Euroopa Parlament
2019-2024

Põhiseaduskomisjon

2022/0085(COD)

31.1.2023

ARVAMUS

Esitaja: põhiseaduskomisjon

Saaja: tööstuse, teadusuuringute ja energeetikakomisjon

ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites, ametites ja asutustes
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Arvamuse koostaja: Markéta Gregorová

PA_Legam

LÜHISELGITUS

Euroopa Liidu institutsioonid, organid ja asutused töötavad viimastel aastatel tehnoloogia pideva digitaalse arengu tingimustes, millega kaasneb ka üha suurem küberturvalisuse oht. Seda olukorda on süvendanud COVID-19 sanitaarkriisi puhkemine ja muu hulgas kaugtöö osatähtsuse suurenemine, millega koos on kasvanud ka eri allikatest pärinevate keerukate rünnakute arv.

Praegu on küberturvalisuse olukord (haldustavad, küberhügieen, üldine suutlikkus ja küpsus) liidu institutsioonides, organites ja asutustes väga erinev, mis omakorda takistab avatud, tõhusat ja sõltumatut Euroopa halduskorralduse toimimist.

Seetõttu nõustub raportöör, et liidu institutsioonides, organites ja asutustes tuleks välja kujundada ühtne üldine hoiak küberturvalisuse ühiste süsteemide ja meetmete kehtestamiseks, et tagada küberturvalisuse areng samas suunas ja suurendada sellega Euroopa halduskorralduse tõhusust ja sõltumatust.

Lisaks on raportöör arvamusel, et tugev ja järjepidev julgeolekuraamistik on äärmiselt oluline, et kaitsta kõiki ELi töötajaid, andmeid, sidevõrke, infosüsteeme ja otsustusprotsesse, millega toetatakse ka Euroopa Liidu demokraatlikku toimimist. Liidu institutsioonide, organite ja asutuste tugevama julgeolekukultuuri abil kohandataks Euroopa digiajastule vastavaks ja pandaks alus inimesi teenivale tulevikukindlale majandusele.

MUUDATUSETTEPANEKUD

Põhiseaduskomisjon palub vastutaval tööstuse, teadusuuringute ja energeetikakomisjonil võtta arvesse järgmisi muudatusettepanekuid:

Muudatusettepanek 1

Ettepanek võtta vastu määrus
Põhjendus 1

Komisjoni ettepanek	*Muudatusettepanek*
(1) Digiajastul on info- ja kommunikatsioonitehnoloogia avatud, tõhusa ja sõltumatu liidu halduskorralduse alustala. Tehnoloogia areng ning digisüsteemide kasvav keerukus ja omavaheline seotus võimendavad küberturvalisuse riske ja suurendavad liidu halduskorralduse vastuvõtlikkust küberohtudele ja -intsidentidele, mis omakorda seab ohtu haldusasutuste	(1) Digiajastul on info- ja kommunikatsioonitehnoloogia avatud, tõhusa ja sõltumatu liidu halduskorralduse alustala. Tehnoloogia areng ning digisüsteemide kasvav keerukus ja omavaheline seotus võimendavad küberturvalisuse riske ja suurendavad liidu halduskorralduse vastuvõtlikkust küberohtudele ja -intsidentidele, mis omakorda seab ohtu haldusasutuste

toimepidevuse ja võime tagada oma andmete turvalisus. Tänapäeval on pilveteenuste kasutamise kasv, ***IT*** kasutamine kõikjal, intensiivne digitaliseeritus, kaugtöö ning tehnoloogia ja ühenduvuse areng liidu haldusüksuste kõigi tegevuste põhielemendid, kuid digivastupidavusvõime ei ole sellesse veel piisavalt sisse ehitatud.	toimepidevuse ja võime tagada oma andmete turvalisus. Tänapäeval on pilveteenuste kasutamise kasv, ***info- ja kommunikatsioonitehnoloogia (IKT)*** kasutamine kõikjal, intensiivne digitaliseeritus, kaugtöö ning tehnoloogia ja ühenduvuse areng liidu haldusüksuste kõigi tegevuste põhielemendid, kuid digivastupidavusvõime ei ole sellesse veel piisavalt sisse ehitatud.

Selgitus

Komisjoni ettepanekus kasutatakse lühendit „IT“, see peaks aga olema „IKT“, mis on küberturvalisuse 2. direktiivis ja ELi küberturvalisuse määruses kasutatud standardmõiste.

Muudatusettepanek 2

Ettepanek võtta vastu määrus
Põhjendus 2

Komisjoni ettepanek	*Muudatusettepanek*
(2) Liidu institutsioone, organeid ja asutusi ümbritsevad küberohud arenevad pidevalt. Ohusubjektide taktika, metoodika ja töövõtted arenevad pidevalt, kuid selliste rünnete peamised ajendid muutuvad vähe: alates väärtusliku avalikustamata teabe varastamisest, kuni raha teenimise, avaliku arvamusega manipuleerimiseni või digitaristu kahjustamiseni. Küberründe korraldatakse aina sagedamini ning ründed ise muutuvad keerukamaks ja automatiseeritumaks; sihikule võetakse ohtudele avatud ja üha suurenevad ründepinnad ning nõrkusi kasutatakse kiiresti ära.	(2) Liidu institutsioone, organeid***, ameteid*** ja asutusi ümbritsevad küberohud arenevad pidevalt. Ohusubjektide taktika, metoodika ja töövõtted arenevad pidevalt, kuid selliste rünnete peamised ajendid muutuvad vähe: alates väärtusliku avalikustamata teabe varastamisest, kuni raha teenimise, avaliku arvamusega manipuleerimiseni või digitaristu kahjustamiseni. Küberründe korraldatakse aina sagedamini ning ründed ise ***ja meetodid*** muutuvad keerukamaks ja automatiseeritumaks; sihikule võetakse ohtudele avatud ja üha suurenevad ründepinnad ning nõrkusi kasutatakse kiiresti ära.

Muudatusettepanek 3

Ettepanek võtta vastu määrus
Põhjendus 3

Komisjoni ettepanek	*Muudatusettepanek*
(3) Liidu institutsioonide, organite ja asutuste ***IT-keskkonnad*** on omavahel seotud, andmevood on integreeritud ja nende kasutajad teevad tihedat koostööd. See omavaheline seotus tähendab, et isegi kui mõni katkestus piirdub esialgu ühe liidu institutsiooni, organi või asutusega, võib see kaasa tuua laiema ahelreaktsiooni, millel võib olla kaugeleulatuv ja pikaajaline negatiivne mõju ka teistele. Lisaks sellele on teatavate institutsioonide, organite ja asutuste ***IT-keskkonnad*** seotud liikmesriikide ***IT-keskkondadega*** ning see tähendab, et intsident ühes liidu üksuses võib seada ohtu liikmesriikide ***IT-keskkonna*** turvalisuse ja vastupidi.	(3) Liidu institutsioonide, organite***, ametite*** ja asutuste ***IKT-keskkonnad*** on omavahel seotud, andmevood on integreeritud ja nende kasutajad teevad tihedat koostööd. See omavaheline seotus tähendab, et isegi kui mõni katkestus piirdub esialgu ühe liidu institutsiooni, organi***, ameti*** või asutusega, võib see kaasa tuua laiema ahelreaktsiooni, millel võib olla kaugeleulatuv ja pikaajaline negatiivne mõju ka teistele. Lisaks sellele on teatavate institutsioonide, organite***, ametite*** ja asutuste ***IKT-keskkonnad*** seotud liikmesriikide ***IKT-keskkondadega*** ning see tähendab, et intsident ühes liidu üksuses võib seada ohtu liikmesriikide ***IKT-keskkonna*** turvalisuse ja vastupidi.

Muudatusettepanek 4
Ettepanek võtta vastu määrus
Põhjendus 4

Komisjoni ettepanek	*Muudatusettepanek*
(4) Liidu institutsioonid, organid ja asutused on atraktiivsed sihtmärgid, keda ähvardavad heade erialaste oskuste ja korralike ressurssidega ohusubjektid, aga ka muud ohud. Samas on kübervastupidavuse tase ning pahatahtliku kübertegevuse avastamise ja sellele reageerimise võime nendes üksustes väga erinev. Seepärast on Euroopa halduskorralduse toimimiseks vaja, et liidu institutsioonid, organid ja asutused saavutaksid küberturvalisuse ühtlaselt kõrge taseme küberturvalisuse baastasemega (ehk küberturvalisuse baaseeskirjadega, mida võrgu- ja infosüsteemid ning nende operaatorid ja kasutajad peaksid küberturvalisuse riskide ***minimeerimiseks*** järgima), ning teabevahetuse ja ***koostööga***	(4) Liidu institutsioonid, organid***, ametid*** ja asutused on atraktiivsed sihtmärgid, keda ähvardavad heade erialaste oskuste ja korralike ressurssidega ohusubjektid, aga ka muud ohud. Samas on kübervastupidavuse tase ning pahatahtliku kübertegevuse avastamise ja sellele reageerimise võime nendes üksustes väga erinev. Seepärast on Euroopa halduskorralduse toimimiseks vaja, et liidu institutsioonid, organid***, ametid*** ja asutused saavutaksid küberturvalisuse ühtlaselt kõrge taseme küberturvalisuse baastasemega (ehk ***ühiste*** küberturvalisuse baaseeskirjadega, mida võrgu- ja infosüsteemid ning nende operaatorid ja kasutajad peaksid küberturvalisuse riskide ***piiramiseks*** järgima), ning ***regulaarse ja tõhusa*** teabevahetuse***, koostöö*** ja ***küberturvalisuse alase koolitusega.***

Muudatusettepanek 5

Ettepanek võtta vastu määrus
Põhjendus 7

Komisjoni ettepanek	*Muudatusettepanek*
(7) Erinevused liidu institutsioonide, organite ja asutuste vahel eeldavad paindlikku rakendamist, sest üks ja sama lahendus ei sobi kõigile. Küberturvalisuse ühtlaselt kõrge taseme tagamise meetmed ***ei tohiks sisaldada kohustusi, mis sekkuvad otseselt*** liidu institutsioonide, organite ja asutuste ülesannete ***täitmisse või piiravad*** nende institutsioonilist sõltumatust. Seega peaksid need institutsioonid, organid ja asutused kehtestama oma küberturvalisuse raamistikud küberturvalisuse alaste riskide juhtimise, haldamise ja kontrollimise jaoks ning võtma vastu oma baastaseme ja küberturvalisuse kavad.	(7) Erinevused liidu institutsioonide, organite***, ametite*** ja asutuste vahel eeldavad paindlikku rakendamist, sest üks ja sama lahendus ei sobi kõigile. Küberturvalisuse ühtlaselt kõrge taseme tagamise meetmed ***peaksid toetama*** liidu institutsioonide, organite***, ametite*** ja asutuste ülesannete ***täitmist ning võtma arvesse*** nende institutsioonilist sõltumatust. Seega peaksid need institutsioonid, organid***, ametid*** ja asutused kehtestama oma küberturvalisuse raamistikud küberturvalisuse alaste riskide juhtimise, haldamise ja kontrollimise jaoks ning võtma vastu oma baastaseme ja küberturvalisuse kavad***, võttes seejuures arvesse vastavate raamistike sidusust ja koostalitlusvõimet, ning mis põhinevad käesolevas määruses sätestatud ühisel raamistikul***.

