Euroopa Parlament
2014-2019

Siseturu- ja tarbijakaitsekomisjon

2017/0225(COD)

22.5.2018

ARVAMUS

Esitaja: siseturu- ja tarbijakaitsekomisjon

Saaja: tööstuse, teadusuuringute ja energeetikakomisjon

ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, mis käsitleb ENISAt ehk ELi küberturvalisuse ametit, millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 ja mis käsitleb info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist („küberturvalisust käsitlev õigusakt“)
(COM(2017)0477 – C8-0310-2017 – 2017/0225(COD))

Arvamuse koostaja: (*) Nicola Danti

(*) Kaasatud komisjon – kodukorra artikkel 54

PA_Legam

LÜHISELGITUS

Digitaalajastul on küberturvalisus Euroopa Liidu majandusliku konkurentsivõime ja turvalisuse ning meie vabade ja demokraatlike ühiskondade terviklikkuse ja neid toetavate protsesside oluline osa. Kübervastupidavusvõime kõrge taseme kindlustamine kogu ELis on ülimalt tähtis tarbijate usalduse saavutamiseks digitaalse ühtse turu vastu ning uuenduslikuma ja konkurentsivõimelisema Euroopa edasi arendamiseks.

Ilma igasuguse kahtluseta on küberohud ja üleilmsed küberründed, näiteks „Wannacry“ ja „Meltdown“, meie üha digiteeritumas ühiskonnas suureneva tähtsusega probleemid. 2017. aasta juulis avaldatud Eurobaromeetri uuringu kohaselt peab 87 % vastanutest küberkuritegevust oluliseks probleemiks ELi sisejulgeolekule ja enamikule neist valmistab muret küberkuritegevuse erinevate vormide ohvriks sattumine. Ühtlasi on 2016. aasta algusest saati toimunud kogu maailmas iga päev rohkem kui 4 000 lunavararünnet, kujutades 300 % kasvu alates 2015. aastast ja mõjutades 80 % ELi ettevõtetest. Need faktid ja andmed viitavad selgelt ELi vajadusele olla rohkem vastupanuvõimelisem ja tulemuslikum küberrünnete vastases võitluses ning vajadusele suurendada oma suutlikkust ELi kodanike, ettevõtete ja avalik-õiguslike asutuste paremaks kaitsmiseks.

Aasta pärast võrgu- ja infoturbe direktiivi jõustumist esitles Euroopa Komisjon ELi küberjulgeoleku strateegia laiemas raamistikus määrust, mille eesmärk on tõsta veelgi ELi kübervastupidavusvõimet, heidutust ja kaitset. 13. septembril 2017 esitles komisjon küberturvalisust käsitlevat õigusakti, mis põhineb kahel sambal:
1) alaline ja tugevam mandaat Euroopa Liidu Võrgu- ja Infoturbeametile (ENISA), et aidata liikmesriike tõhusalt küberrünnete ennetamisel ja neile reageerimisel, ning 2) Euroopa küberturvalisuse sertifitseerimise raamistiku loomine, et kindlustada IKT toodete ja teenuste küberturvalisus.

Üldiselt tunneb arvamuse koostaja heameelt Euroopa Komisjoni välja pakutud käsitluse üle, eriti toetab ta Euroopa küberturvalisuse sertifitseerimise kavade kasutusele võtmist, mille eesmärk on suurendada IKT toodete ja teenuste turvalisust ja vältida ühtse turu kulukat killustatust selles üliolulises valdkonnas. Kuigi esialgu peaks see jääma vabatahtlikuks töövahendiks, loodab arvamuse koostaja, et Euroopa küberturvalisuse sertifitseerimise raamistik ja sellega seonduvad toimingud muutuvad vajalikeks abivahendeiks meie kodanike ja kasutajate usalduse tõstmisel ning ühtsel turul ringlevate toodete ja teenuste turvalisuse suurendamisel.

Arvamuse koostaja on veendunud ka selles, et ettepaneku mitmeid punkte tuleks selgitada ja parandada.

- Esiteks, **ENISA juhtimisel sertifitseerimise ettevalmistava kava koostamisel asjaomaste sidusrühmade kaasamise suurendamine juhtimissüsteemi erinevatesse etappidesse**: arvamuse koostaja arvates on tähtis kaasata ametlikult kõige olulisemad sidusrühmad, näiteks IKT tööstus, tarbijaorganisatsioonid, VKEd, ELi standardiorganisatsioonid ja ELi valdkondlikud asutused jne, ning anda neile võimalus luua uusi ettevalmistavaid kavasid, jagada ENISAga oma pädevust ja teha ENISAga koostööd ettevalmistava kava koostamisel.
- Teiseks on vaja tugevdada Euroopa küberturvalisuse sertifitseerimise rühma (mis koosneb rahvuslikest ametiasutustest ja mida toetab komisjon ja ENISA) koordineerivat rolli, lisades ülesandeid, et pakkuda strateegilist suunist ja **luua tööprogramm ühismeetmete võtmiseks liidu tasandil** sertifitseerimise valdkonnas, aga ka selleks, et koostada ja **perioodiliselt ajakohastada erinimekirja IKT**

toodetest ja teenustest, mille jaoks peab Euroopa küberturvalisuse sertifitseerimise rühm vajalikuks Euroopa küberturvalisuse sertifitseerimise kava.

- Arvamuse koostaja usub siiralt, et tuleks hoiduda kõige soodsamate võimalustega ELi sertifitseerimiskava otsimisest, mis on juba juhtunud teistes sektorites. **ENISA seire ja järelevalve eeskirjad ning riiklikud sertifitseerimise järelevalveasutused peaksid olema tugevalt täiustatud**, et kindlustada liikmesriigis väljastatud Euroopa sertifikaadi vastavus samadele standarditele ja nõuetele võrreldes teises liikmesriigis väljastatud sertifikaadiga. Seetõttu teeb arvamuse koostaja järgmised ettepanekud:

  1) suurendada ENISA järelevalve volitusi: ENISA koos koordineeriva rühmaga peaks hindama menetlusi, mille on kehtestanud ELi sertifikaatide välja andmise eest vastutavad ametid;
  2) riiklikud sertifitseerimise järelevalveasutused peaksid perioodiliselt (vähemalt iga kahe aasta tagant) hindama ELi sertifikaate, mille on väljastanud vastavushindamisasutused;
  3) ühiste siduvate kriteeriumide kehtestamine, mille määratleb sertifitseerimise rühm selles osas, millises ulatuses, millise sisu ja sagedusega peaksid riiklikud sertifitseerimise järelevalveasutused viima ellu punktis 2 viidatud hindamisi.
- Arvamuse koostaja usub, et lõppkasutajatele mõeldud sertifitseeritud IKT toodetele ja teenustele tuleks kehtestada kohustuslik **ELi usaldusmärgis**. See märgis aitaks parandada teadlikkust küberturvalisusest ja annaks hea küberturvalisuse mandaadiga ettevõtetele konkurentsieelise.
- Arvamuse koostaja nõustub Euroopa Komisjoni ühtse ja ühtlustatud käsitlusviisiga, kuid on veendunud, et see peaks olema paindlikum ning kohandatavam iga toote või teenuse eriomadustele ja nõrkustele – puudub ühtne, igas olukorras rakendatav käsitlus. Seetõttu usub arvamuse koostaja, et **usaldusväärsuse tasemed** peaksid olema ümber nimetatud ja neid tuleks kasutada IKT toodete ja teenuste ette nähtud kasutusotstarvet arvesse võttes. Sarnaselt peaks **sertifikaadi kehtivusaeg** olema määratletud kava kaupa.
- Iga sertifitseerimise kava peaks olema kavandatud selliselt, et stimuleerida ja julgustada toodete ja teenuste elutsükli kõigis etappides kõiki osalisi, kes on seotud turvalisuse standardite, tehniliste normide ning **sisseprojekteeritud turbe ja lõimprivaatsuse põhimõtete** välja töötamise ja kasutusele võtmisega.

MUUDATUSETTEPANEKUD

Siseturu- ja tarbijakaitsekomisjon palub vastutaval tööstuse, teadusuuringute ja energeetikakomisjonil võtta arvesse järgmisi muudatusettepanekuid:

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 ***igapäevane*** ühiskondlik tegevus, 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 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	(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.	piiratud kasutamine, et organisatsioonidest ja eraisikutest kasutajatel ei ole IKT toodete ja teenuste küberturvalisuse omaduste kohta piisavalt teavet ning see vähendab usaldust digilahenduste vastu***, mis on oluline digitaalse ühtse turu loomiseks***.

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 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.	(3) Ulatuslikum digiteerimine ja ühenduvus toovad kaasa ***palju*** 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. ***Ühiskond üldiselt, aga ka küberkurjategijad rakendavad tehisintellekti ja masinõppe ümberkujundamisvõimet.*** Et ***neid*** ühiskonna vastu suunatud ***riske*** leevendada, tuleb võtta kõik vajalikud meetmed, et parandada ELis ***kaitset küberrünnete vastu*** 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.

