teenused on küberturvalised, ***ning tarbijaid ja ettevõtjaid tuleb sellest nõuetekohaselt teavitada***. Pigem on see menetlus ja tehniline metoodika tõendamaks, et IKT tooteid***, protsesse*** ja teenuseid on kontrollitud ja et need vastavad teatavatele küberturvalisuse nõuetele, mis on sätestatud mujal, näiteks tehnilistes standardites. ***Tehnilised standardid hõlmavad viidet sellele, kas IKT toode, protsess või teenus on võimeline täitma oma tavaülesandeid, kui ühendus***

internetiga puudub.

Muudatusettepanek 40

Ettepanek võtta vastu määrus
Põhjendus 48

Komisjoni ettepanek	*Muudatusettepanek*
(48) Küberturvalisuse sertifitseerimisel on tähtis ülesanne IKT toodete ja teenuste turvalisuse ja nende vastu usalduse suurendamises. Digitaalne ühtne turg ning eelkõige andmepõhine majandus ja asjade internet saavad olla edukad vaid juhul, kui avalikkusel on kindlustunne, et sellised tooted ja teenused pakuvad teatavat küberturvalisuse taset. Internetiühendusega ja automatiseeritud autod, elektroonilised meditsiiniseadmed, tööstuslikud automatiseeritud juhtimissüsteemid või arukad võrgud on vaid mõned näited sektoritest, kus sertifitseerimist juba ulatuslikult kasutatakse või tõenäoliselt hakatakse lähitulevikus kasutama. Võrgu- ja infoturbe direktiiviga reguleeritud sektorid on ka sektorid, kus küberturvalisuse sertifitseerimine on äärmiselt oluline.	(48) ***Euroopa*** küberturvalisuse sertifitseerimisel on ***vältimatult oluline*** ülesanne IKT toodete***, protsesside*** ja teenuste turvalisuse ja nende vastu usalduse suurendamises. Digitaalne ühtne turg ning eelkõige andmepõhine majandus ja asjade internet saavad olla edukad vaid juhul, kui avalikkusel on kindlustunne, et sellised tooted ja teenused pakuvad ***kõrget*** küberturvalisuse taset. Internetiühendusega ja automatiseeritud autod, elektroonilised meditsiiniseadmed, tööstuslikud automatiseeritud juhtimissüsteemid või arukad võrgud on vaid mõned näited sektoritest, kus sertifitseerimist juba ulatuslikult kasutatakse või tõenäoliselt hakatakse lähitulevikus kasutama. Võrgu- ja infoturbe direktiiviga reguleeritud sektorid on ka sektorid, kus küberturvalisuse sertifitseerimine on äärmiselt oluline.

Muudatusettepanek 41

Ettepanek võtta vastu määrus
Põhjendus 49

Komisjoni ettepanek	*Muudatusettepanek*
(49) 2016. aasta teatises „Euroopa kübervastupidavusvõime süsteemi tugevdamine ning konkurentsivõimelise ja uuendusliku küberjulgeolekutööstuse soodustamine“ tõi komisjon välja vajaduse kvaliteetsete, taskukohaste ja koostalitlusvõimeliste küberturvalisuse toodete ja -lahenduste järele. IKT toodete ja teenuste pakkumine ühtsel turul on	(49) 2016. aasta teatises „Euroopa kübervastupidavusvõime süsteemi tugevdamine ning konkurentsivõimelise ja uuendusliku küberjulgeolekutööstuse soodustamine“ tõi komisjon välja vajaduse kvaliteetsete, taskukohaste ja koostalitlusvõimeliste küberturvalisuse toodete ja -lahenduste järele. IKT toodete***, protsesside*** ja teenuste pakkumine ühtsel

endiselt geograafiliselt väga killustatud. Selle põhjuseks on asjaolu, et küberturvalisuse tööstus on Euroopas peamiselt arenenud riikliku, täpsemalt valitsuse nõudluse najal. Lisaks kuulub kübeturvalisuse ühtse turu kitsaskohtade hulka koostalitusvõimeliste lahenduste (tehniliste standardite), tavade ja kogu ELi hõlmavate sertifitseerimismehhanismide puudumine. Ühest küljest teeb see riiklikul, Euroopa ja üleilmsel tasandil konkureerimise Euroopa ettevõtjate jaoks keerukaks. Teisest küljest tähendab see üksikisikute ja ettevõtjate jaoks võimaliku ja kasutatava küberturvalisuse tehnoloogia kättesaadavust väiksemas valikus. Euroopa digitaalse ühtse turu strateegia rakendamise vahekokkuvõttes rõhutas komisjon vajadust turvaliste võrgustatud toodete ja süsteemide järele ning märkis, et Euroopa IKT turvalisuse raamistiku loomine, millega kehtestatakse õigusnormid selle kohta, kuidas korraldada IKT turvalisuse sertifitseerimist liidus, võib aidata säilitada usaldust interneti vastu ja vähendada küberturvalisuse turu praegust killustatust.	turul on endiselt geograafiliselt väga killustatud. Selle põhjuseks on asjaolu, et küberturvalisuse tööstus on Euroopas peamiselt arenenud riikliku, täpsemalt valitsuse nõudluse najal. Lisaks kuulub kübeturvalisuse ühtse turu kitsaskohtade hulka koostalitusvõimeliste lahenduste (tehniliste standardite), tavade ja kogu ELi hõlmavate sertifitseerimismehhanismide puudumine. Ühest küljest teeb see riiklikul, Euroopa ja üleilmsel tasandil konkureerimise Euroopa ettevõtjate jaoks keerukaks. Teisest küljest tähendab see üksikisikute ja ettevõtjate jaoks võimaliku ja kasutatava küberturvalisuse tehnoloogia kättesaadavust väiksemas valikus. Euroopa digitaalse ühtse turu strateegia rakendamise vahekokkuvõttes rõhutas komisjon vajadust turvaliste võrgustatud toodete ja süsteemide järele ning märkis, et Euroopa IKT turvalisuse raamistiku loomine, millega kehtestatakse õigusnormid selle kohta, kuidas korraldada IKT turvalisuse sertifitseerimist liidus, võib aidata säilitada usaldust interneti vastu ja vähendada küberturvalisuse turu praegust killustatust.

Muudatusettepanek 42

Ettepanek võtta vastu määrus
Põhjendus 50

Komisjoni ettepanek	*Muudatusettepanek*
(50) Praegu kasutatakse IKT toodete ja teenuste küberturvalisuse sertifitseerimist ainult piiratud ulatuses. Kui sertifitseerimine on olemas, siis peamiselt liikmesriigi tasandil või tööstusest lähtuvate kavade raames. Sellistes tingimustes ei tunnusta teised liikmesriigid üldiselt ühe riigi küberturvalisuse asutuse poolt välja antud sertifikaati. Seega võib juhtuda, et ettevõtted peavad sertifitseerima oma tooted ja teenused mitmes liikmesriigis, kus nad tegutsevad, näiteks et osaleda riiklikes hankemenetlustes. Lisaks sellele paistab, et kuigi on tekkimas uusi kavasid, ei ole ühtset ja terviklikku	(50) Praegu kasutatakse IKT toodete***,*** ***protsesside*** ja teenuste küberturvalisuse sertifitseerimist ainult piiratud ulatuses. Kui sertifitseerimine on olemas, siis peamiselt liikmesriigi tasandil või tööstusest lähtuvate kavade raames. Sellistes tingimustes ei tunnusta teised liikmesriigid üldiselt ühe riigi küberturvalisuse asutuse poolt välja antud sertifikaati. Seega võib juhtuda, et ettevõtted peavad sertifitseerima oma tooted***,*** ***protsessid*** ja teenused mitmes liikmesriigis, kus nad tegutsevad, näiteks et osaleda riiklikes hankemenetlustes, ***see aga suurendab kulusid***. Lisaks sellele paistab,

lähenemisviisi küberturvalisuse horisontaalsetele küsimustele, näiteks asjade interneti valdkonnas. Olemasolevatel kavadel on märkimisväärseid puudujääke ning erinevusi tootehõlmavuses, usaldusväärsuse tasemetes, sisulistes kriteeriumides ja tegelikus kasutamises.	et kuigi on tekkimas uusi kavasid, ei ole ühtset ja terviklikku lähenemisviisi küberturvalisuse horisontaalsetele küsimustele, näiteks asjade interneti valdkonnas. Olemasolevatel kavadel on märkimisväärseid puudujääke ning erinevusi tootehõlmavuses, ***riskipõhise*** usaldusväärsuse tasemetes, sisulistes kriteeriumides ja tegelikus kasutamises. ***Vastastikusel tunnustamisel ja liikmesriikidevahelisel usaldusel on seetõttu oluline roll. ENISA-l on tähtis roll liikmesriikide abistamisel, et töötada välja usaldusväärne institutsiooniline struktuur ja arendada eksperditeadmisi võimalike küberrünnete vastase kaitse valdkonnas. Vajalik on juhtumipõhine lähenemisviis, mis aitaks tagada, et teenuste, protsesside ja toodete suhtes kohaldatakse asjakohast sertifitseerimiskava. Peale selle on vaja riskipõhist lähenemisviisi riskide tõhusaks avastamiseks ja leevendamiseks, tunnistades samas, et ühte kõigile sobivat kava ei ole võimalik rakendada.***

Muudatusettepanek 43

Ettepanek võtta vastu määrus
Põhjendus 52

Komisjoni ettepanek	*Muudatusettepanek*
(52) Eelnevat arvestades on vaja luua Euroopa küberturvalisuse sertifitseerimise raamistik, milles kehtestatakse välja töötatavate Euroopa küberturvalisuse sertifitseerimise kavade peamised horisontaalsed nõuded ning mis võimaldab tunnustada ja kasutada IKT toodete ja teenuste sertifikaate kõigis liikmesriikides. Euroopa raamistikul peaks olema kaks eesmärki: ühest küljest peaks see aitama suurendada usaldust nende kavade kohaselt sertifitseeritud IKT toodete ja teenuste vastu. Teisest küljest peaks see vältima üksteisele vastukäivate või kattuvate riiklike küberturvalisuse sertifikaatide	(52) Eelnevat arvestades on vaja ***võtta kasutusele ühine käsitus ja*** luua Euroopa küberturvalisuse sertifitseerimise raamistik, milles kehtestatakse välja töötatavate Euroopa küberturvalisuse sertifitseerimise kavade peamised horisontaalsed nõuded ning mis võimaldab tunnustada ja kasutada IKT toodete***, protsesside*** ja teenuste sertifikaate kõigis liikmesriikides. ***Seejuures on oluline tugineda olemasolevatele riiklikele ja rahvusvahelistele kavadele ning vastastikuse tunnustamise süsteemidele, eelkõige kõrgemate ametnike infosüsteemide turbe rühmale, ning***

paljusust ja seeläbi vähendama digitaalsel ühtsel turul tegutsevate ettevõtjate kulusid. Kavad peaksid olema mittediskrimineerivad ning põhinema rahvusvahelistel ja/või ELi standarditel, välja arvatud juhul, kui need standardid on ebatõhusad või ebasobivad ELi õiguspäraste eesmärkide saavutamiseks selles valdkonnas.	***võimaldada selliste süsteemide kohastelt olemasolevatelt kavadelt sujuvat üleminekut uue Euroopa raamistiku kohastele kavadele***. Euroopa raamistikul peaks olema kaks eesmärki: ühest küljest peaks see aitama suurendada usaldust nende kavade kohaselt sertifitseeritud IKT toodete***, protsesside*** ja teenuste vastu. Teisest küljest peaks see vältima üksteisele vastukäivate või kattuvate riiklike küberturvalisuse sertifikaatide paljusust ja seeläbi vähendama digitaalsel ühtsel turul tegutsevate ettevõtjate kulusid. ***Kui Euroopa küberturvalisuse sertifitseerimise kava on riikliku kava asendanud, tuleks juhtudel, kus oli nõutav sertifitseerimine riikliku kava alusel, lugeda kehtivaks Euroopa kava alusel väljastatud sertifikaadid. Kavades tuleks juhinduda sisseprojekteeritud turbe põhimõttest ja määruses (EL) 2016/679 osutatud põhimõtetest.*** Kavad peaksid ***ühtlasi*** olema mittediskrimineerivad ning põhinema rahvusvahelistel ja/või ELi standarditel, välja arvatud juhul, kui need standardid on ebatõhusad või ebasobivad ELi õiguspäraste eesmärkide saavutamiseks selles valdkonnas.

Muudatusettepanek 44

Ettepanek võtta vastu määrus
Põhjendus 52 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(52a) Euroopa küberturvalisuse sertifitseerimise raamistik tuleb luua ühetaoliselt kõikides liikmesriikides, et vältida sertifikaatide ostlemise tava, mida põhjustab kulude ja nõuete erinevus liikmesriikides.

Muudatusettepanek 45

Ettepanek võtta vastu määrus
Põhjendus 52 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(52b) Sertifitseerimiskavad peaksid tuginema sellele, mis on riiklikul ja rahvusvahelisel tasandil juba olemas. Seejuures tuleks õppida praegustest tugevatest külgedest ning hinnata puudusi ja need kõrvaldada.

Muudatusettepanek 46

Ettepanek võtta vastu määrus
Põhjendus 52 c (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(52c) Selleks et tööstus suudaks ennetada pahatahtlikke rünnakuid ja ohte, on vaja paindlikke küberturvalisuse lahendusi, mistõttu tuleks iga sertifitseerimiskava puhul vältida kiire aegumise ohtu.

Muudatusettepanek 47

Ettepanek võtta vastu määrus
Põhjendus 53

Komisjoni ettepanek	*Muudatusettepanek*
(53) Komisjonile tuleks anda volitused võtta vastu Euroopa küberturvalisuse sertifitseerimise kavad konkreetsete IKT toodete ja teenuste rühmade kohta. Neid kavu peaksid rakendama ja nende üle järelevalvet teostama riiklikud sertifitseerimise järelevalveasutused ning nende kavade kohaselt välja antud sertifikaadid peaksid kehtima ja olema tunnustatud kogu liidus. Tööstuse või muude eraorganisatsioonide rakendatavad sertifitseerimiskavad peaksid jääma väljapoole määruse kohaldamisala. Siiski võivad selliseid kavu haldavad asutused	(53) Komisjonile tuleks anda volitused võtta vastu Euroopa küberturvalisuse sertifitseerimise kavad konkreetsete IKT toodete***, protsesside*** ja teenuste rühmade kohta. Neid kavu peaksid rakendama ja nende üle järelevalvet teostama riiklikud sertifitseerimise järelevalveasutused ning nende kavade kohaselt välja antud sertifikaadid peaksid kehtima ja olema tunnustatud kogu liidus. Tööstuse või muude eraorganisatsioonide rakendatavad sertifitseerimiskavad peaksid jääma väljapoole määruse kohaldamisala. Siiski võivad selliseid kavu haldavad asutused

teha komisjonile ettepaneku kaaluda nende heakskiitmist Euroopa kavana.	teha komisjonile ettepaneku kaaluda nende heakskiitmist Euroopa kavana. ***Amet peaks tegema kindlaks tööstuses või eraorganisatsioonides juba rakendatavad kavad ja neid hindama, et valida välja parimad tavad, mis võiksid saada Euroopa kava osaks. Tööstussektori ettevõtjad võivad enne sertifitseerimist teha oma toodete või teenuste enesehindamise, näidates nii, et nende toode või teenus on nõudmise või vajaduse korral valmis sertifitseerimisprotsessiga alustama.***

Muudatusettepanek 48

Ettepanek võtta vastu määrus
Põhjendus 53 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(53a) Amet ja komisjon peaksid maksimaalselt ära kasutama ELi ja/või rahvusvahelisel tasandil juba olemasolevaid sertifitseerimiskavasid. ENISA-l peaks olema võime hinnata, millised juba kasutuses olevad kavad on eesmärgipärased ja mida saab koostöös ELi standardiorganisatsioonidega lisada Euroopa õigusaktidesse ja mida on võimalikult suurel määral rahvusvaheliselt tunnustatud. Olemasolevaid häid tavasid tuleks koguda ja liikmesriikide vahel jagada.

Muudatusettepanek 49

Ettepanek võtta vastu määrus
Põhjendus 54

Komisjoni ettepanek	*Muudatusettepanek*
(54) Käesoleva määruse sätted ei tohiks mõjutada liidu õigusakte, milles on sätestatud konkreetsed eeskirjad IKT toodete ja teenuste sertifitseerimise kohta. Isikuandmete kaitse üldmäärus sisaldab sätteid selliste	(54) Käesoleva määruse sätted ei tohiks mõjutada liidu õigusakte, milles on sätestatud konkreetsed eeskirjad IKT toodete***, protsesside*** ja teenuste sertifitseerimise kohta. Isikuandmete kaitse üldmäärus sisaldab sätteid selliste

sertifitseerimismehhanismide ning andmekaitsepitserite ja -märgiste kasutuselevõtuks, mille abil saab tõendada, et vastutavate töötlejate ja volitatud töötlejate isikuandmete töötlemise toimingud vastavad kõnealusele määrusele. Sellised sertifitseerimismehhanismid ning andmekaitsepitserid ja -märgised peaksid võimaldama andmesubjektidel kiiresti hinnata asjakohaste toodete ja teenuste andmekaitse taset. Käesolev määrus ei piira andmetöötlustoimingute sertifitseerimist isikuandmete kaitse üldmääruse kohaselt, sealhulgas juhul, kui sellised toimingud sisalduvad toodetes või teenustes.

sertifitseerimismehhanismide ning andmekaitsepitserite ja -märgiste kasutuselevõtuks, mille abil saab tõendada, et vastutavate töötlejate ja volitatud töötlejate isikuandmete töötlemise toimingud vastavad kõnealusele määrusele. Sellised sertifitseerimismehhanismid ning andmekaitsepitserid ja -märgised peaksid võimaldama andmesubjektidel kiiresti hinnata asjakohaste toodete ja teenuste andmekaitse taset. Käesolev määrus ei piira andmetöötlustoimingute sertifitseerimist isikuandmete kaitse üldmääruse kohaselt, sealhulgas juhul, kui sellised toimingud sisalduvad toodetes või teenustes.

Muudatusettepanek 50

Ettepanek võtta vastu määrus
Põhjendus 55

Komisjoni ettepanek	*Muudatusettepanek*
(55) Euroopa küberturvalisuse sertifitseerimise kavade eesmärk on kinnitada, et sellise kava kohaselt sertifitseeritud IKT tooted ja teenused vastavad kirjeldatud nõuetele. Nimetatud nõuded puudutavad võimet pidada teataval ***usaldusväärsuse*** tasemel vastu tegevustele, mille eesmärk on rikkuda salvestatud, edastatud või töödeldud andmete või nende toodete, protsesside, teenuste ja süsteemide asjaomaste funktsioonide või nende poolt pakutavate või nende kaudu juurdepääsetavate teenuste käideldavust, autentsust, terviklust või konfidentsiaalsust käesoleva määruse tähenduses. Käesolevas määruses ei ole võimalik üksikasjalikult kirjeldada kõigi IKT toodete ja teenuste suhtes kohaldatavaid küberturvalisuse nõudeid. IKT tooted ja teenused ning nendega seotud küberturvalisuse vajadused on nii mitmekesised, et on väga raske esitada üldiseid küberturvalisuse nõudeid, mis kehtiksid kõikjal. Seetõttu on vaja sertifitseerimise eesmärgil võtta kasutusele lai ja üldine küberturvalisuse mõiste, mida	(55) Euroopa küberturvalisuse sertifitseerimise kavade eesmärk on kinnitada, et sellise kava kohaselt sertifitseeritud IKT tooted***,*** teenused ja ***protsessid*** vastavad kirjeldatud nõuetele. Nimetatud nõuded puudutavad võimet pidada teataval ***riski*** tasemel vastu tegevustele, mille eesmärk on rikkuda salvestatud, edastatud või töödeldud andmete või nende toodete, protsesside, teenuste ja süsteemide asjaomaste funktsioonide või nende poolt pakutavate või nende kaudu juurdepääsetavate teenuste käideldavust, autentsust, terviklust või konfidentsiaalsust käesoleva määruse tähenduses. Käesolevas määruses ei ole võimalik üksikasjalikult kirjeldada kõigi IKT toodete***,*** teenuste ja ***protsesside*** suhtes kohaldatavaid küberturvalisuse nõudeid. IKT tooted***,*** teenused ja ***protsessid*** ning nendega seotud küberturvalisuse vajadused on nii mitmekesised, et on väga raske esitada üldiseid küberturvalisuse nõudeid, mis kehtiksid kõikjal. Seetõttu on vaja sertifitseerimise eesmärgil võtta kasutusele

täiendab rida konkreetseid küberturvalisuse eesmärke, mida tuleb Euroopa küberturvalisuse sertifitseerimise kavade koostamisel arvesse võtta. Nende eesmärkide saavutamise meetodid konkreetsete IKT toodete ja teenuste puhul tuleks täpsustada üksikasjalikult igas individuaalses sertifitseerimiskavas, mille komisjon vastu võtab, näiteks viidates standarditele või tehnilistele kirjeldustele.

lai ja üldine küberturvalisuse mõiste, mida täiendab rida konkreetseid küberturvalisuse eesmärke, mida tuleb Euroopa küberturvalisuse sertifitseerimise kavade koostamisel arvesse võtta. Nende eesmärkide saavutamise meetodid konkreetsete IKT toodete***,*** teenuste ja ***protsesside*** puhul tuleks täpsustada üksikasjalikult igas individuaalses sertifitseerimiskavas, mille komisjon vastu võtab, näiteks viidates standarditele või tehnilistele kirjeldustele. ***Kõiki ettevõtjaid, kes osalevad konkreetses tarneahelas, tuleks innustada töötama välja turbestandardeid, tehnilisi norme ning sisseprojekteeritud turbe põhimõtteid toote, teenuse või protsessi elutsükli kõikides etappides ja neid vastu võtma; iga Euroopa küberturvalisuse sertifitseerimise kava tuleks koostada selle kohaldamisala jaoks.***

Muudatusettepanek 51

Ettepanek võtta vastu määrus
Põhjendus 56

Komisjoni ettepanek	*Muudatusettepanek*
(56) Komisjonile tuleks anda volitused paluda ENISA-l koostada ettevalmistav sertifitseerimiskava konkreetsete IKT toodete ja teenuste jaoks***. Seejärel tuleks anda komisjonile volitused võtta*** ENISA esitatud ***ettevalmistava kava põhjal rakendusaktidega*** vastu Euroopa küberturvalisuse sertifitseerimise ***kava***. Võttes arvesse käesolevas määruses määratletud üldeesmärki ja turvalisusega seotud eesmärke, tuleks ***komisjoni poolt vastu võetud*** Euroopa küberturvalisuse sertifitseerimise kavades täpsustada konkreetse kava sisu, ulatuse ja toimimise minimaalsed üksikasjad. Need peaksid hõlmama muu hulgas küberturvalisuse sertifikaadi ulatust ja sisu, sealhulgas hõlmatud IKT toodete ja teenuste kategooriad, küberturvalisuse nõuete	(56) Komisjonile tuleks anda volitused paluda ENISA-l koostada ettevalmistav sertifitseerimiskava konkreetsete IKT toodete***, protsesside*** ja teenuste jaoks ***lähtudes õigustatud põhjustest, milleks on olemasolevad siseriiklikud küberturvalisuse sertifitseerimise kavad, mis killustavad siseturgu, olemasolev või prognoositav vajadus toetada liidu õigusakte või liikmesriikide sertifitseerimisrühma või sidusrühmade sertifitseerimisrühma arvamus. Pärast komisjoni taotluse alusel*** ENISA esitatud ***kandidaatide sertifitseerimiskavade hindamist tuleks komisjonile anda volitused võtta delegeeritud õigusaktidega*** vastu Euroopa küberturvalisuse sertifitseerimise ***kavad***. Võttes arvesse käesolevas määruses määratletud

üksikasjalik kirjeldus, näiteks viide standarditele või tehnilistele kirjeldustele, konkreetsed hindamiskriteeriumid ja -meetodid ning kavandatud usaldusväärsuse tase: baastase, märkimisväärne ja/või kõrge tase.	üldeesmärki ja turvalisusega seotud eesmärke, tuleks ***nendes*** Euroopa küberturvalisuse sertifitseerimise kavades täpsustada konkreetse kava sisu, ulatuse ja toimimise minimaalsed üksikasjad. Need peaksid hõlmama muu hulgas küberturvalisuse sertifikaadi ulatust ja sisu, sealhulgas hõlmatud IKT toodete ja teenuste kategooriad, küberturvalisuse nõuete üksikasjalik kirjeldus, näiteks viide standarditele või tehnilistele kirjeldustele, konkreetsed hindamiskriteeriumid ja -meetodid ning kavandatud usaldusväärsuse tase: baastase, märkimisväärne ja/või kõrge tase.

