EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) 2019/881,

17. aprill 2019,

mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus)

(EMPs kohaldatav tekst)

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 114,

võttes arvesse Euroopa Komisjoni ettepanekut,

olles edastanud seadusandliku akti eelnõu liikmesriikide parlamentidele,

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust ([1]),

võttes arvesse Regioonide Komitee arvamust ([2]),

toimides seadusandliku tavamenetluse kohaselt ([3])

ning arvestades järgmist:

(1) Võrgu- ja infosüsteemidel ning elektroonilise side võrkudel ja teenustel on ühiskonnas elutähtis roll ning neist on saanud majanduskasvu tugisammas. Info- ja kommunikatsioonitehnoloogia (IKT) on aluseks keerukatele süsteemidele, mis toetavad igapäevast ühiskondlikku tegevust, tagavad majanduse toimimise võtmetähtsusega sektorites nagu tervis, energeetika, rahandus ja transport ning toetavad ennekõike siseturu toimimist.

(2) Võrgu- ja infosüsteemide kasutamine kogu liidu kodanike, organisatsioonide ja ettevõtjate 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 liidus kasutusele enneolematult palju ühendatud digitaalseid seadmeid. Kuigi üha enam seadmeid on ühendatud internetti, ei ole turvalisus ja vastupidavus neisse piisavalt sisse projekteeritud ning see toob kaasa ebapiisava küberturvalisuse. Sellises olukorras tähendab sertifitseerimise piiratud kasutamine, et eraisikutest, organisatsioonidest ja ettevõtjatest kasutajatel ei ole IKT-toodete, -teenuste ja -protsesside küberturvalisuse omaduste kohta piisavalt teavet ning see vähendab usaldust digilahenduste vastu. Võrgu- ja infosüsteemid on võimelised toetama meie elu kõiki aspekte ja edendama liidu majanduskasvu. Nad on tugisammas digitaalse ühtse turu saavutamiseks.

(3) Ulatuslikum digiteerimine ja ühenduvus toovad kaasa suuremad küberturvalisuse riskid, mille tõttu on kogu ühiskond küberohtude poolt lihtsamini haavatav ning üksikisikute, sh haavatavate isikute (näiteks laste) vastu suunatud ohud tulevad selgemalt esile. Et kõnealuseid riske maandada, tuleb võtta kõik vajalikud meetmed, et parandada liidus küberturvalisust ning pakkuda küberohtude eest paremat kaitset võrgu- ja infosüsteemidele, sidevõrkudele, digitaalsetele toodetele, teenustele ja seadmetele, mida kasutavad kodanikud, organisatsioonid ja ettevõtjad alates väikestest ja keskmise suurusega ettevõtjatest (VKEd), kes on määratletud komisjoni soovituses 2003/361/EÜ ([4]), kuni elutähtsate taristute operaatoriteni.

([1]) ELT C 227, 28.6.2018, lk 86.
([2]) ELT C 176, 23.5.2018, lk 29.
([3]) Euroopa Parlamendi 12. märtsi 2019. aasta seisukoht (*Euroopa Liidu Teatajas* seni avaldamata) ja nõukogu 9. aprilli 2019. aasta otsus.
([4]) Komisjoni 6. mai 2003. aasta soovitus mikro-, väikeste ja keskmise suurusega ettevõtjate määratlemise kohta (ELT L 124, 20.5.2003, lk 36).

(4) Tehes asjakohast teavet üldsusele kättesaadavaks, aitab Euroopa Parlamendi ja nõukogu määrusega (EL) nr 526/2013 ([5]) asutatud Euroopa Liidu Võrgu- ja Infoturbeamet (ENISA) kaasa küberturvalisuse tööstuse, eelkõige VKEde ja idufirmade arendamisele liidus. ENISA peaks püüdlema tihedama koostöö poole ülikoolide ja teadusasutustega, et aidata vähendada sõltumist liiduväliste tootjate ja teenusepakkujate küberturvalisuse toodetest ja teenustest ning tugevdada liidusiseseid tarneahelaid.

(5) 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 õiguskaitseasutuste pädevus ja reageeringud valdavalt riigipõhised. Mastaapsed intsidendid võivad katkestada elutähtsate teenuste pakkumise kogu liidus. See tähendab, et liidu tasandil on vaja tõhusat ning koordineeritud reageerimist ja kriisihaldust, mis tugineks sellekohastele poliitikameetmetele ning Euroopa solidaarsuse ja vastastikuse abi mitmekülgsetele vahenditele. Samuti 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.

(6) Arvestades asjaolu, et liitu ähvardavad küberturvalisuse probleemid kasvavad, on vaja igakülgset meetmete kogumit, mis toetuks liidu varasemale tegevusele ja edendaks üksteist vastastikku tugevdavaid eesmärke. Nende eesmärkide hulka kuulub liikmesriikide ja ettevõtjate suutlikkuse ja valmisoleku ning koostöö edasine parandamine ning teabe jagamine ja koordineerimine liikmesriikide ja liidu institutsioonide, organite ja asutuste vahel. Küberohud ei hooli riigipiiridest ja seepärast tuleb parandada liidu tasandi suutlikkust, et see täiendaks liikmesriikide meetmeid eeskätt mastaapsete piiriüleste intsidentide ja kriiside korral, võttes seejuures arvesse liikmesriikide suutlikkuse säilitamise ja edasise parandamise olulisust igasugustele küberohtudele reageerimisel.

(7) Rohkem tuleb ära teha ka selleks, et parandada kodanike, organisatsioonide ja ettevõtjate teadlikkust küberturvalisuse küsimustest. Ühtlasi, arvestades asjaolu, et intsidendid õõnestavad usaldust digitaalsete teenuste osutajate ning digitaalse ühtse turu enda vastu, eelkõige tarbijate seas, tuleks veelgi suurendada usaldust, pakkudes selleks läbipaistvat teavet IKT-toodete, -teenuste ja -protsesside turvalisuse tasemete kohta, rõhutades, et isegi küberturvalisuse sertifitseerimise kõrge tase ei taga, et IKT-toode, -teenus või -protsess oleks täiesti turvaline. Usalduse suurendamisele saab kaasa aidata kogu liitu hõlmava sertifitseerimisega, mis tagab ühised küberturvalisuse nõuded ja hindamiskriteeriumid liikmesriikide turgudel ja sektorites.

(8) Küberturvalisus ei ole mitte üksnes tehnoloogiline küsimus – oluline on ka inimeste käitumine. Seetõttu tuleks jõuliselt edendada „küberhügieeni“ ehk lihtsaid rutiinseid meetmeid, mis minimeerivad nende regulaarse rakendamise korral kodanike, organisatsioonide ja ettevõtjate kokkupuutumist küberohtudest tulenevate riskidega.

(9) Liidu küberturvalisuse struktuuride tugevdamise eesmärgil on oluline säilitada ja arendada liikmesriikide suutlikkust reageerida küberohtudele, sealhulgas piiriülestele intsidentidele kõikehõlmavalt.

(10) Ettevõtjatel ning üksikisikutest tarbijatel peaks olema täpne teave selle kohta, milline on nende IKT-toodete, -teenuste ja -protsesside turvalisuse sertifitseeritud usaldusväärsuse tase. Samas ei ole ükski IKT-toode või -teenus täielikult küberturvaline ning küberhügieeni põhireegleid tuleb edendada ja seada need prioriteediks. Arvestades asjade interneti seadmete üha suuremat kättesaadavust, on ka mitmeid vabatahtlikke meetmeid, mida erasektor saab võtta, et suurendada usaldust IKT-toodete, -teenuste ja -protsesside turvalisuse vastu.

(11) Kaasaegsed IKT-tooted ja -süsteemid on tihti integreeritud ühte või mitmesse kolmanda osapoole tehnoloogiasse või komponenti, nagu näiteks tarkvara moodulid, teegid või rakendusprogrammeerimise liidesed, ning tuginevad neile. Nimetatud tuginemine ehk sõltumine võib põhjustada täiendavaid küberturvalisuse riske, kuna kolmanda osapoole komponentide turvanõrkus võib mõjutada ka IKT-toodete, -teenuste ja -protsesside turvalisust. Paljudel juhtudel võimaldab selliste sõltumiste tuvastamine ja dokumenteerimine IKT-toodete, -teenuste ja -protsesside lõppkasutajatel edendada oma küberturvalisuse riskihalduse tegevusi, parandades näiteks kasutajate küberturvanõrkuste haldust ja kõrvaldusmeetmeid.

([5]) Euroopa Parlamendi ja nõukogu 21. mai 2013. aasta määrus (EL) nr 526/2013, mis käsitleb Euroopa Liidu Võrgu- ja Infoturbeametit (ENISA) ning millega tunnistatakse kehtetuks määrus (EÜ) nr 460/2004 (ELT L 165, 18.6.2013, lk 41).

(12) IKT-toodete, -teenuste ja-protsesside projekteerimise ja arendamisega seotud organisatsioone, tootjaid ja teenusepakkujaid tuleks julgustada rakendama meetmeid projekteerimise ja arendamise kõige varasemates etappides sellisel viisil, et nende toodete, teenuste ja protsesside turvalisus oleks kaitstud kõige kõrgemal tasemel, et küberrünnakute esinemist eeldataks ja et nende mõju oleks prognoositud ja minimeeritud („sisseprojekteeritud turve“). Turvalisus tuleks tagada kogu IKT-toote, -teenuse ja -protsessi olelusringi vältel, kusjuures projekteerimis- ja arendamisprotsessid peaksid pidevalt arenema, et vähendada kuritahtlikust kasutamisest tuleneva kahju riski.

(13) Ettevõtjad, organisatsioonid ja avalik sektor peaksid enda poolt projekteeritud IKT-tooteid, -teenuseid ja -protsesse konfigureerima viisil, mis tagab turvalisuse kõrge taseme, mis peaks võimaldama esimesel kasutajal saada vaikekonfiguratsioon kõige kõrgema turvalisuse tasemega seadistusega („vaiketurvalisus“), vähendades seega kasutajate jaoks koormust, mis kaasneb vajadusega IKT-toodet, -teenust või -protsessi asjakohaselt konfigureerida. Vaiketurvalisus ei peaks nõudma ulatuslikku konfigureerimist ega kasutajalt spetsiifilisi tehnilisi teadmisi või loogikavälist käitumist, ning peaks pärast rakendamist lihtsalt ja usaldusväärselt töötama. Kui juhtumipõhise riski- ja kasutatavusanalüüsi tulemusel jõutakse järeldusele, et selline vaikeseadistus ei ole teostatav, tuleks kasutajaid suunata valima kõige turvalisem seadistus.

(14) Euroopa Parlamendi ja nõukogu määrusega (EÜ) nr 460/2004 ([6]) asutati ENISA, et aidata kaasa kõrgetasemelise ja tõhusa võrgu- ja infoturbe tagamise eesmärkidele liidus ning arendada võrgu- ja infoturbekultuuri kodanike, tarbijate, ettevõtete ja ametiasutuste heaks. Euroopa Parlamendi ja nõukogu määrusega (EÜ) nr 1007/2008 ([7]) pikendati ENISA volitusi 2012. aasta märtsini. Euroopa Parlamendi ja nõukogu määrusega (EL) nr 580/2011 ([8]) pikendati ENISA volitusi 13. septembrini 2013. Määrusega (EL) nr 526/2013 pikendati ENISA volitusi kuni 19. juunini 2020.

(15) Liit on juba astunud olulisi samme, et tagada küberturvalisus ja suurendada usaldust digitehnoloogia vastu. 2013. aastal võeti vastu Euroopa Liidu küberjulgeoleku strateegia, millest juhinduda liidu poliitilises reageerimises küberohtudele ja riskidele. Et kodanikke veebis paremini kaitsta, võttis liit 2016. aastal vastu küberturvalisuse valdkonna esimese õigusakti – Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 ([9]). Direktiiviga (EL) 2016/1148 pandi paika liikmesriikide suutlikkust puudutavad nõuded küberturvalisuse valdkonnas, kehtestati liikmesriikide vahelise strateegilise ja operatiivkoostöö tõhustamise esimesed mehhanismid ning juurutati turbemeetmete ja intsidentidest teatamise kohustused majanduse ja ühiskonna jaoks eluliselt tähtsates sektorites, nagu energeetika, transport, joogivee varustus ja jaotamine, pangandus, finantsturu taristu, tervishoid, digitaristu, aga ka oluliste digitaalsete teenuste osutajate puhul (otsingumootorid, pilvandmetöötlusteenused ja internetipõhised kauplemiskohad).

ENISA-le anti nimetatud direktiivi rakendamise toetamisel põhiroll. Lisaks on tulemuslik võitlus küberkuritegevusega olulisel kohal ka Euroopa julgeoleku tegevuskavas, kus see aitab kaasa küberturvalisuse kõrge taseme saavutamise üldeesmärgile. Muud õigusaktid, nagu Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 ([10]) ning Euroopa Parlamendi ja nõukogu direktiivid 2002/58/EÜ ([11]) ning (EL) 2018/1972 ([12]), aitavad samuti kaasa digitaalse ühtse turu küberturvalisuse kõrgele tasemele.

([6]) Euroopa Parlamendi ja nõukogu 10. märtsi 2004. aasta määrus (EÜ) nr 460/2004, millega luuakse Euroopa Võrgu- ja Infoturbeamet (ELT L 77, 13.3.2004, lk 1).

([7]) Euroopa Parlamendi ja nõukogu 24. septembri 2008. aasta määrus (EÜ) nr 1007/2008, millega muudetakse määrust (EÜ) nr 460/2004 (millega luuakse Euroopa Võrgu- ja Infoturbeamet) seoses selle kestusega (ELT L 293, 31.10.2008, lk 1).

([8]) Euroopa Parlamendi ja nõukogu 8. juuni 2011. aasta määrus (EL) nr 580/2011, millega muudetakse määrust (EÜ) nr 460/2004 (millega luuakse Euroopa Võrgu- ja Infoturbeamet) seoses selle tegevusaja kestusega (ELT L 165, 24.6.2011, lk 3).

([9]) 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).

([10]) 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).

([11]) Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37).

([12]) Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik (ELT L 321, 17.12.2018, lk 36).

(16) Euroopa Liidu küberjulgeoleku strateegia vastuvõtmisest 2013. aastal ja ENISA volituste viimasest läbivaatamisest möödunud aja jooksul on üldine poliitiline kontekst seoses ebakindlama ja vähem turvalise üldise õhustikuga maailmas oluliselt muutunud. Selles kontekstis ja arvestades positiivset arengut seoses ENISA rolliga nõuandva ja oskusteavet pakkuva kontaktüksusena, koostöö ja suutlikkuse arendamise hõlbustajana ning liidu uue küberturvalisuse poliitika raames, on vaja läbi vaadata ENISA volitused, et määrata kindlaks ENISA roll muutunud küberturvalisuse tingimustes ning tagada, et see annaks tulemusliku panuse sellesse, kuidas liit reageerib põhjalikult muutunud küberohtude maastikul esile kerkivatele küberturvalisuse probleemidele, millega toimetulemiseks ei ole praegused volitused ENISA hindamise kohaselt piisavad.

(17) Käesoleva määrusega asutatav ENISA peaks olema määrusega (EL) nr 526/2013 asutatud ENISA õigusjärglane. ENISA peaks täitma talle käesoleva määruse ja muude küberturvalisuse valdkonna liidu õigusaktidega pandud ülesandeid, pakkudes muu hulgas nõuandeid ja oskusteavet ning tegutsedes selle valdkonna teabe- ja teadmuskeskusena liidus. ENISA peaks edendama parimate tavade vahetamist liikmesriikide ja eraõiguslike sidusrühmade vahel, tehes selleks komisjonile ja liikmesriikidele poliitikameetmete alaseid ettepanekuid, tegutsedes küberturvalisuse küsimustes liidu valdkondliku poliitika algatuste kontaktüksusena ning soodustades nii liikmesriikide omavahelist kui ka liikmesriikide ja liidu institutsioonide, organite ja asutuste vahelist operatiivkoostööd.

(18) Riigipeade ja valitsusjuhtide tasandil kohtunud liikmesriikide esindajate ühisel kokkuleppel tehtud otsuse 2004/97/EÜ, Euratom ([13]) raames otsustasid liikmesriikide esindajad, et ENISA asukohaks saab Kreeka valitsuse määratud linn Kreekas. ENISA asukohaliikmesriik peaks tagama ENISA tõrgeteta ja tõhusaks tegevuseks parimad võimalikud tingimused. ENISA ülesannete nõuetekohaseks ja tulemuslikuks täitmiseks, töötajate värbamiseks ja alalhoidmiseks ning võrgustikuga seotud tegevuse tulemuslikkuse tõhustamiseks peab ENISA asuma sobivas asukohas, mis muu hulgas pakub asjakohaseid transpordiühendusi ning rajatisi ENISA töötajate abikaasade ja laste jaoks. Vajalikud üksikasjad tuleks sätestada ENISA ja asukohaliikmesriigi vahelises kokkuleppes, mis sõlmitakse pärast ENISA haldusnõukogu heakskiitu.

(19) Arvestades liidu ees seisvate küberturvalisuse riskide ja probleemide kasvu, tuleks suurendada ENISA-le eraldatavaid finants- ja inimressursse, et need vastaksid ENISA tõhustatud rollile ja ülesannetele ning ENISA tähtsale positsioonile liidu digitaalse ökosüsteemi kaitsmise organisatsioonide seas, võimaldades ENISA-l tõhusalt täita talle käesoleva määrusega pandud ülesandeid.

(20) ENISA peaks kujundama välja oskusteabe kõrge taseme ja seda alal hoidma ning tegutsema kontaktüksusena, mis tekitab ühtsel turul usaldust ja kindlustunnet tänu oma sõltumatusele, antud nõu ja levitatava teabe kvaliteedile, menetluste ja töömeetodite läbipaistvusele ning oma ülesannete hoolikale täitmisele. Täites oma ülesandeid täielikus koostöös liidu institutsioonide, organite ja asutuste ning liikmesriikidega, peaks ENISA aktiivselt toetama liikmesriikide jõupingutusi ja andma proaktiivse panuse liidu tegevusse, vältides topelttööd ja edendades sünergiat. Lisaks peaks ENISA arendama edasi erasektorilt saadud sisendit, lähtudes erasektori ja muude asjaomaste sidusrühmadega tehtavast koostööst. ENISA ülesannete kogumiga tuleks paika panna, kuidas ENISA peab oma eesmärgid saavutama, tagades talle samas tööks vajaliku paindlikkuse.

(21) Et pakkuda liikmesriikidele piisavat tuge operatiivkoostöös, peaks ENISA veelgi tugevdama oma tehnilist ja inimvõimekust ning oskusi. ENISA peaks suurendama oma oskusteavet ja parandama suutlikkust. ENISA ja liikmesriigid võiksid arendada vabatahtlikkuse alusel programme ENISAsse riiklike ekspertide lähetamiseks, ekspertide salve loomiseks ja töötajate vahetusteks.

(22) ENISA peaks abistama komisjoni nõuannete, arvamuste ja analüüsidega kõigis liidu küsimustes, mis on seotud küberturvalisuse valdkonna ja selle sektoripõhiste aspektide alase poliitika ja õigusaktide väljatöötamise, ajakohastamise ja läbivaatamisega, et suurendada küberturvalisuse mõõdet sisaldavate liidu poliitikameetmete ja õigusaktide asjakohasust ning võimaldada nende järjepidevat rakendamist liikmesriigi tasandil. ELISA peaks tegutsema nõuandva ja oskusteavet pakkuva kontaktüksusena selliste liidu sektoripõhise poliitika ja õigusalaste algatuste jaoks, mis puudutavad küberturvalisust. ENISA peaks korrapäraselt teavitama Euroopa Parlamenti oma tegevusest.

([13]) Riigipeade ja valitsusjuhtide tasandil kohtunud liikmesriikide esindajate ühisel kokkuleppel tehtud 13. detsembri 2003. aasta otsus 2004/97/EÜ, Euratom teatavate Euroopa Liidu ametite ja asutuste asukoha kohta (ELT L 29, 3.2.2004, lk 15).