Muudatusettepanek 6
Ettepanek võtta vastu määrus
Põhjendus 8

Komisjoni ettepanek	*Muudatusettepanek*
(8) Vältimaks ebaproportsionaalse finants- ja halduskoormuse kehtestamist liidu institutsioonidele, organitele ja asutustele, peaksid küberturvalisuse riskide juhtimise nõuded olema ***proportsionaalsed*** asjaomase võrgu- ja infosüsteemi puhul esineva riskiga, võttes seejuures arvesse selliste meetmete kõrget tehnilist taset. Iga liidu institutsioon, organ ja asutus peaks püüdma eraldada oma ***IT-eelarvest piisava osa*** oma küberturvalisuse taseme tõstmiseks***; pikemas perspektiivis tuleks eesmärgiks seada ligikaudu 10 %.***	(8) Vältimaks ebaproportsionaalse finants- ja halduskoormuse kehtestamist liidu institutsioonidele, organitele***, ametitele*** ja asutustele, peaksid küberturvalisuse riskide juhtimise nõuded olema ***vastavuses*** asjaomase võrgu- ja infosüsteemi puhul esineva riskiga, võttes seejuures arvesse selliste meetmete kõrget tehnilist taset. Iga liidu institutsioon, organ***, amet*** ja asutus peaks püüdma eraldada oma ***IKT-eelarvest vähemalt 10%*** oma küberturvalisuse taseme tõstmiseks ***keskpika perioodi vältel ja vajaduse korral***

rohkem pikaajalise perioodi jooksul;

Muudatusettepanek 7

Ettepanek võtta vastu määrus
Põhjendus 9

Komisjoni ettepanek	*Muudatusettepanek*
(9) Küberturvalisuse ühtlaselt kõrge taseme saavutamiseks peab küberturvalisus kuuluma iga liidu institutsiooni, organi ja asutuse kõrgeima ***juhtimistasandi järelevalve alla***, kes peaks kiitma heaks küberturvalisuse baastaseme, mis peaks maandama iga institutsiooni, organi ja asutuse kehtestatava raamistiku kohaselt kindlaks tehtud riske. Tegelemine küberturvalisuse kultuuriga, st igapäevase küberturvalisusega, ***on*** kõigis liidu institutsioonides, organites ja asutustes küberturvalisuse baastaseme ***lahutamatu osa***.	(9) Küberturvalisuse ühtlaselt kõrge taseme saavutamiseks peab küberturvalisus kuuluma ***liiduülese ühisnõukogu järelevalve alla koostöös*** iga liidu institutsiooni, organi***, ameti*** ja asutuse kõrgeima ***juhtimistasandiga***, kes peaks kiitma heaks küberturvalisuse baastaseme, mis peaks maandama iga institutsiooni, organi***, ameti*** ja asutuse kehtestatava raamistiku kohaselt kindlaks tehtud riske. Tegelemine küberturvalisuse kultuuriga, st igapäevase küberturvalisusega, ***peaks muutuma*** kõigis liidu institutsioonides, organites***, ametites*** ja asutustes küberturvalisuse baastaseme ***lahutamatuks osaks***.

Muudatusettepanek 8

Ettepanek võtta vastu määrus
Põhjendus 10

Komisjoni ettepanek	*Muudatusettepanek*
(10) Liidu institutsioonid, organid ja asutused peaksid hindama riske, mis tulenevad suhetest tarnijate ja teenuseosutajatega, sh andmetalletuse ja andmetöötlusteenuste pakkujate või hallatavate turbeteenuste pakkujatega, ning võtma asjakohaseid meetmeid nende riskide vähendamiseks. Need meetmed peaksid olema küberturvalisuse baastaseme osa ning neid tuleks CERT-EU välja antavates juhenddokumentides ja soovitustes täpsemalt kirjeldada. Meetmete ja suuniste kindlaksmääramisel tuleks	(10) Liidu institutsioonid, organid***,*** ***ametid*** ja asutused peaksid hindama riske, mis tulenevad suhetest tarnijate ja teenuseosutajatega, sh andmetalletuse ja andmetöötlusteenuste pakkujate või hallatavate turbeteenuste pakkujatega, ning võtma asjakohaseid meetmeid nende riskide vähendamiseks. ***Neid tarnijaid ja teenuseosutajaid tuleks põhjalikult kontrollida, võttes arvesse kogu tarneahela ulatust ning majanduslikku ja poliitilist keskkonda, kus nad tegutsevad. Kui suhted tarnijate ja teenuseosutajatega***

nõuetekohaselt arvesse võtta asjakohaseid ELi õigusakte ja põhimõtteid, sh võrgu- ja infoturbe koostöörühma tehtud riskihindamisi ja soovitusi, näiteks ELi kooskõlastatud riskihindamine ja ELi meetmepakett 5G-võrkude turvalisuse tagamiseks. Lisaks ***võiks*** nõuda asjaomaste IKT toodete, teenuste ja protsesside sertifitseerimist vastavalt konkreetsetele ELi küberturvalisuse sertifitseerimise kavadele, mis on võetud vastu määruse (EL) 2019/881 artikli 49 kohaselt.

ohustavad ELi demokraatlike protsesside terviklikkust, tuleks need põhjendamatu viivituseta lõpetada. Need meetmed peaksid olema küberturvalisuse baastaseme osa ning neid tuleks CERT-EU välja antavates juhenddokumentides ja soovitustes täpsemalt kirjeldada. Meetmete ja suuniste kindlaksmääramisel tuleks nõuetekohaselt arvesse võtta asjakohaseid ELi õigusakte ja põhimõtteid, sh võrgu- ja infoturbe koostöörühma tehtud riskihindamisi ja soovitusi, näiteks ELi kooskõlastatud riskihindamine ja ELi meetmepakett 5G-võrkude turvalisuse tagamiseks. Lisaks ***tuleks ümbritsevaid küberohtusid ja vastupidavuse suurendamist arvesse võttes*** nõuda ***liidu institutsioonides, organites, ametites ja asutustes kasutatavate*** asjaomaste IKT toodete, teenuste ja protsesside sertifitseerimist vastavalt konkreetsetele ELi küberturvalisuse sertifitseerimise kavadele, mis on võetud vastu määruse (EL) 2019/881 artikli 49 kohaselt.

Muudatusettepanek 9

Ettepanek võtta vastu määrus
Põhjendus 13

Komisjoni ettepanek	*Muudatusettepanek*
(13) Paljud küberründed on osa laiematest rünnakutest, mis on suunatud liidu institutsioonide, organite ja asutuste rühmade vastu või huviringkondade vastu, kuhu kuuluvad ka liidu institutsioonid, organid ja asutused. Ettevaatava tuvastamise, intsidentidele reageerimise ja leevendusmeetmete võimaldamiseks peaksid liidu institutsioonid, organid ja asutused teatama CERT-EU-le olulistest küberohtudest, olulistest nõrkustest ja olulistest intsidentidest ning jagama asjakohaseid tehnilisi üksikasju, et teistes liidu institutsioonides, organites ja asutustes oleks võimalik samalaadseid	(13) Paljud küberründed on osa laiematest rünnakutest, mis on suunatud liidu institutsioonide, organite***, ametite*** ja asutuste rühmade vastu või huviringkondade vastu, kuhu kuuluvad ka liidu institutsioonid, organid***, ametid*** ja asutused. Ettevaatava tuvastamise, intsidentidele reageerimise ja leevendusmeetmete võimaldamiseks peaksid liidu institutsioonid, organid***, ametid*** ja asutused teatama CERT-EU-le olulistest küberohtudest, olulistest nõrkustest ja olulistest intsidentidest ning jagama asjakohaseid tehnilisi üksikasju, et teistes liidu institutsioonides, organites**,**

küberohte, nõrkusi ja intsidente tuvastada või leevendada ja neile reageerida. Järgides samasugust lähenemisviisi, nagu on visandatud direktiivis [küberturvalisuse 2. direktiivi ettepanek], peaks üksustel olema kohustus esitada CERT-EU-le ***esialgne teade*** 24 tunni jooksul pärast seda, kui nad saavad teada olulisest intsidendist. Selline teabevahetus peaks andma CERT-EU-le võimaluse levitada teavet teistele liidu institutsioonidele, organitele ja asutustele ning asjaomastele partneritele, et aidata kaitsta liidu ***IT-keskkondi*** ja liidu partnerite ***IT-keskkondi*** samalaadsete intsidentide, ohtude ja nõrkuste eest.

ametites ja asutustes oleks võimalik samalaadseid küberohte, nõrkusi ja intsidente tuvastada või leevendada ja neile reageerida. Järgides samasugust lähenemisviisi, nagu on visandatud direktiivis [küberturvalisuse 2. direktiivi ettepanek], peaks üksustel olema kohustus esitada CERT-EU-le ***varajane hoiatus viivitamata ja igal juhul hiljemalt*** 24 tunni jooksul pärast seda, kui nad saavad teada olulisest intsidendist. ***Liidu institutsioonidele, organitele, ametitele ja asutustele tuleks eraldada piisavalt vahendeid aruandluskohustuste kiireks ja tõhusaks täitmiseks, et tagada kavandatud süsteemi nõuetekohane toimimine.*** Selline teabevahetus peaks andma CERT-EU-le võimaluse levitada teavet teistele liidu institutsioonidele, organitele***, ametitele*** ja asutustele ning asjaomastele partneritele, et aidata kaitsta liidu ***IKT-keskkondi*** ja liidu partnerite ***IKT-keskkondi*** samalaadsete intsidentide, ohtude ja nõrkuste eest.