Muudatusettepanek 52

Ettepanek võtta vastu määrus
Põhjendus 56 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(56a) Amet peaks olema teabealane kontaktpunkt Euroopa küberturvalisuse sertifitseerimise kavade valdkonnas. Ta peaks haldama veebisaiti, kus on esitatud kogu asjakohane teave, sealhulgas teave tühistatud sertifikaatide ja aegunud sertifikaatide ning riiklike sertifitseerimiste kohta. Amet peaks tagama, et piisav osa tema veebisaidi sisust on tavatarbijatele arusaadav.

Muudatusettepanek 53

Ettepanek võtta vastu määrus
Põhjendus 56 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(56b) Usaldusväärsuse taseme kindlaksmääramine sertifikaatide puhul on vajalik selleks, et osutada lõpptarbijale, milliseid eeldatavaid küberohte on toote, protsessi või teenuse küberturbemeetmed kavandatud ära hoidma. Küberohud tuleb

	määratleda, võttes arvesse eeldatavat riski ning rünnaku autori või autorite võimeid, arvestades asjaomase IKT- toote, protsessi või teenuse eeldatavat kasutust. Usaldusväärsuse baastase tähendab võimet pidada vastu rünnakutele, mida on võimalik vältida elementaarsete küberturbemeetmetega ning mida saab hõlpsasti kontrollida tehniliste dokumentide läbivaatamisega. Märkimisväärne usaldusväärsuse tase tähendab võimet pidada vastu teadaolevat liiki rünnakutele, mille paneb toime teatava keerukusastmega, kuid piiratud vahenditega ründaja. Usaldusväärsuse kõrge tase tähendab võimet pidada vastu tundmatutele turvanõrkustele ja keerukatele rünnakutele, mis pannakse toime tipptasemel tehnikaga ja märkimisväärsete vahenditega, nagu näiteks rahastatud multidistsiplinaarsed meeskonnad.

Muudatusettepanek 54

Ettepanek võtta vastu määrus
Põhjendus 56 c (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(56c) Riiklikest küberturvalisuse kavadest tuleneva siseturu killustatuse vältimiseks, tulevaste õigusaktide toetamiseks ning usaldusväärsuse ja turvalisuse suurendamiseks peaks komisjonil olema õigus võtta kooskõlas Euroopa Liidu toimimise lepingu artikliga 290 vastu delegeeritud õigusakte, milles sätestatakse prioriteedid seoses Euroopa küberturvalisuse sertifitseerimise, jooksva tööprogrammi vastuvõtmise ja Euroopa sertifitseerimiskavade vastuvõtmisega. On eriti oluline, et komisjon korraldaks oma ettevalmistava töö käigus asjakohaseid konsultatsioone, sealhulgas ekspertide tasandil, ja et kõnealused konsultatsioonid viidaks läbi kooskõlas 13. aprilli 2016. aasta

	institutsioonidevahelises parema õigusloome kokkuleppes sätestatud põhimõtetega. Eelkõige selleks, et tagada delegeeritud õigusaktide ettevalmistamises võrdne osalemine, saavad Euroopa Parlament ja nõukogu kõik dokumendid liikmesriikide ekspertidega samal ajal ning nende ekspertidel on pidev juurdepääs komisjoni eksperdirühmade koosolekutele, kus arutatakse delegeeritud õigusaktide ettevalmistamist.

Muudatusettepanek 55

Ettepanek võtta vastu määrus
Põhjendus 56 d (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(56d) Lisaks muudele kõikide Euroopa küberturvalisuse sertifitseerimise kavadega seotud hindamismeetoditele ja -menetlustele tuleks liidu tasandil edendada ka eetilist häkkimist, mille eesmärk on välja selgitada seadmete ja infosüsteemide nõrgad ja haavatavad kohad, ennetades kuritahtlike kavatsustega häkkerite tegevust ja oskusi.

Muudatusettepanek 56

Ettepanek võtta vastu määrus
Põhjendus 57

Komisjoni ettepanek	*Muudatusettepanek*
(57) Euroopa küberturvalisuse sertifitseerimise kasutamine peaks jääma vabatahtlikuks, kui liidu või siseriiklikes õigusaktides pole sätestatud teisiti. Käesoleva määruse eesmärkide saavutamiseks ja siseturu killustumise vältimiseks tuleks siiski lõpetada riiklike küberturvalisuse sertifitseerimise kavade või menetluste kohaldamine Euroopa küberturvalisuse sertifitseerimise kavaga hõlmatud IKT toodete ja teenuste suhtes	(57) Euroopa küberturvalisuse sertifitseerimise kasutamine peaks jääma vabatahtlikuks, kui liidu või siseriiklikes õigusaktides pole sätestatud teisiti. Käesoleva määruse eesmärkide saavutamiseks ja siseturu killustumise vältimiseks tuleks siiski lõpetada riiklike küberturvalisuse sertifitseerimise kavade või menetluste kohaldamine Euroopa küberturvalisuse sertifitseerimise kavaga hõlmatud IKT toodete***, protsesside*** ja

alates kuupäevast, mille komisjon on rakendusaktiga kehtestanud. Lisaks ei peaks liikmesriigid kehtestama uusi riiklikke küberturvalisuse sertifitseerimise kavasid IKT toodetele ja teenustele, mis on juba kaetud kehtiva Euroopa küberturvalisuse sertifitseerimise kavaga.	teenuste suhtes alates kuupäevast, mille komisjon on ***delegeeritud õigusaktiga*** kehtestanud. Lisaks ei peaks liikmesriigid kehtestama uusi riiklikke küberturvalisuse sertifitseerimise kavasid IKT toodetele ja teenustele, mis on juba kaetud kehtiva Euroopa küberturvalisuse sertifitseerimise kavaga. ***Käesolev määrus ei tohiks siiski piirata riiklike kavade kohaldamist, mida liikmesriigid haldavad suveräänsete siseriiklike vajaduste rahuldamiseks kasutatavate IKT toodete, protsesside ja teenuste puhul.***

Muudatusettepanek 57

Ettepanek võtta vastu määrus
Põhjendus 57 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(57a) Selleks et anda tarbijale rohkem teavet ja võimaldada tarbijal teha läbimõeldud valik, kehtestatakse kohustus väljastada tootedeklaratsioon, mis sisaldab struktureeritud teavet toote, protsessi või teenuse sertifitseerimise kohta.

Muudatusettepanek 58

Ettepanek võtta vastu määrus
Põhjendus 57 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(57b) Uute Euroopa küberturvalisuse kavade ettepaneku tegemisel peaksid ENISA ja teised asjaomased asutused pöörama asjakohast tähelepanu ettepaneku konkurentsi mõjutavale dünaamikale, tagades eelkõige, et kui asjakohases sektoris tegutseb palju väikesi ja keskmise suurusega ettevõtjaid (nt tarkvara arendamisel), ei takista sertifitseerimiskavad uute ettevõtjate sektorisse sisenemist ja innovatsiooni.

Muudatusettepanek 59

Ettepanek võtta vastu määrus
Põhjendus 57 c (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(57c) Euroopa küberturvalisuse kavad aitavad ühtlustada ja ühendada küberturvalisuse tavasid ELis. Neist ei tohi aga saada küberturvalisuse miinimumtase. Euroopa küberturvalisuse kavade koostamisel tuleks samuti arvesse võtta ja võimaldada innovaatilist arengut küberturvalisuse valdkonnas.

Muudatusettepanek 60

Ettepanek võtta vastu määrus
Põhjendus 58

Komisjoni ettepanek	*Muudatusettepanek*
(58) Kui Euroopa küberturvalisuse sertifitseerimise kava on vastu võetud, peaksid IKT toodete tootjad või IKT teenuste osutajad saama esitada enda valitud vastavushindamisasutusele taotluse oma toodete või teenuste sertifitseerimiseks. Kui vastavushindamisasutused vastavad käesolevas määruses sätestatud teatavatele konkreetsetele nõuetele, peaks akrediteerimisasutus need akrediteerima. Akrediteeringu saab anda maksimaalselt viieks aastaks ja selle kehtivust võib pikendada samadel tingimustel senikaua, kuni vastavushindamisasutus vastab nõuetele. Akrediteerimisasutus peaks vastavushindamisasutuse akrediteerimise tühistama, kui akrediteerimise tingimused ei ole täidetud või ei ole enam täidetud või asutuse poolt võetavad meetmed rikuvad käesolevat määrust.	(58) Kui Euroopa küberturvalisuse sertifitseerimise kava on vastu võetud, peaksid IKT toodete tootjad või IKT ***protsesside või*** teenuste osutajad saama esitada ***kõikjal liidus*** enda valitud vastavushindamisasutusele taotluse oma toodete või teenuste sertifitseerimiseks. Kui vastavushindamisasutused vastavad käesolevas määruses sätestatud teatavatele konkreetsetele nõuetele, peaks akrediteerimisasutus need akrediteerima. Akrediteeringu saab anda maksimaalselt viieks aastaks ja selle kehtivust võib pikendada samadel tingimustel senikaua, kuni vastavushindamisasutus vastab nõuetele. Akrediteerimisasutus peaks vastavushindamisasutuse akrediteerimise tühistama, kui akrediteerimise tingimused ei ole täidetud või ei ole enam täidetud või asutuse poolt võetavad meetmed rikuvad käesolevat määrust. ***Et vältida õiguslikku arbitraaži, peaks amet tegema auditeid, tagamaks et vastavushindamisasutuste kvaliteedi ja hoolsuse tase on võrdväärne.***

	Tulemustest tuleks teatada ametile, komisjonile ja Euroopa Parlamendile ning need tuleks teha üldsusele kättesaadavaks.

Muudatusettepanek 61

Ettepanek võtta vastu määrus
Põhjendus 58 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(58a) Euroopa küberturvalisuse sertifitseerimise kohustuslik kasutamine peaks olema piiratud juhtudega, mille puhul riskianalüüs põhjendab kulusid tööstuse, kodanike ja tarbijate jaoks. Oluliste teenuste pakkumist katkestavad intsidendid võivad takistada majandustegevust, põhjustada olulist finantskahju, vähendada kasutajate usaldust ja tekitada liidu majandusele suurt kahju. Oluliste teenuste osutajate poolt Euroopa küberturvalisuse sertifitseerimise kohustuslik kasutamine peaks piirduma nende elementidega, mis on toimimise jaoks otsustavalt tähtsad, ning seda ei peaks kohaldama üldotstarbeliste tootete, protsesside ja teenuste suhtes, kuna see tekitaks tööstusele ja tarbijatele põhjendamatut kulu. Komisjon peaks tegema koostööd direktiivi (EL) 2016/1148 artikli 11 alusel loodud koostöörühmaga, et koostada loetelu selliste toodete, protsesside ja teenuste kategooriatest, mis on spetsiaalselt ette nähtud oluliste teenuste osutajate poolt kasutamiseks ning mille mittetoimimine intsidentide puhul võib oluliselt häirida olulise teenuse osutamist. Loetelu tuleks koostada järk-järgult ja seda tuleks vajaduse korral ajakohastada. Ainult sellesse loetellu kantud tooted, protsessid ja teenused peaksid olema oluliste teenuste osutajatele kohustuslikud.

Muudatusettepanek 62

Ettepanek võtta vastu määrus
Põhjendus 58 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(58b) Liikmesriikide õigusaktides olevad ristviited, mis osutavad riiklikule standardile, mis Euroopa sertifitseerimiskava jõustumise tõttu enam õigusmõju ei avalda, võivad tootjate ja lõppkasutajate jaoks segadust põhjustada. Liikmesriigid peaksid aluslepingutest tulenevate kohustuste kohaselt kohandama siseriiklikke õigusakte Euroopa sertifitseerimiskava vastuvõtmise kajastamiseks, et tootjad ei jätkaks selliste tehniliste kirjelduste rakendamist, mis vastavad kehtivuse kaotanud riiklikele sertifikaatidele.

Muudatusettepanek 63

Ettepanek võtta vastu määrus
Põhjendus 59

Komisjoni ettepanek	*Muudatusettepanek*
(59) Liikmesriike tuleb kohustada määrama ühe küberturvalisuse sertifitseerimise järelevalveasutuse, kes jälgiks nende territooriumil asutatud vastavushindamisasutuste ja nende väljastatud sertifikaatide vastavust käesoleva määruse ja vastavate küberturvalisuse sertifitseerimise kavade nõuetele. Riiklikud sertifitseerimise järelevalveasutused peavad käsitlema füüsiliste või juriidiliste isikute esitatud kaebusi seoses nende riigi territooriumil asutatud vastavushindamisasutuste väljastatud sertifikaatidega, uurima asjakohasel määral kaebuse sisu ja teavitama kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest. Lisaks peavad nad tegema koostööd teiste riiklike sertifitseerimise järelevalveasutuste või muude avaliku sektori asutustega,	(59) Liikmesriike tuleb kohustada määrama ühe küberturvalisuse sertifitseerimise järelevalveasutuse, kes jälgiks nende territooriumil asutatud vastavushindamisasutuste ja nende väljastatud sertifikaatide vastavust käesoleva määruse ja vastavate küberturvalisuse sertifitseerimise kavade nõuetele***, ning tagama, et Euroopa küberturvalisuse sertifikaate tunnustatakse nende territooriumil***. Riiklikud sertifitseerimise järelevalveasutused peavad käsitlema füüsiliste või juriidiliste isikute esitatud kaebusi seoses nende riigi territooriumil asutatud vastavushindamisasutuste väljastatud sertifikaatidega ***või seoses nende riigi territooriumil sertifikaatide väidetava mittetunnustamisega***, uurima asjakohasel määral kaebuse sisu ja

sealhulgas jagades teavet IKT toodete ja teenuste võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete küberturvalisuse sertifitseerimise kavade nõuetele.	teavitama kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest. Lisaks peavad nad tegema koostööd teiste riiklike sertifitseerimise järelevalveasutuste või muude avaliku sektori asutustega, sealhulgas jagades teavet IKT toodete***, protsesside*** ja teenuste võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete küberturvalisuse sertifitseerimise kavade nõuetele ***või Euroopa küberturvalisuse sertifikaatide mittetunnustamise kohta. Peale selle peavad nad jälgima ja kontrollima, et vastavusdeklaratsioonid oleksid nõuetekohased ja et vastavushindamisasutused oleksid väljastanud Euroopa küberturvalisuse sertifikaadid vastavalt käesolevas määruses ja muu hulgas Euroopa küberturvalisuse sertifitseerimise rühma vastu võetud eeskirjades ning vastavas Euroopa küberturvalisuse sertifitseerimise kavas sätestatud nõuetele. Riiklike sertifitseerimise järelevalveasutuste vaheline tõhus koostöö on vajalik, et rakendada nõuetekohaselt Euroopa küberturvalisuse sertifitseerimise kavasid ning IKT toodete ja teenuste küberturvalisusega seotud tehnilisi nõudmisi. Komisjon peaks hõlbustama sellist teabevahetust, tehes kättesaadavaks üldise elektroonilise teabe tugisüsteemi, nagu turujärelevalve info- ja teavitussüsteem (ICSMS) ja kiire teabevahetuse süsteem (RAPEX), mida juba kasutavad turujärelevalveasutused vastavalt määrusele (EÜ) nr 765/2008.***

Muudatusettepanek 64

Ettepanek võtta vastu määrus
Põhjendus 60

Komisjoni ettepanek	*Muudatusettepanek*
(60) Et tagada Euroopa küberturvalisuse sertifitseerimise raamistiku järjekindel rakendamine, tuleks luua ***Euroopa***	(60) Et tagada Euroopa küberturvalisuse sertifitseerimise raamistiku järjekindel rakendamine, tuleks luua ***liikmesriikide***

küberturvalisuse sertifitseerimise rühm (edaspidi „rühm“), mis koosneb riiklikest sertifitseerimise järelevalveasutustest. ***Rühma*** peamised ülesanded peaksid olema nõustada ja abistada komisjoni töös, mille eesmärk on tagada Euroopa küberturvalisuse sertifitseerimise raamistiku järjepidev rakendamine ja kohaldamine; aidata ametit ja teha temaga tihedat koostööd ettevalmistavate küberturvalisuse sertifitseerimise kavade koostamisel; soovitada, et komisjon paluks ametil koostada ettevalmistav Euroopa küberturvalisuse sertifitseerimise kava ning võtta vastu komisjonile suunatud arvamusi seoses olemasolevate Euroopa küberturvalisuse sertifitseerimise kavade alalhoidmise ja läbivaatamisega***;***	***sertifitseerimisrühm***, mis koosneb riiklikest sertifitseerimise järelevalveasutustest. ***Liikmesriikide sertifitseerimisrühma*** peamised ülesanded peaksid olema nõustada ja abistada komisjoni töös, mille eesmärk on tagada Euroopa küberturvalisuse sertifitseerimise raamistiku järjepidev rakendamine ja kohaldamine; aidata ametit ja teha temaga tihedat koostööd ettevalmistavate küberturvalisuse sertifitseerimise kavade koostamisel; soovitada, et komisjon paluks ametil koostada ettevalmistav Euroopa küberturvalisuse sertifitseerimise kava ning võtta vastu komisjonile suunatud arvamusi seoses olemasolevate Euroopa küberturvalisuse sertifitseerimise kavade alalhoidmise ja läbivaatamisega***.***

Muudatusettepanek 65

Ettepanek võtta vastu määrus
Põhjendus 60 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(60a) Vastavushindamisasutuste pädevustasemete võrdväärsuse tagamiseks, vastastikuse tunnustamise lihtsustamiseks ning vastavushindamisasutuste väljastatud sertifikaatide ja vastavushindamise tulemuste üldise aktsepteerimise soodustamiseks on vaja, et riiklike sertifitseerimise järelevalveasutuste vahel toimiks range ja läbipaistev vastastikuse hindamise süsteem ja nad läbiksid sellise hindamise regulaarselt.

Muudatusettepanek 66

Ettepanek võtta vastu määrus
Põhjendus 60 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(60b) Riiklike sertifitseerimise

	järelevalveasutuste vaheline tulemuslik koostöö on vastastikuse hindamise nõuetekohaseks rakendamiseks ja seoses piiriülese akrediteerimisega ülimalt oluline. Läbipaistvuse huvides on seetõttu vaja kehtestada riiklikele sertifitseerimise järelevalveasutustele kohustus vahetada omavahel teavet ning edastada asjakohane teave riiklikele ametiasutustele ja komisjonile. Samuti tuleks avalikustada ajakohastatud ja täpne teave riiklike akrediteerimisasutuste osutatavate akrediteerimisteenuste kättesaadavuse kohta. Eelkõige tuleks tagada vastavushindamisasutuste juurepääs kõnealusele teabele.

Muudatusettepanek 67

Ettepanek võtta vastu määrus
Põhjendus 61

Komisjoni ettepanek	*Muudatusettepanek*
(61) Et suurendada teadlikkust ja hõlbustada tulevaste Euroopa küberturvalisuse kavade aktsepteerimist, võib Euroopa Komisjon välja anda üldiseid või sektoripõhiseid küberturvalisuse suuniseid, näiteks küberturvalisuse heade tavade või vastutustundliku küberruumis käitumise kohta, tuues välja sertifitseeritud IKT toodete ja teenuste kasutamise positiivse mõju.	(61) Et suurendada teadlikkust ja hõlbustada tulevaste Euroopa küberturvalisuse kavade aktsepteerimist, võib Euroopa Komisjon välja anda üldiseid või sektoripõhiseid küberturvalisuse suuniseid, näiteks küberturvalisuse heade tavade või vastutustundliku küberruumis käitumise kohta, tuues välja sertifitseeritud IKT toodete***, protsesside*** ja teenuste kasutamise positiivse mõju.