Muudatusettepanek 4

Ettepanek võtta vastu määrus
Põhjendus 4

Komisjoni ettepanek	*Muudatusettepanek*
(4) Küberründeid tuleb ette üha sagedamini ning küberohtude poolt lihtsamini haavatavat ühendatud majandust	(4) Küberründeid 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 tööstuse kui ka kasutajate jaoks.

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. 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 tööstuse kui ka kasutajate jaoks.

Muudatusettepanek 5

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***	(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. ***Võttes arvesse tõsiasja, et küberintsidendid õõnestavad*** usaldust

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.	***digitaalsete teenuste osutajate ja*** digitaalse ühtse turu ***kui sellise*** vastu***, eeskätt tarbijate seas, tuleks ühtlasi veelgi suurendada usaldust, pakkudes*** IKT toodete ja teenuste turvalisuse tasemete kohta ***läbipaistvat teavet***. Sellele saab kaasa aidata kogu ELi hõlmava ***standarditud*** sertifitseerimisega, mis ***põhineb Euroopa või rahvusvahelistel standarditel ning*** tagab ühised küberturvalisuse nõuded ja hindamiskriteeriumid liikmesriikide turgudel ja sektorites. ***Lisaks kogu liitu hõlmavale sertifitseerimisele on olemas mitmesugused vabatahtlikud meetmed, mida võiks võtta erasektoris IKT toodete ja teenuste turvalisuse vastu usalduse suurendamiseks, arvestades eriti asjade interneti seadmete suurenevat kättesaadavust. Näiteks tuleks tõhusamalt kasutada krüptimist ja muid tehnoloogiaid, sealhulgas selliseid, mis aitavad vältida küberrünnakute õnnestumist, nagu plokiaheltehnoloogia, et parendada lõppkasutajate andmete ja teabevahetuse turvalisust ning liidu võrgu- ja infosüsteemide üldist turvalisust.***

Muudatusettepanek 6

Ettepanek võtta vastu määrus
Põhjendus 5 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(5 a) Kuigi IKT protsesside, toodete ja teenuste sertifitseerimine ning nendega seotud muud vastavushindamised on väga olulised, nõuab küberturvalisuse suurendamine mitmetahulist käsitust, mis hõlmab nii inimesi, protsesse kui ka tehnoloogiaid. Samuti peaks EL jätkuvalt tugevalt rõhutama ja edendama muid jõupingutusi, nagu küberturvalisusealane haridus, koolitus ja sellega seotud oskuste arendamine; teadlikkuse parandamine nii ettevõtete tegevjuhtimise kui ka juhatuse

tasandil; küberohtudega seotud vabatahtliku teavitustöö edendamine; ning ohtudele reageerimisel ELi reageerivalt lähenemisviisilt ennetavale lähenemisviisile üleminek, pannes suurt rõhku küberrünnakute õnnestumise ärahoidmisele.

Muudatusettepanek 7

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	(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,*** 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

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

Muudatusettepanek 8

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 positsioonile Euroopa digitaalse ökosüsteemi kaitsmisel.	(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 tähtsale positsioonile Euroopa digitaalse ökosüsteemi kaitsmisel.

Muudatusettepanek 9

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 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	(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 ***küberhügieeni*** parimate tavade ja lahenduste propageerimisele***, mis tähendab lihtsaid rutiinseid meetmeid, mida üksikisikud*** ja ***organisatsioonid saavad võtta, et minimeerida küberohtude riske, näiteks mitmeteguriline autentimine, paikamine, krüptimine*** ja ***pääsuhaldus. Amet peaks selleks koguma ja analüüsima*** avalikult kättesaadavat teavet oluliste intsidentide kohta ning ***koostama ja avaldama aruandeid ja suuniseid***, et pakkuda ettevõtjatele ja kodanikele juhiseid ning parandada valmisoleku 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.	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 ***meetmeist, mida saab võtta, et kaitsta end*** küberkeskkonnas varitseda ***võivate ohtude eest***, sealhulgas ***sellised küberkuriteod*** nagu andmepüügi rünnakud, ***lunavara rünnakud, kaaperdamine,*** robotvõrgud, finants- ja pangapettused, ning tutvustada ***nõuandeid elementaarse mitmetegurilise*** autentimise***, krüptimise, paikamise, pääsuhalduse põhimõtete,*** andmekaitse ***ning muude turvalisust ja eraelu puutumatust soodustavate tehnoloogiate ja andmete anonüümseks muutmise vahendite kohta***. Ametil peaks olema keskne roll selles, et lõppkasutajad saaksid kiiremini teadlikuks seadmete turvalisusest ***ning seadmete turvalisest kasutamisest, edendades liidu tasandil sisseprojekteeritud turvet, mis on äärmiselt oluline ühendatud seadmete turvalisuse parandamiseks eelkõige haavatavate lõppkasutajate, sealhulgas laste jaoks, ja lõimprivaatsust. Amet peaks ergutama kõiki lõppkasutajaid võtma asjakohaseid meetmeid selleks, et ennetada ja vähendada nende võrkude ja infosüsteemide turvalisust ohustavate intsidentide mõju. Tuleks luua partnerlusi akadeemiliste asutustega, kel on teadusuuringute algatused asjakohases küberturvalisuse valdkonnas.***

Muudatusettepanek 10

Ettepanek võtta vastu määrus
Põhjendus 35

Komisjoni ettepanek	*Muudatusettepanek*
(35) Amet peaks innustama liikmesriike ja teenusepakkujaid tõstma oma üldisi turbestandardeid, et kõik internetikasutajad	(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 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.	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 siseturul pakutavate toodete ja teenuste küberturvalisuse taseme kohta ning avaldada teenusepakkujatele ja tootjatele suunatud hoiatusi, milles nõutakse nende toodete turvalisuse, sealhulgas küberturvalisuse parandamist. ***ENISA peaks sellised hoiatused avaldama veebilehel, mis on mõeldud teabe andmiseks sertifitseerimissüsteemide kohta. Amet peaks koostama suunised liidus müüdavate või liidust eksporditavate IT seadmete minimaalsete turvanõuete kohta. Sellistes suunistes võiks nõuda, et tootjad esitaksid kirjaliku avalduse, milles nad kinnitavad, et seade ei sisalda teadaolevate turvanõrkustega riistvara, tarkvara või püsivara komponente ega vahetamatut või krüptimata parooli või juurdepääsukoodi, et see sobib usaldusväärsete ja nõuetekohaselt autenditud turvauuenduste vastuvõtmiseks, et müüjate reageerimine mõjutatud seadmele hõlmab piisavate õiguskaitsevahendite hierarhiat ning et müüjad teavitavad lõppkasutajaid, kui seadme turbetugi lõpeb.***

Muudatusettepanek 11

Ettepanek võtta vastu määrus
Põhjendus 36 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(36 a) Standardid on vabatahtlikud ja turupõhised vahendid, mis pakuvad tehnilisi nõudeid ja suuniseid, ning avatud, läbipaistva ja kaasava protsessi tulemus. Standardite kasutamine edendab kaupade ja teenuste vastavust liidu

	õigusnormidele ning toetab Euroopa poliitikat kooskõlas määrusega (EL) nr 1025/2012 Euroopa standardimise kohta. Amet peaks regulaarselt konsulteerima ja tegema koostööd Euroopa standardiorganisatsioonidega, eriti Euroopa küberturvalisuse sertifitseerimise kavade ettevalmistamisel.

Muudatusettepanek 12

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 alaline sidusrühm, mis tagaks regulaarse dialoogi erasektori, tarbijate organisatsioonide***, teadusasutuste*** ja teiste asjaomaste sidusrühmadega. Tegevdirektori ettepanekul haldusnõukogu asutatud alaline sidusrühm peaks keskenduma sidusrühmade jaoks olulistele küsimustele ja juhtima neile ameti tähelepanu. ***Sidusrühmade asjakohase kaasamise tagamiseks küberturvalisuse sertifitseerimise raamistikku peaks alaline sidusrühm andma nõu ka selle kohta, millised IKT tooted ja teenused tuleks hõlmata tulevaste Euroopa küberturvalisuse sertifitseerimise kavadega ning esitama komisjonile ettepanekuid nõuda ametilt selliste IKT toodete ja teenuste kohta ettevalmistavate kavade koostamist kas omal algatusel või pärast asjaomastelt sidusrühmadelt saadud ettepanekuid.*** Alalise sidusrühma koosseis ja ülesanded (eelkõige tuleb rühmaga konsulteerida tööprogrammi projekti üle) peaksid tagama sidusrühmade ***tõhusa ja võrdse*** esindatuse ameti töös.

Muudatusettepanek 13

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. Enamik ameti töötajaid peaks olema otseselt tegev ameti ***mandaadi*** 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 14

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	(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 ***seonduvaid tavasid ning*** mida teostab sõltumatu kolmas isik ***või mida teostatakse ettevõtja kinnitusega vastavuse kohta***. Sertifitseerimine iseenesest ei taga, et sertifitseeritud IKT tooted ja teenused on küberturvalised***, ning lõppkasutajaid tuleks sellest teavitada***. Pigem on see menetlus ja tehniline metoodika

nõuetele, mis on sätestatud mujal, näiteks tehnilistes standardites.	tõendamaks, et IKT tooteid ja teenuseid ***ning aluseks olevaid protsesse ja süsteeme*** on kontrollitud ja et need vastavad teatavatele küberturvalisuse nõuetele, mis on sätestatud mujal, näiteks tehnilistes standardites.