(23) Avatud interneti avalik tuum, nimelt selle põhilised protokollid ja taristu, mis on üleilmne avalik hüve, tagab interneti kui terviku põhifunktsionaalsuse ja toetab selle tavapärast toimimist. ENISA peaks toetama avatud interneti avaliku tuuma toimimise, sealhulgas põhiliste protokollide (eelkõige domeeninimede süsteem, BGP ja IPv6) turvalisust ja stabiilsust, domeeninimede süsteemi (kaasa arvatud kõigi tippdomeenide) ja juurserverite toimimist.

(24) ENISA põhiülesanne on toetada asjakohase õigusraamistiku järjepidevat rakendamist, eelkõige direktiivi (EL) 2016/1148 ja muude asjakohaste küberturvalisuse aspekte sisaldavate õigusaktide tulemuslikku rakendamist, mis on kübervastupidavusvõime suurendamise jaoks eluliselt tähtis. Arvestades seda, kui kiiresti küberohud muutuvad, on selge, et liikmesriike tuleb toetada igakülgsema ja eri valdkondi hõlmava poliitilise lähenemisega kübervastupidavusvõime loomisele.

(25) ENISA peaks abistama liikmesriike ja liidu institutsioone, organeid ja asutusi nende jõupingutustes, et luua ja parandada suutlikkust ja valmisolekut ennetada ja avastada küberohte ja intsidente ning neile reageerida, ning seoses võrgu- ja infosüsteemide turvalisusega. Eeskätt peaks ENISA toetama direktiivis (EL) 2016/1148 sätestatud riiklike ja liidu küberturbe intsidentide lahendamise üksuste („CSIRTid“) arendamist ja tõhustamist, et neil oleks kogu liidus ühtemoodi kõrge küpsuse aste. ENISA tegevused, mis on seotud liikmesriikide tegevussuutlikkusega, peaksid aktiivselt toetama liikmesriikide endi poolt direktiivist (EL) 2016/1148 tulenevate kohustuste täitmiseks võetud meetmeid ega tohiks neid meetmeid asendada.

(26) Samuti peaks ENISA abistama liidu ja taotluse korral liikmesriikide võrgu- ja infosüsteemide turvalisuse strateegiate väljatöötamist ja ajakohastamist, eelkõige küberturvalisuse osas, ning edendama nende strateegiate levitamist ja jälgima nende rakendamise edusamme. Lisaks peaks ENISA aitama kaasa vajaduse katmisele koolituste ja koolitusmaterjali järele, sealhulgas seoses avalike asutuste vajadustega, ning koolitama asjakohasel juhul suures ulatuses koolitajaid, lähtudes Euroopa kodanike digipädevuse raamistikust ning pidades silmas liikmesriikide ning liidu institutsioonide, organite ja asutuste abistamist nende endi koolitussuutlikkuse väljaarendamisel.

(27) ENISA peaks toetama liikmesriike küberturvalisuse alase teadlikkuse parandamise ja hariduse valdkonnas, hõlbustades liikmesriikide vahel tihedamat koordineerimist ja parimate tavade vahetamist. Selline toetus võiks seisneda riiklike haridusalaste kontaktpunktide võrgustiku ja küberturvalisuse koolitusplatvormi arendamises. Riiklike haridusalaste kontaktpunktide võrgustik võiks toimida liikmesriikide kontaktametnike võrgustiku raames ja olla lähtepunkt tulevaseks liikmesriikide vaheliseks koordineerimiseks.

(28) ENISA peaks abistama direktiiviga (EL) 2016/1148 moodustatud koostöörühma selle ülesannete täitmisel, eeskätt pakkuma oskusteavet ja nõu ning hõlbustama parimate tavade vahetamist muu hulgas seoses oluliste teenuste operaatorite identifitseerimisega liikmesriikide poolt, ning samuti selles osas, mis puudutab riskide ja intsidentidega seotud piiriüleseid sõltuvusseoseid.

(29) Selleks et ergutada avaliku ja erasektori koostööd ning erasektorisisest koostööd ning eelkõige toetada elutähtsate taristute kaitset, peaks ENISA toetama teabe jagamist sektorite sees ja vahel, eeskätt direktiivi (EL) 2016/1148 II lisas loetletud sektorites, levitades parimaid tavasid ja andes suuniseid kättesaadavate töövahendite ja menetluste kohta ning selle kohta, kuidas lahendada teabe jagamisega seotud regulatiivsed küsimused, näiteks hõlbustades valdkondlike teabe jagamise ja analüüsimise keskuste loomist.

(30) Samal ajal kui IKT-toodete, -teenuste ja -protsesside turvanõrkuste potentsiaalne negatiivne mõju järjest suureneb, mängib üldise küberturvalisuse riski vähendamisel tähtsat rolli selliste turvanõrkuste leidmine ja kõrvaldamine. On tõestatud, et organisatsioonide, turvanõrkustega IKT-toodete, -teenuste ja -protsesside tootjate ja pakkujate ning küberturvalisuse teadusuuringute kogukonna liikmete ja valitsuste, kes turvanõrkusi leiavad, vaheline koostöö on märkimisväärselt suurendanud IKT-toodete, -teenuste ja - protsesside turvanõrkuste avastamist ja kõrvaldamist. Turvanõrkuse koordineeritud avalikustamine kujutab endast struktureeritud koostööprotsessi, mille puhul teatatakse turvanõrkusest infosüsteemi omanikule, andes organisatsioonile võimaluse diagnoosida ja kõrvaldada turvanõrkus enne selle kohta üksikasjaliku teabe avalikustamist kolmandatele isikutele või avalikkusele. Protsessiga nähakse ka ette turvanõrkuse leidja ja organisatsiooni vaheline koordineerimine seoses nimetatud turvanõrkuse avalikustamisega. Turvanõrkuse koordineeritud avalikustamise põhimõtetel võib olla tähtis roll küberturvalisuse parandamiseks tehtavates liikmesriikide jõupingutustes.

(31) ENISA peaks koondama ja analüüsima riikide vabatahtlikult jagatud CSIRTide ja Euroopa Parlamendi, Euroopa Ülemkogu, Euroopa Liidu Nõukogu, Euroopa Komisjoni, Euroopa Liidu Kohtu, Euroopa Keskpanga, Euroopa Kontrollikoja, Euroopa välisteenistuse, Euroopa Majandus- ja Sotsiaalkomitee, Euroopa Regioonide Komitee ja Euroopa Investeerimispanga vahelise kokkuleppega liidu institutsioonide, organite ja asutuste infoturbeintsidentidega tegeleva rühma (CERT-EU) töökorralduse ja toimimise kohta ([14]) moodustatud liidu institutsioonide, organite ja asutuste infoturbeintsidentidega tegeleva institutsioonidevahelise rühma (CERT-EU) aruandeid, et aidata kaasa teabevahetuse jaoks ühiste menetluste, keele ja terminoloogia koostamisele. Direktiiviga (EL) 2016/1148 loodi alus vabatahtlikuks tehnilise teabe vahetamiseks operatiivtasandil riiklike küberturbe intsidentide lahendamise üksuste võrgustikus („CSIRTide võrgustik") - selle raames peaks ENISA kaasama erasektori.

(32) ENISA peaks andma oma panuse sellesse, kuidas liidu tasandil reageeritakse ulatuslikele piiriülestele intsidentidele ja küberturvalisusega seotud kriisidele. Seda ülesannet tuleks täita kooskõlas käesoleva määruse kohaste ENISA volitustega ja lähenemisviisiga, mille suhtes peavad liikmesriigid kokku leppima komisjoni soovituse (EL) 2017/1584 ([15]) ning nõukogu 26. juuni 2018. aasta järelduste (ELi koordineeritud reageerimise kohta ulatuslike küberintsidentide ja kriiside korral) kontekstis. See ülesanne võiks hõlmata asjaomase teabe kogumist ning vahendajarolli CSIRTide võrgustiku ja tehnilise kogukonna, aga ka kriisi haldamise eest vastutavate otsusetegijate vahel. Lisaks peaks ENISA toetama ühe või mitme liikmesriigi taotlusel liikmesriikide vahelist operatiivkoostööd intsidentide käsitlemisel tehnilise külje pealt, hõlbustades liikmesriikide vahel vajalike tehniliste lahenduste vahetamist ja pakkudes sisendit avaliku teabevahetuse jaoks. ENISA peaks operatiivkoostööd toetama sellise koostöö üksikasjade testimisega korrapäraste küberturvalisuse õppuste käigus.

(33) Operatiivkoostöö toetamisel peaks ENISA kasutama CERT-EU olemasolevaid tehnilisi ja operatiivseid oskusteadmisi struktureeritud koostöö kaudu. Struktureeritud koostöö võib tugineda ENISA oskusteabele. Asjakohasel juhul tuleks kahe üksuse vahel kehtestada erikord, et määrata kindlaks sellise koostöö praktiline kulg ja vältida tegevuse dubleerimist.

(34) Täites oma ülesannet toetada operatiivkoostööd CSIRTide võrgustikus peaks ENISA olema suuteline pakkuma liikmesriikidele nende taotluse korral toetust, näiteks andma nõu, kuidas parandada intsidentide ennetamise, nende avastamise ja neile reageerimise suutlikkust, hõlbustades märkimisväärse või olulise mõjuga intsidentide tehnilist lahendamist või tagades küberohtude ja intsidentide analüüsimise. ENISA peaks hõlbustama märkimisväärse või olulise mõjuga intsidentide tehnilist lahendamist, eeskätt toetades tehniliste lahenduste vabatahtlikku jagamist liikmesriikide vahel või koostades kombineeritud tehnilist teavet, näiteks liikmesriikide poolt vabatahtlikult jagatud tehnilised lahendused. Soovituse (EL) 2017/1584 kohaselt peaksid liikmesriigid tegema heas usus koostööd ja jagama ilma põhjendamatute viivitusteta nii omavahel kui ka ENISAga teavet ulatuslike intsidentide ja küberturvalisusega seotud kriiside kohta. Sellisest teabest oleks ENISA-l oma operatiivkoostöö toetamise ülesande täitmisel täiendavat abi.

(35) ENISA peaks liidu olukorrateadlikkust toetava tehnilise tasandi korrapärase koostöö raames korrapäraselt ja tihedas koostöös liikmesriikidega koostama intsidentide ja küberohtude kohta ELi küberturvalisuse tehnilist olukorda käsitlevaid põhjalikke aruandeid, mis põhinevad avalikult kättesaadaval teabel, tema enda analüüsidel ja aruannetel, mida jagavad temaga liikmesriikide CSIRTid või direktiivis (EL) 2016/1148 ettenähtud võrgu- ja infosüsteemide turbe valla riiklikud ühtsed kontaktpunktid („ühtsed kontaktpunktid") (mõlemad vabatahtlikkuse alusel), Europoli juures tegutsev küberkuritegevuse vastase võitluse Euroopa keskus (EC3), CERT-EU ja kui see on asjakohane, siis Euroopa välisteenistuse juures tegutsev Euroopa Liidu luure- ja situatsioonikeskus (EU INTCEN). Aruanne tuleks teha kättesaadavaks nõukogule, komisjonile, liidu välisasjade ja julgeolekupoliitika kõrgele esindajale ning CSIRTide võrgustikule.

(36) Märkimisväärse või olulise mõjuga intsidendi puhul peaks ENISA toetus asjaomaste liikmesriikide taotluse korral tehtavale tehnilisele järeluurimisele keskenduma edasiste intsidentide ärahoidmisele. Asjaomased liikmesriigid peaksid pakkuma vajalikku teavet ja abi, et võimaldada ENISA-l tõhusalt toetada tehnilist uurimist.

([14]) ELT C 12, 13.1.2018, lk 1.

([15]) Komisjoni 13. septembri 2017. aasta soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral (ELT L 239, 19.9.2017, lk 36).

(37) Liikmesriigid võivad paluda, et intsidendist mõjutatud ettevõtjad teeksid koostööd ning pakuksid ENISA-le vajalikku teavet ja abi, ilma et see piiraks nende õigust kaitsta tundlikku äriteavet ja avaliku julgeoleku seisukohast olulist teavet.

(38) Et küberturvalisuse valdkonna probleemidest paremini aru saada ning liikmesriikidele ja liidu institutsioonidele, organitele ja asutustele pikaajalist strateegilist nõu anda, peab ENISA analüüsima praeguseid ja kujunemisjärgus küberturvalisuse riske. Sel eesmärgil peaks ENISA koostöös liikmesriikidega ja asjakohasel juhul ka statistikaasutuste ja muude asutustega koguma asjassepuutuvat avalikult kättesaadavat või vabatahtlikult jagatavat teavet ning analüüsima kujunemisjärgus tehnoloogiaid ja andma teemakohaseid hinnanguid võrgu- ja infoturbe, eeskätt küberturvalisuse tehnoloogiliste uuenduste eeldatavale ühiskondlikule, õiguslikule, majanduslikule ja regulatiivsele mõjule. Peale selle peaks ENISA toetama küberohtude, turvanõrkuste ja intsidentide analüüsimise kaudu liikmesriike ja liidu institutsioone, organeid ja asutusi esilekerkivate küberturvalisuse riskide kindlakstegemisel ja intsidentide ennetamisel.

(39) ENISA peaks liidu vastupidavuse suurendamiseks arendama oskusteavet seoses nende küberturvalisuse taristutega, mis toetavad eeskätt direktiivi (EL) 2016/1148 II lisas loetletud sektoreid ja mida kasutavad kõnealuse direktiivi III lisas loetletud digitaalsete teenuste osutajad, andes nõuandeid ja suuniseid ning vahetades parimaid tavasid. Et tagada hõlpsam juurdepääs paremini struktureeritud teabele küberturvalisuse riskide ja võimalike vastumeetmete kohta, peaks ENISA arendama välja liidu teabekeskuse ja hoidma seda käigus; liidu teabekeskus oleks universaalne portaal, mis jagaks üldsusele küberturvalisuse kohta teavet, mis on saadud liidu ja riikide institutsioonidelt, organitelt ja asutustelt. Küberturvalisuse riske ja võimalikke vastumeetmeid käsitlevale paremini struktureeritud teabele juurdepääsu võimaldamine võib ka aidata liikmesriikidel oma suutlikkust parandada ja tavasid ühtlustada ning suurendada seega nende üldist vastupidavusvõimet küberrünnete suhtes.

(40) ENISA peaks aitama parandada üldsuse teadlikkust küberturvalisuse riskidest, sealhulgas ELi ülese teadlikkuse parandamise kampaania kaudu hariduse edendamise abil, ja jagama kodanikele, organisatsioonidele ja ettevõtjatele mõeldud individuaalsete kasutajate headel tavadel põhinevaid suuniseid. ENISA peaks aitama kaasa ka parimate tavade ja lahenduste, sealhulgas küberhügieeni ja küberkirjaoskuse propageerimisele kodanike, organisatsioonide ja ettevõtjate tasandil, kogudes ja analüüsides avalikult kättesaadavat teavet oluliste intsidentide kohta ning koostades ja avaldades aruanded ja suunised kodanikele, organisatsioonidele ja ettevõtjatele, et parandada nende valmisoleku ja vastupidavuse üldist taset. ENISA peaks ka püüdma pakkuda tarbijatele asjakohast teavet kohaldatavate sertifitseerimise kavade kohta, näiteks andes suuniseid ja soovitusi. Lisaks peaks ENISA korraldama kooskõlas komisjoni 17. jaanuari 2018. aasta teatise kohase digiõppe tegevuskavaga ning koostöös liikmesriikide ja liidu institutsioonide, organite ja asutustega korrapäraseid lõppkasutajatele suunatud üldsuse harimise ja teavituskampaaniaid, mille eesmärk on propageerida üksikisikute ohutumat veebikäitumist ja digikirjaoskust, parandada teadlikkust võimalikest küberohtudest, sealhulgas sellisest kriminaalsest tegevusest veebis nagu andmepüügi rünnakud, robotvõrgud, finants- ja pangapettused ning andmetega seotud pettused, ning tutvustada mitmetegurilise autentimise, paikamise, krüptimise, andmete anonüümseks muutmise ja andmekaitse alaseid nõuandeid.

(41) ENISA-l peaks olema keskne roll selles, et lõppkasutajad saaksid kiiremini teadlikuks seadmete turvalisusest ja teenuste turvalisest kasutamisest, ja edendama liidu tasandil sisseprojekteeritud turvet ja lõimprivaatsust. Selle eesmärgi poole püüdlemisel peaks ENISA kasutama olemasolevaid parimaid tavasid ja kogemusi, eriti neid, mis on pärit teadusasutustelt ja IT-turvalisusega tegelevatelt teadlastelt.

(42) Küberturvalisuse sektoris tegutsevate ettevõtjate, aga ka küberturvalisuse lahenduste kasutajate toetuseks peaks ENISA rajama nn turuseirekeskuse ja seda käigus hoidma, analüüsides korrapäraselt nii küberturvalisuse turu nõudluse kui ka pakkumise poole peamisi suundumusi ja jagades selle kohta teavet.

(43) ENISA peaks aitama kaasa liidu jõupingutustele teha koostööd rahvusvaheliste organisatsioonidega ning küberturvalisuse valdkonna asjakohastes rahvusvahelise koostöö raamistikes. Eelkõige peaks ENISA asjakohasel juhul aitama kaasa koostööle selliste organisatsioonidega nagu OECD, OSCE ja NATO. Selline koostöö võiks hõlmata küberturvalisuse ühisõppusi ja intsidentidele ühiselt reageerimise koordineerimist. Need tegevused peavad täielikult austama kaasavuse, vastastikkuse ja liidu otsuste tegemise autonoomsuse põhimõtteid, mõjutamata ühegi liikmesriigi julgeoleku- ja kaitsepoliitika eripära.

(44) Tagamaks, et ENISA saavutab oma eesmärgid täies ulatuses, peaks ta suhtlema asjaomaste liidu järelevalve- ja muude pädevate asutustega, liidu institutsioonide, organite ja asutustega, kelle hulgas on CERT-EU, EC3, Euroopa Kaitseagentuur (EDA), Ülemaailmne Satelliitnavigatsioonisüsteemi Euroopa Agentuur (Euroopa GNSSi Agentuur), Elektroonilise Side Euroopa Reguleerivate Asutuste Ühendatud Amet (BEREC), Vabadusel, Turvalisusel ja Õigusel Rajaneva Ala Suuremahuliste IT-süsteemide Operatiivjuhtimise Euroopa Amet (eu-LISA), Euroopa Keskpank (EKP), Euroopa Pangandusjärelevalve (EBA), Euroopa Andmekaitsenõukogu, Energeetikasektorit Reguleerivate Asutuste Koostööamet (ACER), Euroopa Liidu Lennundusohutusamet (EASA) ja muud liidu asutused, kes tegelevad küberturvalisusega. Samuti peaks ENISA suhtlema andmekaitsega tegelevate ametiasutustega, et vahetada oskusteavet ja parimaid tavasid ning anda nõu küberturvalisuse küsimustes, mis võivad nende tööd mõjutada. Liikmesriikide ja liidu õiguskaitseasutuste ning andmekaitseasutuste esindajad peaksid olema esindatud ENISA nõuanderühmas. Õiguskaitseasutustega koostöö tegemisel võrgu- ja infoturbe küsimustes, mis võivad nende tööd mõjutada, peaks ENISA arvestama olemasolevate teabekanalite ja rajatud võrgustikega.

(45) Tuleks luua partnerlussuhted teadusasutustega, kel on asjaomastes valdkondades teadusalgatusi, ning tuleks tagada asjakohased kanalid tarbija- ja teiste organisatsioonide panustamiseks ja nende panust tuleks arvesse võtta.

(46) ENISA, täites CSIRTide võrgustiku sekretariaadi rolli, peaks toetama liikmesriikide CSIRTe ja CERT-EUd operatiivkoostöös seoses CSIRTide võrgustiku asjaomaste ülesannetega, millele on osutatud direktiivis (EL) 2016/1148. Veelgi enam, ENISA peaks edendama ja toetama asjaomaste CSIRTide koostööd, kui toimuvad intsidendid, ründed või häired CSIRTide hallatavates või kaitstavates võrkudes või taristutes, mis hõlmavad või võivad hõlmata vähemalt kahte CSIRTi, võttes seejuures arvesse CSIRTide võrgustiku standardset töökorda.