Muudatusettepanek 68

Ettepanek võtta vastu määrus
Põhjendus 63

Komisjoni ettepanek	*Muudatusettepanek*
(63) Et vastavushindamisasutuste akrediteerimise kriteeriume veelgi täpsustada, peaks komisjonil olema õigus võtta kooskõlas Euroopa Liidu toimimise lepingu artikliga 290 vastu delegeeritud	(63) Et vastavushindamisasutuste akrediteerimise kriteeriume veelgi täpsustada, peaks komisjonil olema õigus võtta kooskõlas Euroopa Liidu toimimise lepingu artikliga 290 vastu delegeeritud

õigusakte. Komisjon peaks oma ettevalmistustöö jooksul pidama asjakohaseid konsultatsioone, sh ekspertide tasandil. Need konsultatsioonid tuleb läbi viia kooskõlas 13. aprilli 2016. aasta ***institutsioonidevahelise*** parema õigusloome kokkuleppes sätestatud põhimõtetega. Eelkõige selleks, et tagada võrdne osalemine delegeeritud õigusaktide ettevalmistamises, peaksid Euroopa Parlament ja nõukogu saama kõik dokumendid liikmesriikide ekspertidega samal ajal ning nende ekspertidel peaks olema pidev juurdepääs komisjoni eksperdirühmade koosolekutele, millel arutatakse delegeeritud õigusaktide ettevalmistamist.	õigusakte. Komisjon peaks oma ettevalmistustöö jooksul pidama asjakohaseid konsultatsioone, sh ekspertide tasandil ***ja vajaduse korral asjaomaste sidusrühmadega***. Need konsultatsioonid tuleb läbi viia kooskõlas 13. aprilli 2016. aasta ***institutsioonidevahelises*** parema õigusloome kokkuleppes sätestatud põhimõtetega. Eelkõige selleks, et tagada võrdne osalemine delegeeritud õigusaktide ettevalmistamises, peaksid Euroopa Parlament ja nõukogu saama kõik dokumendid liikmesriikide ekspertidega samal ajal ning nende ekspertidel peaks olema pidev juurdepääs komisjoni eksperdirühmade koosolekutele, millel arutatakse delegeeritud õigusaktide ettevalmistamist.

Muudatusettepanek 69

Ettepanek võtta vastu määrus
Põhjendus 65

Komisjoni ettepanek	*Muudatusettepanek*
(65) ***Kontrollimenetlust tuleks kasutada selliste rakendusaktide vastuvõtmiseks***, milles käsitletakse IKT toodete ja teenuste suhtes kohaldatavaid Euroopa küberturvalisuse sertifitseerimise kavasid; ameti korraldatavate uurimiste üksikasju ning asjaolusid, vorminguid ja korda, mille kohaselt riiklikud sertifitseerimise järelevalveasutused teavitavad komisjoni akrediteeritud vastavushindamisasutustest.	(65) ***Lisaks võib vastu võtta delegeeritud õigusakte***, milles käsitletakse IKT toodete***, protsesside*** ja teenuste suhtes kohaldatavaid Euroopa küberturvalisuse sertifitseerimise kavasid; ameti korraldatavate uurimiste üksikasju ning asjaolusid, vorminguid ja korda, mille kohaselt riiklikud sertifitseerimise järelevalveasutused teavitavad komisjoni akrediteeritud vastavushindamisasutustest.

Muudatusettepanek 70

Ettepanek võtta vastu määrus
Põhjendus 66

Komisjoni ettepanek	*Muudatusettepanek*
(66) Ameti tööd tuleks ***hinna*** sõltumatult. Hindamisel tuleks pidada silmas ameti eesmärkide saavutamist, selle töövõtteid	(66) Ameti tööd tuleks ***hinnata pidevalt ja*** sõltumatult. Hindamisel tuleks pidada silmas ameti eesmärkide saavutamist, selle

ning ülesannete asjakohasust**.** Selle ***hindamise käigus tuleks vaadelda ka Euroopa küberturvalisuse sertifitseerimise raamistiku mõju***, ***tulemuslikkust*** ja ***tõhusust***.	töövõtteid ning ülesannete asjakohasust***,*** ***eelkõige*** selle ***koordineerivat rolli liikmesriikide ja nende riiklike ametiasutuste suhtes. Läbivaatamise korral peaks komisjon hindama võimalust***, ***et amet tegutseks liikmesriikide ning liidu institutsioonide*** ja ***organite ühtse kontaktpunktina***.

Muudatusettepanek 71

Ettepanek võtta vastu määrus
Põhjendus 66 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(66a) Selle hindamise käigus tuleks vaadelda ka Euroopa küberturvalisuse sertifitseerimise raamistiku mõju, tulemuslikkust ja tõhusust. Läbivaatamise korral võiks komisjon hinnata ameti rolli seoses liidu turule sisenevate kolmandatest riikidest pärit toodete ja teenuste hindamisega ja nende ettevõtete võimaliku musta nimekirja lisamisega, kes ei täida liidu eeskirju.

Muudatusettepanek 72

Ettepanek võtta vastu määrus
Põhjendus 66 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(66b) Selle hindamise käigus tuleks analüüsida liidus müüdavate toodete ja teenuste küberturvalisuse taset. Läbivaatamise korral peaks komisjon hindama, kas lisada küberturvalisuse olulised nõuded siseturule juurdepääsu tingimuste hulka.

Muudatusettepanek 73

Ettepanek võtta vastu määrus
Artikkel 1 – lõik 1 – punkt a

Komisjoni ettepanek	*Muudatusettepanek*
(a) sätestatakse ***ENISA ehk nn ELi küberturvalisuse ameti*** (edaspidi „amet“) eesmärgid, ülesanded ja organisatsioonilised aspektid ning	a) sätestatakse ***Euroopa Liidu Võrgu- ja Infoturbeameti*** (edaspidi „amet“) eesmärgid, ülesanded ja organisatsioonilised aspektid ning

Muudatusettepanek 74

Ettepanek võtta vastu määrus
Artikkel 1 – lõik 1 – punkt b

Komisjoni ettepanek	*Muudatusettepanek*
(b) sätestatakse Euroopa küberturvalisuse sertifitseerimise kavade kehtestamise raamistik, ***et*** kindlustada liidus IKT toodete ja teenuste küberturvalisuse piisav tase***. Sellise raamistiku*** kohaldamine ei piira konkreetseid sätteid, mis puudutavad muudes liidu õigusaktides ***kirjeldatud*** vabatahtlikku ***või*** kohustuslikku sertifitseerimist.	b) sätestatakse Euroopa küberturvalisuse sertifitseerimise kavade kehtestamise raamistik, ***mille eesmärk on vältida sertifitseerimiskavade killustatust liidus ning*** kindlustada liidus IKT toodete***, protsesside*** ja teenuste küberturvalisuse piisav tase ***ning mille*** kohaldamine ei piira konkreetseid sätteid, mis puudutavad ***käesolevas määruses või*** muudes liidu õigusaktides ***ette nähtud*** vabatahtlikku ***ja asjakohasel juhul*** kohustuslikku sertifitseerimist.

Muudatusettepanek 75

Ettepanek võtta vastu määrus
Artikkel 1 – lõik 1 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Amet täidab oma ülesandeid ilma, et see piiraks liikmesriikide pädevusi seoses küberturvalisusega ning eelkõige liikmesriikide pädevusi avaliku julgeoleku, riigikaitse, riigi julgeoleku ja kriminaalõiguse valdkonnas.

Muudatusettepanek 76

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 1

Komisjoni ettepanek	*Muudatusettepanek*
(1) „küberturvalisus“ – ***hõlmab kõiki tegevusi***, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja mõjutatud isikuid küberohtude eest;	1) „küberturvalisus“ – ***kõik tegevused***, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja mõjutatud isikuid küberohtude eest;

Muudatusettepanek 77

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 2

Komisjoni ettepanek	*Muudatusettepanek*
(2) „võrgu- ja infosüsteem“ – direktiivi (EL) 2016/1148 artikli 4 punktis 1 määratletud ***süsteem***;	2) „võrgu- ja infosüsteem“ – direktiivi (EL) 2016/1148 artikli 4 punktis 1 määratletud ***võrgu- ja infosüsteem***;

Muudatusettepanek 78

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 3

Komisjoni ettepanek	*Muudatusettepanek*
(3) „riiklik võrgu- ja infosüsteemide turvalisuse strateegia“ – direktiivi (EL) 2016/1148 artikli 4 punktis 3 määratletud ***raamistik***;	3) „riiklik võrgu- ja infosüsteemide turvalisuse strateegia“ – direktiivi (EL) 2016/1148 artikli 4 punktis 3 määratletud ***riiklik võrgu- ja infosüsteemide turvalisuse strateegia***;

Muudatusettepanek 79

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 4

Komisjoni ettepanek	*Muudatusettepanek*
(4) „oluliste teenuste operaator“ – direktiivi (EL) 2016/1148 artikli 4 punktis 4 määratletud ***avaliku või***	4) „oluliste teenuste operaator“ – direktiivi (EL) 2016/1148 artikli 4 punktis 4 määratletud ***oluliste teenuste***

erasektori üksus;

operaator;

Muudatusettepanek 80

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 5

Komisjoni ettepanek	*Muudatusettepanek*
(5) „digitaalse teenuse osutaja“ – direktiivi (EL) 2016/1148 artikli 4 punktis 6 määratletud ***juriidiline isik, kes pakub digitaalset teenust***;	5) „digitaalse teenuse osutaja“ – direktiivi (EL) 2016/1148 artikli 4 punktis 6 määratletud ***digitaalse teenuse osutaja***;

Muudatusettepanek 81

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 6

Komisjoni ettepanek	*Muudatusettepanek*
(6) „intsident“ – direktiivi (EL) 2016/1148 artikli 4 punktis 7 määratletud ***sündmus***;	6) „intsident“ – direktiivi (EL) 2016/1148 artikli 4 punktis 7 määratletud ***intsident***;

Muudatusettepanek 82

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 7

Komisjoni ettepanek	*Muudatusettepanek*
(7) „intsidendi käsitlemine“ – direktiivi (EL) 2016/1148 artikli 4 punktis 8 määratletud ***protseduur***;	7) „intsidendi käsitlemine“ – direktiivi (EL) 2016/1148 artikli 4 punktis 8 määratletud ***intsidendi käsitlemine***;

Muudatusettepanek 83

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 8

Komisjoni ettepanek	*Muudatusettepanek*
(8) „küberoht“ – mistahes võimalik asjaolu või ***sündmus***, mis võib kahjustada	8) „küberoht“ – mistahes võimalik asjaolu***, sündmus*** või ***tahtlik tegevus, sh***

võrgu- ja infosüsteeme, nende kasutajaid ja mõjutatud isikuid**.**	***automaatne käsk***, mis võib kahjustada ***või häirida*** võrgu- ja infosüsteeme, nende kasutajaid ja mõjutatud isikuid ***või neile muul viisil kahjulikku mõju avaldada;***

Muudatusettepanek 84

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 8 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	8a) „küberhügieen“ – lihtsad rutiinsed meetmed, mis minimeerivad kasutajate ja ettevõtjate riske küberohtudega kokkupuutumiseks, kui nad neid veebis korrapäraselt rakendavad ja ellu viivad;

Muudatusettepanek 85

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 9

Komisjoni ettepanek	*Muudatusettepanek*
(9) „Euroopa küberturvalisuse sertifitseerimise kava“ – ELi tasandil määratletud normide, tehniliste nõuete, standardite ja menetluste põhjalik kogum, mida kasutatakse selle konkreetse kava kohaldamisalasse kuuluvate info- ja kommunikatsioonitehnoloogia (IKT) toodete ja teenuste sertifitseerimiseks;	9) „Euroopa küberturvalisuse sertifitseerimise kava“ – ELi tasandil ***ning vastavalt rahvusvahelistele ja Euroopa standarditele ja IKT tehnilistele kirjeldustele, mille amet on kindlaks määranud,*** määratletud normide, tehniliste nõuete, standardite ja menetluste põhjalik kogum, mida kasutatakse selle konkreetse kava kohaldamisalasse kuuluvate info- ja kommunikatsioonitehnoloogia (IKT) toodete***, protsesside*** ja teenuste sertifitseerimiseks;

Muudatusettepanek 86

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 10

Komisjoni ettepanek	*Muudatusettepanek*
(10) „Euroopa küberturvalisuse	10) „Euroopa küberturvalisuse

sertifikaat“ – dokument, mille annab välja vastavushindamisasutus ja mis tõendab, et asjaomane IKT toode või ***teenus*** vastab Euroopa küberturvalisuse sertifitseerimise kavas sätestatud konkreetsetele nõuetele;	sertifikaat“ – dokument, mille annab välja vastavushindamisasutus ja mis tõendab, et asjaomane IKT toode***, teenus*** või ***protsess*** vastab Euroopa küberturvalisuse sertifitseerimise kavas sätestatud konkreetsetele nõuetele;

Muudatusettepanek 87

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 11 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	11a) „IKT protsess“ – tegevused, mille käigus IKT toodet või teenust kavandatakse, töötatakse välja, hallatakse ja tarnitakse;

Muudatusettepanek 88

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 11 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	11b) „tarbeelektroonikaseade“ – seadmed, mis koosnevad riist- ja tarkvarast, mis töötlevad isikuandmeid või on koduautomaatika ja kodujuhtimisseadmete, kontoriseadmete, marsruutimisseadmete ja võrku ühendatavate seadmete (nt nutiteler, mänguasjad ja mängukonsoolid, virtuaalsed või personaalsed assistendid, võrku ühendatavad voogedastusseadmed, kantavad seadmed, häälkäsklus- ja virtuaalreaalsussüsteemid) käitamiseks internetiga ühendatavad;

Muudatusettepanek 89

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 16

Komisjoni ettepanek	*Muudatusettepanek*
(16) ***„standard“*** – määruse (EL) nr 1025/2012 artikli 2 ***punktis*** 1 määratletud standard***.***	16) ***„standard, tehniline kirjeldus ja IKT tehniline kirjeldus“*** – määruse (EL) nr 1025/2012 artikli 2 ***punktides*** 1***, 4 ja 5*** määratletud standard***, tehniline kirjeldus ja IKT tehniline kirjeldus;***

Muudatusettepanek 90

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 16 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	16a) „riiklik sertifitseerimise järelevalveasutus“ – organ, mille iga liikmesriik on määranud vastavalt käesoleva määruse artiklile 50;

Muudatusettepanek 91

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 16 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	16b) „enesehindamine“ – tootja deklaratsioon, millega ta kinnitab, et sertifitseerimiskavas sätestatud konkreetsed nõuded seoses toodete, protsesside ja teenustega on täidetud;

Muudatusettepanek 92

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 16 c (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	16c) „vaiketurvalisus“ – olukord, mille puhul esimesele kasutajale tuleks

	seadistada võimalikult turvaline vaikekonfiguratsioon, kui toodet, tarkvara või protsessi saab seadistada nii, et sellega on tagatud kõrgem turvalisuse tase. Kui juhtumipõhise riski- ja kasutatavusanalüüsi tulemusel jõutakse järeldusele, et selline seadistus ei ole teostatav, tuleks kasutajaid suunata valima kõige turvalisem seadistus;

Muudatusettepanek 93

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 16 d (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	16d) „oluliste teenuste operaatorid“ – direktiivi (EL) 2016/1148 artikli 4 punktis 4 määratletud oluliste teenuste operaatorid.

Muudatusettepanek 94

Ettepanek võtta vastu määrus
Artikkel 3 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Amet hakkab tegelema ülesannetega, mis talle käesoleva määrusega pannakse, et panustada ***kõrgetasemelisse küberturvalisusse*** liidus.	1. Amet hakkab tegelema ülesannetega, mis talle käesoleva määrusega pannakse, ***ja ametit tugevdatakse,*** et panustada ***küberturvalisuse ühtlaselt kõrge taseme saavutamisse küberrünnete ärahoidmiseks*** liidus***, vähendada siseturu killustatust ja parandada selle toimimist ning tagada järjepidevus, võttes arvesse liikmesriikide koostöö tulemusi võrgu- ja infoturbe direktiivi raames***.

Muudatusettepanek 95

Ettepanek võtta vastu määrus
Artikkel 4 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Ametist saab küberturvalisuse alaste teadmiste keskus tänu oma sõltumatusele, antava nõu ja abi ning levitatava teabe teaduslikule ja tehnilisele kvaliteedile, töökorra ja töömeetodite läbipaistvusele ning oma ülesannete hoolikale täitmisele.	1. Ametist saab küberturvalisuse alaste ***teoreetiliste ja praktiliste*** teadmiste keskus tänu oma sõltumatusele, antava nõu ja abi ning levitatava teabe teaduslikule ja tehnilisele kvaliteedile, töökorra ja töömeetodite läbipaistvusele ning oma ülesannete hoolikale täitmisele.

Muudatusettepanek 96

Ettepanek võtta vastu määrus
Artikkel 4 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Amet aitab liidu institutsioonidel, ametitel ja asutustel ning liikmesriikidel töötada välja küberturvalisuse valdkonna põhimõtted ja neid rakendada.	2. Amet aitab liidu institutsioonidel, ametitel ja asutustel ning liikmesriikidel töötada välja küberturvalisuse valdkonna põhimõtted ja neid rakendada ***ning suurendada kodanike ja ettevõtjate teadlikkust***.

Muudatusettepanek 97

Ettepanek võtta vastu määrus
Artikkel 4 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. Amet toetab suutlikkuse ja valmisoleku arendamist ***kogu liidus*** sellega, et aitab liidul, liikmesriikidel ning avaliku ja erasektori sidusrühmadel suurendada võrgu- ja infosüsteemide kaitset, arendada küberturvalisuse valdkonna oskusi ja pädevusi ning saavutada kübervastupidavusvõime.	3. Amet toetab suutlikkuse ja valmisoleku arendamist ***liidu institutsioonides, ametites ja asutustes*** sellega, et aitab liidul, liikmesriikidel ning avaliku ja erasektori sidusrühmadel suurendada võrgu- ja infosüsteemide kaitset, ***arendada ja parandada kübervastupidavusvõimet ja reageerimissuutlikkust, suurendada teadlikkust ning*** arendada küberturvalisuse valdkonna oskusi ja pädevusi ning

saavutada kübervastupidavusvõime.

Muudatusettepanek 98

Ettepanek võtta vastu määrus
Artikkel 4 – lõige 4

Komisjoni ettepanek	*Muudatusettepanek*
4. Amet edendab liidu tasandil küberturvalisusega seotud küsimuste alast koostööd ja ***koordineerimist*** liikmesriikide, liidu institutsioonide, ametite ja asutuste ning asjaomaste sidusrühmade seas***, kaasa arvatud erasektoris***.	4. Amet edendab liidu tasandil küberturvalisusega seotud küsimuste alast koostööd***, koordineerimist*** ja ***teabe jagamist*** liikmesriikide, liidu institutsioonide, ametite ja asutuste ning asjaomaste sidusrühmade seas.

Muudatusettepanek 99

Ettepanek võtta vastu määrus
Artikkel 4 – lõige 5

Komisjoni ettepanek	*Muudatusettepanek*
5. Amet ***suurendab*** liidu tasandil küberturvalisuse alast suutlikkust, et täiendada liikmesriikide tegevust küberohtude ennetamisel ja neile reageerimisel, seda eeskätt piiriüleste intsidentide puhul.	5. Amet ***aitab suurendada*** liidu tasandil küberturvalisuse alast suutlikkust, et täiendada liikmesriikide tegevust küberohtude ennetamisel ja neile reageerimisel, seda eeskätt piiriüleste intsidentide puhul***, ning et täita oma ülesannet aidata liidu institutsioonidel töötada välja küberturvalisusega seotud poliitikameetmeid***.

Muudatusettepanek 100

Ettepanek võtta vastu määrus
Artikkel 4 – lõige 6

Komisjoni ettepanek	*Muudatusettepanek*
6. Amet propageerib sertifitseerimist muu hulgas sellega, et aitab kaasa küberturvalisuse sertifitseerimise raamistiku loomisele ja haldamisele liidu tasandil vastavalt käesoleva määruse III jaotisele, et suurendada IKT toodete ja	6. Amet propageerib sertifitseerimist ***eesmärgiga vältida siseturu killustatust ja parandada selle toimimist*** muu hulgas sellega, et aitab kaasa küberturvalisuse sertifitseerimise raamistiku loomisele ja haldamisele liidu tasandil vastavalt

teenuste küberturvalisuse alase usaldusväärsuse läbipaistvust ning tugevdada seeläbi usaldust digitaalse siseturu vastu.	käesoleva määruse III jaotisele, et suurendada IKT toodete***, teenuste*** ja ***protsesside*** küberturvalisuse alase usaldusväärsuse läbipaistvust ning tugevdada seeläbi usaldust digitaalse siseturu vastu ***ja et suurendada olemasolevate riiklike ja rahvusvaheliste sertifitseerimiskavade omavahelist kooskõla***.

Muudatusettepanek 101

Ettepanek võtta vastu määrus
Artikkel 4 – lõige 7

Komisjoni ettepanek	*Muudatusettepanek*
7. Amet edendab kodanike ja ettevõtjate heal tasemel teadlikkust küberturvalisusega seotud ***küsimustest***.	7. Amet edendab ***ja toetab projekte, mis soodustavad*** kodanike ja ettevõtjate heal tasemel teadlikkust***, küberhügieeni ja küberkirjaoskust*** küberturvalisusega seotud ***küsimuste valdkonnas***.

Muudatusettepanek 102

Ettepanek võtta vastu määrus
Artikkel 5 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Abistab ja annab nõu, eeskätt jagab oma sõltumatut arvamust ja teeb ettevalmistusi liidu põhimõtete ja õiguse arendamise ja läbivaatamise jaoks küberturvalisuse valdkonnas, aga ka valdkonnaspetsiifiliste poliitiliste ja õiguslike algatuste jaoks, kui need puudutavad küberturvalisusega seotud küsimusi.	1. Abistab ja annab nõu, eeskätt jagab oma sõltumatut arvamust ***ning esitab küberruumis toimuva asjaomase tegevuse analüüsi*** ja teeb ettevalmistusi liidu põhimõtete ja õiguse arendamise ja läbivaatamise jaoks küberturvalisuse valdkonnas, aga ka valdkonnaspetsiifiliste poliitiliste ja õiguslike algatuste jaoks, kui need puudutavad küberturvalisusega seotud küsimusi.

Muudatusettepanek 103

Ettepanek võtta vastu määrus
Artikkel 5 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Aitab liikmesriikidel järjekindlalt rakendada küberturvalisusega seotud liidu põhimõtteid ja õigusakte eeskätt seoses direktiiviga (EL) 2016/1148, kasutades selleks muu hulgas arvamusi, juhiseid, nõuandeid ja parimaid tavasid sellistes küsimustes nagu riskihaldus, intsidentidest teatamine ja teabe jagamine ning aidates kaasa selle valdkonna parimate tavade jagamisele pädevate asutuste vahel.	2. Aitab liikmesriikidel järjekindlalt rakendada küberturvalisusega seotud liidu põhimõtteid ja õigusakte eeskätt seoses direktiiviga (EL) 2016/1148, ***direktiiviga ... (millega kehtestatakse Euroopa elektroonilise side seadustik), määrusega (EL) 2016/679 ja direktiiviga 2002/58/EÜ,*** kasutades selleks muu hulgas arvamusi, juhiseid, nõuandeid ja parimaid tavasid sellistes küsimustes nagu ***turvaline tarkvara ja süsteemide arendamine,*** riskihaldus, intsidentidest teatamine ja teabe jagamine***, tehnilised ja korralduslikud meetmed, eelkõige nõrkustest teatamise koordineeritud programmide loomine,*** ning aidates kaasa selle valdkonna parimate tavade jagamisele pädevate asutuste vahel.