Muudatusettepanek 15

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) Küberturvalisuse ***Euroopa*** sertifitseerimisel on ***oluline*** 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 ***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 16

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	(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 lähenemisviisi küberturvalisuse horisontaalsetele küsimustele, näiteks asjade interneti valdkonnas. Olemasolevatel kavadel on märkimisväärseid puudujääke ning erinevusi tootehõlmavuses, usaldusväärsuse tasemetes, sisulistes kriteeriumides ja tegelikus kasutamises.	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***, suurendades seega oma kulusid***. Lisaks sellele paistab, 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.

Muudatusettepanek 17

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 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	(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 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 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

ebatõhusad või ebasobivad ELi õiguspäraste eesmärkide saavutamiseks selles valdkonnas.	toodete 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 lugeda juhtudel, kus oli nõutav sertifitseerimine riikliku kava alusel, kehtivaks Euroopa kava alusel väljastatud sertifikaadid. Kavades tuleks juhinduda sisseprojekteeritud turbe ja määruses (EL) 2016/679 osutatud põhimõtetest. Need*** 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 18

Ettepanek võtta vastu määrus
Põhjendus 52 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(52 a) Euroopa küberturvalisuse sertifitseerimise raamistik tuleb luua ühetaoliselt kõikides liikmesriikides, et vältida sertifikaatide ostlemise tava, mille põhjuseks on erinevad kulud ja eri rangusega nõuded liikmesriikides.

Muudatusettepanek 19

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	(55) Euroopa küberturvalisuse sertifitseerimise kavade eesmärk on ***aidata kaasa kõrgetasemelisele lõppkasutaja kaitsele ja Euroopa konkurentsivõimele***

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 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.

ning suurendada turvalisuse taset digitaalsel ühtsel turul, ja veel täpsemalt 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 ***protsesside***, ***toodete***, teenuste ja süsteemide asjaomaste funktsioonide või nende poolt pakutavate või nende kaudu juurdepääsetavate ***protsesside*** 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 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. ***On ülimalt tähtis, et kõik Euroopa küberturvalisuse sertifitseerimise kavad oleksid välja töötatud selliselt, et need motiveeriksid ja julgustaksid kõiki asjaomase sektori osalisi välja töötama ja vastu võtma turvalisuse standardeid, tehnilisi norme ning sisseprojekteeritud turbe põhimõtteid toodete ja teenuste olelusringi kõikides etappides. Kui sertifitseerimiskava näeb ette märgid või märgistused, tuleb välja tuua ka nende märkide või märgistuste kasutamise tingimused. Selline märgis, mis võiks olla esitatud digitaalse logona või QR-***

	koodina, osutaks IKT-toodete ja -teenuste käitamise ja kasutamisega seotud riskidele ning see peaks olema lõpptarbijale selgelt ja hõlpsasti mõistetav.

Muudatusettepanek 20

Ettepanek võtta vastu määrus
Põhjendus 55 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(55 a) Pidades silmas innovatsiooni arengusuundi ning tõsiasja, et asjade interneti seadmed on muutumas üha kättesaadavamaks ja arvukamaks kogu ühiskonna lõikes, tuleb erilist tähelepanu pöörata kõikide, isegi kõige lihtsamate asjade interneti toodete turvalisusele. Kuna sertifitseerimine on üks peamisi viise, mis aitab suurendada usaldust turul ning turvalisust ja vastupidavust, tuleks ELi uues küberturvalisuse sertifitseerimise raamistikus panna suurt rõhku asjade interneti toodetele ja teenustele, et vähendada nende nõrkusi ning muuta need tarbijate ja ettevõtjate jaoks turvalisemaks.

Muudatusettepanek 21

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	(56) ***ENISA peaks haldama lihtsalt kasutatava veebivahendiga spetsiaalset veebisaiti, kust leiab teavet vastuvõetud kavade, ettevalmistavate kavade ja komisjoni nõutud kavade kohta***. 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

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 üksikasjalik kirjeldus, näiteks viide standarditele või tehnilistele kirjeldustele, konkreetsed hindamiskriteeriumid ja -meetodid ning kavandatud usaldusväärsuse tase: ***baastase***, ***märkimisväärne ja/***või ***kõrge tase***	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, ***IKT toote, protsessi või teenuse kasutamise ja käitamisega seotud*** konkreetsed hindamiskriteeriumid ja -meetodid***, nende olemuslikud riskid*** ning kavandatud usaldusväärsuse tase: ***funktsionaalselt turvaline, st usaldusväärsuse tase on funktsionaalsel määral turvaline, märkimisväärselt turvaline, üliturvaline või nende kombinatsioon. Selleks et lõppkasutajat mitte eksitada, ei peaks nimetatud usaldusväärsuse taseme puhul mainima absoluutset turvalisust. Arvesse tuleks võtta ka toote kogu olelusringi. Selleks et täpsustada, milliste riskide suhtes on konkreetne toode või teenus kavandatud vastupanuvõimeline olema, peaks ENISA koordineerima kontrollnimekirja koostamist, kus on loetletud riskid, millega IKT protsess, toode või teenus eeldatavasti kokku puutub konkreetse kasutajakategooria puhul ja konkreetses keskkonnas.***

Muudatusettepanek 22

Ettepanek võtta vastu määrus
Põhjendus 56 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(56 a) Komisjonile tuleks anda õigus paluda ENISA-l koostada ettevalmistav sertifitseerimiskava konkreetsete IKT toodete ja teenuste jaoks. Komisjonile tuleks delegeerida volitus võtta kooskõlas Euroopa Liidu toimimise lepingu artikliga 290 vastu õigusakte seoses Euroopa küberturvalisuse sertifitseerimise kavade kehtestamisega IKT toodetele ja teenustele. Eriti oluline

on see, et komisjon viiks oma ettevalmistava töö käigus läbi 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. Komisjon peaks asjaomaste delegeeritud õigusaktide vastuvõtmisel IKT toodete ja teenuste küberturvalisuse sertifitseerimise kavade aluseks võtma ühe asjaomastest ettevalmistatud kavadest, mille kohta ENISA on ettepaneku teinud. Selleks et tekitada usaldus küberturvalisuse sertifitseerimise raamistiku vastu ning parandada selle prognoositavust ja suurendada avalikkuse teadlikkust raamistikust.

Muudatusettepanek 23

Ettepanek võtta vastu määrus
Põhjendus 56 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(56 b) 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 24

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 teenuste osutajad saama esitada enda valitud vastavushindamisasutusele taotluse oma ***protsesside,*** toodete või teenuste sertifitseerimiseks***, või kinnitama ise, et nende tooted või teenused vastavad asjaomase Euroopa küberturvalisuse setifitseerimise kava nõuetele.***. 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. ***Euroopa Liidu piires ühtse akrediteerimise tagamiseks peaksid riiklikud sertifitseerimise järelevalveasutused kohaldama enda suhtes vastastikust hindamist menetluste puhul, millega kontrollitakse küberturvalisuse sertifitseerimisele kuuluvate toodete vastavust.***

Muudatusettepanek 25

Ettepanek võtta vastu määrus
Põhjendus 59

Komisjoni ettepanek	*Muudatusettepanek*
(59) Liikmesriike tuleb kohustada määrama ühe küberturvalisuse	(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, sealhulgas jagades teavet IKT toodete ja teenuste võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete küberturvalisuse sertifitseerimise kavade nõuetele.

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, sealhulgas jagades teavet IKT toodete ja teenuste võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete küberturvalisuse sertifitseerimise kavade nõuetele. ***Peale selle peavad nad jälgima ja kontrollima, et ettevõtjatepoolne nõuetele vastavuse kinnitus oleks nõuetekohane ja et vastavushindamisasutuste väljastatud Euroopa küberturvalisuse sertifikaadid oleksid väljastatud 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, näiteks turujärelevalve info- ja teavitussüsteem (ICSMS) ja ühenduse kiire teabevahetuse süsteem (RAPEX), mida juba kasutavad turujärelevalveasutused vastavalt***

määrusele (EÜ) nr 765/2008.

Muudatusettepanek 26

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 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.	***välja jäetud***

Muudatusettepanek 27

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	(65) Kontrollimenetlust tuleks kasutada selliste rakendusaktide vastuvõtmiseks, milles käsitletakse IKT ***protsesside,*** 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.	akrediteeritud vastavushindamisasutustest***,*** ***võttes arvesse elektroonilise teavitamise vahendi (uue lähenemisviisi alusel teavitatud ja määratud organisatsioonid (NANDO)) tõendatud tulemuslikkust***.