(47) Selleks et suurendada liidu valmisolekut reageerida intsidentidele, peaks ENISA korrapäraselt korraldama liidu tasandil küberturvalisuse õppusi ning toetama liikmesriike ja liidu institutsioone, organeid ja asutusi nende taotluse korral selliste õppuste korraldamisel. Iga kahe aasta järel tuleks korraldada põhjalik suurõppus, mis hõlmab tehnilisi, operatiivseid ja strateegilisi elemente. Lisaks peaks ENISA saama korrapäraselt korraldada vähem põhjalikke õppusi, millel on sama eesmärk – parandada liidu valmisolekut reageerida intsidentidele.

(48) ENISA peaks edasi arendama ja säilitama oma oskusteavet küberturvalisuse sertifitseerimise kohta, et toetada liidu poliitikat selles valdkonnas. ENISA peaks tuginema olemasolevatele parimatele tavadele ja edendama küberturvalisuse sertifitseerimise kasutuselevõttu liidus muu hulgas sellega, et aitab kehtestada liidu tasandil küberturvalisuse sertifitseerimise raamistiku („Euroopa küberturvalisuse sertifitseerimise raamistik“) ja seda hallata, et suurendada IKT-toodete, -teenuste ja -protsesside küberturvalisuse usaldusväärsuse läbipaistvust ning tugevdada seeläbi usaldust digitaalse siseturu vastu ja selle konkurentsivõimet.

(49) Tõhusad küberturvalisuse alased poliitikameetmed peaksid tuginema hästi väljatöötatud riskihindamismeetoditele, seda nii avalikus kui ka erasektoris. Riskihindamismeetodeid kasutatakse erinevatel tasanditel ning puudub nende tõhusa kohaldamise ühine tava. Riskide hindamise ja koostalitlusvõimeliste riskihalduse lahenduste parimate tavade propageerimine ja arendamine avaliku ja erasektori organisatsioonides tõstab küberturvalisuse taset liidus. Selleks peaks ENISA toetama sidusrühmade koostööd liidu tasandil ja hõlbustama nende jõupingutusi seoses elektrooniliste toodete, süsteemide, võrkude ja teenuste – mis koos tarkvaraga moodustavad võrgu- ja infosüsteemid – riskihalduse ja mõõdetava turvalisuse Euroopa ja rahvusvaheliste standardite väljatöötamise ja kasutuselevõtmisega.

(50) ENISA peaks innustama liikmesriike ning IKT-toodete, - teenuste ja -protsesside tootjaid ja pakkujaid tõstma oma üldisi turbestandardeid, et kõik internetikasutajad saaksid võtta vajalikud meetmed oma isikliku küberturvalisuse tagamiseks ja oleksid motiveeritud seda tegema. Eelkõige peaksid IKT-toodete, - teenuste ja -protsesside tootjad ja pakkujad pakkuma vajalikke uuendusi ning nõudma tagasi, võtma tagasi või taaskasutusse IKT-tooted, -teenused ja -protsessid, mis ei vasta küberturvalisuse standarditele, samas kui importijad ja turustajad peaksid tagama, et nende poolt liidu turule lastud IKT-tooted, -teenused ja -protsessid vastavad kohaldatavatele nõuetele ning ei kujuta endast ohtu liidu tarbijatele.

(51) ENISA peaks saama koostöös pädevate asutustega jagada teavet siseturul pakutavate IKT-toodete, -teenuste ja -protsesside küberturvalisuse taseme kohta ning avaldama IKT-toodete, - teenuste ja -protsesside tootjatele ja pakkujatele suunatud hoiatusi, milles nõutakse nende IKT-toodete, -teenuste ja -protsesside turvalisuse, sealhulgas küberturvalisuse parandamist.

(52) ENISA peaks täies ulatuses võtma arvesse käimasolevaid teadus- arendustegevusi ning tehnoloogilisi hindamisi, eelkõige neid, mida tehakse erinevates liidu teadusalgatustes, et nõustada liidu institutsioone, organeid ja asutusi ning kui see on asjakohane, liikmesriike nende taotlusel seoses vajadusega teadusuuringute järele ja prioriteetidega küberturvalisuse valdkonnas. ENISA peaks teadusuuringute vajaduste ja prioriteetide kindlakstegemiseks konsulteerima ka asjaomaste kasutajarühmadega. Konkreetsemalt tuleks sisse seada koostöö Euroopa Teadusnõukogu, Euroopa Innovatsiooni- ja Tehnoloogiainstituudi ning Euroopa Liidu Julgeoleku-uuringute Instituudiga.

(53) ENISA peaks Euroopa küberturvalisuse sertifitseerimise kavade koostamisel korrapäraselt konsulteerima standardiorganisatsioonidega, eriti Euroopa standardiorganisatsioonidega.

(54) Küberohud on ülemaailmsed. Vaja on teha tihedamat rahvusvahelist koostööd, et parandada küberturvalisuse standardeid (sealhulgas määrata kindlaks ühised käitumisnormid ja võtta vastu tegevusjuhendid), rahvusvaheliste standardite kasutamist ja teabe jagamist, millega edendatakse nii kiiremat rahvusvahelist koostööd võrgu- ja infoturbe probleemidele reageerimise valdkonnas kui ka ühtset ülemaailmset lähenemisviisi neis küsimustes. Selleks peaks ENISA toetama liidu tihedamat kaasamist ning koostööd kolmandate riikide ja rahvusvaheliste organisatsioonidega, pakkudes asjakohasel juhul asjaomastele liidu institutsioonidele, organitele ja asutustele vajalikku oskusteavet ja analüüsi.

(55) ENISA peaks saama reageerida liikmesriikide ja liidu institutsioonide, organite ja asutuste *ad hoc* nõuande- ja abitaotlustele ENISA pädevusse kuuluvates küsimustes.

(56) ENISA juhtimisel on mõistlik ja soovitav rakendada teatavaid põhimõtteid, et järgida 2012. aasta juulis institutsioonidevahelises ELi detsentraliseeritud asutuste töörühmas kokkulepitud ühisavaldust ja ühist lähenemisviisi, mille eesmärk on ühtlustada detsentraliseeritud asutuste tegevust ja parandada nende toimimist. Ühisavalduses ja ühises lähenemisviisis sisalduvad soovitused peaksid samuti asjakohaselt kajastuma ENISA tööprogrammides, ENISA hindamistes ning ENISA aruandlus- ja haldustavades.

(57) Liikmesriikide ja komisjoni esindajatest koosnev haldusnõukogu peaks määrama kindlaks ENISA tegevuse üldsuuna ning tagama, et ENISA täidab oma ülesandeid vastavalt käesolevale määrusele. Haldusnõukogule tuleks anda õigus koostada ENISA eelarve ja kontrollida selle täitmist, võtta vastu kohased finantsreeglid, kehtestada ENISA otsuste tegemiseks läbipaistev kord, võtta vastu ENISA ühtne programmdokument, võtta vastu ENISA kodukord, nimetada ametisse tegevdirektor ning otsustada tegevdirektori ametiaja pikendamise ja tema ametiaja lõpetamise üle.

(58) ENISA nõuetekohaseks ja tulemuslikuks toimimiseks peaksid komisjon ja liikmesriigid tagama, et haldusnõukogu liikmeteks nimetatavatel isikutel on vajalikud erialateadmised ja kogemus. Komisjon ja liikmesriigid peaksid püüdma piirata oma esindajate vahetumist haldusnõukogus, et tagada selle töö järjepidevus.

(59) ENISA sujuvaks toimimiseks on tarvis, et tegevdirektor nimetataks ametisse pidades silmas tema teeneid, dokumenteeritud haldamis- ja juhtimisoskust ning küberturvalisuse alaseid teadmisi ja kogemusi. Tegevdirektori ülesandeid tuleks täita täiesti sõltumatult. Tegevdirektor peaks pärast komisjoniga konsulteerimist koostama ettepaneku ENISA iga-aastase tööprogrammi kohta ning võtma kõik vajalikud meetmed tööprogrammi nõuetekohase elluviimise tagamiseks. Tegevdirektor peaks koostama igal aastal haldusnõukogule esitatava aruande, mis käsitleb ENISA iga-aastase tööprogrammi rakendamist, koostama ENISA tulude ja kulude kalkulatsiooni eelnõu ning vastutama eelarve täitmise eest. Lisaks peaks tegevdirektoril olema võimalik moodustada ajutisi töörühmi selleks, et käsitleda konkreetseid, eeskätt teaduslikku, tehnilist, õiguslikku või sotsiaal-majanduslikku laadi küsimusi. Ajutise töörühma moodustamine on vajalik eelkõige seoses konkreetse Euroopa küberturvalisuse sertifitseerimise ettevalmistava kava („ettevalmistav kava“) koostamisega. Tegevdirektor peaks tagama, et ajutiste töörühmade liikmed valitakse kõige põhjalikumate erialateadmiste põhjal, püüdes tagada soolise tasakaalu ning selle, et seal oleksid (lähtuvalt sellest, kuidas see on konkreetset küsimust arvestades asjakohane) tasakaalustatult esindatud liikmesriikide ametiasutused,

liidu institutsioonid, organid ja asutused ning erasektor, sealhulgas majandusringkonnad, kasutajad ning võrgu- ja infoturbe alal pädevad teadureksperdid.

(60) Juhatus peaks aitama kaasa haldusnõukogu tõhusale toimimisele. Osana haldusnõukogu otsustega seotud ettevalmistustööst peaks juhatus põhjalikult analüüsima asjakohast teavet, olemasolevaid võimalusi ning pakkuma nõuandeid ja lahendusi haldusnõukogu asjakohaste otsuste ettevalmistamiseks.

(61) ENISA-l peaks olema nõuandva organina ENISA nõuanderühm, mis tagaks korrapärase dialoogi erasektori, tarbijate organisatsioonide ja teiste asjaomaste sidusrühmadega. Tegevdirektori ettepanekul haldusnõukogu moodustatud ENISA nõuanderühm peaks keskenduma sidusrühmade jaoks olulistele küsimustele ja juhtima neile ENISA tähelepanu. Eelkõige tuleks ENISA nõuanderühmaga konsulteerida ENISA iga-aastase tööprogrammi kavandi üle. ENISA nõuanderühm koosseis ja ülesanded peaksid tagama sidusrühmade piisava esindatuse ENISA töös.

(62) Tuleks moodustada sidusrühmade küberturvalisuse sertifitseerimise rühm, et aidata ENISA-l ja komisjonil hõlbustada konsulteerimist asjaomaste sidusrühmadega. Sidusrühmade küberturvalisuse sertifitseerimise rühma liikmed peaksid esindama tasakaalustatud viisil tööstust, nii IKT-toodete ja -teenuste nõudluse kui pakkumise poolelt, muu hulgas eelkõige VKEsid, digitaalsete teenuste osutajaid, Euroopa ja rahvusvahelisi standardiasutusi, riiklikke akrediteerimisasutusi, andmekaitse järelevalveasutusi ning Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 765/2008 ([16]) kohaseid vastavushindamisasutusi ning teadusasutusi ja tarbijaorganisatsioone.

(63) ENISA peaks võtma vastu huvide konfliktide ennetamise ja lahendamise normid. ENISA peaks kohaldama ka asjaomaseid liidu sätteid, mis käsitlevad üldsuse juurdepääsu dokumentidele, nagu on sätestatud Euroopa Parlamendi ja nõukogu määruses (EÜ) nr 1049/2001 ([17]). ENISA peaks isikuandmeid töötlema vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2018/1725 ([18]). ENISA peaks teabe, eelkõige tundliku salastamata teabe ja Euroopa Liidu salastatud teabe käitlemisel järgima liidu institutsioonide, organite ja asutuste kohta kehtivaid sätteid ja liikmesriikide õigusakte.

(64) Et tagada ENISA täielik autonoomia ja sõltumatus ning võimaldada tal täita lisaülesandeid, sealhulgas kiireloomulisi erakorralisi ülesandeid, tuleks ENISA-le eraldada piisav ja autonoomne eelarve, mille peamine tulu tuleks liidu toetusest ja ENISA töös osalevate kolmandate riikide rahalisest osalusest. Piisav eelarve on üliloluline tagamaks, et ENISA-l on kõigi oma lisanduvate ülesannete täitmiseks ja eesmärkide saavutamiseks vajalik suutlikkus. Enamik ENISA töötajaid peaks olema otseselt tegevad ENISA volituste täitmisel. Asukohaliikmesriigil ja igal muul liikmesriigil peaks olema lubatud teha ENISA eelarvesse vabatahtlikult sissemakseid. Liidu eelarvemenetluse kohaldamist tuleks jätkata kõigi toetuste suhtes, mida makstakse liidu üldeelarvest. Lisaks sellele peaks ENISA raamatupidamisarvestust läbipaistvuse ja vastutuse tagamiseks auditeerima kontrollikoda.

(65) Küberturvalisuse sertifitseerimisel on tähtis roll IKT-toodete, -teenuste ja -protsesside usaldusväärsuse ja turvalisuse parandamisest. Digitaalne ühtne turg ning eelkõige andmepõhine majandus ja asjade internet saavad olla edukad vaid juhul, kui avalikkusel on kindlustunne, et sellised tooted, teenused ja protsessid pakuvad teatavat küberturvalisuse taset. Internetiühendusega ja automatiseeritud autod, elektroonilised meditsiiniseadmed, tööstuslikud automatiseeritud juhtimissüsteemid ja arukad võrgud on vaid mõned näited sektoritest, kus sertifitseerimist juba ulatuslikult kasutatakse või tõenäoliselt hakatakse lähitulevikus kasutama. Direktiiviga (EL) 2016/1148 reguleeritud sektorid on ka sektorid, kus küberturvalisuse sertifitseerimine on äärmiselt oluline.

([16]) Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta määrus (EÜ) nr 765/2008, millega sätestatakse akrediteerimise ja turujärelevalve nõuded seoses toodete turustamisega ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93 (ELT L 218, 13.8.2008, lk 30).

([17]) Euroopa Parlamendi ja nõukogu 30. mai 2001. aasta määrus (EÜ) nr 1049/2001 üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele (EÜT L 145, 31.5.2001, lk 43).

([18]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39).

(66) 2016. aasta teatises „Euroopa kübervastupidavusvõime süsteemi tugevdamine ning konkurentsivõimelise ja uuenduslikku küberjulgeolekutööstuse soodustamine“ tõi komisjon välja vajaduse kvaliteetsete, taskukohaste ja koostalitlusvõimeliste küberturvalisuse toodete ja -lahenduste järele. IKT-toodete, -teenuste ja -protsesside pakkumine ühtsel turul on geograafiliselt endiselt väga killustatud. Selle põhjuseks on asjaolu, et küberturvalisuse tööstus on Euroopas peamiselt arenenud liikmesriikide valitsuste nõudluse najal. Lisaks kuulub kübeturvalisuse ühtse turu kitsaskohtade hulka koostalitusvõimeliste lahenduste (tehniliste standardite), tavade ja kogu liitu hõlmavate sertifitseerimismehhanismide puudumine. See teeb liikmesriigi, liidu ja üleilmsel tasandil konkureerimise Euroopa ettevõtjate jaoks keerukaks. Samuti tähendab see üksikisikute ja ettevõtjate jaoks võimaliku ja kasutatava küberturvalisuse tehnoloogia kättesaadavust väiksemas valikus. Sarnaselt märkis komisjon oma 2017. aasta teatises „Digitaalse ühtse turu strateegia rakendamise vahekokkuvõte. Ühendatud digitaalne ühtne turg kõigile“ vajadust turvaliste võrgustatud toodete ja süsteemide järele ning märkis, et Euroopa IKT turvalisuse raamistiku loomine, millega kehtestatakse õigusnormid selle kohta, kuidas korraldada IKT turvalisuse sertifitseerimist liidus, võib aidata säilitada usaldust interneti vastu ja vähendada siseturu praegust killustatust.

(67) Praegu kasutatakse IKT-toodete, -teenuste ja -protsesside küberturvalisuse sertifitseerimist üksnes piiratud ulatuses. Kui sertifitseerimine on olemas, siis peamiselt liikmesriigi tasandil või tööstusest lähtuvate kavade raames. Sellistes tingimustes ei tunnusta liikmesriigid üldiselt teise liikmesriigi riikliku küberturvalisuse sertifitseerimise asutuse poolt välja antud sertifikaati. Seega võib juhtuda, et ettevõtted peavad sertifitseerima oma IKT-tooted, -teenused ja -protsessid mitmes liikmesriigis, kus nad tegutsevad, näiteks et osaleda riiklikes hankemenetlustes, mis aga suurendab nende ettevõtete 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, usaldusväärsuse tasemetes, sisulistes kriteeriumides ja tegelikus kasutamises, mis takistab vastastikuse tunnustamise mehhanismide toimimist liidus.

(68) On tehtud mõningaid pingutusi, et tagada liidus sertifikaatide vastastikune tunnustamine. See on olnud aga vaid osaliselt edukas. Kõige olulisem näide siinkohal on kõrgemate ametnike infosüsteemide turvalisuse rühma (SOG-IS, *Senior Officials Group – Information Systems Security*) vastastikuse tunnustamise kokkulepe. Kuigi see on kõige tähtsam koostöö ja vastastikuse tunnustamise mudel turvalisuse sertifitseerimise valdkonnas, hõlmab SOG-IS üksnes mõnda liikmesriiki. See asjaolu on piiranud SOG-IS vastastikuse tunnustamise kokkuleppe tulemuslikkust siseturu seisukohast.

(69) Seetõttu on vaja võtta vastu ühine lähenemisviis 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, -teenuste või -protsesside Euroopa küberturvalisuse sertifikaate ja ELi vastavusdeklaratsioone kõigis liikmesriikides. Seejuures on oluline tugineda olemasolevatele riiklikele ja rahvusvahelistele kavadele ning vastastikuse tunnustamise süsteemidele, eelkõige SOG-ISile, ning võimaldada selliste süsteemide kohastelt olemasolevatelt kavadelt sujuvat üleminekut uue Euroopa küberturvalisuse sertifitseerimise raamistiku kohastele kavadele. Euroopa küberturvalisuse sertifitseerimise raamistikul peaks olema kaks eesmärki. Esiteks peaks see aitama suurendada usaldust Euroopa küberturvalisuse sertifitseerimise kavade kohaselt sertifitseeritud IKT-toodete, -teenuste ja -protsesside vastu. Teiseks peaks see aitama vältida üksteisele vastukäivate või kattuvate riiklike küberturvalisuse sertifitseerimise kavade paljusust ja seeläbi vähendama digitaalsel ühtsel turul tegutsevate ettevõtjate kulusid. Euroopa küberturvalisuse sertifitseerimise kavad peaksid olema mittediskrimineerivad ning põhinema Euroopa või rahvusvahelistel standarditel, välja arvatud juhul, kui need standardid on ebatõhusad või ebasobivad liidu õiguspäraste eesmärkide saavutamiseks selles valdkonnas.

(70) Euroopa küberturvalisuse sertifitseerimise raamistik tuleks kehtestada ühetaoliselt kõikides liikmesriikides, et vältida „sertifikaatide ostlemist“, mida põhjustab nõuete erinevus liikmesriikides.

(71) Euroopa küberturvalisuse sertifitseerimise kavad peaksid tuginema rahvusvahelisel ja riiklikul tasandil juba olemasolevatele kavadele ning vajaduse korral foorumite ja konsortsiumite tehnilistele kirjeldustele, õppides praegustest tugevatest külgedest ning hinnates ja parandades puudusi.

(72) Selleks et tööstus suudaks ennetada küberohte, on vaja paindlikke küberturvalisuse lahendusi, mistõttu tuleks iga sertifitseerimiskava koostada viisil, mis väldib kiire aegumise riski.

(73) Komisjonile tuleks anda õigus võtta vastu Euroopa küberturvalisuse sertifitseerimise kavad konkreetsete IKT-toodete, -teenuste ja -protsesside rühmade kohta. Neid kavu peaksid rakendama ja nende üle järelevalvet tegema riiklikud küberturvalisuse sertifitseerimise asutused ning nende kavade kohaselt välja antud sertifikaadid peaksid kehtima ja olema tunnustatud kogu liidus. Tööstuse või muude eraorganisatsioonide rakendatavad sertifitseerimiskavad peaksid jääma käesoleva määruse kohaldamisalast välja. Siiski peaksid saama selliseid kavu haldavad asutused teha komisjonile ettepaneku kaaluda nende kavade heakskiitmist Euroopa küberturvalisuse sertifitseerimise kavana.