Muudatusettepanek 104

Ettepanek võtta vastu määrus
Artikkel 5 – lõige 2 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	2a. Töötab välja ja edendab poliitikameetmeid, mis toetaksid avatud interneti avaliku tuuma üldist kättesaadavust või terviklikkust, pakuvad interneti kui terviku põhifunktsionaalsust ja toetavad selle tavapärast toimimist, muu hulgas põhiliste protokollide (eelkõige domeeninimede süsteem, BGP ja IPv6) turvalisust ja stabiilsust, domeeninimede süsteemi (sealhulgas kõigi tippdomeenide) toimimist ning juurserverite toimimist.

Muudatusettepanek 105

Ettepanek võtta vastu määrus
Artikkel 5 – lõige 4 – punkt 2

Komisjoni ettepanek	*Muudatusettepanek*
*(*2) elektroonilise side suurema turvalisuse edendamist, muu hulgas oskusteabe ja nõu pakkumisega ning pädevate asutuste vaheliste parimate tavade jagamise soodustamisega.	2) elektroonilise side***, andmete säilitamise ja andmetöötluse*** suurema turvalisuse edendamist, muu hulgas oskusteabe ja nõu pakkumisega ning pädevate asutuste vaheliste parimate tavade jagamise soodustamisega.

Muudatusettepanek 106

Ettepanek võtta vastu määrus
Artikkel 5 – lõige 5 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	5a. Aitab liikmesriikidel järjekindlalt rakendada andmekaitsega seotud liidu põhimõtteid ja õigusakte, eeskätt määrust (EL) 2016/679, ning aitab Euroopa Andmekaitsenõukogul töötada välja suunised, mis on seotud määruse (EL) 2016/679 rakendamisega küberturvalisuse eesmärgil. Euroopa Andmekaitsenõukogu konsulteerib ametiga iga kord, kui ta avaldab arvamuse või otsuse, milles käsitletakse isikuandmete kaitse üldmääruse rakendamist ja küberturvalisust, muu hulgas eraelu puutumatuse mõjuhinnangute, andmetega seotud rikkumisest teatamise, töötlemise turvalisuse, turvanõuete ja lõimprivaatsusega seotud küsimuste puhul.

Muudatusettepanek 107

Ettepanek võtta vastu määrus
Artikkel 6 – lõige 1 – punkt a a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	aa) liikmesriike ja liidu institutsioone nõrkustest teatamise koordineeritud poliitika ja nõrkustest teatamise riiklike läbivaatamisprotsesside loomisel ja rakendamisel, kusjuures nende tavad ja otsused peaksid olema läbipaistvad ning nende suhtes tuleks kohaldada sõltumatut järelevalvet.

Muudatusettepanek 108

Ettepanek võtta vastu määrus
Artikkel 6 – lõige 1 – punkt a b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ab) Amet aitab kaasa pikaajalise Euroopa IT-turvalisuse projekti väljatöötamisele ja käivitamisele, et veelgi edendada küberturvalisuse alaseid teadusuuringuid liidus ja liikmesriikides koostöös Euroopa Teadusnõukogu (ERC) ja Euroopa Innovatsiooni- ja Tehnoloogiainstituudiga (EIT) ning liidu teadusprogrammide valdkonnas;

Muudatusettepanek 109

Ettepanek võtta vastu määrus
Artikkel 6 – lõige 1 – punkt g

Komisjoni ettepanek	*Muudatusettepanek*
(g) liikmesriike, korraldades igal aastal liidu tasandil artikli 7 lõikes 6 osutatud ulatuslikud küberturvalisuse õppused ja andes õppuste hindamise ja õppuste käigus omandatud kogemuste põhjal poliitilisi soovitusi;	g) liikmesriike, korraldades ***korrapäraselt ja vähemalt*** igal aastal liidu tasandil artikli 7 lõikes 6 osutatud ulatuslikud küberturvalisuse õppused ja andes õppuste hindamise ja õppuste käigus omandatud kogemuste põhjal poliitilisi soovitusi ***ja vahetades parimaid tavasid***;

Muudatusettepanek 110

Ettepanek võtta vastu määrus
Artikkel 6 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Amet soodustab valdkondlike teabe jagamise ja analüüsimise keskuste (ISACide) loomist ja toetab neid pidevalt eeskätt direktiivi (EL) 2016/1148 II lisas loetletud valdkondades, pakkudes parimaid tavasid ja juhiseid kättesaadavate töövahendite ja ***menetluste*** kohta ning selle kohta, kuidas lahendada teabe jagamisega seotud regulatiivsed küsimused.	2. Amet soodustab valdkondlike teabe jagamise ja analüüsimise keskuste (ISACide) loomist ja toetab neid pidevalt eeskätt direktiivi (EL) 2016/1148 II lisas loetletud valdkondades, pakkudes parimaid tavasid ja juhiseid kättesaadavate töövahendite***, menetluste*** ja ***küberhügieeni põhimõtete*** kohta ning selle kohta, kuidas lahendada teabe jagamisega seotud regulatiivsed küsimused.

Muudatusettepanek 111

Ettepanek võtta vastu määrus
Artikkel 7 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Amet toetab operatiivkoostööd ***pädevate avalik-õiguslike*** asutuste seas ja sidusrühmade vahel.	1. Amet toetab operatiivkoostööd ***liikmesriikide, liidu institutsioonide, ametite ja*** asutuste seas ja sidusrühmade vahel ***eesmärgiga jõuda koostööni, analüüsides ja hinnates olemasolevaid riiklikke kavasid, töötades välja kava ja viies selle ellu ning kasutades asjakohaseid vahendeid, et saavutada liidus ja liikmesriikides küberturvalisuse sertifitseerimise kõrgeim tase***.

Muudatusettepanek 112

Ettepanek võtta vastu määrus
Artikkel 7 – lõige 4 – lõik 1 – punkt b

Komisjoni ettepanek	*Muudatusettepanek*
(b) pakub liikmesriikidele nende taotlusel tehnilist abi märkimisväärse või	b) pakub liikmesriikidele nende taotlusel ***teabe jagamise ja eksperditeadmiste vormis*** tehnilist abi

olulise mõjuga intsidentide korral;	märkimisväärse või olulise mõjuga intsidentide korral;

Muudatusettepanek 113

Ettepanek võtta vastu määrus
Artikkel 7 – lõige 4 – lõik 1 – punkt b a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ba) kui olukord nõuab intsidendi märkimisväärse häiriva mõju tõttu kiiret tegutsemist, võib liikmesriik taotleda olukorra hindamisel ameti ekspertide abi. Taotlus sisaldab olukorra kirjeldust, võimalikke eesmärke ja prognoositud vajadusi;

Muudatusettepanek 114

Ettepanek võtta vastu määrus
Artikkel 7 – lõige 5 – lõik 1

Komisjoni ettepanek	*Muudatusettepanek*
Kahe või enama asjaomase liikmesriigi taotluse korral ja üksnes selleks, et anda ***nõu*** edasiste intsidentide vältimiseks, teeb amet tehnilise järeluurimise või pakub selleks vajalikku toetust pärast seda, kui mõjutatud ettevõtjad on teatanud märkimisväärse või olulise mõjuga intsidendist vastavalt direktiivile (EL) 2016/1148. Amet teeb sellise uurimise ka juhul, kui selline intsident on mõjutanud rohkem kui ***kaht*** liikmesriiki ning kui komisjon esitab asjaomaste liikmesriikide nõusolekul põhjendatud taotluse.	***Ühe*** või enama asjaomase liikmesriigi taotluse korral ja üksnes selleks, et anda ***abi kas nõuannete vormis*** edasiste intsidentide vältimiseks ***või käimasolevatele suuremahulistele intsidentidele reageerimisel abistamise vormis***, teeb amet tehnilise järeluurimise või pakub selleks vajalikku toetust pärast seda, kui mõjutatud ettevõtjad on teatanud märkimisväärse või olulise mõjuga intsidendist vastavalt direktiivile (EL) 2016/1148. Amet ***täidab eespool nimetatud ülesandeid, saades mõjutatud liikmesriikidest asjakohast teavet ning kasutades ohuanalüüside tegemiseks oma ressursse ja samuti intsidentidele reageerimise ressursse. Amet*** teeb sellise uurimise ka juhul, kui selline intsident on mõjutanud rohkem kui ***üht*** liikmesriiki ning kui komisjon esitab asjaomaste liikmesriikide nõusolekul põhjendatud taotluse. ***Seda tehes tagab amet, et ei***

	avalikusta meetmeid, mida liikmesriigid võtavad oma oluliste riiklike funktsioonide kaitsmiseks, eelkõige seoses riikliku julgeolekuga.

Muudatusettepanek 115

Ettepanek võtta vastu määrus
Artikkel 7 – lõige 6

Komisjoni ettepanek	*Muudatusettepanek*
6. Amet korraldab iga-aastaseid liidu tasandi küberõppusi ning toetab liikmesriike ja ELi institutsioone, organeid ja asutusi nende taotluse korral õppuste korraldamisel. Iga-aastased liidu tasandi õppused sisaldavad tehnilisi, operatiivseid ja strateegilisi elemente, et aidata ette valmistada liidu tasandi koostööl põhinevat reageerimist ulatuslikele piiriülestele küberturvalisuse intsidentidele. Lisaks annab amet vajaduse korral oma panuse valdkondlike küberõppuste korraldamisse ja aitab neid korraldada koos asjaomaste teabe jagamise ja analüüsimise keskustega ning lubab keskustel osaleda ka liidu tasandi küberturvalisuse õppustel.	6. Amet korraldab ***korrapäraseid ja igal juhul vähemalt*** iga-aastaseid liidu tasandi küberõppusi ning toetab liikmesriike ja ELi institutsioone, organeid ja asutusi nende taotluse korral õppuste korraldamisel. Iga-aastased liidu tasandi õppused sisaldavad tehnilisi, operatiivseid ja strateegilisi elemente, et aidata ette valmistada liidu tasandi koostööl põhinevat reageerimist ulatuslikele piiriülestele küberturvalisuse intsidentidele. Lisaks annab amet vajaduse korral oma panuse valdkondlike küberõppuste korraldamisse ja aitab neid korraldada koos asjaomaste teabe jagamise ja analüüsimise keskustega ning lubab keskustel osaleda ka liidu tasandi küberturvalisuse õppustel.

Muudatusettepanek 116

Ettepanek võtta vastu määrus
Artikkel 7 – lõige 7

Komisjoni ettepanek	*Muudatusettepanek*
7. Amet koostab korrapäraselt ELi küberturvalisuse tehnilise olukorra aruandeid intsidentide ja ohtude kohta, võttes aluseks avatud allikatest pärit teabe, omaenda tehtud analüüsid ja aruanded, mida jagavad muu hulgas: liikmesriikide CSIRTid (vabatahtlikkuse alusel) või ELi võrgu- ja infoturbe direktiivi alusel loodud ühtsed kontaktpunktid (vastavalt võrgu- ja infoturbe direktiivi ***artiklit*** 14 lõikele 5);	7. Amet koostab korrapäraselt ***ja põhjalikult*** ELi küberturvalisuse tehnilise olukorra aruandeid intsidentide ja ohtude kohta, võttes aluseks avatud allikatest pärit teabe, omaenda tehtud analüüsid ja aruanded, mida jagavad muu hulgas: liikmesriikide CSIRTid (vabatahtlikkuse alusel) või ELi võrgu- ja infoturbe direktiivi alusel loodud ühtsed kontaktpunktid (vastavalt võrgu- ja

Europoli küberkuritegevuse vastase võitluse Euroopa keskus (EC3), CERT-EU.	infoturbe direktiivi ***artikli*** 14 lõikele 5); Europoli küberkuritegevuse vastase võitluse Euroopa keskus (EC3), CERT-EU. ***Tegevdirektor esitab avalikud järeldused Euroopa Parlamendile, kui see on asjakohane.***

Muudatusettepanek 117

Ettepanek võtta vastu määrus
Artikkel 7 – lõige 7 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	7a. Amet annab vajaduse korral ja komisjoni eelneval nõusolekul panuse küberkoostöösse NATO Küberkaitsekoostöö Keskusega ja NATO side- ja teabeakadeemiaga (NCI).

Muudatusettepanek 118

Ettepanek võtta vastu määrus
Artikkel 7 – lõige 8 – punkt a

Komisjoni ettepanek	*Muudatusettepanek*
(a) koondab riiklikest allikatest pärit aruandeid, et aidata kaasa ühise olukorrateadlikkuse tekitamisele;	a) ***analüüsib ja*** koondab riiklikest allikatest pärit aruandeid, et aidata kaasa ühise olukorrateadlikkuse tekitamisele;

Muudatusettepanek 119

Ettepanek võtta vastu määrus
Artikkel 7 – lõige 8 – punkt c

Komisjoni ettepanek	*Muudatusettepanek*
(c) toetab intsidendi või kriisi tehnilist lahendamist, hõlbustades muu hulgas tehniliste lahenduste jagamist liikmesriikide vahel;	c) toetab intsidendi või kriisi tehnilist lahendamist ***lähtuvalt oma sõltumatutest eksperditeadmistest ja vahenditest***, hõlbustades muu hulgas tehniliste lahenduste ***vabatahtlikku*** jagamist liikmesriikide vahel;

Muudatusettepanek 120

Ettepanek võtta vastu määrus
Artikkel 7 – lõige 8 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	8a. Amet korraldab vajaduse korral arvamuste vahetuse ja abistab liikmesriikide ametiasutusi nende reageerimise koordineerimisel kooskõlas subsidiaarsuse ja proportsionaalsuse põhimõtetega.

Muudatusettepanek 121

Ettepanek võtta vastu määrus
Artikkel 7 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Artikkel 7a
	Ameti tehniline suutlikkus
	1. Artiklis 7 kirjeldatud eesmärkide saavutamiseks ja kooskõlas ameti tööprogrammiga töötab amet muu hulgas välja järgmise tehnilise suutlikkuse ja järgmised oskused:
	a) suutlikkus koguda avatud allikatest teavet küberturvalisuse ohtude kohta ning
	b) suutlikkus kasutada tehnilisi seadmeid, vahendeid ja eksperditeadmisi kaugteel.
	2. Käesoleva artikli lõikes 1 osutatud tehnilise suutlikkuse tagamiseks ja asjakohaste oskuste arendamiseks teeb amet järgmist:
	a) tagab, et tema värbamismenetlustes kajastuvad erinevad nõutud tehnilised oskused, ning
	b) teeb vastavalt käesoleva määruse artikli 7 lõikele 2 koostööd CERT-EU ja Europoliga.

Muudatusettepanek 122

Ettepanek võtta vastu määrus
Artikkel 8 – lõik 1 – punkt a – sissejuhatav osa

Komisjoni ettepanek	*Muudatusettepanek*
(a) toetab ja edendab käesoleva määruse III jaotises kirjeldatud IKT toodete ja ***teenuste*** küberturvalisuse sertifitseerimise alaste liidu põhimõtete arendamist ja rakendamist järgmiselt:	a) toetab ja edendab käesoleva määruse III jaotises kirjeldatud IKT toodete***,*** ***teenuste*** ja ***protsesside*** küberturvalisuse sertifitseerimise alaste liidu põhimõtete arendamist ja rakendamist järgmiselt:

Muudatusettepanek 123

Ettepanek võtta vastu määrus
Artikkel 8 – lõik 1 – punkt a – alapunkt -1 (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	-1) määrab järjepidevalt kindlaks standardid, tehnilised kirjeldused ja IKT tehnilised kirjeldused;

Muudatusettepanek 124

Ettepanek võtta vastu määrus
Artikkel 8 – lõik 1 – punkt a – alapunkt 1

Komisjoni ettepanek	*Muudatusettepanek*
(1) koostab IKT toodete ja ***teenuste*** Euroopa küberturvalisuse sertifitseerimise ettevalmistavad kavad vastavalt käesoleva määruse artiklile 44;	1) koostab ***koostöös valdkonna sidusrühmade ja standardiorganisatsioonidega ametliku, standarditud ning läbipaistva protsessi käigus*** IKT toodete***,*** ***teenuste*** ja ***protsesside*** Euroopa küberturvalisuse sertifitseerimise ettevalmistavad kavad vastavalt käesoleva määruse artiklile 44;

Muudatusettepanek 125

Ettepanek võtta vastu määrus
Artikkel 8 – lõik 1 – punkt a – alapunkt 1 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	1a) hindab koostöös liikmesriikide sertifitseerimisrühmaga vastavalt käesoleva määruse artiklile 53 Euroopa küberturvalisuse sertifikaatide väljastamise menetlusi, mille on kehtestanud käesoleva määruse artiklis 51 osutatud vastavushindamisasutused, eesmärgiga tagada, et vastavushindamisasutused kohaldaksid sertifikaatide väljastamisel käesolevat määrust ühetaoliselt;

Muudatusettepanek 126

Ettepanek võtta vastu määrus
Artikkel 8 – lõik 1 – punkt a – alapunkt 1 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	1b) teeb sõltumatuid perioodilisi järelkontrolle sertifitseeritud IKT toodete, protsesside ja teenuste vastavuse kohta Euroopa küberturvalisuse sertifitseerimise kavadele;

Muudatusettepanek 127

Ettepanek võtta vastu määrus
Artikkel 8 – lõik 1 – punkt a – alapunkt 2

Komisjoni ettepanek	*Muudatusettepanek*
(2) aitab komisjonil pakkuda sekretariaaditeenuseid ***Euroopa küberturvalisuse sertifitseerimise rühmale*** vastavalt käesoleva määruse artiklile 53;	2) aitab komisjonil pakkuda sekretariaaditeenuseid ***liikmesriikide sertifitseerimisrühmale*** vastavalt käesoleva määruse artiklile 53;

Muudatusettepanek 128

Ettepanek võtta vastu määrus
Artikkel 8 – lõik 1 – punkt a – alapunkt 3

Komisjoni ettepanek	*Muudatusettepanek*
(3) koostab ja avaldab juhiseid ja töötab välja häid tavasid IKT toodete ja teenuste küberturvalisuse nõuete kohta, tehes selleks koostööd ***riikide sertifitseerimisega tegelevate*** järelevalveasutuste ja tööstusega;	3) koostab ja avaldab juhiseid ja töötab välja häid tavasid ***(sealhulgas küberhügieeni põhimõtete valdkonnas)*** IKT toodete***, protsesside*** ja teenuste küberturvalisuse nõuete kohta, tehes selleks koostööd ***riiklike sertifitseerimise*** järelevalveasutuste ja tööstusega ***ametliku, standarditud ja läbipaistva protsessi raames***;

Muudatusettepanek 129

Ettepanek võtta vastu määrus
Artikkel 8 – lõik 1 – punkt b

Komisjoni ettepanek	*Muudatusettepanek*
(b) hõlbustab riskihalduse ning IKT toodete ja teenuste turvalisuse Euroopa ja rahvusvaheliste standardite loomist ja kasutuselevõtmist ning koostab koostöös ***liikmesriikidega*** nõuandeid ja juhiseid oluliste teenuste operaatoritele ja digitaalsete teenuste osutajatele esitatavate turvalisusnõuetega seotud tehniliste valdkondade, aga ka juba olemas olevate standardite, kaasa arvatud liikmesriikide riiklike standardite kohta vastavalt direktiivi (EL) 2016/1148 artikli 19 lõikele 2;	b) hõlbustab riskihalduse ning IKT toodete***, protsesside*** ja teenuste turvalisuse Euroopa ja rahvusvaheliste standardite loomist ja kasutuselevõtmist ning koostab koostöös ***liikmesriikide ja tööstusega*** nõuandeid ja juhiseid oluliste teenuste operaatoritele ja digitaalsete teenuste osutajatele esitatavate turvalisusnõuetega seotud tehniliste valdkondade, aga ka juba olemas olevate standardite, kaasa arvatud liikmesriikide riiklike standardite kohta vastavalt direktiivi (EL) 2016/1148 artikli 19 lõikele 2***, ning jagab seda teavet liikmesriikidega***;

Muudatusettepanek 130

Ettepanek võtta vastu määrus
Artikkel 9 – lõik 1 – punkt c

Komisjoni ettepanek	*Muudatusettepanek*
(c) jagab koostöös liikmesriikide ametiasutuste ***ekspertidega*** nõu, juhiseid ja	c) jagab koostöös liikmesriikide ametiasutuste ***ekspertide ja asjaomaste***

parimaid tavasid võrgu- ja infosüsteemide turvalisuse kohta, eeskätt selles osas, mis puudutab internetitaristu ja nende taristute turvalisust, mis toetavad direktiivi (EL) 2016/1148 II lisas loetletud sektoreid;	***sidusrühmadega*** nõu, juhiseid ja parimaid tavasid võrgu- ja infosüsteemide turvalisuse kohta, eeskätt selles osas, mis puudutab internetitaristu ja nende taristute turvalisust, mis toetavad direktiivi (EL) 2016/1148 II lisas loetletud sektoreid;

Muudatusettepanek 131

Ettepanek võtta vastu määrus
Artikkel 9 – lõik 1 – punkt e

Komisjoni ettepanek	*Muudatusettepanek*
(e) suurendab üldsuse teadlikkust küberturvalisuse riskidest ***ja*** jagab kodanikele ja organisatsioonidele mõeldud juhiseid individuaalsete kasutajate heade tavade kohta;	e) suurendab ***pidevalt*** üldsuse teadlikkust küberturvalisuse riskidest***, pakub koolitusi ning*** jagab kodanikele ja organisatsioonidele mõeldud juhiseid individuaalsete kasutajate heade tavade kohta ***ning edendab ennetavate tugevate IT turbemeetmete kasutuselevõttu ja usaldusväärset andmekaitset ja eraelu puutumatust***;

Muudatusettepanek 132

Ettepanek võtta vastu määrus
Artikkel 9 – lõik 1 – punkt g

Komisjoni ettepanek	*Muudatusettepanek*
(g) korraldab koostöös liikmesriikide ja liidu institutsioonide, organite ja asutustega korrapäraselt teavituskampaaniaid, et ***suurendada küberturvalisust ja selle nähtavust liidus.***	g) korraldab koostöös liikmesriikide ja liidu institutsioonide, organite ja asutustega korrapäraselt teavituskampaaniaid, et ***soodustada laiaulatuslikku avalikku arutelu;***

Muudatusettepanek 133

Ettepanek võtta vastu määrus
Artikkel 9 – lõik 1 – punkt g a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ga) toetab liikmesriikidevahelist tihedamat koordineerimist ja parimate

	tavade vahetamist küberturvalisuse alase hariduse ja kirjaoskuse, küberhügieeni ja teadlikkuse suurendamise valdkonnas.