Muudatusettepanek 28

Ettepanek võtta vastu määrus
Põhjendus 66

Komisjoni ettepanek	*Muudatusettepanek*
(66) Ameti tööd tuleks hinna sõltumatult. ***Hindamisel tuleks pidada silmas ameti eesmärkide saavutamist***, selle ***töövõtteid*** ning ülesannete asjakohasust. Selle hindamise käigus tuleks vaadelda ka Euroopa küberturvalisuse sertifitseerimise raamistiku mõju, tulemuslikkust ja tõhusust.	(66) Ameti tööd tuleks hinna sõltumatult. ***Hindamine peaks hõlmama ameti kulude õiguspärasust ja tõhusust***, selle ***eesmärkide saavutamise tõhusust ja selle töövõtete kirjeldust*** ning ülesannete asjakohasust. Selle hindamise käigus tuleks vaadelda ka Euroopa küberturvalisuse sertifitseerimise raamistiku mõju, tulemuslikkust ja tõhusust.

Muudatusettepanek 29

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 1 – punkt 11

Komisjoni ettepanek	*Muudatusettepanek*
(11) „IKT toode ja teenus“ – võrgu- ja infosüsteemide ***mistahes*** element ***või elementide rühm***;	(11) „IKT ***protsess,*** toode ja teenus“ – ***toode, teenus, protsess, süsteem või nende kombinatsioon, mis on*** võrgu- ja infosüsteemide element; *(Muudatusettepanekut kohaldatakse kogu teksti ulatuses. Selle vastuvõtmise korral tehakse vastavad muudatused kogu tekstis.)*

Muudatusettepanek 30

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

Komisjoni ettepanek	*Muudatusettepanek*
	(11 a) „riiklik sertifitseerimise järelevalveasutus“ – liikmesriigi asutus, mis vastutab oma territooriumil küberturvalisuse sertifitseerimisega seotud järelevalve, täitmise tagamise ja seire ülesannete täitmise eest;

Muudatusettepanek 31

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

Komisjoni ettepanek	*Muudatusettepanek*
	(16 a) „ettevõtja kinnitus vastavuse kohta“ – tootja deklaratsioon, milles kinnitatakse, et tema IKT protsess, toode või teenus vastab täpsustatud Euroopa küberturvalisuse sertifitseerimise kavadele;

Muudatusettepanek 32

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, et panustada ***ühise kõrgetasemelise küberturvalisuse saavutamisse, et hoida*** liidus ***ära küberrünnakuid, vähendada siseturu killustatust ja parandada selle toimimist***.

Muudatusettepanek 33

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 kaasa*** liidu tasandil küberturvalisuse ***alase suutlikkuse suurendamisele***, et täiendada ***ja tugevdada*** liikmesriikide tegevust küberohtude ennetamisel ja neile reageerimisel, seda eeskätt piiriüleste intsidentide puhul.

Muudatusettepanek 34

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 teenuste küberturvalisuse alase usaldusväärsuse läbipaistvust ning tugevdada seeläbi usaldust digitaalse ***siseturu*** vastu.	6. Amet propageerib sertifitseerimist***, vältides samal ajal killustatust***, ***mille on põhjustanud liidu olemasolevate kavade koordineerituse puudumine. Amet*** aitab kaasa küberturvalisuse sertifitseerimise raamistiku loomisele ja haldamisele liidu tasandil vastavalt käesoleva määruse ***[III jaotise] artiklitele 43–54***, et suurendada IKT toodete ja teenuste küberturvalisuse alase usaldusväärsuse läbipaistvust ning tugevdada seeläbi usaldust digitaalse ***ühtse turu*** vastu.

Muudatusettepanek 35

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 kodanike***, ametiasutuste*** ja ettevõtjate heal tasemel teadlikkust küberturvalisusega seotud küsimustest.

Muudatusettepanek 36

Ettepanek võtta vastu määrus
Artikkel 5 – lõik 1 – punkt 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 liidu põhimõtete ja õiguse arendamise ja läbivaatamise jaoks küberturvalisuse valdkonnas, aga ka valdkonnaspetsiifiliste poliitiliste ja õiguslike algatuste jaoks, kui need puudutavad küberturvalisusega seotud küsimusi.

Selgitus

Ametile tuleks anda vabadus valida vahendid oma ülesannete täitmiseks.

Muudatusettepanek 37

Ettepanek võtta vastu määrus
Artikkel 5 – lõik 1 – punkt 2 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	2 a. Aitab määrusega (EL) 2016/679 loodud Euroopa Andmekaitsenõukogul määrata tehnilisel tasandil kindlaks tingimused, mis võimaldavad vastutavatel töötlejatel kasutada seaduslikult isikuandmeid IT-turvalisuse eesmärkidel nende taristu kaitsmiseks infosüsteemide vastu suunatud rünnete kindlakstegemise ja tõkestamise kaudu seoses i) määrusega (EL) 2016/679[1a]; ii) direktiiviga (EL) 2016/1148[1b], ja iii) direktiiviga 2002/58/EÜ[1c].
	[1a] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).
	[1b] Euroopa Parlamendi ja nõukogu 27.

aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

[1c] Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.7.2016, lk 1).

Selgitus

Nõuetekohaste koostöömehhanismide loomine.

Muudatusettepanek 38

Ettepanek võtta vastu määrus
Artikkel 5 – lõik 1 – punkt 4 – alapunkt 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 talletamise ja andmetöötluse*** suurema turvalisuse edendamist, muu hulgas oskusteabe ja nõu pakkumisega ning pädevate asutuste vaheliste parimate tavade jagamise soodustamisega.

Muudatusettepanek 39

Ettepanek võtta vastu määrus
Artikkel 6 – lõige 2 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	2 a. Amet hõlbustab Euroopa pikaajalise küberturvalisuse projekti loomist ja käivitamist, et toetada ELi sõltumatu küberturvalisuse tööstuse arengut ja peavoolustada küberturvalisus kõikides ELi IKT-lahendustes.

Selgitus

ENISA peaks nõustama seadusandjaid poliitikameetmete ettevalmistamisel, et võimaldada ELil jõuda järele kolmandate riikide IT-turvalisuse sektoritele. Projekt peaks olema ulatuse poolest võrreldav sellega, mis on saavutatud juba lennundussektoris (Airbusi näide). See on vajalik selleks, et arendada välja tugevam, suveräänne ja usaldusväärne ELi IKT tööstus (vt teaduslike tuleviku-uuringute üksuse (STOA) uuringut PE 614.531).

Muudatusettepanek 40

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 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.

Muudatusettepanek 41

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) koondab riiklikest ***ja rahvusvahelistest*** allikatest pärit aruandeid, et aidata kaasa ühise olukorrateadlikkuse tekitamisele;

Muudatusettepanek 42

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

Komisjoni ettepanek	*Muudatusettepanek*
	(1 a) hindab koostöös Euroopa küberturvalisuse sertifitseerimise rühmaga Euroopa küberturvalisuse sertifikaatide välja andmise menetlusi, mille on kehtestanud artiklis 51 osutatud vastavushindamisasutused ja mille eesmärk on tagada, et sertifikaatide välja andmisel rakendaksid vastavushindamisasutused käesolevat määrust ühetaoliselt;

Muudatusettepanek 43

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

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

Muudatusettepanek 44

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 ja salajaste tagauste tõkestamise valdkonnas,*** IKT toodete ja teenuste küberturvalisuse nõuete kohta, tehes selleks koostööd riikide sertifitseerimisega tegelevate järelevalveasutuste ja tööstusega ***formaalse, standarditud ja läbipaistva protsessi raames***;

Muudatusettepanek 45

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) ***konsulteerib rahvusvaheliste standardiorganisatsioonide ja Euroopa standardiorganisatsioonidega standardite väljatöötamisel, et tagada Euroopa küberturvalisuse sertifitseerimise kavades kasutatud standardite asjakohasus, ning hõlbustab asjakohaste*** 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;

Muudatusettepanek 46

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

Komisjoni ettepanek	*Muudatusettepanek*
	(b a) koostab suunised selle kohta, kuidas ja millal peavad liikmesriigid üksteist teavitama, kui nad saavad teada käesoleva määruse III jaotise kohaselt sertifitseeritud IKT protsessi, toote või teenuse nõrkusest, mis ei ole üldsusele teada, sealhulgas suunised nõrkuste avalikustamise poliitika koordineerimise kohta;

Muudatusettepanek 47

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

Komisjoni ettepanek	*Muudatusettepanek*
	(b b) koostab suunised liidus turule lastud või liidust eksporditud IT seadmete minimaalsete turvanõuete kohta;

Muudatusettepanek 48

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

Komisjoni ettepanek	*Muudatusettepanek*
(d) koondab, korraldab ja teeb avalikkusele spetsiaalse portaali kaudu kättesaadavaks liidu institutsioonide, ametite ja organite esitatud teavet küberturvalisuse kohta;	(d) koondab, korraldab ja teeb avalikkusele spetsiaalse portaali kaudu kättesaadavaks liidu institutsioonide, ametite ja organite esitatud teavet küberturvalisuse kohta***, sealhulgas teavet oluliste küberturvalisuse intsidentide ja suurte andmelekete kohta***;

Muudatusettepanek 49

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 üldsuse teadlikkust küberturvalisuse riskidest ***ning*** jagab kodanikele ja organisatsioonidele mõeldud juhiseid individuaalsete kasutajate heade tavade kohta ***ning edendab ennetavate tugevate IT turvameetmete kasutuselevõttu ning usaldusväärset andmekaitset ja eraelu puutumatust***;

Muudatusettepanek 50

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

Komisjoni ettepanek	*Muudatusettepanek*
	(g a) toetab liikmesriikidevahelist tihedamat koordineerimist ja parimate tavade vahetamist küberturvalisuse alase hariduse, küberhügieeni ja teadlikkuse valdkonnas;

Muudatusettepanek 51

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 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;

Muudatusettepanek 52

Ettepanek võtta vastu määrus
Artikkel 13 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Haldusnõukogusse kuulub igast liikmesriigist üks esindaja ning kaks komisjoni määratud esindajat. Kõigil esindajatel on hääleõigus.	1. Haldusnõukogusse kuulub igast liikmesriigist üks esindaja ning kaks komisjoni ***ja Euroopa Parlamendi*** määratud esindajat. Kõigil esindajatel on hääleõigus.