Muudatusettepanek 10

Ettepanek võtta vastu määrus
Põhjendus 14

Komisjoni ettepanek	*Muudatusettepanek*
(14) Lisaks sellele, et CERT-EU-le antakse rohkem ülesandeid ja laiem tegevusulatus, tuleks luua institutsioonidevaheline küberturvalisuse nõukoda (IICB), mis peaks soodustama küberturvalisuse ühtlaselt kõrget taset liidu institutsioonides, organites ja asutustes sellega, et teeb seiret selle üle, kuidas liidu institutsioonid, organid ja asutused käesolevat määrust rakendavad, ja järelevalvet CERT-EU üldiste prioriteetide ja eesmärkide rakendamise üle ning tagab CERT-EU strateegilise juhtimise. IICB peaks tagama institutsioonide esindatuse ning kaasama organite ja asutuste esindajad läbi liidu asutuste võrgustiku.	(14) Lisaks sellele, et CERT-EU-le antakse rohkem ülesandeid ja laiem tegevusulatus, tuleks luua institutsioonidevaheline küberturvalisuse nõukoda (IICB), mis peaks soodustama küberturvalisuse ühtlaselt kõrget taset liidu institutsioonides, organites***, ametites*** ja asutustes sellega, et teeb seiret selle üle, kuidas liidu institutsioonid, organid***, ametid*** ja asutused käesolevat määrust rakendavad, ja järelevalvet CERT-EU üldiste prioriteetide ja eesmärkide rakendamise üle ning tagab CERT-EU strateegilise juhtimise. IICB peaks tagama institutsioonide ***võrdse*** esindatuse ning kaasama organite***, ametite*** ja asutuste

esindajad läbi liidu asutuste võrgustiku.

Muudatusettepanek 11

Ettepanek võtta vastu määrus
Põhjendus 16

Komisjoni ettepanek	*Muudatusettepanek*
(16) IICB peaks seirama nii käesoleva määruse järgimist kui ka juhenddokumentide ja soovituste ning CERT-EU esitatud üleskutsete järelmeetmeid. Tehnilistes küsimustes peaks IICB-d toetama tehnilised nõuanderühmad, ***mille koosseis vastab IICB äranägemisele ja*** mis peaksid tegema tihedat koostööd CERT-EU, liidu institutsioonide, organite ja asutuste ja muude sidusrühmadega, nagu parasjagu ***vajalik***. Vajaduse korral peaks IICB avaldama ***mittesiduvaid*** hoiatusi ja soovitama ***auditeid***.	(16) IICB peaks seirama nii käesoleva määruse järgimist kui ka juhenddokumentide ja soovituste ning CERT-EU esitatud üleskutsete järelmeetmeid. Tehnilistes küsimustes peaks IICB-d toetama tehnilised nõuanderühmad, mis peaksid tegema tihedat koostööd CERT-EU, liidu institutsioonide, organite***, ametite*** ja asutuste ja muude sidusrühmadega, nagu parasjagu ***asjakohane***. Vajaduse korral peaks IICB avaldama hoiatusi ja soovitama ***auditite läbiviimist***.

Muudatusettepanek 12

Ettepanek võtta vastu määrus
Põhjendus 17

Komisjoni ettepanek	*Muudatusettepanek*
(17) CERT-EU ülesanne peaks olema aidata kaasa kõigi liidu institutsioonide, organite ja asutuste ***IT-keskkonna*** turvalisusele. CERT-EU peaks tegutsema samaväärsena koordineerijaga, kes on liidu institutsioonidele, organitele ja asutustele määratud Euroopa nõrkuste registrile nõrkuste koordineeritud avalikustamise jaoks, nagu on osutatud direktiivi [küberturvalisuse 2. direktiivi ettepanek] artiklis 6.	(17) CERT-EU ülesanne peaks olema aidata kaasa kõigi liidu institutsioonide, organite***, ametite*** ja asutuste ***IKT-keskkonna*** turvalisusele. CERT-EU peaks tegutsema samaväärsena koordineerijaga, kes on liidu institutsioonidele, organitele***, ametitele*** ja asutustele määratud Euroopa nõrkuste registrile nõrkuste koordineeritud avalikustamise jaoks, nagu on osutatud direktiivi [küberturvalisuse 2. direktiivi ettepanek] artiklis 6.

Muudatusettepanek 13

Ettepanek võtta vastu määrus

Põhjendus 18

Komisjoni ettepanek	*Muudatusettepanek*
(18) 2020. aastal püstitas CERT-EU juhtnõukogu uue strateegilise eesmärgi, et CERT-EU kindlustaks kõigi liidu institutsioonide, organite ja asutuste kõikehõlmava küberkaitse, mis oleks piisavalt ulatuslik ja põhjalik ning kohaneks pidevalt olemasolevate või tulevaste ohtudega, nagu ründed mobiilsete seadmete, pilvekeskkondade ja esemevõrgu seadmete vastu. Strateegiline eesmärk hõlmab ka laia tegevusulatusega turbekeskusi, mis tegelevad võrkude seirega ja tõsiste ohtude pideva seirega. CERT-EU peaks toetama suuremate liidu institutsioonide, organite ja asutuste ***IT-turbe*** meeskondi, sh esmatasandi pideva seirega. Väiksematele ja mõnedele keskmise suurusega liidu institutsioonidele, organitele ja asutustele peaks CERT-EU pakkuma kõiki teenuseid.	(18) 2020. aastal püstitas CERT-EU juhtnõukogu uue strateegilise eesmärgi, et CERT-EU kindlustaks kõigi liidu institutsioonide, organite***, ametite*** ja asutuste kõikehõlmava küberkaitse, mis oleks piisavalt ulatuslik ja põhjalik ning kohaneks pidevalt olemasolevate või tulevaste ohtudega, nagu ründed mobiilsete seadmete, pilvekeskkondade ja esemevõrgu seadmete vastu. Strateegiline eesmärk hõlmab ka laia tegevusulatusega turbekeskusi, mis tegelevad võrkude seirega ja tõsiste ohtude pideva seirega. CERT-EU peaks toetama suuremate liidu institutsioonide, organite***, ametite*** ja asutuste ***IKT-turbe*** meeskondi, sh esmatasandi pideva seirega. Väiksematele ja mõnedele keskmise suurusega liidu institutsioonidele, organitele***, ametitele*** ja asutustele peaks CERT-EU pakkuma kõiki teenuseid.

Muudatusettepanek 14

Ettepanek võtta vastu määrus
Põhjendus 19 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(19a) Et tagada küberturvalisuse meetmete ja suuniste parem rakendamine liidu institutsioonides, organites, ametites ja asutustes ning tugevdada neis küberturvalisuse kultuuri, peaks CERT-EU tõhustama koostööd ka küberturvalisuse pädevusvõrgustiku ning -keskusega.

Muudatusettepanek 15

Ettepanek võtta vastu määrus
Põhjendus 20

Komisjoni ettepanek	*Muudatusettepanek*
(20) Operatiivse küberturvalisuse toetamisel peaks CERT-EU kasutama Euroopa Liidu Küberturvalisuse Ameti (ENISA) olemasolevaid oskusteadmisi struktureeritud koostöö kaudu, nagu on sätestatud Euroopa Parlamendi ja nõukogu määruses (EL) 2019/***881***[5]. ***Asjakohasel juhul tuleks*** kahe üksuse vahel kehtestada erikord, et määrata kindlaks sellise koostöö praktiline kulg ja vältida tegevuse dubleerimist. CERT-EU peaks tegema Euroopa Liidu Küberturvalisuse Ametiga ohuanalüüsi alast koostööd ning jagama ametiga regulaarselt oma ohtude kaardistamise aruannet.	(20) Operatiivse küberturvalisuse toetamisel peaks CERT-EU kasutama Euroopa Liidu Küberturvalisuse Ameti (ENISA) olemasolevaid oskusteadmisi struktureeritud koostöö kaudu, nagu on sätestatud Euroopa Parlamendi ja nõukogu määruses (EL) 2019/***881***. Kahe üksuse vahel ***tuleks*** kehtestada erikord, et määrata kindlaks sellise koostöö praktiline kulg ja vältida tegevuse dubleerimist. CERT-EU peaks tegema Euroopa Liidu Küberturvalisuse Ametiga ohuanalüüsi alast koostööd ning jagama ametiga regulaarselt oma ohtude kaardistamise aruannet.
[5] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).	[5] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).

Muudatusettepanek 16
Ettepanek võtta vastu määrus
Põhjendus 24

Komisjoni ettepanek	*Muudatusettepanek*
(24) CERT-EU teenused ja ülesanded on kõigi liidu institutsioonide, organite ja asutuste huvides ning seega peaks iga ***IT-eelarvega*** liidu institutsioon, organ ja asutus andma nende teenuste ja ülesannete jaoks oma ***õiglase*** panuse. Selline panus ei piira liidu institutsioonide, organite ja asutuste eelarveautonoomiat.	(24) CERT-EU teenused ja ülesanded on kõigi liidu institutsioonide, organite***,*** ***ametite*** ja asutuste huvides ning seega peaks iga ***IKT-eelarvega*** liidu institutsioon, organ***, amet*** ja asutus andma nende teenuste ja ülesannete jaoks oma ***proportsionaalse*** panuse. Selline panus ei piira liidu institutsioonide, organite***,*** ***ametite*** ja asutuste eelarveautonoomiat.