(74) Käesoleva määruse sätted ei tohiks mõjutada liidu õigust, milles on sätestatud erinormid IKT-toodete, -teenuste ja -protsesside sertifitseerimise kohta. Eelkõige sisaldab määrus (EL) 2016/679 sätteid selliste sertifitseerimismehhanismide ning andmekaitsepitserite ja -märgiste kasutuselevõtuks, mille abil saab tõendada, et vastutavate töötlejate ja volitatud töötlejate isikuandmete töötlemise toimingud vastavad kõnealusele määrusele. Sellised sertifitseerimismehhanismid ning andmekaitsepitserid ja -märgised peaksid võimaldama andmesubjektidel kiiresti hinnata asjakohaste IKT-toodete, -teenuste ja -protsesside andmekaitse taset. Käesolev määrus ei piira määruse (EL) 2016/679 kohast andmetöötlustoimingute sertifitseerimist, sealhulgas juhul, kui sellised toimingud sisalduvad IKT-toodetes, -teenustes või -protsessides.

(75) Euroopa küberturvalisuse sertifitseerimise kavade eesmärk peaks olema tagada, et nende kavade kohaselt sertifitseeritud IKT-tooted, -teenused ja -protsessid vastavad kirjeldatud nõuetele, eesmärgiga kaitsta salvestatud, edastatud või töödeldud andmete või nende toodete, teenuste ja protsesside asjaomaste funktsioonide või nende poolt pakutavate või nende kaudu juurdepääsetavate teenuste käideldavust, autentsust, terviklust või konfidentsiaalsust kogu olelusringi kestel. Käesolevas määruses ei ole võimalik üksikasjalikult sätestada kõigi IKT-toodete, -teenuste ja -protsesside suhtes kohaldatavaid küberturvalisuse nõudeid. IKT-tooted, -teenused ja -protsessid ning nendega seotud küberturvalisuse vajadused on nii mitmekesised, et on väga raske esitada üldiseid küberturvalisuse nõudeid, mis kehtiksid igas olukorras. Seetõttu on vaja sertifitseerimise eesmärgil võtta kasutusele lai ja üldine küberturvalisuse mõiste, mida peaks täiendama rida konkreetseid küberturvalisuse eesmärke, mida tuleb Euroopa küberturvalisuse sertifitseerimise kavade koostamisel arvesse võtta. Nende eesmärkide saavutamise üksikasjad konkreetsete IKT-toodete, -teenuste ja -protsesside puhul tuleks täiendavalt täpsustada igas individuaalses sertifitseerimiskavas, mille komisjon vastu võtab, näiteks viidates standarditele või tehnilistele kirjeldustele, kui asjakohased standardid puuduvad.

(76) Euroopa küberturvalisuse sertifitseerimise kavas kasutatavad tehnilised kirjeldused peaksid järgima Euroopa Parlamendi ja nõukogu määruse (EL) nr 1025/2012 ([19]) II lisas sätestatud nõudeid. Mõned kõrvalekalded nendest nõuetest võivad siiski olla vajalikud põhjendatud juhtudel, kui nimetatud tehnilisi kirjeldusi kasutatakse Euroopa küberturvalisuse sertifitseerimise kavas, mis osutab kõrgele usaldusväärsuse tasemele. Selliste kõrvalekallete põhjused tuleks teha avalikult kättesaadavaks.

(77) Vastavushindamine on protsess, mille käigus hinnatakse, kas IKT-toote, -teenuse või -protsessiga seotud erinõuded on täidetud. Seda protsessi viib läbi sõltumatu kolmas isik, kes ei ole IKT-toote, -teenuse või -protsessi tootja ega pakkuja. IKT-toote, -teenuse või -protsessi eduka hindamise tulemusel tuleks välja anda Euroopa küberturvalisuse sertifikaat. Euroopa küberturvalisuse sertifikaati tuleks käsitada kinnitusena, et hindamine on nõuetekohaselt läbi viidud. Sõltuvalt usaldusväärsuse tasemest tuleks Euroopa küberturvalisuse sertifikaadi kavas märkida, kas Euroopa küberturvalisuse sertifikaadi annab välja era- või avalik-õiguslik asutus. Vastavushindamine ja sertifitseerimine iseenesest ei taga, et sertifitseeritud IKT-tooted, -teenused ja -protsessid on küberturvalised. Pigem on need menetlused ja tehnilised metoodikad kinnitamaks, et IKT-tooteid, -teenuseid ja -protsesse on kontrollitud ja et need vastavad teatavatele küberturvalisuse nõuetele, mis on sätestatud mujal, näiteks tehnilistes standardites.

(78) Euroopa küberturvalisuse sertifikaadi kasutajate poolne asjakohase sertifitseerimise ja seotud turvanõuete valik peaks põhinema IKT-toote, -teenuse või -protsessi kasutamisega seotud riskianalüüsil. Usaldusväärsuse tase peaks seega vastama IKT-toote, -teenuse või -protsessi ettenähtud kasutamisega seotud riskitasemele.

([19]) Euroopa Parlamendi ja nõukogu 25. oktoobri 2012. aasta määrus (EL) nr 1025/2012, mis käsitleb Euroopa standardimist ning millega muudetakse nõukogu direktiive 89/686/EMÜ ja 93/15/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 94/9/EÜ, 94/25/EÜ, 95/16/EÜ, 97/23/EÜ, 98/34/EÜ, 2004/22/EÜ, 2007/23/EÜ, 2009/23/EÜ ja 2009/105/EÜ ning millega tunnistatakse kehtetuks nõukogu otsus 87/95/EMÜ ning Euroopa Parlamendi ja nõukogu otsus nr 1673/2006/EÜ (ELT L 316, 14.11.2012, lk 12).

(79) Euroopa küberturvalisuse sertifitseerimise kavas võib ette näha vastavushindamise läbiviimine IKT-toodete, -teenuste või -protsesside tootjate -pakkujate ainuvastutusel („vastavuse enesehindamine“). Sellistel juhtudel peaks piisama sellest, kui IKT-toodete, -teenuste või -protsesside tootja või pakkuja teeb ise kõik kontrollid, et tagada IKT-toodete, -teenuste või -protsesside vastavus Euroopa küberturvalisuse sertifitseerimise kavale. Vastavuse enesehindamist tuleks pidada asjakohaseks vähekeerukate (nt lihtsa konstruktsiooni ja tootmismehhanismiga) IKT-toodete, -teenuste ja -protsesside puhul, mis kujutavad endast avalikkusele väikest riski. Lisaks peaks vastavuse enesehindamine olema lubatud üksnes nende IKT-toodete, -teenuste ja -protsesside puhul, mis vastavad usaldusväärsuse baastasemele.

(80) Euroopa küberturvalisuse sertifitseerimise kavas võib ette näha nii IKT-toodete, -teenuste või -protsesside vastavuse enesehindamise kui ka sertifitseerimise. Sellisel juhul tuleks kavas ette näha selged ja arusaadavad vahendid tarbijatele või teistele kasutajatele, et eristada IKT-tooteid, -teenuseid ja -protsesse, mida hinnatakse nende tootja või pakkuja vastutusel, nendest, mida sertifitseerib kolmas isik.

(81) IKT-toodete, -teenuste või -protsessude tootja või pakkuja, kes viib läbi vastavuse enesehindamise, peaks olema vastavushindamismenetluse raames võimeline koostama ELi vastavusdeklaratsiooni ja selle allkirjastama. ELi vastavusdeklaratsioon on dokument, millega kinnitatakse, et teatav IKT-toode, -teenus või -protsess vastab Euroopa küberturvalisuse sertifitseerimise kavas esitatud nõuetele. ELi vastavusdeklaratsiooni koostamisel ja allkirjastamisel võtab IKT- toodete, - teenuste või -protsesside tootja või pakkuja vastutuse IKT-toote, -teenuse või -protsessi vastavuse eest Euroopa küberturvalisuse sertifitseerimise kavas esitatud õiguslikele nõuetele. ELi vastavusdeklaratsiooni koopia tuleks esitada riiklikule küberturvalisuse sertifitseerimise asutusele ja ENISA-le.

(82) IKT-toodete, -teenuste või -protsesside tootja või pakkuja peaks hoidma ELi vastavusdeklaratsiooni, tehnilist dokumentatsiooni ja muud asjaomast teavet, mis puudutab IKT-toodete, -teenuste või -protsesside vastavust Euroopa küberturvalisuse sertifitseerimise kavale, pädevale riiklikule küberturvalisuse sertifitseerimise asutusele kättesaadavana asjaomases Euroopa küberturvalisuse sertifitseerimise kavas kindlaks määratud tähtaja jooksul. Tehnilistes dokumentides tuleks määrata kindlaks kava kohaselt kohaldatavad nõuded ja käsitleda vastavuse enesehindamiseks vajalikul määral IKT-toote, -teenuse või -protsessi projekteerimist, tootmist ja toimimist. Tehniline dokumentatsioon peaks olema koostatud nii, et see võimaldaks hinnata IKT-toote, -teenuse või -protsessi vastavust kava kohaselt kohaldatavatele nõuetele.

(83) Euroopa küberturvalisuse sertifitseerimise raamistiku juhtimises võetakse arvesse liikmesriikide osalemist ja sidusrühmade asjakohast osalemist ning määratakse kindlaks komisjoni roll Euroopa küberturvalisuse sertifitseerimise kava planeerimises ja vastava ettepaneku tegemises, taotlemises, koostamises, vastuvõtmises ja läbivaatamises.

(84) Komisjon, keda toetavad Euroopa küberturvalisuse sertifitseerimise rühm ja sidusrühmade küberturvalisuse sertifitseerimise rühm, peaks pärast avatud ja ulatuslikku konsultatsiooni koostama Euroopa küberturvalisuse sertifitseerimise kavasid käsitleva liidu jooksva tööprogrammi ja avaldama selle mittesiduva dokumendina. Liidu jooksev tööprogramm peaks olema strateegiline dokument, mis võimaldab eelkõige tööstusel, liikmesriikide asutustel ja standardiasutustel valmistuda juba varem ette tulevaste Euroopa küberturvalisuse sertifitseerimise kavade jaoks. Liidu jooksev tööprogramm peaks hõlmama mitmeaastast ülevaadet ettevalmistavate kavade taotluste kohta, mille komisjon kavatseb esitada ENISA-le kindlaksmääratud alusel koostamiseks. Komisjon peaks oma IKT standardimise jooksva kava ja Euroopa standardiorganisatsioonidele esitatavate standarditaotluste koostamisel võtma arvesse liidu jooksvat tööprogrammi. Arvestades uute tehnoloogiate kiiret juurutamist ja kasutuselevõttu, varem tundmatute küberturvalisuse riskide esilekerkimist ning seadusandlikku ja turuarengut, peaks komisjonil või Euroopa küberturvalisuse sertifitseerimise rühmal olema õigus taotleda, et ENISA koostaks ettevalmistavaid kavasid, mis ei sisaldu liidu jooksvas tööprogrammis. Sellistel juhtudel peaksid komisjon ja Euroopa küberturvalisuse sertifitseerimise rühm samuti hindama selliste taotluste vajalikkust, võttes arvesse käesoleva määruse üldeesmärki ning vajadust tagada järjepidevus seoses ENISA ressursside kavandamise ja kasutamisega.

Pärast sellise taotluse saamist peaks ENISA koostama põhjendamatu viivituseta konkreetsete IKT-toodete, -teenuste ja -protsesside jaoks ettevalmistava kava. Komisjon peaks hindama oma taotluse positiivset ja negatiivset mõju asjaomasele turule, eelkõige VKEdele, innovatsioonile, asjaomasele turule sisenemise tõketele ja kulule lõppkasutajate jaoks. Seejärel peaks komisjonile olema õigus võtta ENISA koostatud ettevalmistava kava põhjal rakendusaktidega vastu Euroopa küberturvalisuse sertifitseerimise kava. Võttes arvesse käesolevas määruses sätestatud üldeesmärki ja turvalisusega seotud eesmärke, tuleks komisjoni poolt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavades täpsustada konkreetse kava sisu, ulatuse ja toimimise minimaalsed üksikasjad. Need üksikasjad peaksid hõlmama muu hulgas küberturvalisuse sertifitseerimise ulatust ja sisu, sealhulgas hõlmatud IKT-toodete, -teenuste ja -protsesside kategooriad, küberturvalisuse nõuete üksikasjalik kirjeldus, näiteks viide standarditele või tehnilistele kirjeldustele, konkreetsed hindamiskriteeriumid ja -meetodid ning kavandatud usaldusväärsuse tase (baastase, märkimisväärne või kõrge tase) ning asjakohasel juhul hindamise tasemed. ENISA peaks saama jätta Euroopa küberturvalisuse sertifitseerimise rühma taotluse rahuldamata. Sellise otsuse peaks tegema haldusnõukogu ja see peaks olema põhjendatud.

(85) ENISA peaks haldama veebisaiti, mis tutvustab Euroopa küberturvalisuse sertifitseerimise kavasid ja pakub nende kohta teavet ning mis muu hulgas hõlmab taotlusi ettevalmistava kava koostamiseks ning ENISA poolt ettevalmistavas etapis läbiviidud konsulteerimise käigus saadud tagasisidet. Veebisait peaks samuti pakkuma teavet käesoleva määruse kohaselt välja antud Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide kohta, sealhulgas nende kehtetuks tunnistamise ja kehtivuse lõppemise kohta. Veebisaidil tuleks ka ära märkida need riiklikud küberturvalisuse sertifitseerimise kavad, mis on asendatud Euroopa küberturvalisuse sertifitseerimise kavaga.

(86) Euroopa sertifitseerimise kava usaldusväärsuse tase on aluseks kindlustundele, et IKT-toode, -teenus või -protsess vastab konkreetse Euroopa küberturvalisuse sertifitseerimise kava turvanõuetele. Euroopa küberturvalisuse sertifitseerimise raamistiku järjepidevuse tagamiseks peaks Euroopa küberturvalisuse sertifitseerimise kavas saama täpsustada nimetatud kava alusel väljaantud Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide usaldusväärsuse tasemed. Iga Euroopa küberturvalisuse sertifikaat võib osutada ühele usaldusväärsuse tasemele: baastase, märkimisväärne tase või kõrge tase, samas kui ELi vastavusdeklaratsioon võib osutada üksnes usaldusväärsuse baastasemele. Usaldusväärsuse tasemed näitaksid IKT-toodete, -teenuste või -protsesside hindamise rangust ja põhjalikkust ning need määrataks kindlaks viitega sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilistele kontrollidele, mille eesmärk on vähendada või ennetada intsidente. Iga usaldusväärsuse tase peaks olema järjepidev eri valdkondade lõikes, kus sertifitseerimist kohaldatakse.

(87) Euroopa küberturvalisuse sertifitseerimise kavas võib täpsustada mitu hindamise taset, sõltuvalt kasutatud hindamismetoodika rangusest ja põhjalikkusest. Hindamise tase peaks vastama ühele usaldusväärsuse tasemele ja olema seotud usaldusväärsuse komponentide asjakohase kombinatsiooniga. Kõigi usaldusväärsuse tasemete puhul peaks IKT-toode, -teenus või -protsess vastavalt kavale sisaldama mitmeid turvalisi funktsioone, mis võivad hõlmata järgmist: turvaline tehasekonfiguratsioon (*secure out-of-the-box configuration*), märgiga kood (*signed code*), turvaline uuendus (*secure update*) ja vallutuse leevendus (*exploit mitigations*) ning täielik pinu või kuhja mälu kaitse (*full stack or heap memory protections*). Neid funktsioone tuleks arendada ja hallata, kasutades turvalisusele suunatud arendamisalaseid lähenemisviise ja seotud vahendeid, et tagada tõhusate tarkvara ja riistvara mehhanismide usaldusväärne inkorporeerimine.

(88) Usaldusväärsuse baastaseme puhul tuleks hindamisel juhinduda vähemalt järgmistest usaldusväärsuse komponentidest: hindamine peaks hõlmama vastavushindamisasutuse poolt vähemalt IKT-toote, -teenuse või -protsessi tehnilise dokumentatsiooni läbivaatamist. Kui sertifitseerimine hõlmab IKT-protsesse, peaks tehnilist läbivaatamist kohaldama ka protsesside suhtes, mida on kasutatud IKT-toote või -teenuse projekteerimiseks, arendamiseks ja säilitamiseks. Kui Euroopa küberturvalisuse sertifitseerimise kavas nähakse ette vastavuse enesehindamine, peaks piisama sellest, kui IKT -toodete, -teenuste või -protsesside tootja või pakkuja on viinud läbi enesehindamise IKT-toote, -teenuse või -protsessi vastavuse kohta sertifitseerimise kavale.

(89) Märkimisväärse usaldusväärsuse taseme puhul tuleks hindamisel lisaks usaldusväärsuse baastaseme nõuetele juhinduda vähemalt IKT-toote, -teenuse või -protsessi turvafunktsioonide vastavuse kontrollimisest nimetatud toote, teenuse või protsessi tehnilisele dokumentatsioonile.

(90) Kõrge usaldusväärsuse taseme puhul tuleks hindamisel lisaks märkimisväärsele usaldusväärsuse taseme nõuetele juhinduda vähemalt tõhususe kontrollist, mille käigus hinnatakse IKT-toote, -teenuse või -protsessi turvafunktsioonide võimet panna vastu isikutele, kes panevad märkimisväärsete oskuste ja vahendite abil toime läbimõeldud küberrünnakeid.

(91) Euroopa küberturvalisuse sertifitseerimise ja ELi vastavusdeklaratsiooni kasutamine peaks jääma vabatahtlikuks, kui liidu õiguse või liidu õiguse kohaselt vastu võetud liikmesriikide õiguses pole sätestatud teisiti. Ühtlustatud liidu õiguse puudumise korral võivad liikmesriigid võtta vastu riiklikke tehnilisi norme vastavalt Euroopa Parlamendi ja nõukogu direktiivile (EL) 2015/1535 ([20]), nähes ette kohustusliku sertifitseerimise Euroopa küberturvalisuse sertifitseerimise kava alusel. Liikmesriigid saavad Euroopa küberturvalisuse sertifitseerimist kasutada ka riigihangete ning Euroopa Parlamendi ja nõukogu direktiivi 2014/24/EL ([21]) kontekstis.

(92) Mõnes valdkonnas võib tulevikus olla vajalik kehtestada küberturvalisuse erinõuded ning muuta sertifitseerimine teatavate IKT-toodete, -teenuste või -protsesside puhul kohustuslikuks, et parandada küberturvalisuse taset liidus. Komisjon peaks korrapäraselt jälgima vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavade mõju turvaliste IKT-toodete, -teenuste ja -protsesside kättesaadavusele siseturul ning korrapäraselt hindama sertifitseerimise kavade kasutamist IKT-toodete, -teenuste ja -protsesside tootjate ja pakkujate poolt liidus. Euroopa küberturvalisuse sertifitseerimise kavade tõhusust ja seda, kas konkreetne kava tuleks muuta kohustuslikuks, tuleks hinnata küberturvalisusega seotud liidu õigusakte, eelkõige direktiivi (EL) 2016/1148 silmas pidades ning võttes arvesse oluliste teenuste operaatorite poolt kasutatavate võrgu- ja infosüsteemide turvalisust.

(93) Euroopa küberturvalisuse sertifikaadid ja ELi vastavusdeklaratsioonid peaksid aitama lõppkasutajatel teha teadlikke valikuid. Seega peaks sertifitseeritud või ELi vastavusdeklaratsiooni saanud IKT-toodete, -teenuste ja -protsessidega kaasnema struktureeritud teave, mis on kohandatud kavandatud lõppkasutaja eeldatavale tehnilisele tasemele. Kogu teave peaks olema kättesaadav veebis ning asjakohasel juhul füüsilisel kujul. Lõppkasutajale peaksid olema kättesaadavad viited sertifitseerimiskava numbrile, usaldusväärsuse tasemele, IKT-toote, -teenuse ja -protsessiga seotud küberturvalisuse riskide kirjeldusele, väljaandvale asutusele, või tal peaks olema võimalik saada Euroopa küberturvalisuse sertifikaadi koopia. Lisaks tuleks lõppkasutajat teavitada IKT-toodete, -teenuste ja -protsesside tootja või pakkuja küberturvalisuse toetuspoliitikast, nimelt sellest, kui kaua võib lõppkasutaja eeldada, et ta saab küberturvalisuse uuendusi või parandusi. Kui see on kohaldatav, tuleks anda suuniseid meetmete või seadistuste kohta, mida lõppkasutaja saab kasutada IKT-toote või -teenuse küberturvalisuse säilitamiseks või parandamiseks, ning esitada ühtse kontaktpunkti kontaktandmed küberrünnakutest teatamiseks ja nende puhul toe saamiseks (lisaks automaatsele teatamisele). Seda teavet tuleks korrapäraselt ajakohastada ja see peaks olema kättesaadav Euroopa küberturvalisuse sertifitseerimise kavade kohta teavet pakkuval veebisaidil.