Muudatusettepanek 53

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 54

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

Komisjoni ettepanek	*Muudatusettepanek*
(m) nimetab kooskõlas käesoleva määruse artikliga 33 ametisse tegevdirektori ning vajaduse korral pikendab tema ametiaega või tagandab ta ametist;	(m) nimetab kooskõlas käesoleva määruse artikliga 33 ametisse ***kutsealaste kriteeriumide põhjal valitud*** tegevdirektori ning vajaduse korral pikendab tema ametiaega või tagandab ta ametist;

Muudatusettepanek 55

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 56

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 ***igal aastal*** Euroopa Parlamendile selle taotluse korral aru oma ülesannete täitmise kohta. Nõukogu võib kutsuda tegevdirektori oma ülesannete täitmisest aru andma.

Muudatusettepanek 57

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 alalise sidusrühma, mis koosneb asjaomaseid sidusrühmi esindavatest tunnustatud ekspertidest, näiteks IKT tööstuse ***ning*** avalikkusele kättesaadavate elektroonilise side võrkude või teenuste pakkujate***, eelkõige Euroopa IKT tööstuse*** ja ***teenuste pakkujate, väikeste ja keskmise suurusega ettevõtjate ühenduste,*** tarbijarühmade ***ja -ühenduste*** ekspertidest, ***küberturvalisuse valdkonnaga*** tegelevatest akadeemilistest ***ekspertidest, Euroopa standardiorganisatsioonide ekspertidest, nagu on määratletud määruse (EL) nr 1025/2012 artikli 2 punktis 8, asjaomaste valdkondlike liidu ametite ja asutuste*** ekspertidest ning [Euroopa elektroonilise side seadustiku kehtestamise direktiivi] alusel teavitatud riiklike reguleerivate asutuste esindajatest, samuti liidu õiguskaitseasutuste ja andmekaitse järelevalveasutuste esindajatest.

Muudatusettepanek 58

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 4

Komisjoni ettepanek	*Muudatusettepanek*
4. Alalise sidusrühma liikmete	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.	ametiaeg on kaks ja pool aastat. Haldusnõukogu ***ega juhatuse*** liige***, välja arvatud tegevdirektor,*** 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.

Muudatusettepanek 59

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. 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. ***Rühm võib teha ka ettepaneku selle kohta, et komisjon paluks ametil koostada Euroopa küberturvalisuse sertifitseerimise ettevalmistavad kavad kooskõlas artikliga 44 kas omal algatusel või pärast taotluste esitamist asjaomaste sidusrühmade poolt.***

Muudatusettepanek 60

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 5 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	5 a. Alaline sidusrühm nõustab ametit Euroopa küberturvalisuse sertifitseerimise ettevalmistavate kavade koostamisel.

Muudatusettepanek 61

Ettepanek võtta vastu määrus
Artikkel 23 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Amet tagab üldsusele ja huvitatud isikutele asjakohase, objektiivse, usaldusväärse ja kergesti juurdepääsetava teabe andmise, eelkõige ameti töötulemuste kohta. Ühtlasi avalikustab amet artikli 22 kohaselt esitatud huvide deklaratsioonid.	2. Amet tagab üldsusele ja huvitatud isikutele asjakohase, objektiivse, usaldusväärse ja kergesti juurdepääsetava teabe andmise, eelkõige ameti ***arutelude ja*** töötulemuste kohta. Ühtlasi avalikustab amet artikli 22 kohaselt esitatud huvide deklaratsioonid.

Selgitus

Läbipaistvus peab olema jõustatav, võttes arvesse artikli 24 kohaldamist.

Muudatusettepanek 62

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 ***luuakse, et tõhustada turvalisuse taset digitaalsel ühtsel turul ja et võtta ELi tasandil vastu Euroopa sertifitseerimise ühtlustatud käsitlus, et tagada küberrünnakutele vastupidavad IKT tooted, teenused ja süsteemid. Seejuures kinnitatakse***, et selle kava kohaselt sertifitseeritud IKT ***protsessid,*** tooted ja teenused vastavad kirjeldatud ***ühistele*** nõuetele ***ja omadustele*** selles osas, mis puudutab nende võimet pidada teataval usaldusväärsuse tasemel vastu tegevustele, mille eesmärk on rikkuda salvestatud, edastatud või töödeldud andmete või nende ***protsesside***, ***toodete***, teenuste ja süsteemide funktsioonide või nende poolt pakutavate või nende kaudu juurdepääsetavate teenuste käideldavust, autentsust, terviklust või konfidentsiaalsust.

Muudatusettepanek 63

Ettepanek võtta vastu määrus
Artikkel 43 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Artikkel 43 a
	Tööprogramm
	ENISA koostab pärast Euroopa küberturvalisuse sertifitseerimise rühma ja alalise sidusrühmaga konsulteerimist ning pärast komisjonilt heakskiidu saamist tööprogrammi, milles täpsustatakse liidu tasandil võetavaid ühiseid meetmeid, et tagada käesoleva jaotise ühetaoline kohaldamine, ning mis sisaldab selliste IKT toodete ja teenuste prioriteetide nimekirja, mille puhul on komisjoni hinnangul vaja kohaldada Euroopa küberturvalisuse sertifitseerimise kava.
	Tööprogramm koostatakse hiljemalt [kuus kuud pärast käesoleva määruse jõustumist] ja uus tööprogramm koostatakse seejärel iga kahe aasta tagant. Tööprogramm tehakse üldsusele kättesaadavaks.

Muudatusettepanek 64

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	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“) ***või artikliga 20 loodud alaline sidusrühm*** võivad teha komisjonile

küberturvalisuse sertifitseerimise ettevalmistav kava.

ettepaneku koostada Euroopa küberturvalisuse sertifitseerimise ettevalmistav kava.

Muudatusettepanek 65

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 arvamusi***.	2. Käesoleva artikli lõikes 1 osutatud ettevalmistavat kava koostades konsulteerib ENISA ***alalise sidusrühmaga, eeskätt Euroopa standardiorganisatsioonidega ja*** kõigi ***teiste*** asjaomaste sidusrühmadega ***(sealhulgas tarbijaorganisatsioonidega) formaalse, normitud*** ja ***läbipaistva protsessi abil, ning*** teeb rühmaga tihedat koostööd***, võttes arvesse juba olemasolevaid riiklikke ja rahvusvahelisi standardeid. Iga ettevalmistava kava koostamisel koostab ENISA riskide ja vastavate küberturvalisuse omaduste kontrollnimekirja.*** ***Rühm pakub ENISA-le viimase taotluse korral abi ja eksperdinõu seoses ettevalmistava kava koostamisega, esitades vajaduse korral ka arvamusi.*** ***Kui see on asjakohane, võib ENISA luua ka sidusrühmaga konsulteerimise eksperdirühma, mis koosneb alalise sidusrühma liikmetest ja mis tahes muudest asjakohastest sidusrühmadest, kellel on eriteadmised asjaomase ettevalmistava kava valdkonnas, et pakkuda edaspidi nõu ja abi.***

Muudatusettepanek 66

Ettepanek võtta vastu määrus
Artikkel 44 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. ENISA edastab käesoleva artikli	3. ENISA edastab käesoleva artikli

lõike 2 kohaselt koostatud Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava komisjonile.	lõike 2 kohaselt koostatud Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava komisjonile***, kes hindab selle sobivust lõikes 1 osutatud taotluse eesmärkide saavutamiseks***.

Muudatusettepanek 67

Ettepanek võtta vastu määrus
Artikkel 44 – lõige 3 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	3 a. ENISA hoiab oma käesolevast määrusest tulenevate ülesannete täitmisel saadud kõigi andmete puhul ametisaladust.

Muudatusettepanek 68

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. ***Komisjonile antakse õigus*** võtta kooskõlas ***artikliga*** 55 ***a*** vastu ***delegeeritud õigusakte, milles käsitletakse*** Euroopa küberturvalisuse sertifitseerimise ***kavade koostamist*** IKT toodete ja teenuste jaoks, mis vastavad käesoleva määruse artiklite 45, 46 ja 47 nõuetele. ***Kõnealuste delegeeritud õigusaktide vastuvõtmisel võtab komisjon IKT toodete ja teenuste küberturvalisuse sertifitseerimise kavade aluseks ENISA esitatud asjaomased ettevalmistavad kavad. Komisjon võib enne delegeeritud õigusaktide vastuvõtmist konsulteerida Euroopa Andmekaitsenõukoguga ja võtta arvesse selle seisukohta.***

Muudatusettepanek 69

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. ENISA haldab spetsiaalset veebilehte, mis pakub teavet Euroopa küberturvalisuse sertifitseerimise kavade kohta***, sealhulgas teavet kõigi selliste ettevalmistatud kavade kohta, mida komisjon on palunud ENISA-l koostada,*** ja tutvustab neid.