Muudatusettepanek 17

Ettepanek võtta vastu määrus
Põhjendus 25

Komisjoni ettepanek	*Muudatusettepanek*
(25) IICB peaks CERT-EU abiga läbi vaatama ja hindama käesoleva määruse rakendamist ja teatama oma järeldustest komisjonile. Sellele sisendile toetudes peaks komisjon esitama aruande Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele,	(25) IICB peaks CERT-EU abiga läbi vaatama ja hindama käesoleva määruse rakendamist ja teatama oma järeldustest komisjonile. Sellele sisendile toetudes peaks komisjon esitama ***vähemalt iga kolme aasta järel*** aruande Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele,

Muudatusettepanek 18

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

Komisjoni ettepanek	*Muudatusettepanek*
(a) liidu institutsioonide, organite ja asutuste kohustused kehtestada sisemise küberturvalisuse alaste riskide juhtimise, haldamise ja kontrollimise raamistik,	(a) liidu institutsioonide, organite***,*** ***ametite*** ja asutuste kohustused kehtestada sisemise küberturvalisuse alaste riskide juhtimise, haldamise ja kontrollimise raamistik,

Muudatusettepanek 19

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

Komisjoni ettepanek	*Muudatusettepanek*
(c) liidu institutsioonide, organite ja asutuste küberturvalisuse keskuse (CERT-EU) töökorralduse ja toimimise ning institutsioonidevahelise küberturvalisuse nõukoja töökorralduse ja toimimise eeskirjad.	(c) liidu institutsioonide, organite***,*** ***ametite*** ja asutuste küberturvalisuse keskuse (CERT-EU) töökorralduse ja toimimise ning institutsioonidevahelise küberturvalisuse nõukoja***(IICB)*** töökorralduse ja toimimise eeskirjad.

Muudatusettepanek 20

Ettepanek võtta vastu määrus
Artikkel 2 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Artikkel 2a
	Isikuandmete töötlemine
	CERT-EU, IICB ning kõik liidu institutsioonid, organid, ametid ja asutused töötlevad käesoleva määruse alusel isikuandmeid kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2018/1725.

Muudatusettepanek 21

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

Komisjoni ettepanek	*Muudatusettepanek*
(2) „võrgu- ja infosüsteem“ – ***võrgu- ja infosüsteem*** direktiivi [küberturvalisuse 2. direktiivi ettepanek] artikli ***4 punkti*** 1 ***tähenduses***;	(2) „võrgu- ja infosüsteem“ – direktiivi [küberturvalisuse 2. direktiivi ettepanek] artikli ***6 punktis*** 1 ***määratletud võrgu- ja infosüsteem***;

Muudatusettepanek 22

Ettepanek võtta vastu määrus
Artikkel 3 – lõik 1 – punkt 4

Komisjoni ettepanek	*Muudatusettepanek*
(4) „küberturvalisus“ – ***küberturvalisus direktiivi [küberturvalisuse 2. direktiivi ettepanek] artikli 4 punkti 3 tähenduses***;	(4) „küberturvalisus“ – ***Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881[1a] artikli 2 punktis 1 määratletud küberturvalisus***;
	1a Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus

(EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).

Muudatusettepanek 23

Ettepanek võtta vastu määrus
Artikkel 3 – lõik 1 – punkt 5

Komisjoni ettepanek	*Muudatusettepanek*
(5) „kõrgeim juhtimistasand“ – halduslikult kõige kõrgema tasandi juht, juhtkond või koordineerimise ja järelevalvega tegelev organ, võttes arvesse iga liidu institutsiooni, organi või asutuse kõrgema taseme juhtimise korda;	(5) „kõrgeim juhtimistasand“ – halduslikult kõige kõrgema tasandi juht, juhtkond või koordineerimise ja järelevalvega tegelev organ, ***kellel on volitus teha otsuseid või anda otsuste tegemiseks luba,*** võttes arvesse iga liidu institutsiooni, organi***, ameti*** või asutuse kõrgema taseme juhtimise korda;

Muudatusettepanek 24

Ettepanek võtta vastu määrus
Artikkel 3 – lõik 1 – punkt 7

Komisjoni ettepanek	*Muudatusettepanek*
(7) „oluline intsident“ – mis ***tahes intsident, v.a intsidendid, mille mõju on piiratud ja mille metoodika*** või ***tehnoloogia*** on ***tõenäoliselt juba hästi teada***;	(7) „oluline intsident“ – ***intsident,*** mis ***on põhjustanud või võib põhjustada tõsiseid häireid liidu üksuse toimimisele või asjaomasele liidu üksusele rahalist kahju*** või ***mis*** on ***mõjutanud või võib mõjutada teisi füüsilisi või juriidilisi isikuid, põhjustades neile märkimisväärset materiaalset või mittemateriaalset kahju***;

Muudatusettepanek 25

Ettepanek võtta vastu määrus
Artikkel 3 – lõik 1 – punkt 11

Komisjoni ettepanek	*Muudatusettepanek*
(11) „oluline küberoht“ – ***küberoht, millel eesmärk on põhjustada oluline intsident või millel on võimalus ja suutlikkus põhjustada oluline intsident***;	(11) „oluline küberoht“ – ***direktiivi [küberturvalisuse 2. direktiivi ettepanek] artikli 6 punktis 11 määratletud küberoht***;

Muudatusettepanek 26

Ettepanek võtta vastu määrus
Artikkel 3 – lõik 1 – punkt 14

Komisjoni ettepanek	*Muudatusettepanek*
(14) ***„küberturvalisuse risk“*** *– **mõistlikult tuvastatav asjaolu või sündmus, mis võib kahjustada võrgu- ja infosüsteemide turvalisust***;	(14) ***„risk“ – direktiivi [küberturvalisuse 2. direktiivi ettepanek] artikli 6 punktis 9 määratletud risk***;

Muudatusettepanek 27

Ettepanek võtta vastu määrus
Artikkel 3 – lõik 1 – punkt 14 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(14a) „IKT-keskkond“ – mis tahes kohapealne või virtuaalne IKT-toode, -teenus ja -protsess, nagu on määratletud määruse (EL) 2019/881 artikli 2 punktides 12, 13 ja 14, ning mis tahes võrgu- ja infosüsteem, mida omab ja käitab liidu institutsioon, organ, amet või asutus või mida majutab või käitab kolmas isik, sealhulgas mobiilseadmed, ettevõttevõrgud ja internetiga ühendamata koondisevõrgud ja mistahes seadmed, mis on ühendatud IKT-keskkonnaga;

Selgitus

Mõiste viidi käesoleva ettepaneku artikli 4 lõikest 2 üle mõisteid käsitlevasse artiklisse, võttes arvesse, et seda mõistet kasutatakse kogu tekstis järjepidevalt. Selle mõiste soovitatud määratlus põhineb selle osade määratlustel küberturvalisuse määruse (EL) 2019/881 artiklis 2.

Muudatusettepanek 28

Ettepanek võtta vastu määrus
Artikkel 3 – lõik 1 – punkt 15

Komisjoni ettepanek	*Muudatusettepanek*
(15) „ühine küberüksus“ – liidu erinevate küberturvalisuse kogukondade jaoks tegutsev virtuaalne ja füüsiline koostööplatvorm, milles keskendutakse operatiivsele ja tehnilisele koordineerimisele, et tulla toime oluliste piiriüleste küberohtude ja intsidentidega komisjoni 23. juuni 2021. aasta soovituse tähenduses;	***välja jäetud***

Muudatusettepanek 29
Ettepanek võtta vastu määrus
Artikkel 4 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Iga liidu institutsioon, organ ja asutus ***kehtestab*** oma sisemise küberturvalisuse alaste riskide juhtimise, haldamise ja kontrollimise raamistiku (edaspidi „raamistik“), mis toetab üksuse missiooni ja selle institutsionaalset sõltumatust. Selle töö eest vastutab üksuse kõrgeim juhtimistasand, ***et tagada*** kõigi küberturvalisuse riskide ***tulemuslik*** ja ***usaldusväärne juhtimine***. ***Raamistik tuleb kehtestada hiljemalt ...*** [15 kuud pärast käesoleva määruse ***jõustumist]***.	1. ***Täielikku turvaauditit aluseks võttes kehtestab*** iga liidu institutsioon, organ***, amet*** ja asutus oma sisemise küberturvalisuse alaste riskide juhtimise, haldamise ja kontrollimise raamistiku (edaspidi „raamistik“), mis toetab üksuse missiooni ja selle institutsionaalset sõltumatust***, võttes arvesse oma raamistiku sidusust ja koostalitlusvõimet muude asjaomaste institutsioonide, organite, ametite ja asutuste raamistikega***. Selle töö eest vastutab üksuse kõrgeim juhtimistasand, ***kes tagab*** kõigi küberturvalisuse riskide ***tulemusliku*** ja ***usaldusväärse juhtimise***. Raamistik tuleb kehtestada hiljemalt ... [15 kuud pärast käesoleva määruse ***jõustumise kuupäeva]***.

Muudatusettepanek 30

Ettepanek võtta vastu määrus
Artikkel 4 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Raamistik peab hõlmama asjaomase institutsiooni, organi või asutuse kogu ***IT-keskkonda***, sh ruumides kohapeal	2. Raamistik peab hõlmama asjaomase institutsiooni, organi***, ameti*** või asutuse kogu ***IKT-keskkonda***, sh ruumides

olev ***IT-keskkond***, hanke korras sisse ostetavad varad ja teenused, mis asuvad pilvandmetöötluse keskkondades või mida majutavad kolmandad isikud, mobiilseadmed, ettevõttevõrgud, internetiga ühendamata koondisevõrgud ja mistahes seadmed, mis on ühendatud ***IT-keskkonnaga***. Raamistik võtab arvesse toimepidevust ja kriisijuhtimist ning peab silmas tarneahela turvalisust ja selliste inimriskide juhtimist, mis võivad mõjutada mõjutatud liidu institutsioonide, organite ja asutuste küberturvalisust.	kohapeal olev ***IKT-keskkond***, hanke korras sisse ostetavad varad ja teenused, mis asuvad pilvandmetöötluse keskkondades või mida majutavad kolmandad isikud, mobiilseadmed, ettevõttevõrgud, internetiga ühendamata koondisevõrgud ja mistahes seadmed, mis on ühendatud ***IKT-keskkonnaga***. Raamistik võtab arvesse toimepidevust ja kriisijuhtimist ning peab silmas tarneahela turvalisust ja selliste inimriskide juhtimist, mis võivad mõjutada mõjutatud liidu institutsioonide, organite***,*** ***ametite*** ja asutuste küberturvalisust.