(94) Käesoleva määruse eesmärkide saavutamiseks ja siseturu killustumise vältimiseks tuleks lõpetada riiklike küberturvalisuse sertifitseerimise kavade või menetluste kohaldamine Euroopa küberturvalisuse sertifitseerimise kavaga hõlmatud IKT-toodete, -teenuste ja -protsesside suhtes alates kuupäevast, mille komisjon kehtestab rakendusaktidega. Lisaks ei peaks liikmesriigid kehtestama uusi riiklikke küberturvalisuse sertifitseerimise kavasid IKT-toodetele, -teenustele või -protsessidele, mis on juba kaetud kehtiva Euroopa küberturvalisuse sertifitseerimise kavaga. Liikmesriike ei tohiks aga takistada võtmast vastu või säilitamast riiklikke küberturvalisuse sertifitseerimise kavasid riikliku julgeolekuga seotud eesmärkidel. Liikmesriigid peaksid teatama komisjonile ja Euroopa küberturvalisuse sertifitseerimise rühmale kavatsusest koostada uusi riiklikke küberturvalisuse sertifitseerimise kavasid. Komisjon ja Euroopa küberturvalisuse sertifitseerimise rühm peaksid hindama uute riiklike küberturvalisuse sertifitseerimise kavade mõju siseturu nõuetekohasele toimimisele ning võtma sealjuures arvesse strateegilist huvi taotleda selle asemel Euroopa küberturvalisuse sertifitseerimise kava koostamist.

(95) Euroopa küberturvalisuse sertifitseerimise kavade eesmärk on ühtlustada küberturvalisuse tavasid liidus. Nad peavad aitama kaasa küberturvalisuse taseme tõstmisele liidus. Euroopa küberturvalisuse sertifitseerimise kavade koostamisel tuleks arvesse võtta ja võimaldada innovaatilist arengut küberturvalisuse valdkonnas.

([20]) Euroopa Parlamendi ja nõukogu 9. septembri 2015. aasta direktiiv (EL) 2015/1535, millega nähakse ette tehnilistest eeskirjadest ning infoühiskonna teenuste eeskirjadest teatamise kord (ELT L 241, 17.9.2015, lk 1).

([21]) Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/24/EL riigihangete kohta ja direktiivi 2004/18/EÜ kehtetuks tunnistamise kohta (ELT L 94, 28.3.2014, lk 65).

(96) Euroopa küberturvalisuse sertifitseerimise kavad peaksid võtma arvesse praeguseid tarkvara ja riistvara arendusmeetodeid ning eelkõige sagedaste tarkvara või riistvara uuenduste mõju individuaalsetele Euroopa küberturvalisuse sertifikaatidele. Euroopa küberturvalisuse sertifitseerimise kavades tuleks täpsustada tingimused, mille alusel uuendus võib nõuda IKT-toote, -teenuse või -protsessi uuesti sertifitseerimist või seda, et konkreetse Euroopa küberturvalisuse sertifikaadi kohaldamisala vähendatakse, võttes arvesse uuenduse võimalikku kahjulikku mõju vastavusele kõnealuse sertifikaadi turvalisusnõuetega.

(97) Kui Euroopa küberturvalisuse sertifitseerimise kava on vastu võetud, peaksid IKT-toodete, -teenuste või -protsesside tootjad või pakkujad saama esitada kõikjal liidus enda valitud vastavushindamisasutusele taotluse oma IKT-toodete või -teenuste sertifitseerimiseks. Kui vastavushindamisasutused vastavad käesolevas määruses sätestatud teatavatele konkreetsetele nõuetele, peaks riiklik akrediteerimisasutus need akrediteerima. Akrediteerida saab maksimaalselt viieks aastaks ja akrediteerimise kehtivust võib pikendada samadel tingimustel seni, kuni vastavushindamisasutus vastab jätkuvalt nõuetele. Riiklik akrediteerimisasutus peaks vastavushindamisasutuse akrediteerimist piirama, selle peatama või kehtetuks tunnistama, kui akrediteerimise andmise tingimused ei olnud täidetud või ei ole enam täidetud või kui vastavushindamisasutus rikub käesolevat määrust.

(98) Liikmesriikide õigusaktides sisalduvad viited riiklikele standarditele, mida Euroopa küberturvalisuse sertifitseerimise kava jõustumise tõttu enam ei kohaldata, võivad segadust põhjustada. Seetõttu peaksid liikmesriigid kajastama Euroopa küberturvalisuse sertifitseerimise kava vastuvõtmist oma siseriiklikes õigusaktides.

(99) Et saavutada kogu liidus võrdväärsed standardid, hõlbustada vastastikust tunnustamist ning edendada Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide üldist aktsepteerimist, tuleb kehtestada riiklike küberturvalisuse sertifitseerimise asutuste vaheline vastastikuse hindamise süsteem. Vastastikune hindamine peaks hõlmama menetlusi IKT-toodete, -teenuste ja -protsesside Euroopa küberturvalisuse sertifikaatide nõuetele vastavuse kontrollimiseks, vastavuse enesehindamist läbiviivate IKT-toodete, -teenuste või -protsesside tootjate ja pakkujate kohustuste kontrollimiseks, vastavushindamisasutuste järelevalveks ning selle kontrollimiseks, kas kõrge usaldusväärsuse taseme kohta sertifikaate väljaandvate asutuste töötajatel on sobivad eriteadmised. Komisjon peaks saama kehtestada rakendusaktiga vähemalt viie aastase kestusega vastastikuse hindamise kava ning sätestama vastastikuse hindamise süsteemi toimimise kriteeriumid ja metoodikad.

(100) Ilma et see piiraks üldist vastastikuse hindamise süsteemi, mis kehtestatakse Euroopa küberturvalisuse sertifitseerimise raamistiku raames kõigis riiklikes küberturvalisuse sertifitseerimise asutustes, võivad teatavad Euroopa küberturvalisuse sertifitseerimise kavad hõlmata vastastikuse hindamise mehhanismi asutustele, kes annavad IKT-toodetele, -teenustele või -protsessidele selliste kavade raames välja kõrge usaldusväärsuse tasemega Euroopa küberturvalisuse sertifikaate. Euroopa küberturvalisuse sertifitseerimise rühm peaks toetama selliste vastastikuse hindamise mehhanismide rakendamist. Vastastikuse hindamise käigus tuleks eeskätt hinnata, kas asjaomased asutused täidavad oma ülesandeid harmoneeritud viisil, ja see võib hõlmata edasikaebamise mehhanisme. Vastastikuse hindamise tulemused tuleks teha avalikult kättesaadavaks. Asjaomased asutused võivad võtta asjakohaseid meetmeid, et kohandada oma tavasid ja oskusteavet hinnangule vastavalt.

(101) Liikmesriigid peaksid määrama ühe või mitu riiklikku küberturvalisuse sertifitseerimise asutust, kes jälgiksid käesolevast määrusest tulenevate kohustuste täitmist. Riikliku küberturvalisuse sertifitseerimise asutus võib olla juba olemasolev või uus asutus. Samuti peaks liikmesriikidel olema võimalik kokkuleppel teise liikmesriigiga määrata riiklikuks küberturvalisuse sertifitseerimise asutuseks kõnealuses teises liikmesriigis asuv asutus.

(102) Riiklik küberturvalisuse sertifitseerimise asutus peaks ennekõike jälgima tema riigi territooriumil asuvate IKT-toodete, -teenuste või -protsesside tootjate ja pakkujate kohustusi seoses ELi vastavusdeklaratsiooniga ning tagama nimetatud kohustuste täitmise, abistama riiklikke akrediteerimisasutusi vastavushindamisasutuste tegevuse seire ja järelevalve osas, pakkudes neile oskusteavet ja asjakohast teavet, volitama vastavushindamisasutusi täitma nende ülesandeid, kui nad vastavad Euroopa küberturvalisuse sertifitseerimise kavas sätestatud täiendavatele nõuetele, ja jälgima asjakohast arengut küberturvalisuse sertifitseerimise valdkonnas. Riiklikud küberturvalisuse sertifitseerimise asutused peaksid käsitlema füüsiliste või juriidiliste isikute esitatud kaebusi seoses nende või vastavushindamisasutuste poolt väljaantud kõrge usaldusväärsuse tasemega Euroopa küberturvalisuse sertifikaatidega, uurima asjakohasel määral kaebuse sisu ja teavitama kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest. Lisaks peaksid nad tegema koostööd teiste riiklike küberturvalisuse sertifitseerimise asutustè ja muude avaliku

sektori asutustega, sealhulgas jagades teavet IKT-toodete, -teenuste ja -protsesside võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade nõuetele. Komisjon peaks hõlbustama seda teabevahetust, tehes kättesaadavaks üldise elektroonilise teabe tugisüsteemi, nagu turujärelevalve info- ja teavitussüsteem (ICSMS) ja kiire teabevahetuse süsteem toiduks mittekasutatavate toodete kohta (RAPEX), mida turujärelevalveasutused juba kasutavad vastavalt määrusele (EÜ) nr 765/2008.

(103) Et tagada Euroopa küberturvalisuse sertifitseerimise raamistiku järjekindel kohaldamine, tuleks luua Euroopa küberturvalisuse sertifitseerimise rühm, mis koosneb riiklike küberturvalisuse sertifitseerimise asutuste või muude asjakohaste liikmesriikide asutuste esindajatest. Euroopa küberturvalisuse sertifitseerimise rühma peamised ülesanded peaksid olema nõustada ja abistada komisjoni töös, mille eesmärk on tagada Euroopa küberturvalisuse sertifitseerimise raamistiku järjepidev rakendamine ja kohaldamine; aidata ENISAt ja teha temaga tihedat koostööd küberturvalisuse sertifitseerimise ettevalmistavate kavade koostamisel; põhjendatud juhtudel taotleda, et ENISA koostaks ettevalmistava kava; ja võtta vastu ENISA-le suunatud arvamusi ettevalmistavate kavade kohta ning komisjonile suunatud arvamusi olemasolevate Euroopa küberturvalisuse sertifitseerimise kavade haldamise ja läbivaatamise kohta. Euroopa küberturvalisuse sertifitseerimise rühm peaks soodustama heade tavade ja oskusteabe vahetamist riiklike küberturvalisuse sertifitseerimise asutuste vahel, kes vastutavad vastavushindamisasutustele lubade andmise ja Euroopa küberturvalisuse sertifikaatide väljaandmise eest.

(104) Et parandada teadlikkust ja hõlbustada tulevaste Euroopa küberturvalisuse sertifitseerimise kavade omaksvõttu, võib komisjon välja anda üldiseid või sektoripõhiseid küberturvalisuse suuniseid, näiteks küberturvalisuse heade tavade või vastutustundliku küberruumis käitumise kohta, tuues välja sertifitseeritud IKT-toodete, -teenuste ja -protsesside kasutamise positiivse mõju.

(105) Et veelgi enam hõlbustada kaubavahetust ja tunnistades, et IKT tarneahelad on ülemaailmsed, võib liit sõlmida kooskõlas Euroopa Liidu toimimise lepingu („ELi toimimise leping“) artikliga 218 Euroopa küberturvalisuse sertifikaatide vastastikuse tunnustamise lepinguid. Võttes arvesse ENISA-lt ja Euroopa küberturvalisuse sertifitseerimise rühmalt saadud nõu, võib komisjon soovitada alustada vastavaid läbirääkimisi. Igas Euroopa küberturvalisuse sertifitseerimise kavas tuleks näha ette kolmandate riikidega toimuva vastastikuse tunnustamise lepingute konkreetsed tingimused.

(106) Et tagada käesoleva määruse ühetaolised rakendamistingimused, tuleks komisjonile anda rakendusvolitused. Neid volitusi tuleks teostada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 182/2011 ([22]).

(107) Kontrollimenetlust tuleks kasutada nende rakendusaktide vastuvõtmiseks, milles käsitletakse IKT-toodete, -teenuste ja -protsesside suhtes kohaldatavaid Euroopa küberturvalisuse sertifitseerimise kavasid; ENISA toimetatavate uurimiste üksikasju; riiklike küberturvalisuse sertifitseerimise asutuste vastastikuse hindamise kava ning asjaolusid, vorminguid ja korda, mille kohaselt riiklikud küberturvalisuse sertifitseerimise asutused teavitavad komisjoni akrediteeritud vastavushindamisasutustest.

(108) ENISA tööd tuleks hinnata korrapäraselt ja sõltumatult. Hindamisel tuleks pidada silmas ENISA eesmärke, selle töövõtteid ning ülesannete asjakohasust, eelkõige seoses liidu tasandil operatiivkoostööga seotud ülesannetega. Hindamise käigus tuleks analüüsida ka Euroopa küberturvalisuse sertifitseerimise raamistiku mõju, tulemuslikkust ja tõhusust. Läbivaatamise korral peaks komisjon hindama, kuidas saab tugevdada ENISA rolli nõuandva ja oskusteavet pakkuva kontaktüksusena, ning samuti hindama ENISA võimalikku rolli seoses selliste kolmandatest riikidest pärit IKT-toodete, -teenuste ja -protsesside hindamise toetamisega, kui sellised tooted, teenused ja protsessid ei täida liitu sisenemisel liidu norme.

([22]) Euroopa Parlamendi ja nõukogu 16. veebruari 2011. aasta määrus (EL) nr 182/2011, millega kehtestatakse eeskirjad ja üldpõhimõtted, mis käsitlevad liikmesriikide läbiviidava kontrolli mehhanisme, mida kohaldatakse komisjoni rakendamisvolituste teostamise suhtes (ELT L 55, 28.2.2011, lk 13).

(109) Kuna käesoleva määruse eesmärke ei suuda liikmesriigid piisavalt saavutada, küll aga saab neid selle ulatuse ja toime tõttu paremini saavutada liidu tasandil, võib liit võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev määrus nimetatud eesmärkide saavutamiseks vajalikust kaugemale.

(110) Määrus (EL) nr 526/2013 tuleks kehtetuks tunnistada,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I JAOTIS

ÜLDSÄTTED

Artikkel 1

Reguleerimisese ja kohaldamisala

1. Et tagada siseturu nõuetekohane toimimine ja püüelda samas küberturvalisuse, kübervastupidavusvõime ja usalduse kõrge taseme poole liidus, sätestatakse käesolevas määruses:

a) ENISA (Euroopa Liidu Küberturvalisuse Amet) eesmärgid, ülesanded ja organisatsioonilised aspektid, ning

b) Euroopa küberturvalisuse sertifitseerimise kavade kehtestamise raamistik, et kindlustada liidus IKT-toodete, -teenuste ja -protsesside küberturvalisuse piisav tase ning vältida siseturu killustatust seoses küberturvalisuse sertifitseerimise kavadega liidus.

Esimese lõigu punktis b osutatud raamistiku kohaldamine ei piira muude liidu õigusaktide erinormide kohaldamist, mis puudutavad vabatahtlikku või kohustuslikku sertifitseerimist.

2. Käesolev määrus ei piira liikmesriikide pädevust seoses tegevusega, mis on seotud avaliku julgeoleku, riigikaitse, riikliku julgeoleku ja riigi tegevusega kriminaalõiguse valdkonnas.

Artikkel 2

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) „küberturvalisus“– tegevused, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid küberohtude eest;

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

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

4) „oluliste teenuste operaator“– direktiivi (EL) 2016/1148 artikli 4 punktis 4 määratletud oluliste teenuste operaator;

5) „digitaalse teenuse osutaja“– direktiivi (EL) 2016/1148 artikli 4 punktis 6 määratletud digitaalse teenuse osutaja;

6) „intsident“– direktiivi (EL) 2016/1148 artikli 4 punktis 7 määratletud intsident;

7) „intsidendi käsitlemine“– direktiivi (EL) 2016/1148 artikli 4 punktis 8 määratletud intsidendi käsitlemine;

8) „küberoht“– võimalik asjaolu, sündmus või tegevus, mis võib kahjustada või häirida võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid või neile muul viisil halba mõju avaldada;

9) „Euroopa küberturvalisuse sertifitseerimise kava“– liidu tasandil kindlaks määratud normide, tehniliste nõuete, standardite ja menetluste põhjalik kogum, mida kasutatakse konkreetsete IKT-toodete, -teenuste ja -protsesside sertifitseerimiseks või nende vastavuse hindamiseks;

10) „riiklik küberturvalisuse sertifitseerimise kava“– riigi ametiasutuse välja töötatud ja kehtestatud normide, tehniliste nõuete, standardite ja menetluste põhjalik kogum, mida kasutatakse konkreetse kava kohaldamisalasse kuuluvate IKT-toodete, -teenuste ja -protsesside sertifitseerimiseks või nende vastavuse hindamiseks;

11) „Euroopa küberturvalisuse sertifikaat“– asjakohase asutuse välja antud dokument, mis tõendab, et hinnatud on asjaomase IKT-toote, -teenuse või -protsessi vastavust Euroopa küberturvalisuse sertifitseerimise kavas sätestatud konkreetsetele turvanõuetele;

12) „IKT-toode“– võrgu- või infosüsteemi element või elementide rühm;

13) „IKT-teenus“– teenus, mis koosneb täielikult või peamiselt võrgu- ja infosüsteemide kaudu teabe edastamisest, säilitamisest, väljavõtmisest või töötlemisest;

14) „IKT-protsess“– tegevused, mille käigus projekteeritakse või töötatakse välja IKT-toode või -teenus, seda tarnitakse või hallatakse;

15) „akrediteerimine“– määruse (EÜ) nr 765/2008 artikli 2 punktis 10 määratletud akrediteerimine;

16) „riiklik akrediteerimisasutus“– määruse (EÜ) nr 765/2008 artikli 2 punktis 11 määratletud riiklik akrediteerimisasutus;

17) „vastavushindamine“– määruse (EÜ) nr 765/2008 artikli 2 punktis 12 määratletud vastavushindamine;

18) „vastavushindamisasutus“– määruse (EÜ) nr 765/2008 artikli 2 punktis 13 määratletud vastavushindamisasutus;

19) „standard“– määruse (EL) nr 1025/2012 artikli 2 punktis 1 määratletud standard;

20) „tehniline kirjeldus“– dokument, milles nähakse ette IKT-tootele, -teenusele või -protsessile või nendega seotud vastavushindamismenetlustele esitatavad tehnilised nõuded;

21) „usaldusväärsuse tase“– alus kindlustundele, et IKT-toode, -teenus või -protsess vastab konkreetse Euroopa küberturvalisuse sertifitseerimise kava turvanõuetele ning mis näitab, millisel tasemel on seda hinnatud; usaldusväärsuse tase ei mõõda IKT-toote, -teenuse või -protsessi enda turvalisust;

22) „vastavuse enesehindamine“– IKT-toodete, -teenuste või -protsesside tootja või pakkuja läbi viidavad tegevused, millega hinnatakse nende IKT-toodete, -teenuste või -protsesside vastavust Euroopa küberturvalisuse sertifitseerimise kavas sätestatud nõuetele.

II JAOTIS

ENISA (EUROOPA LIIDU KÜBERTURVALISUSE AMET)

I PEATÜKK

Volitused ja eesmärgid

Artikkel 3

Volitused

1. ENISA täidab talle käesoleva määrusega pandud ülesandeid, et saavutada küberturvalisuse kõrge ühine tase kogu liidus, muu hulgas toetades aktiivselt liikmesriike ja liidu institutsioone, organeid ja asutusi küberturvalisuse parandamisel. ENISA tegutseb küberturvalisuse vallas liidu institutsioonidele, organitele ja asutustele ning teistele asjaomastele liidu sidusrühmadele nõu andva ja oskusteavet pakkuva kontaktüksusena.