Muudatusettepanek 70

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:	***Iga*** Euroopa küberturvalisuse sertifitseerimise kava peab olema koostatud nii, et võtta ***arvesse vähemalt*** järgmisi turvalisusega seotud eesmärke***, kuivõrd need on asjakohased***:

Muudatusettepanek 71

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 ***tark- ja riistvaraga***, mis ei sisalda teadaolevaid turvaauke***; tagada, et need on projekteeritud ja rakendatud nii, et piirata tulemuslikult vastuvõtlikkust turvaaukudele***, ning ***tagada,*** et olemas on mehhanismid turvaliseks tarkvara uuendamiseks***, sealhulgas riistvara uuendamine ja automaatsed turvauuendused;***

Muudatusettepanek 72

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

Komisjoni ettepanek	*Muudatusettepanek*
	(g a) tagada, et IKT tooted ja teenused töötatakse välja ja neid käitatakse sellise viisil, et küberturvalisuse ja andmekaitse kõrge tase on eelkonfigureeritud kooskõlas sisseprojekteeritud turbe põhimõttega.

Muudatusettepanek 73

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. ***Igas Euroopa*** küberturvalisuse sertifitseerimise kavas määratakse selle kava raames sertifitseeritud IKT toodetele ja teenustele üks või mitu järgmist ***riskipõhist*** usaldusväärsuse taset: ***„funktsionaalselt turvaline“; „märkimisväärselt turvaline“*** ja/või ***„üliturvaline“***. ***Iga Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava usaldusväärsuse tase määratakse kindlaks artikli 44 lõike 2 alusel koostatud kontrollnimekirjas määratud riskide põhjal ning nende küberturvalisuse omaduste alusel, mis on kättesaadavad selliste riskide kõrvaldamiseks IKT toodetes ja teenustes, mille suhtes sertifitseerimiskava kohaldatakse.***

Muudatusettepanek 74

Ettepanek võtta vastu määrus
Artikkel 46 – lõige 1 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	1 a. Igas kavas osutatakse hindamismetoodikale või hindamisprotsessile, mida tuleb iga usaldusväärsuse taseme sertifikaatide väljastamisel järgida, olenevalt selles kavas hõlmatud IKT toodete ja teenuste kasutusotstarbest ja neile omasest riskist.

Muudatusettepanek 75

Ettepanek võtta vastu määrus
Artikkel 46 – lõige 2 – sissejuhatav osa

Komisjoni ettepanek	*Muudatusettepanek*
2. ***Baastase***, ***märkimisväärne ja kõrge usaldusväärsuse*** tase vastavad järgmistele tingimustele:	2. ***„Funktsionaalselt turvaline“***, ***„märkimisväärselt turvaline“ ja „üliturvaline“*** tase vastavad järgmistele tingimustele:

Muudatusettepanek 76

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 ***tase „funktsionaalselt turvaline“*** osutab Euroopa küberturvalisuse sertifitseerimise kava raames väljastatud sertifikaadile, mis annab ***piisava*** 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;

Muudatusettepanek 77

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) ***usaldusväärsuse*** tase ***„märkimisväärselt turvaline“*** osutab Euroopa küberturvalisuse sertifitseerimise kava raames väljastatud sertifikaadile, mis annab märkimisväärse usalduse IKT ***protsessi,*** 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;

Muudatusettepanek 78

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) ***usaldusväärsuse*** tase ***„üliturvaline“*** osutab Euroopa küberturvalisuse sertifitseerimise kava raames väljastatud sertifikaadile, mis annab kõrgema usalduse IKT ***protsessi,*** toote või teenuse väidetavate või kinnitatud küberturvalisuse omaduste vastu kui usaldusväärsuse tasemega ***„märkimisväärselt turvaline“*** sertifikaat ning mille kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk on vältida küberturvalisuse intsidente. ***Seda kohaldatakse eelkõige oluliste teenuste operaatorite kasutuseks mõeldud toodete ja teenuste suhtes, nagu see on määratletud direktiivi 2016/1148/EL artikli 4 lõikes 4.***

Muudatusettepanek 79

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 1 – sissejuhatav osa

Komisjoni ettepanek	*Muudatusettepanek*
1. ***Euroopa*** küberturvalisuse sertifitseerimise kava sisaldab järgmisi elemente:	1. ***Iga Euroopa*** küberturvalisuse sertifitseerimise kava sisaldab ***vajaduse korral vähemalt*** järgmisi elemente:

Muudatusettepanek 80

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 ***kava*** sisu ja ulatus, sealhulgas ***kõik hõlmatud konkreetsed sektorid, ning*** hõlmatud IKT toodete ja teenuste liik või kategooria;

Muudatusettepanek 81

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 ja teenuste puhul hinnatavate küberturvalisuse nõuete üksikasjalik kirjeldus, näiteks viidates ***eelkõige rahvusvahelistele, Euroopa*** või ***riiklikele*** standarditele või tehnilistele kirjeldustele;

Muudatusettepanek 82

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

Komisjoni ettepanek	*Muudatusettepanek*
	(b a) üksikasjalik kirjeldus selle kohta, kas väljastatud sertifikaati saab kohaldada üksnes üksiktoote või tooteseeria suhtes (näiteks sama alusstruktuuriga toote erinevad versioonid/mudelid);

Muudatusettepanek 83

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

Komisjoni ettepanek	*Muudatusettepanek*
	(c a) teave selle kohta, kas ettevõtja kinnitus vastavuse kohta on kava raames lubatud, ja vastavushindamise või ettevõtja vastavuskinnituse või mõlema suhtes kohaldatav menetlus;

Muudatusettepanek 84

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

Komisjoni ettepanek	*Muudatusettepanek*
	(c b) sertifitseerimisnõuded, mis on kindlaks määratud nii, et asjaomase sertifitseerimise saab lisada tootja süstemaatilistesse küberturvalisuse protsessidesse, mida järgitakse IKT protsessi, toote või teenuse projekteerimisel, väljatöötamisel ja olelusringi vältel, või see võib nendel põhineda;

Muudatusettepanek 85

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) kui kava näeb ette märgi või märgistuse, ***näiteks ELi küberturvalisuse vastavusmärgise, mis tähendab, et IKT protsess, toode või teenus vastab kava kriteeriumidele,*** tingimused sellise märgi või märgistuse kasutamiseks;

Muudatusettepanek 86

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***, näiteks vajaduse ja teostatavuse korral asjaomase IKT protsessi, toote või teenuse kohustuslik ajakohastamine, uuendus või paigad***;

Muudatusettepanek 87

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

Komisjoni ettepanek	*Muudatusettepanek*
(h) tingimused sertifitseerimise võimaldamiseks, säilitamiseks, jätkamiseks ning sertifitseerimise ulatuse laiendamiseks ja vähendamiseks;	(h) tingimused sertifitseerimise võimaldamiseks, säilitamiseks, jätkamiseks ***ja uuendamiseks*** ning sertifitseerimise ulatuse laiendamiseks ja vähendamiseks;

Muudatusettepanek 88

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 sertifitseeritud IKT toodete ***ning*** teenuste sertifitseerimistingimustele mittevastavuse tagajärgede ***kohta ning üldine teave käesoleva määruse artiklis 54 sätestatud karistuste*** kohta;

Muudatusettepanek 89

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 IKT toodete ja teenuste varem avastamata küberturvalisuse nõrkustest teada anda ja kuidas neid menetleda***, sealhulgas nõrkuste avalikustamise koordineeritud protsesside abil***;

Muudatusettepanek 90

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 või teenuseid hõlmavate riiklike ***või rahvusvaheliste*** küberturvalisuse sertifitseerimise kavade ***või olemasolevate rahvusvaheliste vastastikuse tunnustamise lepingute*** kindlakstegemine;

Muudatusettepanek 91

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

Komisjoni ettepanek	*Muudatusettepanek*
	(m a) sertifikaatide maksimaalne kehtivusaeg;

Muudatusettepanek 92

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

Komisjoni ettepanek	*Muudatusettepanek*
	(m b) usaldusväärsuse üliturvalise turvalisuse taseme vastupanu- ja vastupidavuskatsed.

Muudatusettepanek 93

Ettepanek võtta vastu määrus
Artikkel 47 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. Kui konkreetses liidu õigusaktis on nii sätestatud, võib Euroopa küberturvalisuse sertifitseerimise kava kohast sertifitseerimist kasutada tõendamaks kõnealuse õigusakti nõuetele vastavuse eeldust.	3. Kui konkreetses ***tulevases*** liidu õigusaktis on nii sätestatud, võib Euroopa küberturvalisuse sertifitseerimise kava kohast sertifitseerimist kasutada tõendamaks kõnealuse õigusakti nõuetele vastavuse eeldust.