Muudatusettepanek 134

Ettepanek võtta vastu määrus
Artikkel 10 – lõik 1 – punkt a

Komisjoni ettepanek	*Muudatusettepanek*
(a) annab liidule ja liikmesriikidele nõu küberturvalisuse ***valdkonnas*** vajalike teadusuuringute ja prioriteetide kohta, et võimaldada tulemuslikku reageerimist praegustele ja tulevastele riskidele ja ohtudele, sealhulgas seoses uue ja kujunemisjärgus info- ja kommunikatsioonitehnoloogiaga, ning riskiennetustehnoloogia tõhusat kasutamist;	a) ***tagab eelneva konsulteerimise asjaomaste kasutajarühmadega ning*** annab liidule ja liikmesriikidele nõu küberturvalisuse***, andmekaitse ja eraelu puutumatuse valdkondades*** vajalike teadusuuringute ja prioriteetide kohta, et võimaldada tulemuslikku reageerimist praegustele ja tulevastele riskidele ja ohtudele, sealhulgas seoses uue ja kujunemisjärgus info- ja kommunikatsioonitehnoloogiaga, ning riskiennetustehnoloogia tõhusat kasutamist;

Muudatusettepanek 135

Ettepanek võtta vastu määrus
Artikkel 10 – lõik 1 – punkt b a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ba) tellib oma teadustegevust huvivaldkondades, mis ei ole olemasolevate liidu teadusprogrammidega veel hõlmatud, kui on olemas selgelt määratletud Euroopa lisaväärtus.

Muudatusettepanek 136

Ettepanek võtta vastu määrus
Artikkel 11 – lõik 1 – punkt c a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ca) nõustab ja toetab komisjoni

	koostöös artikli 53 alusel loodud liikmesriikide sertifitseerimisrühmaga küsimustes, mis puudutavad kolmandate riikidega sõlmitud küberturvalisuse sertifikaatide vastastikuse tunnustamise lepinguid.

Muudatusettepanek 137

Ettepanek võtta vastu määrus
Artikkel 12 – lõik 1 – punkt d

Komisjoni ettepanek	*Muudatusettepanek*
(d) ***alaline sidusrühm***, kes täidab artiklis 20 sätestatud ülesandeid.	d) ***ENISA nõuanderühm***, kes täidab artiklis 20 sätestatud ülesandeid.

Muudatusettepanek 138

Ettepanek võtta vastu määrus
Artikkel 14 – lõige 1 – punkt e

Komisjoni ettepanek	*Muudatusettepanek*
(e) annab hinnangu konsolideeritud aastaaruandele ameti tegevuse kohta ja võtab aruande vastu ning saadab nii aruande kui ka hinnangu hiljemalt järgmise aasta 1. juuliks Euroopa Parlamendile, nõukogule, komisjonile ja kontrollikojale. Aastaaruanne hõlmab raamatupidamisaruannet ***ning*** selles kirjeldatakse, ***kuidas*** amet täitis oma tulemuslikkuse näitajaid. Aastaaruanne avalikustatakse;	e) annab hinnangu konsolideeritud aastaaruandele ameti tegevuse kohta ja võtab aruande vastu ning saadab nii aruande kui ka hinnangu hiljemalt järgmise aasta 1. juuliks Euroopa Parlamendile, nõukogule, komisjonile ja kontrollikojale. Aastaaruanne hõlmab raamatupidamisaruannet***,*** selles kirjeldatakse ***kulude tasuvust ja hinnatakse***, ***kui tõhus*** amet ***on olnud ning mil määral*** täitis ***amet*** oma tulemuslikkuse näitajaid. Aastaaruanne avalikustatakse;

Muudatusettepanek 139

Ettepanek võtta vastu määrus
Artikkel 14 – lõige 1 – punkt m

Komisjoni ettepanek	*Muudatusettepanek*
(m) nimetab kooskõlas käesoleva määruse artikliga 33 ametisse	m) nimetab kooskõlas käesoleva määruse artikliga 33 ametisse ***kutsealaste***

tegevdirektori ning vajaduse korral pikendab tema ametiaega või tagandab ta ametist;	***kriteeriumide põhjal valitud*** tegevdirektori ning vajaduse korral pikendab tema ametiaega või tagandab ta ametist;

Muudatusettepanek 140

Ettepanek võtta vastu määrus
Artikkel 14 – lõige 1 – punkt o

Komisjoni ettepanek	*Muudatusettepanek*
(o) teeb kõik otsused ameti sisestruktuuri loomise ja vajaduse korral selle muutmise kohta, võttes arvesse ameti tegevusega seotud vajadusi ja lähtudes usaldusväärsest eelarvehaldusest;	o) teeb kõik otsused ameti sisestruktuuri loomise ja vajaduse korral selle muutmise kohta, võttes arvesse ameti tegevusega seotud vajadusi***, nagu on loetletud käesolevas määruses,*** ja lähtudes usaldusväärsest eelarvehaldusest;

Muudatusettepanek 141

Ettepanek võtta vastu määrus
Artikkel 16 – lõige 4

Komisjoni ettepanek	*Muudatusettepanek*
4. ***Alalise sidusrühma*** liikmed võivad esimehe kutsel osaleda haldusnõukogu koosolekutel ilma hääleõiguseta.	4. ***ENISA nõuanderühma*** liikmed võivad esimehe kutsel osaleda haldusnõukogu koosolekutel ilma hääleõiguseta.

Muudatusettepanek 142

Ettepanek võtta vastu määrus
Artikkel 18 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. Juhatuse moodustavad haldusnõukogu liikmete seast nimetatud viis liiget, nende hulgas haldusnõukogu esimees, kes võib olla ka juhatuse esimees, ning üks komisjoni esindaja. Tegevdirektor osaleb juhatuse koosolekutel, kuid tal ei ole hääleõigust.	3. Juhatuse moodustavad haldusnõukogu liikmete seast nimetatud viis liiget, nende hulgas haldusnõukogu esimees, kes võib olla ka juhatuse esimees, ning üks komisjoni esindaja. Tegevdirektor osaleb juhatuse koosolekutel, kuid tal ei ole hääleõigust. ***Ametissenimetamisega püütakse saavutada tasakaalustatud sooline esindatus juhatuses.***

Selgitus

Juhatuse liikmete nimetamisel tuleb samuti seada eesmärgiks sooline tasakaal, peegeldades haldusnõukogu käsitlevaid sätteid artikli 13 lõikes 3.

Muudatusettepanek 143

Ettepanek võtta vastu määrus
Artikkel 19 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Tegevdirektor annab Euroopa Parlamendile selle taotluse korral aru oma ülesannete täitmise kohta. Nõukogu võib kutsuda tegevdirektori oma ülesannete täitmisest aru andma.	2. Tegevdirektor annab Euroopa Parlamendile ***igal aastal või*** selle taotluse korral aru oma ülesannete täitmise kohta. Nõukogu võib kutsuda tegevdirektori oma ülesannete täitmisest aru andma.

Muudatusettepanek 144

Ettepanek võtta vastu määrus
Artikkel 19 – lõige 5 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	5a. Tegevdirektoril on samuti õigus tegutseda küberturvalisuse poliitika valdkonnas Euroopa Komisjoni presidendi institutsioonilise erinõunikuna, kelle mandaat on kindlaks määratud komisjoni 6. veebruari 2014. aasta otsuses C(2014) 541.

Muudatusettepanek 145

Ettepanek võtta vastu määrus
Artikkel 20 – pealkiri

Komisjoni ettepanek	*Muudatusettepanek*
Alaline sidusrühm	***ENISA nõuanderühm***
	(Muudatusettepanekut kohaldatakse kogu teksti ulatuses. Selle vastuvõtmise korral tehakse vastavad muudatused kogu tekstis.)

Muudatusettepanek 146

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Haldusnõukogu loob tegevdirektori ettepanekul ***alalise sidusrühma***, mis koosneb asjaomaseid sidusrühmi esindavatest tunnustatud ***ekspertidest***, näiteks IKT tööstuse, avalikkusele kättesaadavate elektroonilise side võrkude või teenuste pakkujate ja tarbijarühmade ekspertidest, küberturvalisusega tegelevatest akadeemilistest ekspertidest ning [Euroopa elektroonilise side seadustiku kehtestamise direktiivi] alusel teavitatud riiklike reguleerivate asutuste esindajatest, samuti liidu õiguskaitseasutuste ja andmekaitse järelevalveasutuste esindajatest.	1. Haldusnõukogu loob tegevdirektori ettepanekul ***läbipaistval viisil ENISA nõuanderühma***, mis koosneb asjaomaseid sidusrühmi esindavatest tunnustatud ***turbeekspertidest***, näiteks IKT tööstuse ***(sealhulgas VKEd), võrgu- ja infoturbe direktiivi kohaste oluliste teenuste operaatorite***, avalikkusele kättesaadavate elektroonilise side võrkude või teenuste pakkujate ja tarbijarühmade ekspertidest, küberturvalisusega tegelevatest akadeemilistest ekspertidest***, Euroopa standardiorganisatsioonidest, ELi asutustest*** ning [Euroopa elektroonilise side seadustiku kehtestamise direktiivi] alusel teavitatud riiklike reguleerivate asutuste esindajatest, samuti liidu õiguskaitseasutuste ja andmekaitse järelevalveasutuste esindajatest. ***Haldusnõukogu tagab eri sidusrühmade vahelise sobiva tasakaalu.***

Muudatusettepanek 147

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Eeskätt ***alalise sidusrühma*** liikmete arvu, koosseisu ja nimetamist haldusnõukogu poolt, tegevdirektori ettepanekut ja rühma tegevust käsitlev kord täpsustatakse ameti sise-eeskirjades ning see avalikustatakse.	2. Eeskätt ***ENISA nõuanderühma*** liikmete arvu, koosseisu ja nimetamist haldusnõukogu poolt, tegevdirektori ettepanekut ja rühma tegevust käsitlev kord täpsustatakse ameti sise-eeskirjades ning see avalikustatakse.

Muudatusettepanek 148

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. ***Alalist sidusrühma*** juhatab tegevdirektor või isik, kelle tegevdirektor nimetab iga konkreetse juhtumi korral eraldi.	3. ***ENISA nõuanderühma*** juhatab tegevdirektor või isik, kelle tegevdirektor nimetab iga konkreetse juhtumi korral eraldi.

Muudatusettepanek 149

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 4

Komisjoni ettepanek	*Muudatusettepanek*
4. ***Alalise sidusrühma*** liikmete ametiaeg on kaks ja pool aastat. Haldusnõukogu liige ei või olla ***alalise sidusrühma*** liige. Komisjoni ja liikmesriikide ekspertidel on õigus viibida ***alalise sidusrühma*** koosolekutel ning osaleda rühma töös. Kui tegevdirektor peab seda asjakohaseks, võib kutsuda ***alalise sidusrühma*** koosolekutel ning selle töös osalema teiste asutuste esindajaid, kes ei ole ***alalise sidusrühma*** liikmed.	4. ***ENISA nõuanderühma*** liikmete ametiaeg on kaks ja pool aastat. Haldusnõukogu liige ei või olla ***ENISA nõuanderühma*** liige. Komisjoni ja liikmesriikide ekspertidel on õigus viibida ***ENISA nõuanderühma*** koosolekutel ning osaleda rühma töös. Kui tegevdirektor peab seda asjakohaseks, võib kutsuda ***ENISA nõuanderühma*** koosolekutel ning selle töös osalema teiste asutuste esindajaid, kes ei ole ***ENISA nõuanderühma*** liikmed.

Muudatusettepanek 150

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 4 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	4a. ENISA nõuanderühm esitab korrapäraselt ajakohastatud teavet oma plaanide kohta kogu aasta vältel ja kehtestab eesmärgid oma tööprogrammis, mis avaldatakse läbipaistvuse tagamiseks iga kuue kuu tagant.

Muudatusettepanek 151

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 5

Komisjoni ettepanek	*Muudatusettepanek*
5. ***Alaline sidusrühm*** nõustab ametit tema ülesannete täitmisel. Eelkõige annab rühm tegevdirektorile soovitusi ameti tööprogrammi ettepaneku koostamiseks ning tagab teabevahetuse asjaomaste sidusrühmadega ***kõikides*** tööprogrammiga seotud küsimustes.	5. ***ENISA nõuanderühm*** nõustab ametit tema ülesannete täitmisel***, välja arvatud seoses käesoleva määruse III jaotise kohaldamisega***. Eelkõige annab rühm tegevdirektorile soovitusi ameti tööprogrammi ettepaneku koostamiseks ning tagab teabevahetuse asjaomaste sidusrühmadega tööprogrammiga seotud küsimustes.

Muudatusettepanek 152

Ettepanek võtta vastu määrus
Artikkel 20 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Artikkel 20a
	Sidusrühmade sertifitseerimisrühm
	1. Tegevdirektor loob sidusrühmade sertifitseerimisrühma, mis koosneb üldisest nõuandekomiteest, mis annab üldiseid nõuandeid käesoleva määruse III jaotise kohaldamise kohta ja moodustab ajutisi komiteesid iga ettevalmistava kava esitamiseks, arendamiseks ja vastuvõtmiseks. Selle rühma liikmed valitakse asjaomaseid sidusrühmi esindavatest tunnustatud turbeekspertidest, näiteks IKT tööstuse (sealhulgas VKEd), võrgu- ja infoturbe direktiivi kohaste oluliste teenuste operaatorite, avalikkusele kättesaadavate elektroonilise side võrkude või teenuste pakkujate ja tarbijarühmade ekspertidest, küberturvalisusega tegelevatest akadeemilistest ekspertidest, Euroopa standardiorganisatsioonidest ning [Euroopa elektroonilise side seadustiku kehtestamise direktiivi] alusel teavitatud riiklike reguleerivate asutuste

	esindajatest, samuti liidu õiguskaitseasutuste ja andmekaitse järelevalveasutuste esindajatest.
	2. Eeskätt sidusrühmade sertifitseerimisrühma liikmete arvu, koosseisu ja nimetamist tegevdirektori poolt ja rühma tegevust käsitlev kord täpsustatakse ameti sise-eeskirjades, see järgib parimaid tavasid kõigi sidusrühmade õiglase esindatuse ja võrdsete õiguste tagamisel ning see avalikustatakse.
	3. Haldusnõukogu liige ei või olla sidusrühmade sertifitseerimisrühma liige. ENISA nõuanderühma liige võib olla ka sidusrühmade sertifitseerimisrühma liige. Komisjoni ja liikmesriikide ekspertidel on õigus viibida sidusrühmade sertifitseerimisrühma koosolekutel, kui neid kutsutakse. Kui tegevdirektor peab seda asjakohaseks, võib kutsuda sidusrühmade sertifitseerimisrühma koosolekutel ning selle töös osalema teiste asutuste esindajaid.
	4. Sidusrühmade sertifitseerimisrühm nõustab ametit tema ülesannete täitmisel seoses käesoleva määruse III jaotisega. Eelkõige on rühmal õigus teha komisjonile ettepanek koostada Euroopa küberturvalisuse sertifitseerimise ettevalmistav kava, nagu on sätestatud käesoleva määruse artiklis 44, ning osaleda kõnealuste kavade heakskiitmisel käesoleva määruse artiklites 43–48 ja artiklis 53 osutatud menetlustes.

Muudatusettepanek 153

Ettepanek võtta vastu määrus
Artikkel 21 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Artikkel 21a
	Ametile esitatav taotlus
	1. Amet peaks looma ühtse kontaktpunkti,

mille kaudu adresseeritakse ameti eesmärkide ja ülesannete hulka kuuluvaid nõuande- ja abitaotluseid, ja seda haldama. Kõnealustele taotlustele tuleks lisada käsitletavat küsimust selgitav taustteave. Amet peaks esitama võimaliku mõju vahenditele ning esimesel võimalusel ka taotluste järelmeetmed. Kui amet lükkab taotluse tagasi, põhjendab ta seda.

2. Lõikes 1 osutatud taotlusi võivad esitada

a) Euroopa Parlament;

b) nõukogu;

c) komisjon ning

d) kõik liikmesriikide määratud pädevad asutused, näiteks direktiivi 2002/21/EÜ artiklis 2 määratletud riigi reguleerivad asutused.

3. Haldusnõukogu sätestab ameti sise-eeskirjades lõigete 1 ja 2 kohaldamise praktilise korra, eelkõige seoses taotluste esitamise, tähtsuse järgi järjestamise, järelmeetmete ja teavitamisega.

Muudatusettepanek 154

Ettepanek võtta vastu määrus
Artikkel 24 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Haldusnõukogu liikmed, tegevdirektor, ***alalise sidusrühma*** liikmed, ajutistes töörühmades osalevad väliseksperdid ning ameti töötajad, sealhulgas liikmesriikide poolt ajutiselt lähetatud ametnikud järgivad Euroopa Liidu toimimise lepingu (ELi toimimise leping) artiklis 339 sätestatud konfidentsiaalsuse nõudeid, seda isegi pärast nende töökohustuste lõppemist.	2. Haldusnõukogu liikmed, tegevdirektor, ***ENISA nõuanderühma*** liikmed, ajutistes töörühmades osalevad väliseksperdid ning ameti töötajad, sealhulgas liikmesriikide poolt ajutiselt lähetatud ametnikud järgivad Euroopa Liidu toimimise lepingu (ELi toimimise leping) artiklis 339 sätestatud konfidentsiaalsuse nõudeid, seda isegi pärast nende töökohustuste lõppemist.

Muudatusettepanek 155

Ettepanek võtta vastu määrus
Artikkel 26 – lõige 1 – lõik 1 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Esialgne eelarvestuse projekt põhineb käesoleva määruse artikli 21 lõikes 1 osutatud ühtse programmdokumendi eesmärkidel ja oodatavatel tulemustel ning selles võetakse arvesse kõnealuste eesmärkide ja oodatavate tulemuste saavutamiseks vajalikke finantsressursse tulemuspõhise eelarvestamise põhimõtte kohaselt.

Muudatusettepanek 156

Ettepanek võtta vastu määrus
Artikkel 30 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Kontrollikojal on õigus auditeerida dokumentide põhjal ja kohapeal kõiki toetusesaajaid, töövõtjaid ja alltöövõtjaid, keda amet on rahastanud liidu vahenditest.	2. Kontrollikojal on õigus auditeerida dokumentide põhjal ja kohapeal ***kontrollida*** kõiki toetusesaajaid, töövõtjaid ja alltöövõtjaid, keda amet on rahastanud liidu vahenditest.

Muudatusettepanek 157

Ettepanek võtta vastu määrus
Artikkel 36 – lõige 5

Komisjoni ettepanek	*Muudatusettepanek*
5. Teenistujate vastutust ameti ees reguleerivad ameti töötajate suhtes kohaldatavad sätted.	5. Teenistujate vastutust ameti ees reguleerivad ameti töötajate suhtes kohaldatavad sätted. ***Tagatakse töötajate tõhus töölevõtmine.***

Muudatusettepanek 158

Ettepanek võtta vastu määrus
Artikkel 37 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Ameti toimimiseks vajalikke tõlketeenuseid osutab Euroopa Liidu Asutuste Tõlkekeskus.	2. Ameti toimimiseks vajalikke tõlketeenuseid osutab Euroopa Liidu Asutuste Tõlkekeskus ***või osutavad muud tõlketeenuse osutajad kooskõlas hanke-eeskirjadega ning asjakohastes finantseeskirjades ette nähtud piirides***.

Muudatusettepanek 159

Ettepanek võtta vastu määrus
Artikkel 39 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Niivõrd kui see on vajalik käesoleva määruse eesmärkide saavutamiseks, võib amet teha koostööd kolmandate riikide pädevate asutuste ja/või rahvusvaheliste organisatsioonidega. Selleks võib amet komisjoni eelneval nõusolekul leppida kolmandate riikide asutuste ja rahvusvaheliste organisatsioonidega kokku koostöökorra. Kõnealune koostöökord ei too liidule ega selle liikmesriikidele kaasa õiguslikke kohustusi.	1. Niivõrd kui see on vajalik käesoleva määruse eesmärkide saavutamiseks, võib amet teha koostööd kolmandate riikide pädevate asutuste ja/või rahvusvaheliste organisatsioonidega. Selleks võib amet komisjoni eelneval nõusolekul leppida kolmandate riikide asutuste ja rahvusvaheliste organisatsioonidega kokku koostöökorra. ***Koostöö NATOga (kui see toimub) võib hõlmata küberturvalisuse ühisõppusi ja küberintsidentidele ühiselt reageerimise koordineerimist.*** Kõnealune koostöökord ei too liidule ega selle liikmesriikidele kaasa õiguslikke kohustusi.

Selgitus

Arvestades küberintsidentide piiriülest laadi, peaks ENISA tegema koostööd küberturvalisuse osalistega Euroopas (nt NATO), kui see on asjakohane. See on eriti oluline, kuna NATO-l võib olla kübervaldkonnas suutlikkus, mida ENISA-l ei ole, ja vastupidi. Liikmesriikide kui terviku vastu suunatud küberrünnete arvu suurenemist arvesse võttes on Euroopa julgeoleku seisukohast hädavajalik, et ENISA teeks rahvusvahelisel tasandil koostööd selliste rahvusvaheliste organisatsioonidega nagu NATO.

Muudatusettepanek 160

Ettepanek võtta vastu määrus
Artikkel 41 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Ameti asukohaliikmesriik tagab ametile parimad võimalikud tegutsemistingimused, et tagada ameti nõuetekohane toimimine, sealhulgas asukoha ligipääsetavus, sobivate haridusasutuste olemasolu töötajate laste jaoks, laste ja abikaasade piisav juurdepääs tööturule, sotsiaalkindlustusele ja arstiabile.	2. Ameti asukohaliikmesriik tagab ametile parimad võimalikud tegutsemistingimused, et tagada ameti nõuetekohane toimimine, sealhulgas ***üks asukoht kogu ameti jaoks,*** asukoha ligipääsetavus, sobivate haridusasutuste olemasolu töötajate laste jaoks, laste ja abikaasade piisav juurdepääs tööturule, sotsiaalkindlustusele ja arstiabile.

Selgitus

Ameti praegune struktuur (juhatuse asukoht Irákleios ja peamine tegevuskoht Ateenas) on osutunud ebatõhusaks ja kulukaks. Seepärast peaksid kõik ENISA töötajad töötama ühes linnas. Käesolevas lõikes nimetatud kriteeriumide põhjal peaks see asukoht olema Ateenas.