ENISA aitab käesoleva määrusega talle pandud ülesannete täitmisega kaasa siseturu killustatuse vähendamisele.

2. ENISA täidab ülesandeid, mis pannakse talle liidu õigusaktidega, milles sätestatakse meetmed liikmesriikide küberturvalisusega seotud õigus- ja haldusnormide lähendamiseks.

3. Oma ülesannete täitmisel tegutseb ENISA sõltumatult, vältides seejuures liikmesriikide tegevuse dubleerimist ja võttes arvesse olemasolevat liikmesriikide oskusteavet.

4. ENISA arendab talle kuuluvaid, käesoleva määrusega talle pandud ülesannete täitmiseks vajalikke vahendeid, sealhulgas tehnilist ja inimvõimekust ning oskusi.

Artikkel 4

Eesmärgid

1. ENISA on küberturvalisuse alaste teadmiste keskus tänu oma sõltumatusele, antava nõu ja abi ning levitatava teabe teaduslikule ja tehnilisele kvaliteedile, töökorra läbipaistvusele, töömeetoditele ja oma ülesannete hoolikale täitmisele.

2. ENISA aitab liidu institutsioonidel, organitel ja asutustel ning liikmesriikidel töötada välja ja rakendada liidu küberturvalisuse alaseid poliitikameetmeid, sealhulgas küberturvalisuse valdkondlikke poliitikameetmeid.

3. ENISA toetab suutlikkuse ja valmisoleku arendamist kogu liidus sellega, et aitab liidu institutsioonidel, organitel ja asutustel ja liikmesriikidel ning avaliku ja erasektori sidusrühmadel suurendada nende võrgu- ja infosüsteemide kaitset, arendada ja parandada kübervastupanuvõimet ja reageerimissuutlikkust ning arendada küberturvalisuse valdkonna oskusi ja pädevusi.

4. ENISA edendab liidu tasandil küberturvalisusega seotud küsimuste alast koostööd, sealhulgas teabe jagamist, ja koordineerimist liikmesriikide, liidu institutsioonide, organite ja asutuste ning asjaomaste era- ja avaliku sektori sidusrühmade seas.

5. ENISA aitab kaasa küberturvalisuse alase suutlikkuse suurendamisele liidu tasandil, et toetada liikmesriikide tegevust küberohtude ennetamisel ja neile reageerimisel, seda eeskätt piiriüleste intsidentide puhul.

6. ENISA propageerib Euroopa küberturvalisuse sertifitseerimise kasutamist, et vältida siseturu killustatust. ENISA aitab kaasa Euroopa küberturvalisuse sertifitseerimise raamistiku loomisele ja haldamisele vastavalt käesoleva määruse III jaotisele, et suurendada IKT-toodete, -teenuste ja -protsesside küberturvalisuse läbipaistvust ning tugevdada seeläbi usaldust digitaalse siseturu vastu ja selle konkurentsivõimet.

7. ENISA edendab kodanike, organisatsioonide ja ettevõtjate heal tasemel küberturvalisuse alast teadlikkust, sealhulgas küberhügieeni ja küberkirjaoskust.

II PEATÜKK

Ülesanded

Artikkel 5

Liidu poliitikameetmete ja õiguse arendamine ja rakendamine

ENISA aitab liidu poliitikameetmete ja õiguse arendamisele ja rakendamisele kaasa järgmiselt:

1) abistab ja annab nõu, eeskätt esitades oma sõltumatu arvamuse ja analüüsi, ning teeb ettevalmistavat tööd liidu poliitikameetmete ja õiguse arendamise ja läbivaatamise jaoks küberturvalisuse valdkonnas, samuti valdkonnaspetsiifiliste poliitiliste ja õiguslike algatuste jaoks, kui need puudutavad küberturvalisusega seotud küsimusi;

2) aitab liikmesriikidel järjekindlalt rakendada küberturvalisusega seotud liidu poliitikameetmeid ja õigust eeskätt seoses direktiiviga (EL) 2016/1148, kasutades selleks muu hulgas arvamusi, suuniseid, nõuandeid ja parimaid tavasid sellistes küsimustes nagu riskihaldus, intsidentidest teatamine ja teabe jagamine, ning soodustades pädevate asutuste vahel asjakohaste parimate tavade jagamist;

3) aitab liikmesriikidel ning liidu institutsioonidel, organitel ja asutustel välja töötada ja edendada küberturvalisuse alaseid poliitikameetmeid, mis on seotud interneti avaliku tuuma üldise kättesaadavuse ja terviklikkuse säilitamisega;

4) annab oma panuse direktiivi (EL) 2016/1148 artikli 11 alusel moodustatud koostöörühma töösse, pakkudes selleks oma oskusteavet ja abi;

5) toetab:

   a) liidu poliitikameetmete arendamist ja rakendamist e-identimise ja usaldusteenuste valdkonnas, eeskätt andes nõu ja tehnilisi suuniseid ning soodustades pädevate asutuste vahel parimate tavade vahetamist;

   b) elektroonilise side suurema turvalisuse edendamist, muu hulgas andes nõu ja oskusteavet ning soodustades pädevate asutuste vahel parimate tavade jagamist;

   c) liikmesriike andmekaitse ja eraelu puutumatusega seotud liidu poliitikameetmete ja õiguse spetsiifiliste küberturvalisuse aspektide rakendamisel, sealhulgas andes taotluse korral nõu Euroopa Andmekaitsenõukogule;

6) toetab liidu poliitikameetmetega seotud tegevuse regulaarset läbivaatamist ning koostab selleks igal aastal aruande vastava õigusraamistiku rakendamise seisu kohta seoses järgmisega:

   a) teave liikmesriikide intsidente käsitlevate teadete kohta, mille ühtsed kontaktpunktid on esitanud koostöörühmale vastavalt direktiivi (EL) 2016/1148 artikli 10 lõikele 3;

   b) kokkuvõtted usaldusteenuse osutajatelt saadud turvarikkumise või tervikluse kao teadetest, mille järelevalveasutused esitavad ENISA-le vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 ([23]) artikli 19 lõikele 3;

   c) üldkasutatavate elektroonilise side võrkude või üldkasutatavate elektroonilise side teenuste pakkujate edastatud teated turvaintsidentide kohta, mille pädevad asutused esitavad ENISA-le vastavalt direktiivi (EL) 2018/1972 artiklile 40.

([23]) Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (ELT L 257, 28.8.2014, lk 73).

Artikkel 6

Suutlikkuse arendamine

1. ENISA abistab:

a) liikmesriike nende tegevuses, et parandada küberohtude ja intsidentide ennetamist, avastamist, analüüsimist ja neile reageerimise suutlikkust, pakkudes liikmesriikidele teadmisi ja oskusteavet;

b) liikmesriike ning liidu institutsioone, organeid ja asutusi turvanõrkuste avalikustamise poliitikameetmete vabatahtlikkuse alusel loomisel ja rakendamisel;

c) liidu institutsioone, organeid ja asutusi nende tegevuses, et parandada küberohtude ja intsidentide ennetamist, avastamist, analüüsimist ja neile reageerimise suutlikkust, eeskätt pakkudes asjakohast toetust CERT-EUle;

d) liikmesriike riiklike CSIRTide väljatöötamisel, kui nad seda taotlevad vastavalt direktiivi (EL) 2016/1148 artikli 9 lõikele 5;

e) liikmesriike riiklike võrgu- ja infosüsteemide turvalisuse strateegiate väljatöötamisel, kui nad seda taotlevad vastavalt direktiivi (EL) 2016/1148 artikli 7 lõikele 2, ning edendab nimetatud strateegiate levitamist ja sedastab nende rakendamisel tehtavad edusammud kogu liidus, et propageerida parimaid tavasid;

f) liidu institutsioone liidu küberturvalisuse alaste strateegiate väljatöötamisel ja läbivaatamisel, nende levitamisel ja nende rakendamisel tehtavate edusammude jälgimisel;

g) riiklikke ja liidu CSIRTe nende suutlikkuse arendamisel, muu hulgas edendades dialoogi ja teabevahetust tagamaks vastavalt tehnika tasemele, et iga CSIRTi võimekus vastab ühistele miinimumsuutlikkuse nõuetele ning et iga CSIRT toimib kooskõlas parimate tavadega;

h) liikmesriike, korraldades korrapäraselt ja vähemalt iga kahe aasta järel liidu tasandil artikli 7 lõikes 5 osutatud küberturvalisuse õppuseid ja andes õppuste hindamise ja õppuste käigus omandatud kogemuste põhjal soovitusi poliitika kujundamiseks;

i) asjaomaseid avalik-õiguslikke asutusi, pakkudes neile asjakohasel juhul koostöös sidusrühmadega küberturvalisuse alast koolitust;

j) koostöörühma parimate tavade vahetamisel eeskätt seoses oluliste teenuste operaatorite identifitseerimisega liikmesriikide poolt, sealhulgas mis puudutab riskide ja intsidentidega seotud piiriüleseid sõltuvusseoseid vastavalt direktiivi (EL) 2016/1148 artikli 11 lõike 3 punktile l.

2. ENISA toetab teabe jagamist sektorite siseselt ja sektorite vahel, eeskätt direktiivi (EL) 2016/1148 II lisas loetletud valdkondades, levitades häid tavasid ja andes suuniseid kättesaadavate töövahendite ja menetluste kohta ning selle kohta, kuidas lahendada teabe jagamisega seotud regulatiivsed küsimused.

Artikkel 7

Operatiivkoostöö liidu tasandil

1. ENISA toetab operatiivkoostööd liikmesriikide, liidu institutsioonide, organite ja asutuste ning sidusrühmade vahel.

2. ENISA teeb operatiivtasandil koostööd ja loob koostoimet liidu institutsioonide, organite ja asutustega (sealhulgas CERT-EUga), nende talitustega, kelle tegevus puudutab küberkuritegevust, ning järelevalveasutustega, kes tegelevad eraelu puutumatuse ja isikuandmete kaitsega, et lahendada ühist muret tekitavaid küsimusi, sealhulgas järgmisel moel:

a) oskusteabe ja parimate tavade vahetamine;

b) nõu ja suuniste andmine küberturvalisusega seotud asjaomastes küsimustes;

c) konkreetsete ülesannete täitmise praktilise korra kehtestamine pärast komisjoniga konsulteerimist.

3. ENISA tagab CSIRTide võrgustiku sekretariaaditeenused vastavalt direktiivi (EL) 2016/1148 artikli 12 lõikele 2 ning toetab seda ülesannet täites aktiivselt teabe jagamist ja koostööd võrgustiku liikmete vahel.

4. ENISA toetab liikmesriike CSIRTide võrgustikus toimuvas operatiivkoostöös järgmiselt:

a) annab nõu, kuidas parandada intsidentide ennetamise, avastamise ja neile reageerimise suutlikkust ning annab ühe või mitme liikmesriigi taotluse korral nõu seoses konkreetse küberohuga;

b) annab ühe või mitme liikmesriigi taotluse korral abi märkimisväärse või olulise mõjuga intsidentide hindamisel, pakkudes oskusteavet ja soodustades selliste intsidentide tehnilist käsitlemist, muu hulgas toetades eeskätt asjaomase teabe ja tehniliste lahenduste vabatahtlikku jagamist liikmesriikide vahel;

c) analüüsib turvanõrkuseid ja intsidente, võttes aluseks üldsusele kättesaadava teabe või liikmesriikide poolt vabatahtlikult sel eesmärgil esitatava teabe, ning

d) toetab ühe või mitme liikmesriigi taotluse korral selliste intsidentide tehnilist järeluurimist, millel on märkimisväärne või oluline mõju direktiivi (EL) 2016/1148 tähenduses.

Et saada kasu koostoimest ning vältida tegevuse dubleerimist, teevad ENISA ja CERT-EU neid ülesandeid täites struktureeritud koostööd.

5. ENISA korraldab korrapäraselt liidu tasandi küberõppusi ning toetab liikmesriike ja liidu institutsioone, organeid ja asutusi nende taotluse korral küberturvalisuse õppuste korraldamisel. Liidu tasandi küberturvalisuse õppused võivad hõlmata tehnilisi, operatiivseid ja strateegilisi elemente. Iga kahe aasta järel korraldab ENISA põhjaliku suurõppuse.

Lisaks annab ENISA asjakohasel juhul oma panuse valdkondlike küberõppuste korraldamisse ja aitab neid korraldada koos asjaomaste organisatsioonidega, kes võivad osaleda ka liidu tasandi küberturvalisuse õppustel.

6. ENISA koostab tihedas koostöös liikmesriikidega korrapäraselt ELi küberturvalisuse tehnilise olukorra põhjalikke aruandeid intsidentide ja küberohtude kohta, võttes aluseks üldiselt kättesaadava teabe, omaenda tehtud analüüsid ja aruanded, mida jagavad muu hulgas liikmesriikide CSIRTid või direktiivi (EL) 2016/1148 kohased ühtsed kontaktpunktid (mõlemad vabatahtlikkuse alusel), ning EC3 ja CERT-EU.

7. ENISA annab oma panuse, et töötada välja liidu ja liikmesriikide tasandi koostööl põhinev reageering ulatuslikele piiriülestele intsidentidele ja küberturvalisusega seotud kriisidele, tehes selleks peamiselt järgmist:

a) koondab ja analüüsib riiklikest allikatest pärit üldkasutatavaid ja vabatahtlikult jagatud aruandeid, et aidata kaasa ühise olukorrateadlikkuse kujundamisele;

b) tagab teabe tõhusa liikumise ja eskaleerimismehhanismide olemasolu CSIRTide võrgustiku ning liidu tasandi tehniliste ja poliitiliste otsuste tegijate vahel;

c) hõlbustab taotluse korral intsidendi või kriisi tehnilist lahendamist, sealhulgas toetades eeskätt tehniliste lahenduste vabatahtlikku jagamist liikmesriikide vahel;

d) toetab liidu institutsioone, organeid ja asutusi ning taotluse korral liikmesriike intsidenti või kriisi puudutava avaliku teabevahetuse puhul;

e) testib sellistele intsidentidele või kriisidele reageerimiseks mõeldud koostööplaane liidu tasandil ja toetab liikmesriike nende taotluse korral koostööplaanide testimisel riiklikul tasandil.

Artikkel 8

Turg, küberturvalisuse sertifitseerimine ja standardimine

1. ENISA toetab ja edendab käesoleva määruse III jaotises sätestatud IKT-toodete, -teenuste ja -protsesside küberturvalisuse sertifitseerimise alaste liidu poliitikameetmete arendamist ja rakendamist järgmiselt:

a) jälgib pidevalt arengut seonduvates standardimise valdkondades ja soovitab asjakohaseid tehnilisi kirjeldusi artikli 54 lõike 1 punkti c kohaste Euroopa küberturvalisuse sertifitseerimise kavade väljatöötamiseks, kui standardid puuduvad;

b) koostab IKT-toodete, -teenuste ja -protsesside Euroopa küberturvalisuse sertifitseerimise ettevalmistavad kavad („ettevalmistavad kavad“) vastavalt artiklile 49;

c) hindab vastu võetud Euroopa küberturvalisuse sertifitseerimise kavasid kooskõlas artikli 49 lõikega 8;

d) osaleb artikli 59 lõike 4 kohaselt vastastikustes hindamistes;

e) aitab komisjonil pakkuda sekretariaaditeenuseid Euroopa küberturvalisuse sertifitseerimise rühmale vastavalt artikli 62 lõikele 5.

2. ENISA pakub sekretariaaditeenuseid sidusrühmade küberturvalisuse sertifitseerimise rühmale vastavalt artikli 22 lõikele 4.

3. ENISA koostab ja avaldab suuniseid ning töötab välja häid tavasid IKT-toodete, -teenuste ja -protsesside küberturvalisuse nõuete kohta, tehes selleks koostööd riiklike küberturvalisuse sertifitseerimise asutustega ja tööstusega ametliku, struktureeritud ja läbipaistva protsessi raames.

4. ENISA aitab kaasa hindamise ja sertifitseerimise protsessidega seotud suutlikkuse arendamisele, koostades ja andes suuniseid ning toetades liikmesriike nende taotluse korral.

5. ENISA hõlbustab riskihalduse ning IKT-toodete, -teenuste ja -protsesside turvalisuse Euroopa ja rahvusvaheliste standardite koostamist ja kasutuselevõtmist.

6. ENISA koostab koostöös liikmesriikide ja tööstusega nõuandeid ja suuniseid oluliste teenuste operaatoritele ja digitaalsete teenuste osutajatele esitatavate turvalisusnõuetega seotud tehniliste valdkondade, aga ka juba olemasolevate standardite, kaasa arvatud liikmesriikide riiklike standardite kohta vastavalt direktiivi (EL) 2016/1148 artikli 19 lõikele 2.

7. ENISA analüüsib korrapäraselt nii nõudluse kui ka pakkumise poole peamisi suundumusi küberturvalisuse turul ja levitab analüüsi tulemusi, et arendada küberturvalisuse turgu liidus.

Artikkel 9

Teadmised ja teave

ENISA:

a) analüüsib kujunemisjärgus tehnoloogiaid ja annab teemapõhiseid hinnanguid sellele, milline on tehnoloogiliste uuenduste eeldatav sotsiaalne, õiguslik, majanduslik ja regulatiivne mõju küberturvalisusele;

b) koostab pikaajalisi strateegilisi analüüse küberohtude ja intsidentide kohta, et teha kindlaks väljakujunevad suundumused ja aidata ennetada intsidente;

c) koostöös liikmesriikide ametiasutuste ja asjaomaste sidusrühmade ekspertidega annab nõu ja suuniseid ning levitab parimaid tavasid võrgu- ja infosüsteemide turvalisuse kohta, eeskätt selles osas, mis puudutab nende infrastruktuuride turvalisust, mis toetavad direktiivi (EL) 2016/1148 II lisas loetletud sektoreid ja mida kasutavad kõnealuse direktiivi III lisas loetletud digitaalsete teenuste osutajad;

d) koondab, korraldab ja teeb avalikkusele spetsiaalse portaali kaudu kättesaadavaks liidu institutsioonide, organite ja asutuste ning vabatahtlikkuse alusel liikmesriikide ning era- ja avaliku sektori sidusrühmade poolt esitatud teavet küberturvalisuse kohta;

e) kogub ja analüüsib avalikult kättesaadavat teavet oluliste intsidentide kohta ning koostab aruandeid, et anda suuniseid kodanikele, organisatsioonidele ja ettevõtjatele kogu liidus.

Artikkel 10

Teadlikkuse suurendamine ja haridus

ENISA:

a) parandab üldsuse teadlikkust küberturvalisuse riskidest ja annab kodanikele, organisatsioonidele ja ettevõtjatele suuniseid individuaalsete kasutajate heade tavade, sealhulgas küberhügieeni ja küberkirjaoskuse kohta;

b) korraldab koostöös liikmesriikide, liidu institutsioonide, organite, asutuste ja tööstusega korrapäraselt teavituskampaaniaid, et suurendada küberturvalisust ja selle nähtavust liidus, ja soodustab ulatuslikku avalikku arutelu;

c) abistab liikmesriike nende jõupingutustes, et suurendada küberturvalisuse alast teadlikkust ja edendada küberturvalisuse alast haridust;

d) toetab liikmesriikidevahelist tihedamat koordineerimist ja parimate tavade vahetamist küberturvalisuse alase teadlikkuse ja hariduse valdkonnas.

Artikkel 11

Teadusuuringud ja innovatsioon

Teadusuuringute ja innovatsiooni vallas ENISA:

a) annab liidu institutsioonidele, organitele ja asutustele ning liikmesriikidele nõu küberturvalisuse valdkonnas vajalike teadusuuringute ja prioriteetide kohta, et võimaldada tulemuslikku reageerimist praegustele ja tulevastele riskidele ja küberohtudele, sealhulgas seoses uue ja kujunemisjärgus info- ja kommunikatsioonitehnoloogiaga, ning riskiennetustehnoloogia tõhusat kasutamist;

b) osaleb teadusuuringute ja innovatsiooni rahastamise programmide rakendamisetapis, kui komisjon on talle delegeerinud asjakohased volitused, või tegutseb toetusesaajana;

c) annab küberturvalisuse valdkonnas panuse strateegilisse teadusuuringute ja innovatsiooni liidu tasandi tegevuskavasse.