Muudatusettepanek 31
Ettepanek võtta vastu määrus
Artikkel 4 – lõige 4

Komisjoni ettepanek	*Muudatusettepanek*
4. Igas liidu institutsioonis, organis ja asutuses peavad olema toimivad mehhanismid, mis tagavad, et küberturvalisusele kulutatakse ***piisav osa IT-eelarvest***.	4. Igas liidu institutsioonis, organis***,*** ***ametis*** ja asutuses peavad olema toimivad mehhanismid, mis tagavad, et küberturvalisusele kulutatakse ***keskpika perioodi jooksul vähemalt 10 % IKT üldeelarvest***.

Muudatusettepanek 32

Ettepanek võtta vastu määrus
Artikli 4 – lõige 5 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	5a. Kohalik küberturvalisuse ametnik teeb koostööd määruse (EL) 2018/1725 artiklis 43 osutatud andmekaitseametnikuga, kui ta tegeleb kattuvate tegevustega, mida kohaldatakse lõimitud ja vaikimisi andmekaitse küberturvalisuse meetmete suhtes kui valitakse välja küberturvalisuse meetmed, mis hõlmavad isikuandmete kaitset, integreeritud riskijuhtimist ja turvaintsidentide integreeritud käsitlemist.

Muudatusettepanek 33

Ettepanek võtta vastu määrus
Artikkel 5 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Iga liidu institutsiooni, organi ja asutuse kõrgeim juhtimistasand kiidab heaks üksuse enda küberturvalisuse baastaseme, et vähendada artikli 4 lõikes 1 osutatud raamistiku kohaselt kindlaks tehtud riske. Ta teeb seda oma missiooni toetamiseks ja institutsioonilise sõltumatuse teostamiseks. Küberturvalisuse baastase tuleb kehtestada hiljemalt ... [18 kuud pärast käesoleva määruse ***jõustumist]*** ning selles tuleb käsitleda I lisas loetletud valdkondi ja II lisas loetletud meetmeid.	1. Iga liidu institutsiooni, organi***,*** ***ameti*** ja asutuse kõrgeim juhtimistasand kiidab heaks üksuse enda küberturvalisuse baastaseme, et vähendada artikli 4 lõikes 1 osutatud raamistiku kohaselt kindlaks tehtud riske. Ta teeb seda oma missiooni toetamiseks ja institutsioonilise sõltumatuse teostamiseks ***täielikus kooskõlas käesoleva määruse nõuetega ning võttes arvesse oma raamistiku sidusust ja koostalitlusvõimet muude asjaomaste institutsioonide, organite, ametite ja asutuste raamistikega ning samuti IICB poolt CERT-EU ettepanekul vastu võetud juhenddokumente ja soovitusi ning kohaldatavaid ELi küberturvalisuse sertifitseerimise kavasid***. Küberturvalisuse baastase tuleb kehtestada hiljemalt ... [18 kuud pärast käesoleva määruse ***jõustumise kuupäeva]*** ning selles tuleb käsitleda I lisas loetletud valdkondi ja II lisas loetletud meetmeid.

Muudatusettepanek 34

Ettepanek võtta vastu määrus
Artikkel 5 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Iga liidu institutsiooni, organi ja asutuse kõrgem juhtkond osaleb regulaarselt spetsiaalsetel koolitustel, et omandada piisavad teadmised ja oskused, et mõista ja hinnata küberturvalisuse riske ja riskide juhtimistavasid ning nende mõju organisatsiooni ***tegevusele***.	2. Iga liidu institutsiooni, organi***,*** ***ameti*** ja asutuse kõrgem juhtkond osaleb regulaarselt spetsiaalsetel koolitustel, et omandada piisavad teadmised ja oskused, et mõista ja hinnata küberturvalisuse riske ja riskide juhtimistavasid ning nende mõju organisatsiooni ***tegevusele koos vajalike ressurssidega. Lisaks sellistele erikoolitustele ning küberturvalisuse kultuuri loomise ja tugevdamise eesmärgil lisatakse küberturvalisuse kavasse***

	töötajate korrapärase küberturvalisuse koolituse kava ja seda ajakohastatakse vähemalt iga kahe aasta järel. Kvaliteetse koolituse pakkumiseks tuleb tagada piisavad vahendid.

Muudatusettepanek 35

Ettepanek võtta vastu määrus
Artikkel 6 – lõik 1

Komisjoni ettepanek	*Muudatusettepanek*
Iga liidu institutsioon, organ ja asutus hindab küberturvalisuse küpsuse taset vähemalt iga ***kolme*** aasta järel, kattes kõik ***IT-keskkonna*** elemendid, nagu on kirjeldatud artiklis 4, ja võttes arvesse asjaomaseid juhenddokumente ja soovitusi, mis on vastu võetud kooskõlas artikliga 13.	Iga liidu institutsioon, organ***, amet*** ja asutus hindab küberturvalisuse küpsuse taset ***hiljemalt ... [kuus kuud pärast käesoleva määruse jõustumist] ning seejärel*** vähemalt iga ***kahe*** aasta järel, kattes kõik ***IKT-keskkonna*** elemendid, nagu on kirjeldatud artiklis 4, ja võttes arvesse asjaomaseid juhenddokumente ja soovitusi, mis on vastu võetud kooskõlas artikliga 13. ***Küpsuse hindamine peab põhinema kontrollitud teenuseosutajate sõltumatutel küberturvalisuse audititel.***

Muudatusettepanek 36

Ettepanek võtta vastu määrus
Artikkel 7 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Lähtudes küpsustaseme hindamise põhjal tehtud järeldustest ning võttes arvesse artikli 4 kohaselt kindlaks tehtud varasid ja riske, kiidab iga liidu institutsiooni, organi ja asutuse kõrgeim juhtimistasand pärast riskide juhtimise, haldamise ja kontrollimise raamistiku ja küberturvalisuse baastaseme kehtestamist ilma põhjendamatult viivitamata heaks küberturvalisuse kava. Kava eesmärk on suurendada asjaomase üksuse üldist küberturvalisust ja aidata seeläbi saavutada küberturvalisuse ühtlaselt kõrge tase liidu	1. Lähtudes küpsustaseme hindamise põhjal tehtud järeldustest ning võttes arvesse artikli 4 kohaselt kindlaks tehtud varasid ja riske, kiidab iga liidu institutsiooni, organi***, ameti*** ja asutuse kõrgeim juhtimistasand pärast riskide juhtimise, haldamise ja kontrollimise raamistiku ja küberturvalisuse baastaseme kehtestamist ilma põhjendamatult viivitamata heaks küberturvalisuse kava. Kava eesmärk on suurendada asjaomase üksuse üldist küberturvalisust ja aidata seeläbi saavutada küberturvalisuse ühtlaselt

institutsioonides, organites ja asutustes või seda parandada. Selleks et toetada üksuse ülesannete täitmist institutsionaalse sõltumatuse alusel, sisaldab kava vähemalt I lisas loetletud valdkondi, II lisas loetletud meetmeid ning meetmeid, mis on seotud intsidentideks valmisoleku, intsidentidele reageerimise ja neist taastumisega, näiteks turvaseire ja logimine. Kava vaadatakse läbi vähemalt iga ***kolme*** aasta järel pärast artikli 6 kohaselt tehtud küpsustaseme hindamist.	kõrge tase liidu institutsioonides, organites***,*** ***ametites*** ja asutustes või seda parandada. Selleks et toetada üksuse ülesannete täitmist institutsionaalse sõltumatuse alusel, sisaldab kava vähemalt I lisas loetletud valdkondi, II lisas loetletud meetmeid ning meetmeid, mis on seotud intsidentideks valmisoleku, intsidentidele reageerimise ja neist taastumisega, näiteks ***tarnijate ja teenuste turvaalane hindamine,*** turvaseire ja logimine. Kava vaadatakse läbi vähemalt iga ***kahe*** aasta järel pärast artikli 6 kohaselt tehtud küpsustaseme hindamist.

Muudatusettepanek 37

Ettepanek võtta vastu määrus
Artikkel 7 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Küberturvalisuse kavas kirjeldatakse, millised on töötajate ülesanded ja kohustused kava rakendamisel.	2. Küberturvalisuse kavas kirjeldatakse, millised on töötajate ülesanded***, valmisolek*** ja kohustused kava rakendamisel.

Muudatusettepanek 38

Ettepanek võtta vastu määrus
Artikkel 7 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. Küberturvalisuse kava ***arvestab muude kohaldatavate*** CERT-EU välja antud ***juhenddokumentide*** ja ***soovitustega***.	3. Küberturvalisuse kava ***hõlmab kõiki kavandatud meetmeid, mis sisalduvad kohaldatavates*** CERT-EU välja antud ***juhenddokumentides*** ja ***soovitustes***.

Muudatusettepanek 39

Ettepanek võtta vastu määrus
Artikli 7 – lõige 3 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	3 a. Liidu institutsioonid, organid, ametid ja asutused esitavad oma küberturvalisuse kavad IICB-le. Neid kavasid jagatakse võimalikult suures ulatuses, ohustamata liidu üksuse konkreetset tehnilist küberturvalisuse korda ja suutlikkust käsitleva tundliku või konfidentsiaalse teabe avalikustamist volitamata kolmandatele isikutele.

Muudatusettepanek 40

Ettepanek võtta vastu määrus
Artikkel 9 – lõige 2 – punkt a

Komisjoni ettepanek	*Muudatusettepanek*
(a) teha seiret selle üle, kuidas liidu institutsioonid, organid ja asutused käesolevat määrust rakendavad;	(a) teha seiret selle üle, kuidas liidu institutsioonid, organid***, ametid*** ja asutused käesolevat määrust rakendavad ***ning anda soovitusi küberturvalisuse ühtlaselt kõrge taseme saavutamiseks***;

Muudatusettepanek 41

Ettepanek võtta vastu määrus
Artikkel 9 – lõige 3 – lõik 1 – sissejuhatav osa

Komisjoni ettepanek	*Muudatusettepanek*
IICBsse kuuluvad kolm esindajat, kelle nimetab liidu asutuste võrgustik (EUAN) oma IKT nõuandekomitee ettepanekul ja kes esindavad ise oma ***IT-keskkonda*** haldavate organite ja asutuste huve, ning üks esindaja, kes määratakse igast järgmisest organisatsioonist:	IICBsse kuuluvad kolm esindajat, kelle nimetab liidu asutuste võrgustik (EUAN) oma IKT nõuandekomitee ettepanekul ja kes esindavad ise oma ***IKT-keskkonda*** haldavate ***ametite,*** organite ja asutuste huve, ning üks esindaja, kes määratakse igast järgmisest organisatsioonist:

Muudatusettepanek 42

Ettepanek võtta vastu määrus
Artikkel 9 – lõige 3 – lõik 1 – punkt k a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(ka) Euroopa Andmekaitseinspektor.