Muudatusettepanek 161

Ettepanek võtta vastu määrus
Artikkel 43 – lõik 1

Komisjoni ettepanek	*Muudatusettepanek*
Euroopa küberturvalisuse sertifitseerimise kava kinnitab, et ***selle kava kohaselt sertifitseeritud IKT tooted ja teenused*** vastavad kirjeldatud nõuetele selles osas, mis puudutab nende võimet pidada teataval usaldusväärsuse tasemel vastu tegevustele, mille eesmärk on rikkuda salvestatud, edastatud või töödeldud andmete või nende toodete, protsesside***, teenuste*** ja ***süsteemide*** funktsioonide või nende poolt pakutavate või nende kaudu juurdepääsetavate teenuste käideldavust, autentsust, terviklust või konfidentsiaalsust.	Euroopa küberturvalisuse sertifitseerimise kava kinnitab, et ***kavaga hõlmatud IKT toodetel, protsessidel ja teenustel ei ole sertifitseerimise ajal ühtegi teadaolevat turvanõrkust ning need*** vastavad kirjeldatud nõuetele***, mis võivad viidata Euroopa ja rahvusvahelistele standarditele, tehnilistele kirjeldustele või IKT tehnilisele kirjeldusele,*** selles osas, mis puudutab nende võimet pidada ***kogu nende olelusringi ajal*** teataval usaldusväärsuse tasemel vastu tegevustele, mille eesmärk on rikkuda salvestatud, edastatud või töödeldud andmete või nende toodete, protsesside ja ***teenuste*** funktsioonide või nende poolt pakutavate või nende kaudu juurdepääsetavate teenuste käideldavust, autentsust, terviklust või konfidentsiaalsust***, ning vastavad***

konkreetsetele turvalisusega seotud eesmärkidele.

Muudatusettepanek 162

Ettepanek võtta vastu määrus
Artikkel 44 – lõige -1 (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	-1. Komisjon võtab kooskõlas artikliga 55a vastu delegeeritud õigusaktid käesoleva määruse täiendamiseks, kehtestades Euroopa küberturvalisuse sertifitseerimise kavadele liidu jooksva tööprogrammi. Kõnealuste delegeeritud õigusaktidega määratakse kindlaks liidu tasandil võetavad ühismeetmed ja strateegilised prioriteedid. Liidu jooksev tööprogramm sisaldab eelkõige loetelu prioriteetsetest Euroopa küberturvalisuse sertifitseerimise kava jaoks sobilikest IKT toodetest, protsessidest ja teenustest ning analüüsi selle kohta, kas vastavushindamisasutuste ja riiklike sertifitseerimise järelevalveasutuste kvaliteedi, oskusteabe ja teadmiste tase on võrdväärne, ning vajaduse korral ettepanekut meetmete kohta, mille abil see võrdväärne tase saavutatakse.
	Liidu esialgne jooksev tööprogramm kehtestatakse hiljemalt ... [kuus kuud pärast käesoleva määruse jõustumist] ja seda ajakohastatakse seejärel vajaduse korral, kuid vähemalt iga kahe aasta järel. Liidu jooksev tööprogramm tehakse üldsusele kättesaadavaks.
	Enne liidu jooksva tööprogrammi vastuvõtmist või ajakohastamist konsulteerib komisjon avatud, läbipaistval ja kaasaval viisil liikmesriikide sertifitseerimisrühma, ameti ja sidusrühmade sertifitseerimisrühmaga.

Muudatusettepanek 163

Ettepanek võtta vastu määrus
Artikkel 44 – lõige -1 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	-1a. Põhjendatud juhul võib komisjon paluda ametil koostada Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava. Taotlus peab põhinema liidu jooksval tööprogrammil.

Muudatusettepanek 164

Ettepanek võtta vastu määrus
Artikkel 44 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. ***Komisjoni taotluse põhjal koostab ENISA*** Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava, ***mis vastab käesoleva määruse artiklites 45***, ***46 ja*** 47 ***sätestatud tingimustele***. ***Liikmesriigid või artikliga 53 loodud Euroopa küberturvalisuse sertifitseerimise rühm (edaspidi „rühm“) võivad teha komisjonile ettepaneku koostada Euroopa küberturvalisuse sertifitseerimise ettevalmistav kava***.	1. Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava ***koostamise taotlus peab sisaldama ulatust***, ***artiklis 45 osutatud kohaldatavaid turvalisusega seotud eesmärke***, ***artiklis*** 47 ***osutatud kohaldatavaid elemente ja tähtaega, mil konkreetne ettevalmistav kava jõustub***. ***Taotluse koostamisel võib komisjon konsulteerida ameti, liikmesriikide sertifitseerimisrühma ja sidusrühmade sertifitseerimisrühmaga***.

Muudatusettepanek 165

Ettepanek võtta vastu määrus
Artikkel 44 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. ***Käesoleva artikli*** lõikes 1 osutatud ettevalmistavat kava koostades konsulteerib ***ENISA*** kõigi asjaomaste sidusrühmadega ja ***teeb rühmaga*** tihedat koostööd. ***Rühm pakub ENISA-le viimase*** taotluse korral abi ja eksperdinõu seoses ettevalmistava sertifitseerimiskava koostamisega, esitades vajaduse korral ka	2. Lõikes **-**1 ***(uus)*** osutatud ettevalmistavat kava koostades konsulteerib ***amet*** kõigi asjaomaste sidusrühmadega ***ametliku, avatud, läbipaistva*** ja ***kaasava konsulteerimise abil ning teeb*** tihedat koostööd ***liikmesriikide sertifitseerimisrühma, sidusrühmade sertifitseerimisrühma, käesoleva määruse artiklile 20 a vastavate***

arvamusi.	***ajutiste komiteede ja Euroopa standardiorganisatsioonidega***. ***Nad pakuvad ametile ameti*** taotluse korral abi ja eksperdinõu seoses ettevalmistava sertifitseerimiskava koostamisega, esitades vajaduse korral ka arvamusi.

Muudatusettepanek 166

Ettepanek võtta vastu määrus
Artikkel 44 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. ***ENISA*** edastab käesoleva artikli ***lõike*** 2 kohaselt koostatud ***Euroopa küberturvalisuse sertifitseerimise*** ettevalmistava kava komisjonile.	3. ***Amet*** edastab käesoleva artikli ***lõigete 1 ja*** 2 kohaselt koostatud ettevalmistava kava komisjonile.

Muudatusettepanek 167

Ettepanek võtta vastu määrus
Artikkel 44 – lõige 4

Komisjoni ettepanek	*Muudatusettepanek*
4. Komisjon võib ***ENISA*** esitatud ettevalmistava kava põhjal võtta kooskõlas ***artikli*** 55 ***lõikega 1 vastu rakendusaktid***, ***millega nähakse*** ette Euroopa küberturvalisuse sertifitseerimise kavad IKT toodete ja teenuste jaoks, mis vastavad ***käesoleva määruse*** artiklite 45, 46 ja 47 nõuetele.	4. Komisjon võib ***ameti*** esitatud ettevalmistava kava põhjal võtta kooskõlas ***artikliga*** 55***a vastu delegeeritud õigusaktid käesoleva määruse täiendamiseks***, ***nähes*** ette Euroopa küberturvalisuse sertifitseerimise kavad IKT toodete***, protsesside*** ja teenuste jaoks, mis vastavad artiklite 45, 46 ja 47 nõuetele.

Muudatusettepanek 168

Ettepanek võtta vastu määrus
Artikkel 44 – lõige 5

Komisjoni ettepanek	*Muudatusettepanek*
5. ***ENISA*** haldab spetsiaalset veebilehte, mis pakub teavet Euroopa küberturvalisuse sertifitseerimise kavade kohta ja tutvustab neid.	5. ***Amet*** haldab spetsiaalset veebilehte, mis pakub teavet Euroopa küberturvalisuse sertifitseerimise kavade***, sealhulgas tühistatud ja aegunud sertifikaatide ning***

hõlmatud riiklike sertifitseerimiste kohta ja tutvustab neid.

Juhul kui Euroopa küberturvalisuse sertifitseerimise kava vastab nõuetele, millele see peab eesmärgi kohaselt vastama kooskõlas asjakohaste liidu ühtlustamisõigusaktidega, avaldab komisjon viivitamata viite sellele kavale Euroopa Liidu Teatajas ja liidu asjakohases ühtlustamisõigusaktis sätestatud muul viisil.

Muudatusettepanek 169

Ettepanek võtta vastu määrus
Artikkel 44 – lõige 5 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	5a. Amet vaatab vastuvõetud kavad kooskõlas käesoleva määruse alusel kehtestatud struktuuriga läbi nende kehtivuse lõppemisel vastavalt artikli 47 lõike 1 punktile ac või komisjoni taotluse korral, võttes arvesse asjaomastelt sidusrühmadelt saadud tagasisidet.

Muudatusettepanek 170

Ettepanek võtta vastu määrus
Artikkel 45 – lõik 1 – sissejuhatav osa

Komisjoni ettepanek	*Muudatusettepanek*
Euroopa küberturvalisuse sertifitseerimise kava peab olema koostatud nii, et võtta vajaduse korral arvesse ***järgmisi*** turvalisusega seotud eesmärke:	Euroopa küberturvalisuse sertifitseerimise kava peab olema koostatud nii, et võtta vajaduse korral arvesse turvalisusega seotud eesmärke:

Muudatusettepanek 171

Ettepanek võtta vastu määrus
Artikkel 45 – lõik 1 – punkt a

Komisjoni ettepanek	*Muudatusettepanek*
(a) ***kaitsta salvestatud***, ***edastatud või muul moel töödeldud andmeid juhusliku või volitamata salvestamise***, ***töötlemise***, ***juurdepääsu või avalikustamise eest***;	a) ***tagada teenuste***, ***funktsioonide ja andmete konfidentsiaalsus***, ***terviklus***, ***käideldavus ja privaatsus***;

Muudatusettepanek 172

Ettepanek võtta vastu määrus
Artikkel 45 – lõik 1 – punkt b

Komisjoni ettepanek	*Muudatusettepanek*
(b) ***kaitsta salvestatud***, ***edastatud või muul moel töödeldud andmeid juhusliku või volitamata hävitamise*** ja ***juhusliku kaotsimineku või muutmise eest***;	b) ***tagada, et teenustele***, ***funktsioonidele ja andmetele pääsevad juurde ja neid saavad kasutada üksnes volitatud isikud*** ja***/või volitatud süsteemid ja programmid***;

Muudatusettepanek 173

Ettepanek võtta vastu määrus
Artikkel 45 – lõik 1 – punkt c

Komisjoni ettepanek	*Muudatusettepanek*
(c) tagada, et ***volitatud kasutajatel***, ***programmidel ja masinatel oleks juurdepääs üksnes neile andmetele, teenustele või funktsioonidele, millele neil on juurdepääsuõigused***;	c) tagada, et ***kehtestatud on protsess***, ***millega tehakse kindlaks ja dokumenteeritakse IKT toodete, protsesside ja teenuste kõik sõltuvusseosed ja teadaolevad turvanõrkused***;

Muudatusettepanek 174

Ettepanek võtta vastu määrus
Artikkel 45 – lõik 1 – punkt d

Komisjoni ettepanek	*Muudatusettepanek*
(d) ***talletada***, ***milliseid andmeid***,	d) ***tagada***, ***et IKT toodetel***, ***protsessidel***

teenuseid või funktsioone on edastatud, millal ja kelle poolt;	***ja teenustel ei ole teadaolevaid turvanõrkusi***;

Muudatusettepanek 175

Ettepanek võtta vastu määrus
Artikkel 45 – lõik 1 – punkt e

Komisjoni ettepanek	*Muudatusettepanek*
(e) tagada ***võimalus kontrollida***, ***millal ja kes*** on ***pääsenud juurde millistele andmetele***, ***teenustele või funktsioonidele või neid kasutanud***;	e) tagada, ***et kehtestatud*** on ***protsess IKT toodete***, ***protsesside ja teenuste uute avastatud turvanõrkuste kõrvaldamiseks***;

Muudatusettepanek 176

Ettepanek võtta vastu määrus
Artikkel 45 – lõik 1 – punkt f

Komisjoni ettepanek	*Muudatusettepanek*
(f) ***taastada füüsilise või tehnilise intsidendi korral õigeaegselt andmete***, ***teenuste*** ja ***funktsioonide käideldavus*** ja ***juurdepääs neile***;	f) ***tagada, et IKT tooted***, ***protsessid*** ja ***teenused on vaikimisi*** ja ***sisseprojekteeritult turvalised***;

Muudatusettepanek 177

Ettepanek võtta vastu määrus
Artikkel 45 – lõik 1 – punkt g

Komisjoni ettepanek	*Muudatusettepanek*
(g) tagada, et IKT tooteid ja teenuseid pakutakse ajakohastatud tarkvaraga, mis ei sisalda teadaolevaid turvaauke, ning et olemas on mehhanismid turvaliseks tarkvara uuendamiseks***.***	g) tagada, et IKT tooteid ja teenuseid pakutakse ajakohastatud tarkvaraga, mis ei sisalda teadaolevaid turvaauke, ning et olemas on mehhanismid turvaliseks tarkvara uuendamiseks***;***

Muudatusettepanek 178

Ettepanek võtta vastu määrus
Artikkel 45 – lõik 1 – punkt g a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ga) tagada, et muud küberintsidentidega seotud ohud, nagu oht elule, tervisele, keskkonnale ja muudele olulistele õiguslikele huvidele, on minimaalsed.

Muudatusettepanek 179

Ettepanek võtta vastu määrus
Artikkel 46 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Euroopa küberturvalisuse sertifitseerimise kavas määratakse selle kava raames sertifitseeritud IKT toodetele ja teenustele üks või mitu järgmist usaldusväärsuse taset: baastase, märkimisväärne ja/või kõrge tase.	1. Euroopa küberturvalisuse sertifitseerimise kavas määratakse selle kava raames sertifitseeritud IKT toodetele***,*** ***protsessidele*** ja teenustele ***vastavalt kontekstile ja nende ettenähtud kasutusele*** üks või mitu järgmist ***riskipõhist*** usaldusväärsuse taset: baastase, märkimisväärne ja/või kõrge tase.

Muudatusettepanek 180

Ettepanek võtta vastu määrus
Artikkel 46 – lõige 2 – punkt a

Komisjoni ettepanek	*Muudatusettepanek*
(a) usaldusväärsuse baastase ***osutab Euroopa küberturvalisuse sertifitseerimise kava raames väljastatud sertifikaadile, mis annab piiratud usalduse*** IKT toote ***või*** teenuse ***väidetavate või kinnitatud küberturvalisuse omaduste vastu ning mille kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele***, ***standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk*** on ***vähendada küberturvalisuse intsidentide riski***;	a) usaldusväärsuse baastase ***vastab kombineeritud tõenäosuse ja kahju puhul väikesele riskile*** IKT toote***, protsessi ja*** teenuse ***suhtes, arvestades toote, protsessi või teenuse ettenähtud kasutust ja konteksti. Usaldusväärsuse baastase annab kindlustunde***, ***et küberintsidentide teadaolevatele põhiriskidele*** on ***võimalik vastu pidada***;

Muudatusettepanek 181

Ettepanek võtta vastu määrus
Artikkel 46 – lõige 2 – punkt b

Komisjoni ettepanek	*Muudatusettepanek*
(b) märkimisväärne usaldusväärsuse tase ***osutab Euroopa küberturvalisuse sertifitseerimise kava raames väljastatud sertifikaadile, mis annab märkimisväärse usalduse*** IKT toote ***või*** teenuse ***väidetavate või kinnitatud küberturvalisuse omaduste vastu ning mille kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk*** on ***vähendada märkimisväärselt küberturvalisuse intsidentide riski***;	b) märkimisväärne usaldusväärsuse tase ***vastab kombineeritud tõenäosuse ja kahju puhul suuremale riskile*** IKT toote***, protsessi ja*** teenuse ***suhtes. Märkimisväärne usaldusväärsuse tase annab kindlustunde, et küberintsidentide teadaolevaid riske on võimalik ennetada ning et ka piiratud vahenditega toime pandavatele küberrünnetele*** on ***võimalik vastu pidada***;

Muudatusettepanek 182

Ettepanek võtta vastu määrus
Artikkel 46 – lõige 2 – punkt c

Komisjoni ettepanek	*Muudatusettepanek*
(c) kõrge usaldusväärsuse tase ***osutab Euroopa küberturvalisuse sertifitseerimise kava raames väljastatud sertifikaadile***, ***mis annab kõrgema usalduse IKT toote või*** teenuse ***väidetavate või kinnitatud küberturvalisuse omaduste vastu kui märkimisväärse*** usaldusväärsuse ***tasemega sertifikaat ning mille kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk*** on ***vältida küberturvalisuse intsidente***.	c) kõrge usaldusväärsuse tase ***vastab kahju puhul suurele riskile IKT toote***, ***protsessi ja*** teenuse ***suhtes. Kõrge*** usaldusväärsuse ***tase annab kindlustunde, et küberintsidentide riske on võimalik ennetada ning et ka uusimatele märkimisväärsete vahenditega toime pandavatele küberrünnetele*** on ***võimalik vastu pidada***.

Muudatusettepanek 183

Ettepanek võtta vastu määrus
Artikkel 46 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Artikkel 46a
	Euroopa küberturvalisuse sertifitseerimise kavade usaldusväärsuse tasemete hindamine
	1. Usaldusväärsuse baastaseme korral võib IKT toodete tootja või pakkuja, IKT protsesside pakkuja ja IKT teenuste osutaja teha nõuetele vastavuse hindamise omal vastutusel ise.
	2. Märkimisväärse usaldusväärsuse taseme korral juhindutakse hindamisel vähemalt toote, protsessi või teenuse turvafunktsioonide tehnilisele dokumentatsioonile vastavuse kontrollimisest.
	3. Kõrge usaldusväärsuse taseme hindamismetoodika põhineb vähemalt tõhususe kontrollimisel, mille käigus hinnatakse turvafunktsioonide võimet pidada vastu märkimisväärsete vahendite abil toime pandavatele küberrünnetele.

Muudatusettepanek 184

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt a

Komisjoni ettepanek	*Muudatusettepanek*
(a) sertifitseerimise sisu ja ulatus, sealhulgas hõlmatud IKT toodete ja teenuste liik või kategooria;	a) sertifitseerimise sisu ja ulatus, sealhulgas hõlmatud IKT toodete***,*** ***protsesside*** ja teenuste liik või kategooria;

Muudatusettepanek 185

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt a a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	aa) ulatus ja küberturvalisuse nõuded; vajaduse korral kajastavad ulatus ja nõuded nende riiklike küberturvalisuse sertifitseerimiste ulatust ja nõudeid, mida kava asendab või mis on sätestatud õigusaktides;

Muudatusettepanek 186

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt a b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ab) sertifitseerimiskava kehtivusaeg;

Muudatusettepanek 187

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt b

Komisjoni ettepanek	*Muudatusettepanek*
(b) konkreetsete IKT toodete ja teenuste puhul hinnatavate küberturvalisuse nõuete üksikasjalik kirjeldus , näiteks viidates ***liidu*** või rahvusvahelistele standarditele või tehnilistele kirjeldustele;	b) konkreetsete IKT toodete***,*** ***protsesside*** ja teenuste puhul hinnatavate küberturvalisuse nõuete üksikasjalik kirjeldus, näiteks viidates ***Euroopa*** või rahvusvahelistele standarditele***, tehnilistele kirjeldustele*** või ***IKT*** tehnilistele kirjeldustele; ***nõuded on kindlaks määratud nii, et asjaomase sertifitseerimise saab lisada tootja süstemaatilistesse turvalisuse protsessidesse, mida järgitakse asjaomase toote või teenuse väljatöötamisel ja olelusringi vältel, või see võib nendel protsessidel põhineda;***

Muudatusettepanek 188

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt b a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ba) teave teadaolevate küberohtude kohta, mida sertifitseerimine ei hõlma, ja nendega toimetulemise juhised;

Muudatusettepanek 189

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt c

Komisjoni ettepanek	*Muudatusettepanek*
(c) vajaduse korral üks või mitu usaldusväärsuse taset;	c) vajaduse korral üks või mitu usaldusväärsuse taset***, võttes muu hulgas arvesse riskipõhist lähenemisviisi***;

Muudatusettepanek 190

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt c a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ca) teave selle kohta, kas kava raames on lubatud nõuetele vastavust ise hinnata, ja vastavushindamise või ettevõtja vastavuskinnituse või mõlema suhtes kohaldatav menetlus;

Muudatusettepanek 191

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt d

Komisjoni ettepanek	*Muudatusettepanek*
(d) konkreetsed hindamiskriteeriumid ***ja meetodid***, ***sealhulgas hindamise*** liigid***, mida kasutati*** tõendamaks, et artiklis 45 osutatud konkreetsed eesmärgid on	d) konkreetsed hindamiskriteeriumid, ***vastavushindamise*** liigid ***ja meetodid,*** tõendamaks, et artiklis 45 osutatud konkreetsed eesmärgid on täidetud;

täidetud;

Muudatusettepanek 192

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt e

Komisjoni ettepanek	*Muudatusettepanek*
(e) sertifitseerimiseks vajalik teave, mille taotleja peab esitama vastavushindamisasutustele;	e) sertifitseerimiseks vajalik teave, mille taotleja peab esitama vastavushindamisasutustele;

Muudatusettepanek 193

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt f

Komisjoni ettepanek	*Muudatusettepanek*
(f) ***kui kava näeb ette märgi või märgistuse, tingimused sellise märgi või märgistuse kasutamiseks***;	f) ***küberturvalisuse teave vastavalt käesoleva määruse artiklile 47a***;

Muudatusettepanek 194

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt g

Komisjoni ettepanek	*Muudatusettepanek*
(g) ***kui kava osaks on järelevalve,*** eeskirjad sertifikaatide nõuete täitmise kontrollimiseks, sealhulgas mehhanismid tõestamaks konkreetsete küberturvalisuse nõuete jätkuvat täitmist;	g) eeskirjad sertifikaatide nõuete täitmise kontrollimiseks, sealhulgas mehhanismid tõestamaks konkreetsete küberturvalisuse nõuete jätkuvat täitmist;

Muudatusettepanek 195

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt h

Komisjoni ettepanek	*Muudatusettepanek*
(h) tingimused ***sertifitseerimise***	h) tingimused ***sertifikaadi***

võimaldamiseks, säilitamiseks, jätkamiseks ***ning sertifitseerimise*** ulatuse laiendamiseks ja vähendamiseks;	***väljastamiseks***, säilitamiseks, jätkamiseks ***ja läbivaatamiseks, sertifikaadi*** ulatuse laiendamiseks ja vähendamiseks ***ning sertifikaadi kehtivusaeg***;

Muudatusettepanek 196

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt h a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ha) eeskirjad pärast sertifikaadi väljastamist tekkida võivate turvanõrkuste kõrvaldamiseks, kehtestades dünaamilise ja pideva organisatsioonilise protsessi, mis hõlmab nii pakkujaid kui ka kasutajaid;

Muudatusettepanek 197

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt i

Komisjoni ettepanek	*Muudatusettepanek*
(i) eeskirjad sertifitseeritud IKT toodete ja teenuste sertifitseerimistingimustele mittevastavuse tagajärgede kohta;	i) eeskirjad ***ettevõtja hinnatud ja*** sertifitseeritud IKT toodete ja teenuste sertifitseerimistingimustele mittevastavuse tagajärgede kohta;

Muudatusettepanek 198

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt j

Komisjoni ettepanek	*Muudatusettepanek*
(j) eeskirjad selle kohta, kuidas tuleks IKT toodete ja teenuste ***varem avastamata*** küberturvalisuse nõrkustest ***teada anda*** ja kuidas neid menetleda;	j) eeskirjad selle kohta, kuidas tuleks ***teada anda*** IKT toodete ja teenuste küberturvalisuse nõrkustest***, mis ei ole üldsusele teada,*** ja kuidas neid ***pärast nende avastamist*** menetleda;

Muudatusettepanek 199

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt l

Komisjoni ettepanek	*Muudatusettepanek*
*(*l) sama liiki või kategooriasse kuuluvaid IKT tooteid või teenuseid hõlmavate riiklike küberturvalisuse sertifitseerimise kavade kindlakstegemine;	l) sama liiki või kategooriasse kuuluvaid IKT tooteid***, *protsesse*** või teenuseid***, turvalisuse nõudeid ning hindamiskriteeriumeid ja -meetodeid*** hõlmavate riiklike ***või rahvusvaheliste*** küberturvalisuse sertifitseerimise kavade kindlakstegemine;

Muudatusettepanek 200

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – punkt m a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ma) tingimused sertifitseerimiskavade vastastikuseks tunnustamiseks kolmandate riikidega.