Artikkel 12

Rahvusvaheline koostöö

ENISA annab panuse liidu jõupingutustesse teha koostööd kolmandate riikide ja rahvusvaheliste organisatsioonidega ning asjaomastes rahvusvahelistes koostööraamistikes, et edendada rahvusvahelist koostööd küberturvalisusega seotud küsimustes, sealhulgas:

a) osaleb asjakohasel juhul vaatlejana rahvusvaheliste õppuste korraldamises ning analüüsib selliste õppuste tulemusi ja annab nende kohta aru haldusnõukogule;

b) soodustab komisjoni taotluse korral parimate tavade vahetamist;

c) pakub komisjonile taotluse korral oskusteavet;

d) koostöös artikli 62 kohaselt moodustatud Euroopa küberturvalisuse sertifitseerimise rühmaga annab komisjonile nõu ja pakub komisjonile toetust küsimustes, mis puudutavad kolmandate riikidega sõlmitavaid küberturvalisuse sertifikaatide vastastikuse tunnustamise lepinguid.

III PEATÜKK

ENISA töökorraldus

Artikkel 13

ENISA struktuur

ENISA haldus- ja juhtimisstruktuuri kuuluvad:

a) haldusnõukogu;

b) juhatus;

c) tegevdirektor;

d) ENISA nõuanderühm;

e) riiklike kontaktametnike võrgustik.

1. jagu

Haldusnõukogu

Artikkel 14

Haldusnõukogu koosseis

1. Haldusnõukogusse kuulub igast liikmesriigist üks esindaja, kes on määratud liikmesriigi poolt, ning kaks komisjoni esindajat, kes on määratud komisjoni poolt. Kõigil liikmetel on hääleõigus.

2. Igal haldusnõukogu liikmel on asendusliige. Asendusliige esindab liiget tema äraolekul.

3. Haldusnõukogu liikmed ja nende asendusliikmed määratakse ametisse lähtuvalt nende küberturvalisuse alastest teadmistest, võttes arvesse nende asjaomaseid juhtimis-, haldus- ja eelarvealaseid oskusi. Komisjon ja liikmesriigid püüavad piirata oma esindajate vahetumist haldusnõukogus, et tagada selle töö järjepidevus. Komisjoni ja liikmesriikide eesmärk on saavutada haldusnõukogus sooline tasakaal.

4. Haldusnõukogu liikmete ja asendusliikmete ametiaeg on neli aastat. Neid võib ametisse tagasi nimetada.

Artikkel 15

Haldusnõukogu ülesanded

1. Haldusnõukogu:

a) määrab kindlaks ENISA tegevuse üldise suuna ning tagab, et ENISA tegutseb kooskõlas käesolevas määruses sätestatud normide ja põhimõtetega; samuti tagab haldusnõukogu, et ENISA tegevus on kooskõlas liikmesriikide ja liidu tasandi tegevusega;

b) võtab vastu artiklis 24 osutatud ENISA ühtse programmdokumendi kavandi enne, kui see esitatakse arvamuse saamiseks komisjonile;

c) võtab komisjoni arvamust arvestades vastu ENISA ühtse programmdokumendi;

d) teeb järelevalvet ühtses programmdokumendis sisalduva iga-aastase ja mitmeaastase tööprogrammi rakendamise üle;

e) võtab vastu ENISA aastaeelarve ja täidab muid ENISA eelarvega seotud ülesandeid vastavalt IV peatükile;

f) annab hinnangu konsolideeritud aastaaruandele ENISA tegevuse kohta, mis hõlmab raamatupidamisaruannet ja milles kirjeldatakse, kuidas ENISA on täitnud oma tulemuslikkuse näitajaid, ja võtab selle vastu ning saadab nii aastaaruande kui ka sellele antud hinnangu hiljemalt järgmise aasta 1. juuliks Euroopa Parlamendile, nõukogule, komisjonile ja kontrollikojale ning avalikustab selle;

g) võtab vastavalt artiklile 32 vastu ENISA suhtes kohaldatavad finantsreeglid;

h) võtab vastu pettustevastase strateegia, mis on proportsionaalses vastavuses pettuste riskiga, pidades silmas rakendatavate meetmete tasuvusanalüüsi;

i) võtab vastu normid oma liikmete huvide konfliktide vältimiseks ja lahendamiseks;

j) tagab, et Euroopa Pettustevastase Ameti (OLAF) juurdlustest ning erinevatest sise- ja välisauditite aruannetest ja hindamistest tulenevate järelduste ja soovituste põhjal võetakse piisavad järelmeetmed;

k) võtab vastu oma kodukorra, milles muu hulgas käsitletakse esialgsete otsuste tegemist konkreetsete ülesannete delegeerimise kohta vastavalt artikli 19 lõikele 7;

l) kasutab kooskõlas käesoleva artikli lõikega 2 ENISA töötajate suhtes nõukogu määrusega (EMÜ, Euratom, ESTÜ) nr 259/68 ([24]) kehtestatud Euroopa Liidu ametnike personalieeskirjade ja muude teenistujate teenistustingimustega („personalieeskirjad“ ja „muude teenistujate teenistustingimused“) ametisse nimetavale asutusele ja ametiisikule ning teenistuslepingute sõlmimise pädevust omavale asutusele või ametiisikule antud volitusi („ametisse nimetava asutuse volitused“);

m) võtab personalieeskirjade artiklis 110 sätestatud korras vastu personalieeskirjade ja muude teenistujate teenistustingimuste rakendussätted;

n) nimetab kooskõlas artikliga 36 ametisse tegevdirektori ning kohasel juhul pikendab tema ametiaega või tagandab ta ametist;

o) nimetab ametisse peaarvepidaja, kes võib olla komisjoni peaarvepidaja, kes on oma ülesannete täitmisel täiesti sõltumatu;

p) teeb kõik otsused ENISA sisestruktuuri kehtestamise ja vajaduse korral selle muutmise kohta, võttes arvesse ENISA tegevusega seotud vajadusi ja usaldusväärset eelarvehaldust;

q) annab loa kehtestada töökord seoses artikliga 7;

r) annab loa kehtestada koostöökord või sõlmida koostöökokkulepe vastavalt artiklile 42.

2. Haldusnõukogu võtab kooskõlas personalieeskirjade artikliga 110 vastu personalieeskirjade artikli 2 lõikel 1 ja muude teenistujate teenistustingimuste artiklil 6 põhineva otsuse, millega delegeeritakse asjakohased ametisse nimetava asutuse volitused tegevdirektorile ja määratakse kindlaks tingimused, mille alusel võib volituste delegeerimise peatada. Tegevdirektoril on õigus need volitused edasi delegeerida.

([24]) EÜT L 56, 4.3.1968, lk 1.

3. Erandlike asjaolude korral võib haldusnõukogu võtta vastu otsuse, millega ajutiselt peatatakse tegevdirektorile delegeeritud ja tema poolt edasi delegeeritud ametisse nimetava asutuse volitused ning täidetakse kõnealuseid volitusi ise või delegeeritakse need ühele oma liikmetest või mõnele töötajale, välja arvatud tegevdirektorile.

Artikkel 16

Haldusnõukogu esimees

Haldusnõukogu valib oma liikmete seast kahekolmandikulise häälteenamusega esimehe ja aseesimehe, kelle ametiaeg on neli aastat ja kelle võib ühe korra ametisse tagasi nimetada. Kui nende liikmesus haldusnõukogus lõpeb mis tahes ajal nende ametiaja jooksul, lõpeb nende ametiaeg automaatselt samal päeval. Aseesimees asendab esimeest *ex officio* juhul, kui esimehel ei ole võimalik oma ülesandeid täita.

Artikkel 17

Haldusnõukogu koosolekud

1. Haldusnõukogu koosoleku kutsub kokku haldusnõukogu esimees.

2. Haldusnõukogul on aastas vähemalt kaks korralist koosolekut. Haldusnõukogu korraldab erakorralisi koosolekuid oma esimehe, komisjoni või vähemalt ühe kolmandiku liikmete nõudmisel.

3. Tegevdirektor osaleb haldusnõukogu koosolekutel ilma hääleõiguseta.

4. ENISA nõuanderühma liikmed võivad esimehe kutsel osaleda haldusnõukogu koosolekutel ilma hääleõiguseta.

5. Haldusnõukogu liikmed ja nende asendusliikmed võivad vastavalt haldusnõukogu kodukorrale kasutada haldusnõukogu koosolekutel nõustajate või ekspertide abi.

6. Haldusnõukogule osutab sekretariaaditeenust ENISA.

Artikkel 18

Haldusnõukogu hääletuskord

1. Haldusnõukogu võtab otsused vastu oma liikmete häälteenamusega.

2. Ühtse programmdokumendi ja aastaeelarve vastuvõtmiseks ning tegevdirektori ametisse nimetamiseks, tema ametiaja pikendamiseks ja ametist tagandamiseks on vaja haldusnõukogu liikmete kahekolmandikulist häälteenamust.

3. Igal liikmel on üks hääl. Liikme puudumise korral võib hääleõigust kasutada tema asendusliige.

4. Haldusnõukogu esimees osaleb hääletamisel.

5. Tegevdirektor ei osale hääletamisel.

6. Haldusnõukogu kodukorraga kehtestatakse üksikasjalikum hääletamiskord, eelkõige tingimused, mille korral üks liige võib tegutseda teise liikme nimel.

2. jagu

Juhatus

Artikkel 19

Juhatus

1. Haldusnõukogu abistab juhatus.

2. Juhatus:

a) valmistab ette haldusnõukogus vastu võetavad otsused;

b) tagab koos haldusnõukoguga, et OLAFi juurdlustest ning erinevatest sise- ja välisauditite aruannetest ja hindamistest tulenevate järelduste ja soovituste põhjal võetakse piisavad järelmeetmed;

c) abistab ja nõustab tegevdirektorit haldusnõukogu haldus- ja eelarveküsimusi käsitlevate otsuste rakendamisel vastavalt artiklile 20, ilma et see piiraks tegevdirektori ülesandeid, mis on sätestatud artiklis 20.

3. Juhatusse kuuluvad viis liiget. Juhatuse liikmed nimetatakse haldusnõukogu liikmete seast. Üheks liikmeks peab olema haldusnõukogu esimees, kes võib ka juhatust juhtida, ning üks liige peab olema komisjoni esindaja. Juhatuse liikmete ametisse nimetamisel püütakse saavutada tasakaalustatud sooline esindatus juhatuses. Tegevdirektor osaleb juhatuse koosolekutel ilma hääleõiguseta.

4. Juhatuse liikmete ametiaeg on neli aastat. Neid võib ametisse tagasi nimetada.

5. Juhatuse koosolekud toimuvad vähemalt üks kord kolme kuu tagant. Juhatuse esimees kutsub juhatuse liikmete taotlusel kokku täiendavaid koosolekuid.

6. Haldusnõukogu kehtestab juhatuse kodukorra.

7. Kiireloomulistel juhtudel võib juhatus vajaduse korral teha haldusnõukogu nimel teatavaid esialgseid otsuseid, eeskätt halduskü simustes, sealhulgas ametisse nimetava asutuse volituste delegeerimise peatamise ja eelarveküsimuste kohta. Haldusnõukogu teavitatakse sellistest esialgsetest otsustest viivitamata. Haldusnõukogu otsustab seejärel hiljemalt kolme kuu möödumisel pärast esialgse otsuse tegemist, kas see heaks kiita või tagasi lükata. Juhatus ei tee haldusnõukogu nimel otsuseid, mille tegemiseks on vaja haldusnõukogu kahekolmandikulist häälteenamust.

3. jagu

Tegevdirektor

Artikkel 20

Tegevdirektori ülesanded

1. ENISAt juhib tegevdirektor, kes on oma ülesannete täitmisel sõltumatu. Tegevdirektor annab aru haldusnõukogule.

2. Tegevdirektor annab Euroopa Parlamendile viimase taotluse korral aru oma ülesannete täitmise kohta. Nõukogu võib kutsuda tegevdirektori oma ülesannete täitmisest aru andma.

3. Tegevdirektor vastutab järgmiste tegevuste eest:

a) juhib ENISA igapäevast tööd;

b) rakendab haldusnõukogus vastuvõetud otsuseid;

c) koostab ühtse programmdokumendi kavandi ja esitab selle heakskiitmiseks haldusnõukogule enne, kui see esitatakse komisjonile;

d) rakendab ühtset programmdokumenti ja annab haldusnõukogule selle kohta aru;

e) koostab ENISA konsolideeritud aastaaruande, sealhulgas ENISA iga-aastase tööprogrammi rakendamise kohta, ning esitab selle hindamiseks ja vastuvõtmiseks haldusnõukogule;

f) koostab järelhindamise järelduste põhjal võetavaid järelmeetmeid sisaldava tegevuskava ning esitab iga kahe aasta järel komisjonile aruande edusammude kohta;

g) koostab sise- või välisauditi aruannete ja hindamiste ning OLAFi juurdluste järelduste põhjal järelmeetmete võtmiseks tegevuskava ning annab tehtud edusammudest kaks korda aastas aru komisjonile ja korrapäraselt haldusnõukogule;

h) koostab artiklis 32 osutatud ENISA suhtes kohaldatavate finantsreeglite kavandi;

i) koostab ENISA tulude ja kulude eelarvestuse projekti ning täidab ENISA eelarvet;

j) kaitseb liidu finantshuve, kohaldades pettuste, korruptsiooni ja muu ebaseadusliku tegevuse vastu ennetusmeetmeid, tehes tõhusaid kontrolle, nõudes õigusnormide rikkumise tuvastamise korral tagasi alusetult väljamakstud summad ning kohaldades asjakohasel juhul tõhusaid, proportsionaalseid ja hoiatavaid haldus- ja rahalisi karistusi;

k) koostab ENISA pettustevastase strateegia ja esitab selle heakskiitmiseks haldusnõukogule;

l) arendab ja hoiab kontakte äriringkondade ja tarbijaorganisatsioonidega, et tagada korrapärane dialoog asjaomaste sidusrühmadega;

m) vahetab korrapäraselt arvamusi ja teavet liidu institutsioonide, organite ja asutustega seoses nende tegevusega küberturvalisuse vallas, et tagada sidusus liidu poliitika väljatöötamisel ja rakendamisel;

n) täidab muid käesoleva määrusega tegevdirektorile pandud ülesandeid.

4. Vajaduse korral ning kooskõlas ENISA eesmärkide ja ülesannetega võib tegevdirektor moodustada ajutisi töörühmi, kuhu kuuluvad eksperdid, sealhulgas liikmesriikide pädevate asutuste eksperdid. Tegevdirektor teavitab sellest eelnevalt haldusnõukogu. ENISA sise-eeskirjas sätestatakse eeskätt töörühmade koosseisu, tegevdirektori poolt töörühmade ekspertide määramist ja töörühmade tegevust käsitlev kord.

5. Vajaduse korral ja kohasele kulude-tulude analüüsile tuginedes võib tegevdirektor otsustada ENISA ülesannete tõhusaks ja tulemuslikuks täitmiseks asutada ühes või mitmes liikmesriigis ühe kohaliku kontori või mitu kohalikku kontorit. Enne kui tegevdirektor otsustab asutada kohaliku kontori, peab ta küsima asjaomaste liikmesriikide, sealhulgas ENISA asukohaliikmesriigi arvamust ning saama komisjonilt ja haldusnõukogult eelneva nõusoleku. Kui konsulteerimise käigus lähevad tegevdirektori ja asjaomaste liikmesriikide arvamused lahku, esitatakse küsimus arutamiseks nõukogule. Töötajate koguarv kõigis kohalikes kontorites peab olema minimaalne ega tohi moodustada kokku rohkem kui 40 % ENISA asukohaliikmesriigis asuvate ENISA töötajate koguarvust. Ühegi kohaliku kontori puhul ei tohi töötajate arv olla suurem kui 10 % ENISA asukohaliikmesriigis asuvate ENISA töötjate koguarvust.

Kohaliku kontori asutamise otsuses määratakse kindlaks kohaliku kontori tegevuse ulatus, et vältida tarbetuid kulusid ja ENISA haldusülesannete dubleerimist.

4. jagu

ENISA nõuanderühm, sidusrühmade küberturvalisuse sertifitseerimise rühm ja liikmesriikide kontaktametnike võrgustik

Artikkel 21

ENISA nõuanderühm

1. Haldusnõukogu moodustab tegevdirektori ettepaneku põhjal läbipaistval viisil ENISA nõuanderühma, mis koosneb asjaomaseid sidusrühmi, näiteks IKT tööstust, avalikkusele kättesaadavate elektroonilise side võrkude või teenuste pakkujaid, VKEsid, oluliste teenuste operaatoreid, tarbijarühmi ja küberturvalisusega tegelevaid akadeemilisi eksperte esindavatest tunnustatud ekspertidest ning direktiivi (EL) 2018/1972 kohaselt teavitatavate pädevate asutuste, Euroopa standardiorganisatsioonide ning õiguskaitseasutuste ja andmekaitse järelevalveasutuste esindajatest. Haldusnõukogu eesmärk on tagada asjakohane sooline ja geograafiline tasakaal ning tasakaal erinevate sidusrühmade vahel.

2. ENISA sise-eeskirjas sätestatakse eeskätt ENISA nõuanderühma koosseisu, lõikes 1 osutatud tegevdirektori ettepanekut, liikmete arvu ja nimetamist ning ENISA nõuanderühma tegevust käsitlev kord ning see avalikustatakse.

3. ENISA nõuanderühma juhatab tegevdirektor või isik, kelle tegevdirektor nimetab igal üksikjuhul eraldi.

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

5. ENISA nõuanderühm nõustab ENISAt tema ülesannete täitmisel, välja arvatud seoses käesoleva määruse III jaotise kohaldamisega. Eelkõige annab ENISA nõuanderühm tegevdirektorile soovitusi ENISA iga-aastase tööprogrammi ettepaneku koostamiseks ning tagab teabevahetuse asjaomaste sidusrühmadega iga-aastase tööprogrammiga seotud küsimustes.

6. ENISA nõuanderühm teavitab korrapäraselt haldusnõukogu oma tegevusest.

Artikkel 22

Sidusrühmade küberturvalisuse sertifitseerimise rühm

1. Moodustatakse sidusrühmade küberturvalisuse sertifitseerimise rühm.

2. Sidusrühmade küberturvalisuse sertifitseerimise rühm koosneb asjaomaseid sidusrühmi esindavatest tunnustatud ekspertidest. Komisjon valib sidusrühmade küberturvalisuse sertifitseerimise rühma liikmed ENISA ettepaneku põhjal läbipaistva ja avatud valikumenetluse teel, tagades tasakaalu erinevate sidusrühmade vahel ning asjakohase soolise ja geograafilise tasakaalu.

3. Sidusrühmade küberturvalisuse sertifitseerimise rühm:

a) annab komisjonile nõu strateegilistes küsimustes seoses Euroopa küberturvalisuse sertifitseerimise raamistikuga;

b) annab ENISA-le taotluse korral nõu üldistes ja strateegilistes küsimustes seoses turu, küberturvalisuse sertifitseerimise ja standardimisega seonduvate ENISA ülesannetega;

c) abistab komisjoni artiklis 47 osutatud liidu jooksva tööprogrammi koostamisel;

d) esitab artikli 47 lõike 4 kohaselt arvamuse liidu jooksva tööprogrammi kohta ning

e) annab kiireloomulistel juhtudel komisjonile ja Euroopa küberturvalisuse sertifitseerimise rühmale nõu seoses vajadusega täiendavate liidu jooksva tööprogrammiga hõlmamata sertifitseerimise kavade järele, nagu on sätestatud artiklites 47 ja 48.

4. Sidusrühmade küberturvalisuse sertifitseerimise rühma juhivad koos komisjoni ja ENISA esindajad ning sellele osutab sekretariaaditeenuseid ENISA.

Artikkel 23

Liikmesriikide kontaktametnike võrgustik

1. Haldusnõukogu loob tegevdirektori ettepanekul liikmesriikide kontaktametnike võrgustiku, mis koosneb kõigi liikmesriikide esindajatest („liikmesriikide kontaktametnikud"). Iga liikmesriik nimetab liikmesriikide kontaktametnike võrgustikku ühe esindaja. Liikmesriikide kontaktametnike võrgustiku koosolekuid võib pidada erinevates ekspertide koosseisudes.