Muudatusettepanek 43

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

Komisjoni ettepanek	*Muudatusettepanek*
	(aa) kiidab CERT-EU juhi ettepanekul küberturvalisuse ühtlaselt kõrge taseme saavutamiseks heaks soovitused, mis on suunatud ühele või kõigile liidu institutsioonidele, organitele, ametitele ja asutustele;

Muudatusettepanek 44

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

Komisjoni ettepanek	*Muudatusettepanek*
(a) esitada hoiatuse; kui see on mõjuva küberturvalisuse riski tõttu vajalik, esitatakse hoiatus asjakohaselt piiratud sihtrühmale;	(a) esitada hoiatuse; kui see on mõjuva küberturvalisuse riski tõttu vajalik, esitatakse hoiatus ***ühiselt kokku lepitud metoodikat järgides*** asjakohaselt piiratud sihtrühmale;

Muudatusettepanek 45

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

Komisjoni ettepanek	*Muudatusettepanek*
(b) ***soovitada auditi tegemiseks sobivat audiitorit***.	(b) ***teha sobivale audiitorile ülesandeks teha audit***.

Muudatusettepanek 46

Ettepanek võtta vastu määrus

Artikkel 12 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. CERT-EU ehk kõigi liidu institutsioonide, organite ja asutuste sõltumatu institutsioonidevahelise küberturvalisuse keskuse ülesanne on aidata kaasa kõigi liidu institutsioonide, organite ja asutuste salastamata ***IT-keskkonna*** turvalisusele, andes neile küberturvalisuse alast nõu, aidates neil intsidente ära hoida, tuvastada ja leevendada ja intsidentidele reageerida ning tegutsedes nende küberturvalisuse alase teabevahetuse ja intsidentidele reageerimise koordineerimise keskusena.	1. CERT-EU ehk kõigi liidu institutsioonide, organite***, ametite*** ja asutuste sõltumatu institutsioonidevahelise küberturvalisuse keskuse ülesanne on aidata kaasa kõigi liidu institutsioonide, organite***, ametite*** ja asutuste salastamata ***IKT-keskkonna*** turvalisusele, andes neile küberturvalisuse alast nõu, aidates neil intsidente ära hoida, tuvastada ja leevendada ja intsidentidele reageerida ning tegutsedes nende küberturvalisuse alase teabevahetuse ja intsidentidele reageerimise koordineerimise keskusena.

Muudatusettepanek 47

Ettepanek võtta vastu määrus
Artikkel 12 – lõige 2 – punkt d

Komisjoni ettepanek	*Muudatusettepanek*
(d) juhib IICB tähelepanu teemadele, mis on seotud käesoleva määruse rakendamisega ning juhenddokumentide, soovituste ja üleskutsete rakendamisega;	(d) juhib IICB tähelepanu teemadele, mis on seotud käesoleva määruse rakendamisega ning juhenddokumentide, soovituste ja üleskutsete rakendamisega***, ning esitab ettepanekuid heastamiseks***;

Muudatusettepanek 48

Ettepanek võtta vastu määrus
Artikkel 12 – lõige 4

Komisjoni ettepanek	*Muudatusettepanek*
4. CERT-EU teeb Euroopa Liidu Küberturvalisuse Ametiga struktureeritud koostööd suutlikkuse suurendamise, operatiivkoostöö ja küberohtude pikaajalise strateegilise analüüsi vallas kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/881.	4. CERT-EU teeb Euroopa Liidu Küberturvalisuse Ametiga struktureeritud koostööd suutlikkuse suurendamise, operatiivkoostöö ja küberohtude pikaajalise strateegilise analüüsi vallas kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/881. ***Lisaks võib CERT-EU teha koostööd ja vahetada teavet***

	küberkuritegevuse vastase võitluse Euroopa keskusega.

Muudatusettepanek 49

Ettepanek võtta vastu määrus
Artikkel 12 – lõige 5 – sissejuhatav osa

Komisjoni ettepanek	*Muudatusettepanek*
5. CERT-EU võib pakkuda järgmisi teenuseid, mida ei ole kirjeldatud tema teenuste kataloogis („tasulised teenused“):	5. CERT-EU võib pakkuda ***liidu institutsioonidele, organitele, ametitele ja asutustele*** järgmisi teenuseid, mida ei ole kirjeldatud tema teenuste kataloogis („tasulised teenused“):

Muudatusettepanek 50

Ettepanek võtta vastu määrus
Artikkel 12 – lõige 5 – punkt a

Komisjoni ettepanek	*Muudatusettepanek*
(a) teenused, mis toetavad liidu institutsioonide, organite ja asutuste ***IT-keskkonna*** küberturvalisust ja mida ei ole nimetatud lõikes 2, teenustaseme kokkulepete põhjal ja vastavalt kasutatavate ressursside olemasolule;	(a) teenused, mis toetavad liidu institutsioonide, organite***, ametite*** ja asutuste ***IKT-keskkonna*** küberturvalisust ja mida ei ole nimetatud lõikes 2, teenustaseme kokkulepete põhjal ja vastavalt kasutatavate ressursside olemasolule;

Muudatusettepanek 51

Ettepanek võtta vastu määrus
Artikkel 12 – lõige 5 – punkt b

Komisjoni ettepanek	*Muudatusettepanek*
(b) teenused, mis toetavad liidu institutsioonide, organite ja asutuste küberturvalisuse toiminguid või projekte, välja arvatud nende ***IT-keskkonna***	(b) teenused, mis toetavad liidu institutsioonide, organite***, ametite*** ja asutuste küberturvalisuse toiminguid või projekte, välja arvatud nende ***IKT-***

kaitsmiseks mõeldud teenused, kirjaliku lepingu põhjal ja IICB eelneval heakskiidul;	***keskkonna*** kaitsmiseks mõeldud teenused, kirjaliku lepingu põhjal ja IICB eelneval heakskiidul;

Muudatusettepanek 52
Ettepanek võtta vastu määrus
Artikkel 12 – lõige 5 – punkt c

Komisjoni ettepanek	*Muudatusettepanek*
(c) teenused, mis toetavad selliste organisatsioonide ***IT-keskkonna*** turvalisust, mis ei ole liidu institutsioonid, organid ja asutused, kuid teevad liidu institutsioonide, organite ja asutustega tihedat koostööd, näiteks kui neile on liidu õiguse alusel määratud ülesandeid või kohustusi, kirjaliku lepingu põhjal ja IICB eelneval heakskiidul.	(c) teenused, mis toetavad selliste organisatsioonide ***IKT-keskkonna*** turvalisust, mis ei ole liidu institutsioonid, organid***, ametid*** ja asutused, kuid teevad liidu institutsioonide, organite***, ametite*** ja asutustega tihedat koostööd, näiteks kui neile on liidu õiguse alusel määratud ülesandeid või kohustusi, kirjaliku lepingu põhjal ja IICB eelneval heakskiidul.

Muudatusettepanek 53

Ettepanek võtta vastu määrus
Artikkel 12 – lõige 6

Komisjoni ettepanek	*Muudatusettepanek*
6. CERT-EU võib korraldada küberturvalisuse õppusi või soovitada osaleda olemasolevatel õppustel tihedas koostöös Euroopa Liidu Küberturvalisuse Ametiga alati, kui see on asjakohane, et kontrollida liidu institutsioonide, organite ja asutuste küberturvalisuse taset.	6. CERT-EU võib korraldada küberturvalisuse õppusi või soovitada osaleda olemasolevatel õppustel tihedas koostöös Euroopa Liidu Küberturvalisuse Ametiga alati, kui see on asjakohane, et kontrollida ***korrapäraselt*** liidu institutsioonide, organite***, ametite*** ja asutuste küberturvalisuse taset. ***Lisaks võib CERT-EU tõhustatud koostöö ja ühisprogrammide kaudu küberturvalisuse pädevusvõrgustiku ja küberturvalisuse valdkonna Euroopa pädevuskeskusega toetada teadusuuringuid ja innovatsiooni ning aidata tugevdada liidu institutsioonide, organite, ametite ja asutuste küberturvalisuse alast suutlikkust.***

Muudatusettepanek 54

Ettepanek võtta vastu määrus
Artikkel 12 – lõige 7

Komisjoni ettepanek	*Muudatusettepanek*
7. CERT-EU ***võib pakkuda*** liidu institutsioonidele, organitele ja asutustele abi salastatud ***IT-keskkondade*** intsidentide puhul, kui asjaomane ***asjaosaline*** seda temalt selgelt taotleb.	7. CERT-EU ***pakub*** liidu institutsioonidele, organitele***, ametitele*** ja asutustele abi salastatud ***IKT-keskkondade*** intsidentide puhul, kui asjaomane ***liidu institutsioon, organ, amet või asutus*** seda temalt selgelt taotleb ***ja kui CERT-EU käsutuses on selleks vajalikud vahendid või ta saab need asjaomaselt üksuselt***.

Muudatusettepanek 55

Ettepanek võtta vastu määrus
Artikkel 14 – lõik 1

Komisjoni ettepanek	*Muudatusettepanek*
CERT-EU juht esitab IICB-le ja IICB juhatajale ***korrapäraselt*** aruandeid CERT-EU tegevuse, finantsplaneerimise, tulude, eelarve rakendamise, teenustaseme kokkulepete ja sõlmitud kirjalike lepingute, vastaspoolte ja partneritega tehtava koostöö ning töötajate lähetuste kohta, sh artikli 10 lõikes 1 osutatud aruandeid.	CERT-EU juht esitab IICB-le ja IICB juhatajale ***vähemalt kord aastas*** aruandeid CERT-EU tegevuse, finantsplaneerimise, tulude, eelarve rakendamise, teenustaseme kokkulepete ja sõlmitud kirjalike lepingute, vastaspoolte ja partneritega tehtava koostöö ning töötajate lähetuste kohta, sh artikli 10 lõikes 1 osutatud aruandeid.