Muudatusettepanek 201

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	1a. Hooldusprotsessid, mis toovad kaasa väiksemad uuendused, ei muuda sertifikaati kehtetuks, kui sellised uuendused ei avalda olulist kahjulikku mõju IKT toote, protsessi või teenuse turvalisusele.

Muudatusettepanek 202

Ettepanek võtta vastu määrus
Artikkel 47 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Artikkel 47a
	Sertifitseeritud toodete, protsesside ja teenuste küberturvalisuse teave
	1. Käesoleva määruse kohase sertifitseerimiskavaga hõlmatud IKT toodete tootja või pakkuja, IKT protsesside pakkuja või IKT teenuste osutaja esitab lõppkasutajale elektroonilise või paberdokumendi, mis sisaldab vähemalt järgmist teavet: IKT toote, protsessi ja teenuse ettenähtud kasutusega seotud ja sertifikaadiga tagatud usaldusväärsuse tase; nende riskide kirjeldus, millele vastupidamise suhtes sertifikaat peaks kindlustunde tagama; soovitused selle kohta, kuidas kasutajad saavad uuenduste järel suurendada toote, protsessi või teenuse küberturvalisust, eeskirjadele vastavust ja toetusperioodi; vajaduse korral teave selle kohta, kuidas kasutajad saavad ründe korral säilitada toote, protsessi või teenuse põhiomadusi.
	2. Käesoleva artikli lõikes 1 osutatud dokument peab olema kättesaadav kogu toote, protsessi või teenuse olelusringi ajal kuni need on turul kättesaadavad, kuid vähemalt viis aastat.
	3. Komisjon võtab vastu rakendusaktid, millega kehtestatakse dokumendi vorm. Komisjon võib paluda ametilt ettevalmistava vormi esitamist. Nimetatud rakendusaktid võetakse vastu kooskõlas käesoleva määruse artiklis 55 osutatud kontrollimenetlusega.

Muudatusettepanek 203

Ettepanek võtta vastu määrus
Artikkel 48 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Kui IKT tooted ja teenused on sertifitseeritud Euroopa küberturvalisuse sertifitseerimise kava kohaselt, mis on vastu võetud kooskõlas artikliga 44, eeldatakse, et nad vastavad sellise kava nõuetele.	1. Kui IKT tooted***, protsessid*** ja teenused on sertifitseeritud Euroopa küberturvalisuse sertifitseerimise kava kohaselt, mis on vastu võetud kooskõlas artikliga 44, eeldatakse, et nad vastavad sellise kava nõuetele.

Muudatusettepanek 204

Ettepanek võtta vastu määrus
Artikkel 48 – lõige 4 – sissejuhatav osa

Komisjoni ettepanek	*Muudatusettepanek*
4. Erandina lõikest 3 ***võib*** nõuetekohaselt põhjendatud juhtudel teatavas Euroopa küberturvalisuse sertifitseerimise kavas ette näha, et sellest kavast tuleneva Euroopa küberturvalisuse sertifikaadi võib välja anda üksnes avalik-õiguslik asutus. Selline avalik-õiguslik asutus on ***üks järgnevatest asutustest:***	4. Erandina lõikest 3 ***ja vaid*** nõuetekohaselt põhjendatud juhtudel***, näiteks riikliku julgeoleku kaalutlustel, võib*** teatavas Euroopa küberturvalisuse sertifitseerimise kavas ette näha, et sellest kavast tuleneva Euroopa küberturvalisuse sertifikaadi võib välja anda üksnes avalik-õiguslik asutus. Selline avalik-õiguslik asutus on ***käesoleva määruse artikli 51 lõike 1 kohaselt vastavushindamisasutusena akrediteeritud asutus. Füüsiline või juriidiline isik, kes esitab oma IKT tooted või teenused sertifitseerimiseks, peab tegema artiklis 51 osutatud vastavushindamisasutusele kättesaadavaks kogu sertifitseerimismenetluse läbiviimiseks vajaliku teabe.***

Muudatusettepanek 205

Ettepanek võtta vastu määrus
Artikkel 48 – lõige 5

Komisjoni ettepanek	*Muudatusettepanek*
5. Füüsiline või juriidiline isik, kes esitab oma IKT tooted või ***teenused*** sertifitseerimiseks, peab esitama artiklis 51 osutatud vastavushindamisasutusele kogu sertifitseerimismenetluse läbiviimiseks vajaliku teabe.	5. Füüsiline või juriidiline isik, kes esitab oma IKT tooted***, teenused*** või ***protsessid*** sertifitseerimiseks, peab esitama artiklis 51 osutatud vastavushindamisasutusele kogu sertifitseerimismenetluse läbiviimiseks vajaliku teabe***, sealhulgas teabe kõigi teadaolevate turvanõrkuste kohta. IKT toote, teenuse või protsessi saab esitada hindamiseks ükskõik millisele artiklis 51 osutatud vastavushindamisasutusele***.

Muudatusettepanek 206

Ettepanek võtta vastu määrus
Artikkel 48 – lõige 6

Komisjoni ettepanek	*Muudatusettepanek*
6. Sertifikaat antakse maksimaalselt ***kolmeks*** aastaks ja selle kehtivust võib pikendada samadel tingimustel senikaua, kuni asjakohased nõuded on täidetud.	6. Sertifikaat antakse maksimaalselt ***perioodiks, mis määratakse kindlaks iga kava puhul eraldi, arvestades mõistlikku olelusringi, kuid igal juhul mitte rohkem kui viieks*** aastaks***,*** ja selle kehtivust võib pikendada samadel tingimustel senikaua, kuni asjakohased nõuded on täidetud.

Selgitus

See tagab paindlikkuse, et kohandada kehtivusaega ettenähtud kasutusega.

Muudatusettepanek 207

Ettepanek võtta vastu määrus
Artikkel 48 – lõige 7

Komisjoni ettepanek	*Muudatusettepanek*
7. Käesoleva artikli kohaselt välja antud Euroopa küberturvalisuse sertifikaati	7. Käesoleva artikli kohaselt välja antud Euroopa küberturvalisuse sertifikaati tunnustatakse kõigis liikmesriikides ***selle***

tunnustatakse kõigis liikmesriikides.	***sertifikaadiga hõlmatud IKT toodete ja protsesside ning tarbeelektroonikaseadmetega seotud kohalikele küberturvalisuse nõuetele vastavana, võttes arvesse artiklis 46 osutatud konkreetset usaldusväärsuse taset, ning keelatud on diskrimineerimine nende sertifikaatide päritoluliikmesriigi või selle välja andnud, artiklis 51 osutatud vastavushindamisasutuse alusel***.

Selgitus

Et vältida killustatust Euroopa küberturvalisuse sertifitseerimise kavade tunnustamises ja/või vastavuses, tuleb selles artiklis rõhutada, et keelatud on diskrimineerimine sertifikaadi väljaandmise koha alusel.

Muudatusettepanek 208

Ettepanek võtta vastu määrus
Artikkel 48 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Artikkel 48a
	Oluliste teenuste operaatorite sertifitseerimiskavad
	1. Kui Euroopa küberturvalisuse sertifitseerimise kavad on võetud vastu käesoleva artikli lõike 2 kohaselt, kasutavad oluliste teenuste operaatorid direktiivi (EL) 2016/1148 artiklis 14 sätestatud turvanõuete täitmiseks kõnealuste sertifitseerimiskavadega hõlmatud tooteid, protsesse ja teenuseid.
	2. Hiljemalt [üks aasta pärast käesoleva määruse jõustumist] võtab komisjon pärast direktiivi (EL) 2016/1148 artiklis 11 osutatud koostöörühmaga konsulteerimist kooskõlas artikliga 55a vastu delegeeritud õigusaktid käesoleva määruse täiendamiseks, loetledes nende toodete, protsesside ja teenuste kategooriad, mis vastavad mõlemale järgmisele kriteeriumile:
	a) need on ette nähtud kasutamiseks

oluliste teenuste operaatoritele ja

b) nende mittenõuetekohane toimimine häiriks oluliselt olulise teenuse osutamist.

3. Komisjon võtab kooskõlas artikliga 55a vastu delegeeritud õigusaktid käesoleva määruse muutmiseks, ajakohastades vajaduse korral käesoleva artikli lõikes 3 osutatud toodete, protsesside ja teenuste kategooriate loetelu.

4. Komisjon palub ametil koostada kooskõlas käesoleva määruse artikli 44 lõikega -1 Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava käesoleva artikli lõigetes 2 ja 3 osutatud toodete, protsesside ja teenuste kategooriatele niipea, kui kõnealune loetelu on vastu võetud või seda on ajakohastatud. Selliste Euroopa küberturvalisuse sertifitseerimise kavade kohaselt välja antud sertifikaatidega tagatud usaldusväärsuse tase on kõrge.

Muudatusettepanek 209

Ettepanek võtta vastu määrus
Artikkel 48 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Artikkel 48b
	Euroopa küberturvalisuse sertifitseerimise kavade suhtes ametlike vastuväidete esitamine
	1. Kui liikmesriik on seisukohal, et Euroopa küberturvalisuse sertifitseerimise kava ei vasta täielikult nõuetele, millele ta peab eesmärgi kohaselt vastama ja mis on sätestatud liidu asjaomastes ühtlustamisõigusaktides, teatab ta sellest komisjonile ja esitab üksikasjaliku selgituse. Komisjon otsustab vajaduse korral pärast liidu asjaomase ühtlustamisõigusakti kohaselt loodud komiteega või valdkonna ekspertidega

muus vormis konsulteerimist, kas

a) avaldada Euroopa Liidu Teatajas viited asjaomasele Euroopa küberturvalisuse sertifitseerimise kavale, jätta need avaldamata või avaldada piiranguga;

b) säilitada Euroopa Liidu Teatajas viited asjaomasele Euroopa küberturvalisuse sertifitseerimise kavale, säilitada need piiranguga või kõrvaldada.

2. Komisjon avaldab oma veebisaidil teabe Euroopa küberturvalisuse sertifitseerimise kavade kohta, mille kohta on tehtud käesoleva artikli lõikes 1 osutatud otsus.

3. Komisjon teavitab ametit käesoleva artikli lõikes 1 nimetatud otsusest ja taotleb vajaduse korral asjaomase Euroopa küberturvalisuse sertifitseerimise kava läbivaatamist.

4. Käesoleva artikli lõike 1 punktis a osutatud otsus võetakse vastu kooskõlas käesoleva määruse artikli 55 lõikes 2 osutatud nõuandemenetlusega.

5. Käesoleva artikli lõike 1 punktis b osutatud otsus võetakse vastu kooskõlas käesoleva määruse artikli 55 lõikes 2a osutatud kontrollimenetlusega.

Muudatusettepanek 210

Ettepanek võtta vastu määrus
Artikkel 49 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Ilma et see piiraks lõike 3 kohaldamist, lõpeb riiklike küberturvalisuse sertifitseerimise kavade ja Euroopa küberturvalisuse sertifitseerimise kavaga hõlmatud IKT toodete ja teenustega seotud menetluste õiguslik toime artikli 44 lõike 4 kohaselt vastu võetud rakendusaktis sätestatud kuupäeval. Olemasolevad riiklikud küberturvalisuse sertifitseerimise kavad ja Euroopa küberturvalisuse	1. Ilma et see piiraks lõike 3 kohaldamist, lõpeb riiklike küberturvalisuse sertifitseerimise kavade ja Euroopa küberturvalisuse sertifitseerimise kavaga hõlmatud IKT toodete***, protsesside*** ja teenustega seotud menetluste õiguslik toime artikli 44 lõike 4 kohaselt vastu võetud rakendusaktis sätestatud kuupäeval. Olemasolevad riiklikud küberturvalisuse sertifitseerimise kavad ja Euroopa

sertifitseerimise kavaga hõlmamata IKT toodete ja teenustega seotud menetlused jäävad alles.	küberturvalisuse sertifitseerimise kavaga hõlmamata IKT toodete***, protsesside*** ja teenustega seotud menetlused jäävad alles.

Muudatusettepanek 211

Ettepanek võtta vastu määrus
Artikkel 49 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Liikmesriigid ei kehtesta uusi riiklikke küberturvalisuse sertifitseerimise kavasid IKT toodetele ja teenustele, mis on kaetud kehtiva Euroopa küberturvalisuse sertifitseerimise kavaga.	2. Liikmesriigid ei kehtesta uusi riiklikke küberturvalisuse sertifitseerimise kavasid IKT toodetele***, protsessidele*** ja teenustele, mis on kaetud kehtiva Euroopa küberturvalisuse sertifitseerimise kavaga.

Muudatusettepanek 212

Ettepanek võtta vastu määrus
Artikkel 49 – lõige 3 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	3a. Liikmesriigid teavitavad komisjoni kõigist riiklike küberturvalisuse sertifitseerimise kavade koostamise taotlustest ja esitavad nende kehtestamise põhjused.

Muudatusettepanek 213

Ettepanek võtta vastu määrus
Artikkel 49 – lõige 3 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	3b. Liikmesriigid saadavad teistele liikmesriikidele, ametile ja komisjonile taotluse korral ja vähemalt elektroonilises vormis riiklike küberturvalisuse sertifitseerimise kavade projektid.

Muudatusettepanek 214

Ettepanek võtta vastu määrus
Artikkel 49 – lõige 3 c (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	3c. Ilma et see piiraks direktiivi (EL) 2015/1535 kohaldamist, peavad liikmesriigid vastama teiselt liikmesriigilt, ametilt või komisjonilt käesoleva artikli lõikes 3b osutatud projektide kohta saadud märkustele kolme kuu jooksul ja võtma neid nõuetekohaselt arvesse.

Muudatusettepanek 215

Ettepanek võtta vastu määrus
Artikkel 49 – lõige 3 d (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	3d. Kui käesoleva artikli lõike 3c kohaselt saadud märkustes osutatakse, et riikliku küberturvalisuse sertifitseerimise kava projektil on tõenäoliselt negatiivne mõju siseturu nõuetekohasele toimimisele, peab vastuvõttev liikmesriik enne kava projekti vastuvõtmist konsulteerima ameti ja komisjoniga ning võtma nende märkusi võimalikult suurel määral arvesse.

Muudatusettepanek 216

Ettepanek võtta vastu määrus
Artikkel 50 – lõige 5

Komisjoni ettepanek	*Muudatusettepanek*
5. Määruse tõhusaks rakendamiseks on asjakohane, et need asutused osaleksid aktiivselt, tõhusalt, tulemuslikult ja turvaliselt artikli 53 kohaselt asutatud ***Euroopa küberturvalisuse sertifitseerimise rühma*** töös.	5. Määruse tõhusaks rakendamiseks on asjakohane, et need asutused osaleksid aktiivselt, tõhusalt, tulemuslikult ja turvaliselt artikli 53 kohaselt asutatud ***liikmesriikide sertifitseerimisrühma*** töös.

Muudatusettepanek 217

Ettepanek võtta vastu määrus
Artikkel 50 – lõige 6 – punkt a

Komisjoni ettepanek	*Muudatusettepanek*
(a) jälgivad käesoleva jaotise sätete kohaldamist riiklikul tasandil ja tagavad nende täitmise ning ***teevad järelevalvet*** nende riigi territooriumil asutatud vastavushindamisasutuse poolt välja antud sertifikaatide ***vastavuse üle*** käesolevas jaotises ja vastavas Euroopa küberturvalisuse ***sertifikaadi*** kavas sätestatud nõuetele;	a) jälgivad käesoleva jaotise sätete kohaldamist riiklikul tasandil ja tagavad nende täitmise ning ***kontrollivad kooskõlas eeskirjadega, mille Euroopa küberturvalisuse sertifitseerimise rühm on võtnud vastu vastavalt artikli 53 lõike 3 punktile da,***
	i) nende riigi territooriumil asutatud vastavushindamisasutuse poolt välja antud sertifikaatide ***vastavust*** käesolevas jaotises ja vastavas Euroopa küberturvalisuse ***sertifitseerimise*** kavas sätestatud nõuetele***, ja***
	ii) ettevõtja vastavuskinnituste vastavust, mis on esitatud kava alusel IKT protsessi, toote või teenuse kohta;

Muudatusettepanek 218

Ettepanek võtta vastu määrus
Artikkel 50 – lõige 6 – punkt b

Komisjoni ettepanek	*Muudatusettepanek*
(b) jälgivad ja kontrollivad vastavushindamisasutuste tegevust käesoleva määruse kohaldamisel, sealhulgas seoses käesoleva määruse artiklis 52 sätestatud vastavushindamisasutustest teavitamise ja sellega seotud ülesannetega;	b) jälgivad ja kontrollivad ***ning hindavad vähemalt iga kahe aasta järel*** vastavushindamisasutuste tegevust käesoleva määruse kohaldamisel, sealhulgas seoses käesoleva määruse artiklis 52 sätestatud vastavushindamisasutustest teavitamise ja sellega seotud ülesannetega;

Muudatusettepanek 219

Ettepanek võtta vastu määrus
Artikkel 50 – lõige 6 – punkt b a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ba) teevad auditeid, tagamaks et liidus kohaldatakse võrdväärseid standardeid, ning esitavad tulemused ametile ja sertifitseerimisrühmale;

Selgitus

See aitab tagada, et kogu ELis on teenused ja kvaliteet ühesugusel tasemel, ning vältida soodsamate sertifitseerimistingimuste valimise võimalust.

Muudatusettepanek 220

Ettepanek võtta vastu määrus
Artikkel 50 – lõige 6 – punkt c

Komisjoni ettepanek	*Muudatusettepanek*
(c) käsitlevad füüsiliste või juriidiliste isikute esitatud kaebusi seoses nende riigi territooriumil asutatud vastavushindamisasutuste väljastatud sertifikaatidega, uurivad asjakohasel määral kaebuse sisu ja teavitavad kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest;	c) käsitlevad füüsiliste või juriidiliste isikute esitatud kaebusi seoses nende riigi territooriumil asutatud vastavushindamisasutuste väljastatud sertifikaatidega ***või ettevõtja tehtud vastavushindamistega***, uurivad asjakohasel määral kaebuse sisu ja teavitavad kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest;

Muudatusettepanek 221

Ettepanek võtta vastu määrus
Artikkel 50 – lõige 6 – punkt c a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ca) esitavad punktis a osutatud kontrollimise ja punktis b osutatud hindamise tulemused ametile ja Euroopa küberturvalisuse sertifitseerimise rühmale;

Muudatusettepanek 222

Ettepanek võtta vastu määrus
Artikkel 50 – lõige 6 – punkt d

Komisjoni ettepanek	*Muudatusettepanek*
(d) teevad koostööd teiste riiklike sertifitseerimise järelevalveasutuste või muude avaliku sektori asutusega, sealhulgas jagades teavet IKT toodete ja teenuste võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade nõuetele;	d) teevad koostööd teiste riiklike sertifitseerimise järelevalveasutuste või muude avaliku sektori asutusega, ***näiteks riiklike andmekaitse järelevalveasutustega,*** sealhulgas jagades teavet IKT toodete***, protsesside*** ja teenuste võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade nõuetele;

Muudatusettepanek 223

Ettepanek võtta vastu määrus
Artikkel 50 – lõige 6 – punkt d

Komisjoni ettepanek	*Muudatusettepanek*
(d) teevad koostööd teiste riiklike sertifitseerimise järelevalveasutuste või muude avaliku sektori asutusega, sealhulgas jagades teavet IKT toodete ja teenuste võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa ***küberturvalisuse*** sertifitseerimise kavade nõuetele;	d) teevad koostööd teiste riiklike sertifitseerimise järelevalveasutuste või muude avaliku sektori asutusega, ***näiteks riiklike andmekaitse järelevalveasutustega,*** sealhulgas jagades teavet IKT toodete ja teenuste võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa ***IT-turvalisuse*** sertifitseerimise kavade nõuetele;

Selgitus

Tuginedes Euroopa Andmekaitseinspektori arvamusele.

Muudatusettepanek 224

Ettepanek võtta vastu määrus
Artikkel 50 – lõige 7 – punkt c a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ca) tunnistada kehtetuks selliste vastavushindamisasutuste

	akrediteerimine, mis ei vasta käesoleva määruse nõuetele;

Muudatusettepanek 225

Ettepanek võtta vastu määrus
Artikkel 50 – lõige 7 – punkt e

Komisjoni ettepanek	*Muudatusettepanek*
(e) võtta ***siseriiklike*** õigusaktide kohaselt tagasi sertifikaadid, mis ei ole kooskõlas käesoleva määrusega või Euroopa küberturvalisuse sertifitseerimise kavaga;	e) võtta ***riigisiseste*** õigusaktide kohaselt tagasi sertifikaadid, mis ei ole kooskõlas käesoleva määrusega või Euroopa küberturvalisuse sertifitseerimise kavaga***, ning teavitada sellest riiklikke akrediteerimisasutusi***;

Muudatusettepanek 226

Ettepanek võtta vastu määrus
Artikkel 50 – lõige 8

Komisjoni ettepanek	*Muudatusettepanek*
8. Riiklikud sertifitseerimise järelevalveasutused teevad omavahel ja komisjoniga koostööd ning vahetavad eelkõige teavet, kogemusi ja häid tavasid seoses küberturvalisuse sertifitseerimisega ning IKT toodete ja teenuste küberturvalisust puudutavate tehniliste küsimustega.	8. Riiklikud sertifitseerimise järelevalveasutused teevad omavahel ja komisjoniga koostööd ning vahetavad eelkõige teavet, kogemusi ja häid tavasid seoses küberturvalisuse sertifitseerimisega ning IKT toodete***, protsesside*** ja teenuste küberturvalisust puudutavate tehniliste küsimustega.