Muudatusettepanek 94

Ettepanek võtta vastu määrus
Artikkel 48 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Sertifitseerimine on vabatahtlik, kui liidu õigusnormides ei ole sätestatud teisiti.	2. ***Sertifitseerimine Euroopa küberturvalisuse sertifitseerimise kava raames on kohustuslik kõrge riskiastmega IKT toodete ja teenuste puhul, mis on mõeldud spetsiaalselt oluliste teenuste operaatorite kasutuseks, nagu see on määratletud direktiivi 2016/1148/EL***

	artikli 4 lõikes 4. Kõigi teiste IKT toodete ja teenuste puhul on sertifitseerimine vabatahtlik, kui liidu õigusnormides ei ole sätestatud teisiti.

Muudatusettepanek 95

Ettepanek võtta vastu määrus
Artikkel 48 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. Käesoleva artikli ***kohase*** Euroopa küberturvalisuse ***sertifikaadi*** annavad välja artiklis 51 osutatud vastavushindamisasutused artikli 44 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavas sisalduvate kriteeriumide alusel.	3. Käesoleva artikli ***kohaseid*** Euroopa küberturvalisuse ***sertifikaate*** annavad välja artiklis 51 osutatud vastavushindamisasutused artikli 44 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavas sisalduvate kriteeriumide alusel. ***Vastavushindamisasutuste sertifitseerimise alternatiivina võivad toote tootjad ja teenuste pakkujad esitada juhul, kui selline võimalus on ette nähtud, ettevõtja kinnituse vastavuse kohta, milles nad kinnitavad, et protsess, toode või teenus vastab sertifitseerimise kava kriteeriumidele. Sellistel juhtudel peab toote tootja või teenuste pakkuja esitama riikliku järelevalveasutuse ja ENISA taotlusel neile ettevõtja kinnituse vastavuse kohta.***

Muudatusettepanek 96

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	4. Erandina lõikest 3 võib nõuetekohaselt põhjendatud juhtudel***, näiteks riikliku julgeoleku kaalutlustel,*** teatavas Euroopa küberturvalisuse sertifitseerimise kavas ette näha, et sellest kavast tuleneva Euroopa küberturvalisuse sertifikaadi võib välja anda üksnes avalik-

asutus on üks järgnevatest asutustest:	õiguslik asutus. Selline avalik-õiguslik asutus on üks järgnevatest asutustest:

Muudatusettepanek 97

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 või teenused sertifitseerimiseks, peab esitama artiklis 51 osutatud vastavushindamisasutusele kogu sertifitseerimismenetluse läbiviimiseks vajaliku teabe***, sealhulgas teabe iga teadaoleva turvaaugu kohta***.

Muudatusettepanek 98

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 ***igas küberturvalisuse sertifitseerimise kavas sätestatud maksimaalseks ajaks, mille jooksul see ka kehtib ning*** selle kehtivust võib pikendada samadel tingimustel senikaua, kuni ***kõnealuse kava nõuded, sealhulgas mis tahes läbivaadatud või muudetud*** nõuded on täidetud.

Muudatusettepanek 99

Ettepanek võtta vastu määrus
Artikkel 48 – lõige 6 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	6 a. Sertifikaat jääb kehtima protsessi, toote või teenuse kõigi uute versioonide korral, kui uue versiooni peamine põhjus on teadaolevate või potentsiaalsete

	turvanõrkuste või -ohtude paikamine, parandamine või muul viisil kõrvaldamine.

Muudatusettepanek 100

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 sertifitseerimise kavaga hõlmamata IKT toodete ja teenustega seotud menetlused jäävad alles.	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 ***delegeeritud õigusaktis*** sätestatud kuupäeval***. Komisjon jälgib käesoleva lõigu sätete järgimist, et hoida ära konkureerivate kavade eksisteerimise.*** Olemasolevad riiklikud küberturvalisuse sertifitseerimise kavad ja Euroopa küberturvalisuse sertifitseerimise kavaga hõlmamata IKT toodete ja teenustega seotud menetlused jäävad alles.

Muudatusettepanek 101

Ettepanek võtta vastu määrus
Artikkel 49 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. ***Riiklike*** küberturvalisuse sertifitseerimise kavade alusel väljastatud sertifikaadid jäävad kehtima kuni oma kehtivusaja lõpuni.	3. ***Euroopa küberturvalisuse sertifitseerimise kavaga hõlmatud riiklike*** küberturvalisuse sertifitseerimise kavade alusel väljastatud sertifikaadid jäävad kehtima kuni oma kehtivusaja lõpuni.

Muudatusettepanek 102

Ettepanek võtta vastu määrus
Artikkel 50 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. Iga riiklik sertifitseerimise järelevalveasutus on oma organisatsiooni, rahastamisotsuste, õigusliku struktuuri ja otsuste tegemise poolest sõltumatu üksustest, mille üle ta järelevalvet teostab.	3. Iga riiklik sertifitseerimise järelevalveasutus on oma organisatsiooni, rahastamisotsuste, õigusliku struktuuri ja otsuste tegemise poolest sõltumatu üksustest, mille üle ta järelevalvet teostab***, ning ta ei või olla vastavushindamisasutus ega riiklik akrediteerimisasutus***.

Muudatusettepanek 103

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 ***kooskõlas eeskirjadega, mille Euroopa küberturvalisuse sertifitseerimise rühm on võtnud vastu vastavalt artikli 53 lõike 3 punktile d a, ning teevad järelevalvet:*** ***i) nende riigi territooriumil asutatud vastavushindamisasutuse poolt välja antud sertifikaatide vastavuse üle käesolevas jaotises ja vastavas Euroopa küberturvalisuse sertifitseerimise kavas sätestatud nõuetele, ning*** ***ii) ettevõtja kinnituste üle vastavuse kohta, mis on kava kohaselt esitatud IKT protsessi, toote või teenuse puhul;***

Muudatusettepanek 104

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

Komisjoni ettepanek	*Muudatusettepanek*
(b) jälgivad ja ***kontrollivad*** vastavushindamisasutuste tegevust käesoleva määruse kohaldamisel,	(b) jälgivad***, kontrollivad*** ja ***vähemalt iga kahe aasta järel hindavad*** vastavushindamisasutuste tegevust

sealhulgas seoses käesoleva määruse artiklis 52 sätestatud vastavushindamisasutustest teavitamise ja sellega seotud ülesannetega;	käesoleva määruse kohaldamisel, sealhulgas seoses käesoleva määruse artiklis 52 sätestatud vastavushindamisasutustest teavitamise ja sellega seotud ülesannetega;

Muudatusettepanek 105

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 ***sertifikaatide või ettevõtjate esitatud kinnitustega vastavuse kohta***, uurivad asjakohasel määral kaebuse sisu ja teavitavad kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest;

Muudatusettepanek 106

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

Komisjoni ettepanek	*Muudatusettepanek*
	(c a) esitavad ENISA-le ja Euroopa küberturvalisuse sertifitseerimise rühmale aruanded punktis a nimetatud järelevalve ja punktides b ja c nimetatud hindamiste tulemuste kohta;

Muudatusettepanek 107

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

Komisjoni ettepanek	*Muudatusettepanek*
(d) teevad koostööd teiste riiklike sertifitseerimise järelevalveasutuste või	(d) teevad koostööd teiste riiklike sertifitseerimise järelevalveasutuste **,**

muude avaliku sektori asutusega, sealhulgas jagades teavet IKT toodete ja teenuste võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade nõuetele;	***riiklike akrediteerimisasutuste*** või muude avaliku sektori asutusega, sealhulgas jagades teavet IKT toodete ja teenuste võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade nõuetele***, sealhulgas sertifitseerimist puudutavate eksitavate, valede või võltsitud väidete kohta***;

Muudatusettepanek 108

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

Komisjoni ettepanek	*Muudatusettepanek*
	(c a) tunnistada kehtetuks selliste vastavushindamisasutuste akrediteerimine, kes ei vasta käesoleva määruse nõuetele;

Muudatusettepanek 109

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 siseriiklike õigusaktide kohaselt tagasi sertifikaadid, mis ei ole kooskõlas käesoleva määrusega või Euroopa küberturvalisuse sertifitseerimise kavaga***, ning teavitada sellest riiklikke akrediteerimisasutusi***;

Muudatusettepanek 110

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

Komisjoni ettepanek	*Muudatusettepanek*
	(f a) teha ettepanekuid ENISA ekspertide kohta, kes võiksid kuuluda

artikli 44 lõikes 2 osutatud sõltumatu eksperdirühma koosseisu.

Muudatusettepanek 111

Ettepanek võtta vastu määrus
Artikkel 50 – lõige 8 – lõik 1 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Teabevahetuse eesmärgil teeb komisjon kättesaadavaks üldise elektroonilise teabe tugisüsteemi.