Muudatusettepanek 56

Ettepanek võtta vastu määrus
Artikkel 16 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. CERT-EU teeb liikmesriikide samalaadsete asutustega, sh CERTidega, riikide küberturvalisuse keskustega, CSIRTidega ja direktiivi [küberturvalisuse 2. direktiivi ettepanek] artiklis 8 osutatud ühtsete kontaktpunktidega koostööd ja vahetab teavet küsimustes, mis puudutavad küberohte, nõrkusi, intsidente ja	1. CERT-EU teeb liikmesriikide samalaadsete asutustega, sh CERTidega, riikide küberturvalisuse keskustega, CSIRTidega ja direktiivi [küberturvalisuse 2. direktiivi ettepanek] artiklis 8 osutatud ühtsete kontaktpunktidega koostööd ja vahetab teavet küsimustes, mis puudutavad küberohte, nõrkusi, intsidente ja

võimalikke vastumeetmeid, ja kõiges, mis on asjakohane liidu institutsioonide, organite ja asutuste ***IT-keskkondade*** kaitse parandamiseks, sh direktiivi [küberturvalisuse 2. direktiivi ettepanek] artiklis 13 osutatud CSIRTide võrgustiku kaudu.	võimalikke vastumeetmeid, ja kõiges, mis on asjakohane liidu institutsioonide, organite***, ametite*** ja asutuste ***IKT-keskkondade*** kaitse parandamiseks, sh direktiivi [küberturvalisuse 2. direktiivi ettepanek] artiklis 13 osutatud CSIRTide võrgustiku kaudu.

Muudatusettepanek 57

Ettepanek võtta vastu määrus
Artikkel 16 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. CERT-EU võib vahetada liikmesriikide samalaadsete asutustega teavet konkreetse intsidendi kohta, et hõlbustada samalaadsete küberohtude või intsidentide avastamist, ilma mõjutatud ***asjaosalise*** nõusolekuta. Sellist teavet, millest ilmneb küberturvalisuse intsidendi sihtmärgi identiteet, võib CERT-EU intsidendi kohta vahetada üksnes mõjutatud ***asjaosalise*** nõusolekul.	2. CERT-EU võib vahetada liikmesriikide samalaadsete asutustega teavet konkreetse intsidendi kohta, et hõlbustada samalaadsete küberohtude või intsidentide avastamist, ilma mõjutatud ***liidu institutsiooni, organi, ameti või asutuse*** nõusolekuta***, kui isikuandmeid töödeldakse määruse (EL) 2018/1725 sätete kohaselt***. Sellist teavet, millest ilmneb küberturvalisuse intsidendi sihtmärgi identiteet, võib CERT-EU intsidendi kohta vahetada üksnes mõjutatud ***liidu institutsiooni, organi, ameti või asutuse*** nõusolekul.

Muudatusettepanek 58

Ettepanek võtta vastu määrus
Artikkel 17 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. CERT-EU võib teha töövahendite ja meetodite, nt tehnika, taktika, menetluste ja heade tavade, ning küberohtude ja nõrkuste alast koostööd kolmandate riikide samalaadsete asutustega, sh sektoripõhiste samalaadsete asutustega. CERT-EU taotleb IICB heakskiitu igasuguseks koostööks selliste samalaadsete asutustega, seda ka raamistikes, kus kolmandate riikide samalaadsed asutused teevad koostööd	1. CERT-EU võib teha töövahendite ja meetodite, nt tehnika, taktika, menetluste ja heade tavade, ning küberohtude ja nõrkuste alast koostööd kolmandate riikide samalaadsete asutustega, sh sektoripõhiste samalaadsete asutustega. CERT-EU taotleb IICB heakskiitu igasuguseks koostööks selliste samalaadsete asutustega, seda ka raamistikes, kus kolmandate riikide samalaadsed asutused teevad koostööd

liikmesriikide samalaadsete asutustega.	liikmesriikide samalaadsete asutustega. ***Selles koostöös austatakse ELi demokraatlikku terviklikkust.***

Muudatusettepanek 59

Ettepanek võtta vastu määrus
Artikkel 17 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. CERT-EU võib teha koostööd muude partneritega, näiteks äriettevõtjate, rahvusvaheliste organisatsioonide, Euroopa Liidu väliste riiklike üksuste või üksikekspertidega, et koguda teavet üldiste või konkreetsete küberohtude, nõrkuste ja võimalike vastumeetmete kohta. Ulatuslikumaks koostööks selliste partneritega taotleb CERT-EU IICB eelnevat heakskiitu.	2. CERT-EU võib teha koostööd muude partneritega, näiteks äriettevõtjate, rahvusvaheliste organisatsioonide, Euroopa Liidu väliste riiklike üksuste või üksikekspertidega, et koguda teavet üldiste või konkreetsete küberohtude, nõrkuste ja võimalike vastumeetmete kohta. Ulatuslikumaks koostööks selliste partneritega taotleb CERT-EU IICB eelnevat heakskiitu. ***Selles koostöös austatakse ELi demokraatlikku terviklikkust.***

Muudatusettepanek 60

Ettepanek võtta vastu määrus
Artikkel 17 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. CERT-EU võib intsidendist mõjutatud ***asjaosalise*** nõusolekul esitada intsidendi kohta käivat teavet partneritele, kes võivad aidata seda intsidenti analüüsida.	3. CERT-EU võib intsidendist mõjutatud ***liidu institutsiooni, organi, ameti või asutuse*** nõusolekul esitada intsidendi kohta käivat teavet partneritele, kes võivad aidata seda intsidenti analüüsida.

Muudatusettepanek 61

Ettepanek võtta vastu määrus
Artikkel 19 – lõige -1 (uus)

Komisjoni ettepanek	*Muudatusettepanek*

	-1. Liidu institutsioonid, organid, ametid ja asutused võivad vabatahtlikult anda CERT-EU-le teavet neid mõjutavate küberohtude, intsidentide, ohuolukordade ja nõrkuste kohta. CERT-EU tagab tõhusate sidevahendite olemasolu, et hõlbustada liidu üksustega teabe jagamist. CERT-EU võib seada kohustuslike teadete menetlemise vabatahtlike teadete menetlemisest tähtsamale kohale.

Muudatusettepanek 62

Ettepanek võtta vastu määrus
Artikkel 19 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Et ***CERT-EU saaks koordineerida nõrkuste haldamist*** ja ***intsidentidele reageerimist***, võib ***ta*** paluda liidu institutsioonidel, organitel ja asutustel esitada talle oma ***IT-süsteemide*** varade loendist teavet, mis ***on CERT-EU toetuse seisukohast asjakohane***. Taotluse saanud ***institutsioon, organ või asutus*** edastab taotletud teabe ja kõik selle hilisemad ajakohastused põhjendamatu viivituseta.	1. Et ***täita oma artiklis 12 määratletud missiooni*** ja ***ülesandeid***, võib ***CERT-EU*** paluda liidu institutsioonidel, organitel***, ametitel*** ja asutustel esitada talle oma ***IKT-süsteemide*** varade loendist teavet, ***sealhulgas teavet,*** mis ***käsitleb küberohtusid, ohuolukordi, nõrkusi, turvarikke indikaatoreid, küberturvalisuse hoiatusi ning soovitusi seoses küberintsidentide avastamiseks vajalike küberturvalisuse vahendite konfiguratsiooniga***. Taotluse saanud ***üksus*** edastab taotletud teabe ja kõik selle hilisemad ajakohastused põhjendamatu viivituseta.

Muudatusettepanek 63

Ettepanek võtta vastu määrus
Artikkel 19 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Liidu institutsioonid, organid ja asutused esitavad CERT-EU taotluse peale CERT-EU-le põhjendamatu viivituseta digitaalse teabe, mis on tekkinud nende vastavate intsidentidega seotud elektrooniliste seadmete kasutamisel.	2. Liidu institutsioonid, organid***, ametid*** ja asutused esitavad CERT-EU taotluse peale CERT-EU-le põhjendamatu viivituseta digitaalse teabe, mis on tekkinud nende vastavate intsidentidega seotud elektrooniliste seadmete

CERT-EU võib täiendavalt selgitada, millist liiki digitaalset teavet tal on olukorrateadlikkuse ja intsidentidele reageerimise jaoks vaja.	kasutamisel. CERT-EU võib täiendavalt selgitada, millist liiki digitaalset teavet tal on olukorrateadlikkuse ja intsidentidele reageerimise jaoks vaja.

Muudatusettepanek 64
Ettepanek võtta vastu määrus
Artikkel 20 – pealkiri

Komisjoni ettepanek	*Muudatusettepanek*
Teatamiskohustused	***Aruandekohustused***

Muudatusettepanek 65

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 1 – lõik 1

Komisjoni ettepanek	*Muudatusettepanek*
Kõik liidu institutsioonid, organid ja asutused esitavad CERT-EU-le ***esialgse teate*** oluliste küberohtude, oluliste nõrkuste ja oluliste intsidentide kohta ilma põhjendamatult viivitamata ja igal juhul hiljemalt 24 tunni jooksul pärast seda, kui on neist teada saanud.	Kõik liidu institutsioonid, organid***, ametid*** ja asutused esitavad CERT-EU-le ***varajase hoiatuse*** oluliste küberohtude, oluliste nõrkuste ja oluliste intsidentide kohta ilma põhjendamatult viivitamata ja igal juhul hiljemalt 24 tunni jooksul pärast seda, kui on neist teada saanud. ***Vajaduse korral osutatakse varajases hoiatuses sellele, kas on kahtlus, et olulise intsidendi põhjuseks on ebaseaduslik või pahatahtlik tegevus, ning kas sellel on või võib olla piiriülene mõju.***

Muudatusettepanek 66

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 1 – lõik 2

Komisjoni ettepanek	*Muudatusettepanek*
Nõuetekohaselt põhjendatud juhtudel ja kokkuleppel CERT-EUga võib asjaomane liidu institutsioon, organ või asutus kalduda ***kõrvale eelmises lõikes sätestatud***	Nõuetekohaselt põhjendatud juhtudel ja kokkuleppel CERT-EUga võib asjaomane liidu institutsioon, organ***, amet*** või asutus kalduda ***sellest tähtajast kõrvale***.

tähtajast.