Muudatusettepanek 227

Ettepanek võtta vastu määrus
Artikkel 50 – lõige 8 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	8a. Kõik riiklikud sertifitseerimise järelevalveasutused ning riikliku sertifitseerimise järelevalveasutuse liikmed ja töötajad on kooskõlas liidu või liikmesriigi õigusega kohustatud nii oma ametiajal kui ka pärast ametist lahkumist

hoidma ametisaladust konfidentsiaalse teabe suhtes, mis on neile teatavaks saanud nende tööülesannete või volituste täitmisel.

Muudatusettepanek 228

Ettepanek võtta vastu määrus
Artikkel 50 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Artikkel 50a
	Vastastikune eksperdihinnang
	1. Riiklike sertifitseerimise järelevalveasutuste artikli 50 kohase tegevuse suhtes rakendatakse vastastikust hindamist, mille korraldab amet.
	2. Vastastikune hindamine toimub mõistlike ja läbipaistvate kriteeriumide ja menetluste alusel, mis käsitlevad eelkõige struktuuridele, inimressurssidele ja menetlustele esitatavaid nõudeid, konfidentsiaalsust ja kaebusi. Kaebuste esitamiseks kõnealuse hindamise tulemusel vastu võetud otsuste peale kehtestatakse asjakohased menetlused.
	3. Vastastikuse eksperdihinnangu raames hinnatakse riiklike sertifitseerimise järelevalveasutuste kehtestatud menetlusi, eeskätt neid, mille abil kontrollitakse sertifikaatide nõuetele vastavust, vastavushindamisasutuste tegevuse kontrollimise ja järelevalve menetlusi, töötajate pädevust, kontrollide ja inspekteerimismetoodika õigsust ning tulemuste õigsust. Vastastikuse eksperdihinnangu raames hinnatakse ka seda, kas asjaomastel riiklikel sertifitseerimise järelevalveasutustel on piisavad vahendid oma ülesannete nõuetekohaseks täitmiseks, nagu nõutakse artikli 50 lõikes 4.
	4. Riikliku sertifitseerimise järelevalveasutuse vastastikuse eksperdihinnangu annavad kaks muu

	liikmesriigi riiklikku sertifitseerimise järelevalveasutust ja komisjon ning seda tehakse vähemalt iga viie aasta järel. Amet võib vastastikuses eksperdihinnangus osaleda, kui ta riskianalüüsi põhjal nii otsustab.
	5. Komisjonil on õigus võtta kooskõlas artikliga 55a vastu delegeeritud õigusaktid käesoleva määruse täiendamiseks, kehtestades vastastikuste eksperdihinnangute kava vähemalt viieks aastaks, sätestades selles vastastikuse eksperdihinnangu rühma koosseisu kriteeriumid, hindamismetoodika, hindamiste ajakava, sageduse ja muud vastastikuse eksperdihinnanguga seotud ülesanded. Nende delegeeritud õigusaktide vastuvõtmisel võtab komisjon nõuetekohaselt arvesse liikmesriikide sertifitseerimisrühma arvamusi.
	6. Vastastikuse eksperdihinnangu tulemusi kontrollib liikmesriikide sertifitseerimisrühm. Amet koostab tulemuste kokkuvõtte ning vajaduse korral suunised ja parimaid tavasid käsitleva dokumendi ja avalikustab need.

Muudatusettepanek 229

Ettepanek võtta vastu määrus
Artikkel 51 – lõige 1 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	1a. Kõrge usaldusväärsuse taseme puhul peab vastavushindamisasutus olema lisaks akrediteeringule ka riikliku sertifitseerimise järelevalveasutuse poolt teatatud asutus tema pädevuse ja teadmiste põhjal küberturvalisuse hindamise valdkonnas. Riiklik sertifitseerimise järelevalveasutus kontrollib regulaarselt teatatud vastavushindamisasutuste pädevusi ja teadmisi.

Selgitus

Kõrge usaldusväärsuse tase eeldab tõhususe kontrollimist. Tõhususe kontrolle korraldavate vastavushindamisasutuste teadmisi ja pädevusi tuleb regulaarselt kontrollida, et tagada eeskätt katsete kvaliteet.

Muudatusettepanek 230

Ettepanek võtta vastu määrus
Artikkel 51 – lõige 2 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	2a. Et tagada võrdväärsete standardite kohaldamine liidus, tehakse auditeid, mille tulemused teatatakse ametile ja sertifitseerimisrühmale.

Muudatusettepanek 231

Ettepanek võtta vastu määrus
Artikkel 51 – lõige 2 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	2b. Kui tootjad otsustavad esitada vastavuse kohta käesoleva määruse artikli 48 lõike 3 kohase ettevõtja vastavuskinnituse, võtavad vastavushindamisasutused lisameetmeid, et kontrollida, milliseid ettevõttesiseseid menetlusi tootjad kasutasid, et tagada nende toodete ja/või teenuste vastavus Euroopa küberturvalisuse sertifitseerimise kava nõuetele.

Muudatusettepanek 232

Ettepanek võtta vastu määrus
Artikkel 52 – lõige 5

Komisjoni ettepanek	*Muudatusettepanek*
5. Komisjon võib määrata ***rakendusaktidega*** kindlaks käesoleva artikli lõikes 1 osutatud teavitamise asjaolud, vormingud ja menetlused.	5. Komisjon võib määrata ***delegeeritud õigusaktidega*** kindlaks käesoleva artikli lõikes 1 osutatud teavitamise asjaolud, vormingud ja menetlused. Kõnealused

Kõnealused ***rakendusaktid*** võetakse vastu vastavalt artikli 55 lõikes 2 osutatud kontrollimenetlusele.	***delegeeritud õigusaktid*** võetakse vastu vastavalt artikli 55 lõikes 2 osutatud kontrollimenetlusele.

Muudatusettepanek 233

Ettepanek võtta vastu määrus
Artikkel 53 – pealkiri

Komisjoni ettepanek	*Muudatusettepanek*
Euroopa küberturvalisuse sertifitseerimise rühm	***Liikmesriikide sertifitseerimisrühm***
	(Muudatusettepanekut kohaldatakse kogu teksti ulatuses. Selle vastuvõtmise korral tehakse vastavad muudatused kogu tekstis.)

Muudatusettepanek 234

Ettepanek võtta vastu määrus
Artikkel 53 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Luuakse ***Euroopa küberturvalisuse sertifitseerimise rühm (edaspidi „rühm“)***.	1. Luuakse ***liikmesriikide sertifitseerimisrühm***.

Muudatusettepanek 235

Ettepanek võtta vastu määrus
Artikkel 53 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. ***Rühm*** koosneb riiklikest sertifitseerimise järelevalveasutustest. Riiklikke sertifitseerimise järelevalveasutusi esindavad nende juhid või muud kõrgetasemelised esindajad.	2. ***Liikmesriikide sertifitseerimisrühm*** koosneb ***kõigi liikmesriikide*** riiklikest sertifitseerimise järelevalveasutustest. Riiklikke sertifitseerimise järelevalveasutusi esindavad nende juhid või muud kõrgetasemelised esindajad. ***Sidusrühmade sertifitseerimisrühma liikmeid võidakse kutsuda osalema sertifitseerimisrühma koosolekutel ning rühma töös.***

Muudatusettepanek 236

Ettepanek võtta vastu määrus
Artikkel 53 – lõige 3 – sissejuhatav osa

Komisjoni ettepanek	*Muudatusettepanek*
3. ***Rühmal*** on järgmised ülesanded:	3. ***Liikmesriikide sertifitseerimisrühmal*** on järgmised ülesanded:

Muudatusettepanek 237

Ettepanek võtta vastu määrus
Artikkel 53 – lõige 3 – punkt b

Komisjoni ettepanek	*Muudatusettepanek*
(b) abistada ja nõustada ***ENISAt*** ja teha temaga koostööd seoses ettevalmistava kava koostamisega kooskõlas käesoleva määruse artikliga 44;	b) abistada ja nõustada ***ametit*** ja teha temaga koostööd seoses ettevalmistava kava koostamisega kooskõlas käesoleva määruse artikliga 44;

Muudatusettepanek 238

Ettepanek võtta vastu määrus
Artikkel 53 – lõige 3 – punkt d a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	da) võtta vastu soovitused, millega määratakse kindlaks, kui sageli peavad riiklikud sertifitseerimise järelevalveasutused sertifikaate ja ettevõtjate tehtud vastavushindamisi kontrollima, ja selliste kontrollide kriteeriumid, ulatus ja kohaldamisala, ning võtta artikli 50 lõike 6 kohaselt vastu ühised aruandluseeskirjad ja -normid;

Muudatusettepanek 239

Ettepanek võtta vastu määrus
Artikkel 53 – lõige 3 – punkt e

Komisjoni ettepanek	*Muudatusettepanek*
(e) analüüsida küberturvalisuse sertifitseerimise valdkonna asjakohaseid arenguid ***ja*** vahetada häid tavasid seoses küberturvalisuse sertifitseerimise kavadega;	e) analüüsida küberturvalisuse sertifitseerimise valdkonna asjakohaseid arenguid ***ning*** vahetada ***teavet ja*** häid tavasid seoses küberturvalisuse sertifitseerimise kavadega;

Muudatusettepanek 240

Ettepanek võtta vastu määrus
Artikkel 53 – lõige 3 – punkt f a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	fa) hõlbustada Euroopa küberturvalisuse sertifitseerimise kavade kohandamist rahvusvaheliselt tunnustatud standarditele, sealhulgas olemasolevate kavade läbivaatamise abil, ja vajaduse korral esitada ametile soovitusi teha koostööd asjaomaste rahvusvaheliste standardiorganisatsioonidega, et kõrvaldada olemasolevate rahvusvaheliselt tunnustatud standardite puudused või lüngad;

Muudatusettepanek 241

Ettepanek võtta vastu määrus
Artikkel 53 – lõige 3 – punkt f b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	fb) luua vastastikuste eksperdihinnangute andmise menetlus. Menetluse puhul võetakse eelkõige arvesse riiklike sertifitseerimise järelevalveasutuste nõutavat tehnilist pädevust nende artiklites 48 ja 50 osutatud ülesannete täitmiseks ning see hõlmab vajaduse korral suuniste ja

	parimaid tavasid käsitlevate dokumentide koostamist, et parandada riiklike sertifitseerimise järelevalveasutuste vastavust käesolevale määrusele;

Muudatusettepanek 242

Ettepanek võtta vastu määrus
Artikkel 53 – lõige 3 – punkt f c (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	fc) teha järelevalvet sertifikaatide kontrollimise ja säilitamise üle;

Muudatusettepanek 243

Ettepanek võtta vastu määrus
Artikkel 53 – lõige 3 – punkt f d (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	fd) võtta arvesse ettevalmistava kava koostamisel kooskõlas artikliga 44 läbiviidud sidusrühmadega konsulteerimise tulemusi.

Muudatusettepanek 244

Ettepanek võtta vastu määrus
Artikkel 53 – lõige 4

Komisjoni ettepanek	*Muudatusettepanek*
4. Komisjon juhatab ***rühma*** ja osutab sellele sekretariaaditeenust, komisjoni abistab ***ENISA*** kooskõlas artikli 8 punktiga a.	4. Komisjon juhatab ***liikmesriikide sertifitseerimisrühma*** ja osutab sellele sekretariaaditeenust, komisjoni abistab ***amet*** kooskõlas artikli 8 punktiga a.

Muudatusettepanek 245

Ettepanek võtta vastu määrus
Artikkel 53 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Artikkel 53a
	Õigus kasutada tõhusat õiguskaitsevahendit järelevalveasutuse või vastavushindamisasutuse vastu
	1. Ilma et see piiraks ühegi muu halldusliku või kohtuvälise kaitsevahendi kohaldamist, on igal füüsilisel või juriidilisel isikul õigus kasutada tõhusat õiguskaitsevahendit
	a) vastavushindamisasutuse või riikliku sertifitseerimise järelevalveasutuse otsuse vastu, mis teda puudutab, sealhulgas vajaduse korral seoses Euroopa küberturvalisuse sertifikaadi väljastamise või väljastamata jätmise või talle kuuluva sertifikaadi tunnustamisega, ja
	b) juhul, kui riiklik sertifitseerimise järelevalveasutus ei vaata läbi asutuse pädevusse kuuluvat kaebust.
	2. Vastavushindamisasutuse või riikliku sertifitseerimise järelevalveasutuse vastu algatatakse menetlus selle liikmesriigi kohtus, kus vastavushindamisasutus või riiklik sertifitseerimise järelevalveasutus asub.

Muudatusettepanek 246

Ettepanek võtta vastu määrus
Artikkel 55 – lõige 2 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	2a. Käesolevale lõikele viitamisel kohaldatakse määruse (EL) nr 182/2011 artiklit 5.

Muudatusettepanek 247

Ettepanek võtta vastu määrus
Artikkel 55 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Artikkel 55a
	Delegeeritud volituste rakendamine
	1. Komisjonile antakse õigus võtta vastu delegeeritud õigusakte käesolevas artiklis sätestatud tingimustel.
	2. Artiklites 44 ja 48a osutatud õigus võtta vastu delegeeritud õigusakte antakse komisjonile määramata ajaks alates ... [alusakti jõustumise kuupäev].
	3. Euroopa Parlament ja nõukogu võivad artiklites 44 ja 48a osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast selle avaldamist Euroopa Liidu Teatajas või otsuses nimetatud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.
	4. Enne delegeeritud õigusakti vastuvõtmist konsulteerib komisjon kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes sätestatud põhimõtetega iga liikmesriigi määratud ekspertidega.
	5. Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, teeb ta selle samal ajal teatavaks Euroopa Parlamendile ja nõukogule.
	6. Artiklite 44 ja 48a alusel vastu võetud delegeeritud õigusakt jõustub üksnes juhul, kui Euroopa Parlament ega nõukogu ei ole kahe kuu jooksul pärast õigusakti teatavakstegemist Euroopa Parlamendile ja nõukogule esitanud selle suhtes vastuväidet või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväidet. Euroopa

	Parlamendi või nõukogu algatusel pikendatakse seda tähtaega kahe kuu võrra.

Muudatusettepanek 248

Ettepanek võtta vastu määrus
Artikkel 56 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Hiljemalt ***viis*** aastat pärast artiklis 58 osutatud kuupäeva ja seejärel iga ***viie*** aasta tagant hindab komisjon ameti ja selle töökorralduse mõju, tulemuslikkust ja tõhusust ning võimalikku vajadust muuta ameti mandaati ja kõigi selliste muudatuste finantsmõju. Hindamisel arvestatakse tagasisidet, mida amet on oma töö kohta saanud. Kui komisjon leiab, et ameti töö jätkamine ei ole ametile seatud eesmärkide, mandaadi ja ülesannete seisukohast enam põhjendatud, võib ta teha ettepaneku käesolevat määrust ametiga seotud sätete osas muuta.	1. Hiljemalt ***kaks*** aastat pärast artiklis 58 osutatud kuupäeva ja seejärel iga ***kahe*** aasta tagant hindab komisjon ameti ja selle töökorralduse mõju, tulemuslikkust ja tõhusust ning võimalikku vajadust muuta ameti mandaati ja kõigi selliste muudatuste finantsmõju. Hindamisel arvestatakse tagasisidet, mida amet on oma töö kohta saanud. Kui komisjon leiab, et ameti töö jätkamine ei ole ametile seatud eesmärkide, mandaadi ja ülesannete seisukohast enam põhjendatud, võib ta teha ettepaneku käesolevat määrust ametiga seotud sätete osas muuta.

Muudatusettepanek 249

Ettepanek võtta vastu määrus
Artikkel 56 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Selle hindamise käigus vaadeldakse ka III jaotise sätete mõju, tulemuslikkust ja tõhusust seoses eesmärgiga tagada IKT toodete ja teenuste piisav küberturvalisus ELis ja parandada siseturu toimimist.	2. Selle hindamise käigus vaadeldakse ka III jaotise sätete mõju, tulemuslikkust ja tõhusust seoses eesmärgiga tagada IKT toodete***, protsesside*** ja teenuste piisav küberturvalisus ELis ja parandada siseturu toimimist.

Muudatusettepanek 250

Ettepanek võtta vastu määrus
Artikkel 56 – lõige 2 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	2a. Hindamise käigus vaadeldakse, kas küberturvalisusega seotud olulised siseturule pääsu käsitlevad nõuded on vajalikud selleks, et vältida selliste toodete, teenuste ja protsesside liidu turule jõudmist, mis ei vasta põhilistele küberturvalisuse nõuetele.

Muudatusettepanek 251

Ettepanek võtta vastu määrus
-I lisa (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	-I LISA
	ELi küberturvalisuse sertifitseerimise raamistiku kasutuselevõtmisel on tõenäoline, et tähelepanu koondub sellele, kuidas vahetut huvi pakkuvad valdkonnad tulevad toime kujunemisjärgus tehnoloogiaga seotud probleemidega. Eritähelepanu pakub asjade interneti valdkond, kuna see hõlmab nii tarbijate kui ka tööstuse nõudeid. Tehakse ettepanek lisada sertifitseerimise raamistikku järgmine prioriteetide loetelu:
	1) pilveteenuse osutamise sertifitseerimine;
	2) asjade interneti seadmete sertifitseerimine, sealhulgas:
	a) isiku tasandi seadmed, nagu kantavad nutiseadmed;
	b) kogukonna tasandi seadmed, nagu arukad autod, arukad kodud ja terviseseadmed;
	c) ühiskonna tasandi seadmed, nagu arukad linnad ja arukad võrgud;

	3) tööstus 4.0, mis hõlmab arukaid, omavahel ühendatud küberfüüsikalisi süsteeme, mis automatiseerivad kõik tööstusliku tegevuse etapid alates projekteerimisest ja tootmisest kuni käitamise, tarneahela ja tehnilise hoolduseni;
	4) igapäevases elus kasutatavate tehnoloogiate ja teenuste sertifitseerimine. Selle näiteks võivad olla võrguseadmed, nagu kodus kasutatavad internetiruuterid.

Muudatusettepanek 252

Ettepanek võtta vastu määrus
I lisa – lõik 1 – punkt 5 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	5a. Kui vastavushindamisasutus kuulub avalik-õiguslikule üksusele või asutusele või on selle hallatav asutus, tuleb tagada selle sõltumatus ning sertifitseerimise järelevalveasutuse ja vastavushindamisasutuse vahelise huvide konflikti puudumine ning see dokumenteerida.

Muudatusettepanek 253

Ettepanek võtta vastu määrus
I lisa – lõik 1 – punkt 8

Komisjoni ettepanek	*Muudatusettepanek*
8. Vastavushindamisasutus peab olema võimeline täitma kõiki vastavushindamisülesandeid, mis talle käesoleva määrusega on määratud, seda nii juhul, kui vastavushindamisasutus täidab ülesandeid ise, kui ka juhul, kui neid täidetakse tema nimel ja vastutusel.	8. Vastavushindamisasutus peab olema võimeline täitma kõiki vastavushindamisülesandeid, mis talle käesoleva määrusega on määratud, seda nii juhul, kui vastavushindamisasutus täidab ülesandeid ise, kui ka juhul, kui neid täidetakse tema nimel ja vastutusel. ***Mis tahes alltöövõtt või konsulteerimine asutuseväliste töötajatega peab olema nõuetekohaselt dokumenteeritud ja ellu viidud ilma vahendajateta ning selle kohta tuleb sõlmida kirjalik leping, milles***

	käsitletakse muu hulgas konfidentsiaalsuse ja huvide konflikti küsimusi. Asjaomane vastavushindamisasutus vastutab täidetud ülesannete eest täiel määral.

Muudatusettepanek 254

Ettepanek võtta vastu määrus
I lisa – lõik 1 – punkt 12

Komisjoni ettepanek	*Muudatusettepanek*
12. Tuleb tagada vastavushindamisasutuste, nende kõrgema juhtkonna ja ***hindamistöötajate*** erapooletus.	12. Tuleb tagada vastavushindamisasutuste, nende kõrgema juhtkonna***, hindamistöötajate*** ja ***alltöövõtjate*** erapooletus.

Muudatusettepanek 255

Ettepanek võtta vastu määrus
I lisa – lõik 1 – punkt 15

Komisjoni ettepanek	*Muudatusettepanek*
15. ***Vastavushindamisasutuse*** töötajad peavad hoidma ametisaladust teabe osas, mis on saadud käesoleva määruse või selle jõustamiseks vastuvõetud ***siseriiklike*** õigusaktide kohaselt täidetud ülesannete käigus, välja arvatud teabevahetus selle liikmesriigi pädevate asutustega, kus asutus tegutseb.	15. ***Vastavushindamisasutus ja selle töötajad, komiteed, allüksused, alltöövõtjad ning sellega seotud mis tahes asutused ja välisorganite*** töötajad peavad ***tagama konfidentsiaalsuse ja*** hoidma ametisaladust teabe osas, mis on saadud käesoleva määruse või selle jõustamiseks vastuvõetud ***riigisiseste*** õigusaktide kohaselt täidetud ülesannete käigus, välja arvatud ***juhul, kui teabe avalikustamist nõuab nendele isikutele kohaldatav liidu või liikmesriigi õigus, välja arvatud*** teabevahetus selle liikmesriigi pädevate asutustega, kus asutus tegutseb. ***Tagada tuleb omandiõiguste kaitse. Vastavushindamisasutusel peavad olema käesoleva punkti 15 nõuete täitmiseks kehtestatud dokumenteeritud menetlused.***

Muudatusettepanek 256

Ettepanek võtta vastu määrus
I lisa – lõik 1 – punkt 15 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	15a. Käesoleva lisa nõuded, välja arvatud punkti 15 nõuded, ei takista mingil viisil tehnilise teabe ja regulatiivsete suuniste vahetamist vastavushindamisasutuse ja sertifikaati taotleva või selle taotlemist kaaluva isiku vahel.

Muudatusettepanek 257

Ettepanek võtta vastu määrus
I lisa – lõik 1 – punkt 15 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	15b. Vastavushindamisasutus tegutseb vastavalt sidusatele, õiglastele ja mõistlikele tingimustele, võttes seoses tasudega arvesse soovituses 2003/361/EÜ määratletud väikeste ja keskmise suurusega ettevõtjate huve.