Muudatusettepanek 112

Ettepanek võtta vastu määrus
Artikkel 50 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Artikkel 50 a
	Vastastikune eksperdihinnang
	1. Riiklikud sertifitseerimise järelevalveasutused hindavad vastastikku käesoleva määruse artikli 50 kohaselt toimuvat tegevust.
	2. Vastastikune eksperdihinnang hõlmab riiklike sertifitseerimise järelevalveasutuste kehtestatud menetluste hindamist, eeskätt selliste menetluste puhul, mille abil kontrollitakse küberturvalisuse sertifitseerimisele kuuluvate toodete nõuetele vastavust, töötajate pädevust, kontrollide ja inspekteerimismetoodika õigsust ning tulemuste õigsust. Vastastikuse eksperdihinnangu raames hinnatakse ka seda, kas riiklikel sertifitseerimise järelevalveasutustel on piisavad vahendid oma ülesannete nõuetekohaseks täitmiseks, nagu nõutakse artikli 50 lõikes 4.
	3. Riiklike sertifitseerimise järelevalveasutuste vastastikust

	eksperdihinnangut teostavad vähemalt kord iga viie aasta järel kahe teise liikmesriigi sertifitseerimise järelevalveasutused ja komisjon. ENISA võib vastastikuses eksperdihinnangus osaleda, kui ta riskianalüüsi põhjal nii otsustab.
	4. Komisjonil on õigus võtta kooskõlas artikliga 55 a vastu delegeeritud õigusakte, et kehtestada vastastikuste eksperdihinnangute kava vähemalt viieks aastaks, sätestades selles vastastikuse eksperdihinnangu meeskonna koosseisu kriteeriumid, hindamismetoodika, hindamiste ajakava, sageduse ja muud vastastikuse eksperdihinnanguga seotud ülesanded. Nende delegeeritud õigusaktide vastuvõtmisel võtab komisjon nõuetekohaselt arvesse rühma arvamusi.
	5. Vastastikuse eksperdihinnangu tulemusi kontrollib rühm. ENISA koostab tulemuste kokkuvõtte ja avalikustab selle.

Muudatusettepanek 113

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

Komisjoni ettepanek	*Muudatusettepanek*
	2 a. Kui tootjad otsustavad esitada käesoleva määruse artikli 48 lõike 3 kohase ettevõtja kinnituse vastavuse kohta, võtavad vastavushindamisasutused lisameetmeid, et kontrollida, milliseid ettevõttesiseseid menetlusi tootjad kasutasid selle tagamiseks, et nende tooted ja/või teenused vastaksid Euroopa küberturvalisuse sertifitseerimise kava nõuetele.

Muudatusettepanek 114

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

Komisjoni ettepanek	*Muudatusettepanek*
	(d a) võtta vastu siduvad eeskirjad, millega määratakse kindlaks, kui sageli peavad riiklikud sertifitseerimise järelevalveasutused sertifikaate ja ettevõtjate vastavuskinnitusi kontrollima, ja selliste kontrollide kriteeriumid, ulatus ja kohaldamisala, ning võtta artikli 50 lõike 6 kohaselt vastu ühised aruandlusnormid ja -eeskirjad;

Muudatusettepanek 115

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 116

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

Komisjoni ettepanek	*Muudatusettepanek*
	(f a) vahetada parimaid tavasid seoses vastavushindamisasutuste, Euroopa küberturvalisuse sertifikaadi omanike ning tootjate ja teenusepakkujate uurimistega, kes on esitanud ettevõtja kinnitused vastavuse kohta;

Muudatusettepanek 117

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

Komisjoni ettepanek	*Muudatusettepanek*
	(f b) soodustada Euroopa küberturvalisuse sertifitseerimise kavade ühtlustamist rahvusvaheliselt tunnustatud standarditega ning, kui see on asjakohane, soovitada ENISA-le valdkondi, kus ta peaks tegema koostööd asjaomaste rahvusvaheliste ja Euroopa standardiorganisatsioonidega, et kõrvaldada rahvusvaheliselt tunnustatud standardite puudused või lüngad;

Muudatusettepanek 118

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

Komisjoni ettepanek	*Muudatusettepanek*
	(f c) artiklis 43 a osutatud tööprogrammi koostamisel anda ENISA-le nõu selliste IKT toodete ja teenuste prioriteetide nimekirja kohta, mille suhtes ta peab vajalikuks kohaldada Euroopa küberturvalisuse sertifitseerimise kava;

Muudatusettepanek 119

Ettepanek võtta vastu määrus
Artikkel 53 – lõige 4 – lõik 1 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ENISA tagab, et rühma iga koosoleku järel koosoleku kava, päevakord ja vastuvõetud otsused registreeritakse ning nende dokumentide avaldatud versioonid tehakse ENISA veebisaidil üldsusele kättesaadavaks.

Muudatusettepanek 120

Ettepanek võtta vastu määrus
Artikkel 55 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Artikkel 55 a
	Delegeeritud volituste rakendamine
	Komisjonile antakse õigus võtta vastu delegeeritud õigusakte käesolevas artiklis sätestatud tingimustel.
	Artikli 44 lõikes 4 ja artikli 50 a lõikes 4 osutatud õigus võtta vastu delegeeritud õigusakte antakse komisjonile viieks aastaks alates [alusõigusakti jõustumise kuupäev]. Komisjon esitab delegeeritud volituste kohta aruande hiljemalt üheksa kuud enne viieaastase tähtaja möödumist. Volituste delegeerimist pikendatakse automaatselt samaks ajavahemikuks, välja arvatud juhul, kui Euroopa Parlament või nõukogu esitab selle suhtes vastuväite hiljemalt kolm kuud enne iga ajavahemiku lõppemist.
	Euroopa Parlament ja nõukogu võivad artikli 44 lõikes 4 ja artikli 50 a lõikes 4 osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast avaldamist Euroopa Liidu Teatajas või otsuses nimetatud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.
	Enne delegeeritud õigusakti vastuvõtmist konsulteerib komisjon kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes sätestatud põhimõtetega iga liikmesriigi määratud ekspertidega.
	Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, teeb ta selle samal ajal teatavaks Euroopa Parlamendile ja nõukogule.
	Artikli 44 lõike 4 ja artikli 50 a lõike 4 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.

NÕUANDVA KOMISJONI MENETLUS

Pealkiri	Määrus, mis käsitleb ENISAt ehk ELi küberturvalisuse ametit, millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 ja mis käsitleb info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist („küberturvalisust käsitlev õigusakt“)
Viited	COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)
Vastutav komisjon istungil teada andmise kuupäev	ITRE 23.10.2017
Arvamuse esitaja(d) istungil teada andmise kuupäev	IMCO 23.10.2017
Kaasatud komisjonid - istungil teada andmise kuupäev	18.1.2018
Arvamuse koostaja nimetamise kuupäev	Nicola Danti 25.9.2017
Läbivaatamine parlamendikomisjonis	21.2.2018 21.3.2018
Vastuvõtmise kuupäev	17.5.2018
Lõpphääletuse tulemus	+: 31 –: 2 0: 1
Lõpphääletuse ajal kohal olnud liikmed	John Stuart Agnew, Pascal Arimont, Dita Charanzová, Carlos Coelho, Anna Maria Corazza Bildt, Daniel Dalton, Nicola Danti, Dennis de Jong, Pascal Durand, Evelyne Gebhardt, Robert Jarosław Iwaszkiewicz, Liisa Jaakonsaari, Marlene Mizzi, Nosheena Mobarik, Jiří Pospíšil, Andreas Schwab, Olga Sehnalová, Jasenko Selimovic, Ivan Štefanec, Catherine Stihler, Mylène Troszczynski, Mihai Ţurcanu, Anneleen Van Bossuyt, Marco Zullo
Lõpphääletuse ajal kohal olnud asendusliikmed	Jan Philipp Albrecht, Kaja Kallas, Arndt Kohn, Emma McClarkin, Adam Szejnfeld, Marc Tarabella, Lambert van Nistelrooij, Kerstin Westphal
Lõpphääletuse ajal kohal olnud asendusliikmed (art 200 lg 2)	Inés Ayala Sender, Flavio Zanonato

NIMELINE LÕPPHÄÄLETUS NÕUANDVAS KOMISJONIS

31	+
ALDE	Dita Charanzová, Kaja Kallas, Jasenko Selimovic
ECR	Daniel Dalton, Emma McClarkin, Nosheena Mobarik, Anneleen Van Bossuyt
EFDD	Marco Zullo
GUE/NGL	Dennis de Jong
PPE	Pascal Arimont, Carlos Coelho, Anna Maria Corazza Bildt, Jiří Pospíšil, Andreas Schwab, Ivan Štefanec, Adam Szejnfeld, Mihai Ţurcanu, Lambert van Nistelrooij
S&D	Inés Ayala Sender, Nicola Danti, Evelyne Gebhardt, Liisa Jaakonsaari, Arndt Kohn, Marlene Mizzi, Olga Sehnalová, Catherine Stihler, Marc Tarabella, Kerstin Westphal, Flavio Zanonato
Verts/ALE	Jan Philipp Albrecht, Pascal Durand

2	–
EFDD	John Stuart Agnew, Robert Jarosław Iwaszkiewicz

1	0
ENF	Mylène Troszczynski

Kasutatud tähised:
+ : poolt
– : vastu
0 : erapooletu