Muudatusettepanek 67

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 2 – sissejuhatav osa

Komisjoni ettepanek	*Muudatusettepanek*
2. Liidu institutsioonid, organid ja asutused ***teatavad*** CERT-EU-le põhjendamatult viivitamata ***ka*** küberohtude, nõrkuste ja intsidentide ***asjakohased tehnilised üksikasjad***, mis aitavad kaasa tuvastamisele, intsidentidele reageerimisele või leevendusmeetmetele. Teatatakse järgmistest asjaoludest, kui see teave on olemas:	2. Liidu institutsioonid, organid***,*** ***ametid*** ja asutused ***saadavad teavituse*** CERT-EU-le põhjendamatult viivitamata***, kuid igal juhul 72 tunni jooksul pärast olulisest intsidendist teada saamist, ajakohastavad varajast hoiatust ning annavad sellele intsidendile ning selle raskusastmele ja mõjule esialgse hinnangu koos*** küberohtude, nõrkuste ja intsidentide ***asjakohaste tehniliste üksikasjadega***, mis aitavad kaasa tuvastamisele, intsidentidele reageerimisele või leevendusmeetmetele. Teatatakse järgmistest asjaoludest, kui see teave on olemas:

Muudatusettepanek 68
Ettepanek võtta vastu määrus
Artikkel 20 – lõige 2 – lõik 1 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	Nõuetekohaselt põhjendatud juhtudel ja kokkuleppel CERT-EUga võib asjaomane liidu institutsioon, organ, amet või asutus kalduda sellest tähtajast kõrvale.

Muudatusettepanek 69

Ettepanek võtta vastu määrus
Artikli 20 – lõige 2 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	2 a. Hiljemalt üks kuu pärast olulisest intsidendist teatamist esitavad liidu

	institutsioonid, organid, ametid ja asutused CERT-EU-le lõpparuande, mis sisaldab vähemalt järgmist:
	(a) olulise intsidendi, selle raskusastme ja mõju üksikasjalik kirjeldus;
	(b) olulise intsidendi tõenäoliselt põhjustanud ohu liik või algpõhjus;
	(c) juba kohaldatud ja kohaldamisel olevad leevendusmeetmed;
	(d) asjakohasel juhul olulise intsidendi piiriülene mõju.
	Kui esimeses lõigus osutatud lõpparuande esitamise ajal ei ole oluline intsidentide endiselt kõrvaldatud, tuleb esitada hetkeseisu käsitlev eduaruanne ja lõpparuanne ühe kuu jooksul pärast intsidendist teatamist.

Muudatusettepanek 70

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 2 b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	2b. Nõuetekohaselt põhjendatud juhtudel ja kokkuleppel CERT-EUga võib asjaomane liidu institutsioon, organ, amet või asutus kalduda kõrvale lõikes 2a sätestatud tähtajast.

Muudatusettepanek 71

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. CERT-EU esitab ENISA-le kord kuus koondaruande, mis sisaldab anonüümitud ja koondatud andmeid oluliste küberohtude, oluliste nõrkuste ja oluliste intsidentide kohta, millest on teatatud vastavalt lõikele 1.	3. CERT-EU esitab ENISA-le kord kuus koondaruande, mis sisaldab anonüümitud ja koondatud andmeid oluliste küberohtude, oluliste nõrkuste ja oluliste intsidentide kohta, millest on teatatud vastavalt lõikele 1. ***See aruanne***

	on sisend direktiivi [küberturvalisuse 2. direktiivi ettepanek] artikli 18 kohaselt iga kahe aasta tagant esitatavasse aruandesse, milles käsitletakse küberturvalisuse olukorda liidus.

Muudatusettepanek 72

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 4

Komisjoni ettepanek	*Muudatusettepanek*
4. IICB ***võib anda*** välja juhenddokumente või soovitusi teadete esitamise korra ja sisu kohta. CERT-EU levitab asjakohaseid tehnilisi üksikasju, et liidu institutsioonid, organid ja asutused saaksid tegeleda ennetava avastamise, intsidentidele reageerimise või leevendusmeetmetega.	4. IICB ***annab*** välja juhenddokumente või soovitusi teadete esitamise korra ja sisu kohta. CERT-EU levitab asjakohaseid tehnilisi üksikasju, et liidu institutsioonid, organid***, ametid*** ja asutused saaksid tegeleda ennetava avastamise, intsidentidele reageerimise või leevendusmeetmetega.

Muudatusettepanek 73

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 5

Komisjoni ettepanek	*Muudatusettepanek*
5. Teatamiskohustused ei laiene ELi salastatud teabele ega teabele, mille liidu institutsioon, organ või asutus on saanud liikmesriigi julgeoleku- või luureteenistuselt või õiguskaitseasutuselt selgesõnalisel tingimusel, et seda ei jagata CERT-EUga.	***välja jäetud***

Muudatusettepanek 74

Ettepanek võtta vastu määrus
Artikkel 24 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Komisjon esitab Euroopa	2. Komisjon esitab Euroopa

Parlamendile ja nõukogule aruande käesoleva määruse rakendamise kohta hiljemalt ***48*** kuud pärast määruse jõustumist ja seejärel iga ***kolme*** aasta tagant.	Parlamendile ja nõukogule aruande käesoleva määruse rakendamise kohta hiljemalt ***36*** kuud pärast määruse jõustumist ja seejärel iga ***kahe*** aasta tagant.

Muudatusettepanek 75

Ettepanek võtta vastu määrus
Artikkel 24 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. Komisjon hindab määruse toimimist ning esitab Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ja Regioonide Komiteele aruande mitte varem kui ***viis*** aastat pärast määruse jõustumist.	3. Komisjon hindab määruse toimimist ning esitab Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ja Regioonide Komiteele aruande mitte varem kui ***kolm*** aastat pärast määruse jõustumist***, arvestades kiiresti muutuvaid küberohte***.

Muudatusettepanek 76

Ettepanek võtta vastu määrus
I lisa – lõik 1 – sissejuhatav osa

Komisjoni ettepanek	*Muudatusettepanek*
Küberturvalisuse baastase puudutab järgmisi valdkondi:	Küberturvalisuse baastase puudutab ***vähemalt*** järgmisi valdkondi:

Muudatusettepanek 77

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

Komisjoni ettepanek	*Muudatusettepanek*
	(1a) töötajatele küberturvalisuse alase koolituse pakkumine;

Muudatusettepanek 78

Ettepanek võtta vastu määrus
I lisa – lõik 1 – punkt 3

Komisjoni ettepanek	*Muudatusettepanek*
(3) varade haldamine, sh ***IT-varade*** inventeerimine ja ***IT-võrgu*** kaardistamine;	(3) varade ***omandamine ja*** haldamine, sh ***IKT-varade*** inventeerimine ja ***IKT-võrgu*** kaardistamine;

Muudatusettepanek 79

Ettepanek võtta vastu määrus
I lisa – lõik 1 – punkt 7

Komisjoni ettepanek	*Muudatusettepanek*
(7) süsteemi soetamine, arendamine ja hooldamine;	(7) süsteemi soetamine, arendamine ja hooldamine***, sealhulgas asutusesisene avatud lähtekoodiga tarkvara arendamine***;

Muudatusettepanek 80

Ettepanek võtta vastu määrus
I lisa – lõik 1 – punkt 7 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(7a) küberturvalisuse auditid;

Muudatusettepanek 81

Ettepanek võtta vastu määrus
I lisa – lõik 1 – punkt 9

Komisjoni ettepanek	*Muudatusettepanek*
(9) intsidentide haldamine, sh lähenemisviisid, et parandada intsidentideks valmisolekut, neile reageerimist ja neist taastumist, ning koostöö CERT-EUga, nt turvaseire ja logimise käigushoidmine;	(9) intsidentide haldamine, sh lähenemisviisid, et parandada intsidentideks valmisolekut, neile reageerimist***, aruandluskohustustest kinnipidamist*** ja ***nende tähtaegade lühendamist ning*** neist taastumist, ning koostöö CERT-EUga, nt turvaseire ja logimise käigushoidmine;

Muudatusettepanek 82

Ettepanek võtta vastu määrus
II lisa – lõik 1 – punkt 3 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(3a) töötajatele korrapärase küberturvalisuse alase koolituse pakkumine;

Muudatusettepanek 83

Ettepanek võtta vastu määrus
II lisa – lõik 1 – punkt 4 – alapunkt a

Komisjoni ettepanek	*Muudatusettepanek*
(a) selliste lepinguliste tõkete kõrvaldamine, mis piiravad võimalust jagada CERT-EUga ***IT-teenuste*** pakkujate teavet intsidentide, nõrkuste ja küberohtude kohta;	(a) selliste lepinguliste tõkete kõrvaldamine, mis piiravad võimalust jagada CERT-EUga ***IKT-teenuste*** pakkujate teavet intsidentide, nõrkuste ja küberohtude kohta;

NÕUANDVA KOMISJONI MENETLUS

Pealkiri	Meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites, ametites ja asutustes
Viited	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Vastutav komisjon istungil teada andmise kuupäev	ITRE 4.4.2022
Arvamuse esitajad istungil teada andmise kuupäev	AFCO 4.4.2022
Arvamuse koostaja nimetamise kuupäev	Markéta Gregorová 20.6.2022
Läbivaatamine parlamendikomisjonis	26.10.2022 1.12.2022
Vastuvõtmise kuupäev	25.1.2023
Lõpphääletuse tulemus	+: 24 –: 0 0: 0
Lõpphääletuse ajal kohal olnud liikmed	Gerolf Annemans, Gabriele Bischoff, Damian Boeselager, Gwendoline Delbos-Corfield, Salvatore De Meo, Daniel Freund, Charles Goerens, Esteban González Pons, Laura Huhtasaari, Victor Negrescu, Max Orville, Domènec Ruiz Devesa, Helmut Scholz, Pedro Silva Pereira, Sven Simon, Guy Verhofstadt, Loránt Vincze, Rainer Wieland
Lõpphääletuse ajal kohal olnud asendusliikmed	Nathalie Colin-Oesterlé, Pascal Durand, Seán Kelly, Jaak Madison, Maite Pagazaurtundúa
Lõpphääletuse ajal kohal olnud asendusliikmed (art 209 lg 7)	Leszek Miller

NIMELINE LÕPPHÄÄLETUS NÕUANDVAS KOMISJONIS

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

0	-

0	0

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