2. Eelkõige soodustab liikmesriikide kontaktametnike võrgustik ENISA ja liikmesriikide vahelist teabevahetust ning toetab ENISAt tema tegevust ja töö tulemusi käsitleva teabe ning soovituste levitamisel asjaomastele sidusrühmadele kogu liidus.

3. Liikmesriikide kontaktametnikud tegutsevad riigi tasandil kontaktpunktina, et hõlbustada ENISA ja riiklike ekspertide koostööd ENISA iga-aastase tööprogrammi rakendamisel.

4. Kuigi liikmesriikide kontaktametnikud teevad tihedat koostööd oma liikmesriigi haldusnõukogu esindajatega, ei dubleeri liikmesriikide kontaktametnike võrgustik ei haldusnõukogu ega teiste liidu foorumite tööd.

5. Liikmesriikide kontaktametnike võrgustiku ülesanded ja menetlused sätestatakse ENISA sise-eeskirjas ja need avalikustatakse.

5. jagu

Tegevus

Artikkel 24

Ühtne programmdokument

1. ENISA tegutseb kooskõlas ühtse programmdokumendiga, mis sisaldab ENISA iga-aastast ja mitmeaastast tööprogrammi ning mis hõlmab kõiki ENISA kavandatud tegevusi.

2. Tegevdirektor koostab igal aastal ühtse programmdokumendi kavandi, mis sisaldab iga-aastast ja mitmeaastast tööprogrammi ning sellele vastavat finants- ja inimressursside kavandamist ning mis on kooskõlas komisjoni delegeeritud määruse (EL) nr 1271/2013 ([25]) artikliga 32 ja milles võetakse arvesse komisjoni kehtestatud suuniseid.

3. Haldusnõukogu võtab lõikes 1 osutatud ühtse programmdokumendi vastu iga aasta 30. novembriks ning saadab Euroopa Parlamendile, nõukogule ja komisjonile hiljemalt järgmise aasta 31. jaanuariks programmdokumendi ja kõik selle hilisemad ajakohastatud versioonid.

4. Ühtne programmdokument muutub lõplikuks pärast liidu üldeelarve lõplikku vastuvõtmist ja vajaduse korral kohandatakse seda vastavalt.

([25]) Komisjoni 30. septembri 2013. aasta delegeeritud määrus (EL) nr 1271/2013 raamfinantsmääruse kohta asutustele, millele viidatakse Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) nr 966/2012 artiklis 208 (ELT L 328, 7.12.2013, lk 42).

5. Iga-aastane tööprogramm sisaldab üksikasjalikke eesmärke ja oodatavaid tulemusi, sealhulgas tulemusnäitajaid. Samuti sisaldab see rahastatavate meetmete kirjeldust koos igale meetmele eraldatavate rahaliste vahendite ja inimressurssidega vastavalt tegevuspõhise eelarvestamise ja juhtimise põhimõtetele. Iga-aastane tööprogramm peab olema kooskõlas lõikes 7 osutatud mitmeaastase tööprogrammiga. Selles näidatakse selgelt ära ülesanded, mis võrreldes eelmise eelarveaastaga on lisatud või välja jäetud või mida on muudetud.

6. Kui ENISA-le pannakse uus ülesanne, muudab haldusnõukogu vastuvõetud iga-aastast tööprogrammi. Kõik iga-aastase tööprogrammi olulised muudatused võetakse vastu sama korra kohaselt nagu algne iga-aastane tööprogramm. Haldusnõukogu võib delegeerida tegevdirektorile õiguse teha iga-aastases tööprogrammis vähetähtsaid muudatusi.

7. Mitmeaastases tööprogrammis esitatakse üldine strateegiline programm, sealhulgas eesmärgid, oodatavad tulemused ja tulemusnäitajad. Selles esitatakse ka vahendite eraldamise programm, sealhulgas mitmeaastase eelarve ja töötajate jaoks.

8. Vahendite eraldamise programmi ajakohastatakse igal aastal. Strateegilist programmi ajakohastatakse, kui selle järele on vajadus, eeskätt artiklis 67 osutatud hindamise tulemuste arvesse võtmiseks.

Artikkel 25

Huvide deklaratsioon

1. Haldusnõukogu liikmed, tegevdirektor ning liikmesriikide poolt ajutiselt lähetatud ametnikud esitavad kohustuste deklaratsiooni ning deklaratsiooni, milles nad kinnitavad, et neil puudub või on olemas otsene või kaudne huvi, mida võib pidada nende sõltumatust kahjustavaks. Deklaratsioon peab olema täpne ja täielik, see esitatakse kirjalikult kord aastas ja vajaduse korral seda ajakohastatakse.

2. Haldusnõukogu liikmed, tegevdirektor ning ajutistes töörühmades osalevad väliseksperdid teevad hiljemalt iga koosoleku alguses täpse ja täieliku deklaratsiooni oma huvide kohta, mida võib pidada päevakorraküsimusega seoses nende sõltumatust kahjustavaks, ning nad ei võta osa selliste küsimuste arutamisest ega hääletusest.

3. ENISA sätestab oma sise-eeskirjas lõigetes 1 ja 2 osutatud huvide deklaratsioone käsitlevate normide rakendamise praktilise korra.

Artikkel 26

Läbipaistvus

1. ENISA viib oma tegevust läbi maksimaalselt läbipaistvalt ning kooskõlas artikliga 28.

2. ENISA tagab üldsusele ja huvitatud isikutele asjakohase, objektiivse, usaldusväärse ja kergesti juurdepääsetava teabe andmise, eelkõige ENISA töötulemuste kohta. Samuti avalikustab ENISA artikli 25 kohaselt esitatud huvide deklaratsioonid.

3. Haldusnõukogu võib tegevdirektori ettepanekul lubada huvitatud isikutel jälgida ENISA mõne tegevusega seotud menetlust.

4. ENISA sätestab oma sise-eeskirjas lõigetes 1 ja 2 osutatud läbipaistvusnormide rakendamise praktilise korra.

Artikkel 27

Konfidentsiaalsus

1. Ilma et see piiraks artikli 28 kohaldamist, ei anna ENISA kolmandatele isikutele tema poolt töödeldavat või saadud teavet, mille kohta on esitatud põhjendatud taotlus käsitleda seda teavet konfidentsiaalsena.

2. Haldusnõukogu liikmed, tegevdirektor, ENISA nõuanderühma liikmed, ajutistes töörühmades osalevad väliseksperdid ning ENISA töötajad, sealhulgas liikmesriikide poolt ajutiselt lähetatud ametnikud järgivad ELi toimimise lepingu artiklis 339 sätestatud konfidentsiaalsuse nõudeid, ja seda ka pärast nende töökohustuste lõppemist.

3. ENISA sätestab oma sise-eeskirjas lõigetes 1 ja 2 osutatud konfidentsiaalsuse nõuete rakendamise praktilise korra.

4. Haldusnõukogu otsustab lubada ENISA-l käidelda salastatud teavet, kui see on vajalik ENISA ülesannete täitmiseks. Sellisel juhul võtab haldusnõukogu kokkuleppel komisjoni talitustega vastu julgeolekunormid, millega kohaldatakse komisjoni otsustes (EL, Euratom) 2015/443 ([26]) ja 2015/444 ([27]) sätestatud julgeolekupõhimõtteid. Nimetatud julgeolekunormid hõlmavad salastatud teabe vahetust, töötlemist ja säilitamist käsitlevaid sätteid.

Artikkel 28

Juurdepääs dokumentidele

1. ENISA valduses olevate dokumentide suhtes kohaldatakse määrust (EÜ) nr 1049/2001.

2. Haldusnõukogu võtab vastu menetluse määruse (EÜ) nr 1049/2001 rakendamiseks hiljemalt 28. detsembriks 2019.

3. Määruse (EÜ) nr 1049/2001 artikli 8 kohaselt vastu võetud ENISA otsuste peale võib esitada vastavalt ELi toimimise lepingu artiklile 228 kaebuse Euroopa ombudsmanile või pöörduda vastavalt ELi toimimise lepingu artiklile 263 Euroopa Liidu Kohtusse.

IV PEATÜKK

ENISA eelarve koostamine ja struktuur

Artikkel 29

ENISA eelarve koostamine

1. Igal aastal koostab tegevdirektor ENISA järgmise eelarveaasta tulude ja kulude eelarvestuse projekti ning saadab selle koos ametikohtade loetelu kavaga haldusnõukogule. Tulud ja kulud peavad olema tasakaalus.

2. Haldusnõukogu koostab igal aastal eelarvestuse projekti põhjal ENISA järgmise eelarveaasta tulude ja kulude eelarvestuse projekti.

3. Haldusnõukogu saadab eelarvestuse projekti, mis on osa ühtse programmdokumendi kavandist, hiljemalt iga aasta 31. jaanuariks komisjonile ja kolmandatele riikidele, kellega liit on sõlminud artikli 42 lõikes 2 osutatud kokkulepped.

4. Eelarvestuse projektist lähtudes sisestab komisjon liidu üldeelarve projekti kalkulatsioonid, mida ta peab ametikohtade loetelu põhjal vajalikuks, ja liidu üldeelarvest makstava toetuse suuruse, ning esitab selle kooskõlas ELi toimimise lepingu artikliga 314 Euroopa Parlamendile ja nõukogule.

5. Euroopa Parlament ja nõukogu kinnitavad liidu poolt ENISA toetuseks eraldatavad assigneeringud.

6. Euroopa Parlament ja nõukogu kinnitavad ENISA ametikohtade loetelu.

([26]) Komisjoni 13. märtsi 2015. aasta otsus (EL, Euratom) 2015/443 komisjoni julgeoleku kohta (ELT L 72, 17.3.2015, lk 41).
([27]) Komisjoni 13. märtsi 2015. aasta otsus (EL, Euratom) 2015/444 ELi salastatud teabe kaitseks vajalike julgeolekunormide kohta (ELT L 72, 17.3.2015, lk 53).

7. Haldusnõukogu kinnitab ENISA eelarve koos ühtse programmdokumendiga. ENISA eelarve muutub lõplikuks pärast liidu üldeelarve lõplikku vastuvõtmist. Haldusnõukogu kohandab vajaduse korral ENISA eelarvet ja ühtset programmdokumenti kooskõlas liidu üldeelarvega.

Artikkel 30

ENISA eelarve struktuur

1. Ilma et see piiraks muid sissetulekuallikaid, koosnevad ENISA tulud järgmistest vahenditest:

a) toetus liidu üldeelarvest;

b) tulu, mis on ette nähtud konkreetsete kuluartiklite rahastamiseks kooskõlas artiklis 32 osutatud finantsreeglitega;

c) liidu rahalised vahendid delegeerimiskokkulepete või sihtotstarbeliste toetuste vormis kooskõlas artiklis 32 osutatud finantsreeglitega ja liidu poliitikameetmeid toetavate asjakohaste õigusaktide sätetega;

d) ENISA töös osalevate kolmandate riikide rahaline osalus, millele on osutatud artiklis 42;

e) liikmesriikide vabatahtlikud rahalised või mitterahalised osamaksed.

Esimese lõigu punkti e kohaseid vabatahtlikke osamakseid tegevatel liikmesriikidel ei ole õigust nõuda sellest tulenevalt teatavaid õigusi või teenuseid.

2. ENISA kulud hõlmavad muu hulgas personali- ja halduskulusid, tehnilise abi kulusid, taristu kulusid, tegevuskulusid ning kulusid, mis tulenevad kolmandate isikutega sõlmitud lepingutest.

Artikkel 31

ENISA eelarve täitmine

1. ENISA eelarve täitmise eest vastutab tegevdirektor.

2. Komisjoni siseaudiitoril on ENISA suhtes samad volitused kui komisjoni talituste suhtes.

3. ENISA peaarvepidaja saadab eelarveaasta (aasta N) esialgse raamatupidamise aastaaruande komisjoni peaarvepidajale ja kontrollikojale järgmise eelarveaasta (aasta N + 1) 1. märtsiks.

4. Pärast seda, kui peaarvepidaja on saanud Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) 2018/1046 ([28]) artikli 246 kohaselt kontrollikoja tähelepanekud ENISA esialgse raamatupidamise aastaaruande kohta, koostab ta omal vastutusel ENISA lõpliku raamatupidamise aastaaruande ning saadab selle haldusnõukogule arvamuse saamiseks.

5. Haldusnõukogu esitab oma arvamuse ENISA lõpliku raamatupidamise aastaaruande kohta.

6. Hiljemalt aasta N + 1 31. märtsiks saadab tegevdirektor eelarve täitmise ja finantsjuhtimise aruande Euroopa Parlamendile, nõukogule, komisjonile ja kontrollikojale.

7. ENISA peaarvepidaja saadab aasta N + 1 1. juuliks ENISA lõpliku raamatupidamisaruande ja haldusnõukogu arvamuse Euroopa Parlamendile, nõukogule, komisjoni peaarvepidajale ja kontrollikojale.

([28]) Euroopa Parlamendi ja nõukogu 18. juuli 2018. aasta määrus (EL, Euratom) 2018/1046, mis käsitleb liidu üldeelarve suhtes kohaldatavaid finantsreegleid ja millega muudetakse määrusi (EL) nr 1296/2013, (EL) nr 1301/2013, (EL) nr 1303/2013, (EL) nr 1304/2013, (EL) nr 1309/2013, (EL) nr 1316/2013, (EL) nr 223/2014 ja (EL) nr 283/2014 ja otsust nr 541/2014/EL ning tunnistatakse kehtetuks määrus (EL, Euratom) nr 966/2012 (ELT L 193, 30.7.2018, lk 1).

8. ENISA lõpliku raamatupidamisaruande esitamise tähtpäevaga samaks kuupäevaks saadab peaarvepidaja kontrollikojale esitiskirja kõnealuse raamatupidamisaruande kohta ning selle koopia komisjoni peaarvepidajale.

9. Tegevdirektor avaldab lõpliku raamatupidamisaruande aasta N + 1 15. novembriks *Euroopa Liidu Teatajas*.

10. Tegevdirektor saadab hiljemalt N + 1 aasta 30. septembriks kontrollikojale vastuse selle tähelepanekute kohta ning vastuse koopia haldusnõukogule ja komisjonile.

11. Euroopa Parlamendi taotluse korral esitab tegevdirektor Euroopa Parlamendile määruse (EL, Euratom) 2018/1046 artikli 261 lõike 3 kohaselt kogu teabe, mida on vaja asjaomast eelarveaastat käsitleva eelarve täitmisele heakskiidu andmise menetluse tõrgeteta läbiviimiseks.

12. Euroopa Parlament annab nõukogu soovituse põhjal heakskiidu tegevdirektori tegevusele aasta N eelarve täitmise kohta enne aasta N + 2 15. maid.

Artikkel 32

Finantsreeglid

Haldusnõukogu võtab pärast komisjoniga konsulteerimist vastu ENISA suhtes kohaldatavad finantsreeglid. Need ei või lahkneda delegeeritud määrusest (EL) nr 1271/2013, välja arvatud juhul, kui see on konkreetselt vajalik ENISA toimimiseks ja komisjon on selleks eelnevalt nõusoleku andnud.

Artikkel 33

Pettustevastane võitlus

1. Selleks et hõlbustada võitlust pettuste, korruptsiooni ja muu ebaseadusliku tegevuse vastu vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL, Euratom) nr 883/2013 ([29]), ühineb ENISA hiljemalt 28. detsembriks 2019 Euroopa Parlamendi, Euroopa Liidu Nõukogu ja Euroopa Ühenduste Komisjoni 25. mai 1999. aasta institutsioonidevahelise kokkuleppega, mis käsitleb Euroopa Pettustevastase Ameti (OLAF) sisejuurdlust ([30]). ENISA võtab vastu kõikide oma töötajate suhtes kohaldatavad asjakohased sätted, kasutades kõnealuse kokkuleppe lisas esitatud vormi.

2. Kontrollikojal on õigus auditeerida nii dokumentide alusel kui ka kontrollida kohapeal kõiki toetusesaajaid, töövõtjaid ja alltöövõtjaid, keda ENISA on rahastanud liidu vahenditest.

3. OLAF võib korraldada uurimisi, sealhulgas kohapealseid kontrolle ja inspekteerimisi vastavalt määruse (EL, Euratom) nr 883/2013 ja nõukogu määruse (Euratom, EÜ) nr 2185/96 ([31]) sätetele ja neis määrustes sätestatud korras, et teha kindlaks, kas ENISA rahastatava toetuse või lepinguga seoses on esinenud pettust, korruptsiooni või muud liidu finantshuve kahjustavat ebaseaduslikku tegevust.

4. Ilma et see piiraks lõigete 1, 2 ja 3 kohaldamist, sisaldavad ENISA ning kolmandate riikide ja rahvusvaheliste organisatsioonide vahelised koostöölepingud ning ENISA lepingud, toetuslepingud ja toetuse määramise otsused sätteid, mis annavad kontrollikojale ja OLAFile sõnaselgelt õiguse korraldada oma vastava pädevuse piires sellist auditeerimist ja uurimist.

([29]) Euroopa Parlamendi ja nõukogu 11. septembri 2013. aasta määrus (EL, Euratom) nr 883/2013, mis käsitleb Euroopa Pettustevastase Ameti (OLAF) juurdlusi ning millega tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1073/1999 ja nõukogu määrus (Euratom) nr 1074/1999 (ELT L 248, 18.9.2013, lk 1).

([30]) EÜT L 136, 31.5.1999, lk 15.

([31]) Nõukogu 11. novembri 1996. aasta määrus (Euratom, EÜ) nr 2185/96, mis käsitleb komisjoni tehtavat kohapealset kontrolli ja inspekteerimist, et kaitsta Euroopa ühenduste finantshuve pettuste ja igasuguse muu eeskirjade eiramiste eest (EÜT L 292, 15.11.1996, lk 2).

V PEATÜKK

Töötajad

Artikkel 34

Üldsätted

ENISA töötajate suhtes kohaldatakse personalieeskirju ja muude teenistujate teenistustingimusi ning personalieeskirjade ja muude teenistujate teenistustingimuste täitmiseks liidu institutsioonide kokkuleppel vastu võetud sätteid.

Artikkel 35

Privileegid ja immuniteedid

ENISA ja selle töötajate suhtes kohaldatakse ELi lepingule ja ELi toimimise lepingule lisatud protokolli nr 7 Euroopa Liidu privileegide ja immuniteetide kohta.

Artikkel 36

Tegevdirektor

1. Tegevdirektor võetakse tööle muude teenistujate teenistustingimuste artikli 2 punkti a kohase ENISA ajutise töötajana.

2. Tegevdirektori nimetab ametisse haldusnõukogu komisjoni esitatud kandidaatide nimekirjast pärast avatud ja läbipaistvat valikumenetlust.

3. Tegevdirektoriga töölepingu sõlmimisel esindab ENISAt haldusnõukogu esimees.

4. Enne ametisse nimetamist kutsutakse haldusnõukogu valitud kandidaat esinema Euroopa Parlamendi pädeva komisjoni ette ja vastama parlamendiliikmete küsimustele.

5. Tegevdirektori ametiaeg on viis aastat. Ametiaja lõpuks hindab komisjon tegevdirektori tegevust ning ENISA edasisi ülesandeid ja väljakutseid.

6. Tegevdirektori ametisse nimetamise, ametiaja pikendamise ja ametist tagandamise otsused teeb haldusnõukogu vastavalt artikli 18 lõikele 2.

7. Komisjoni ettepanekul, milles võetakse arvesse lõikes 5 osutatud hinnangut, võib haldusnõukogu pikendada tegevdirektori ametiaega üks kord viie aasta võrra.

8. Haldusnõukogu teatab tegevdirektori ametiaja pikendamise kavatsusest Euroopa Parlamendile. Kolme kuu jooksul enne ametiaja pikendamist esineb tegevdirektor Euroopa Parlamendi pädeva komisjoni kutsel selle ees ja vastab parlamendiliikmete küsimustele.

9. Tegevdirektor, kelle ametiaega on pikendatud, ei või edaspidi osaleda samale ametikohale korraldatavas valikumenetluses.

10. Tegevdirektori võib ametist tagandada üksnes otsusega, mille haldusnõukogu teeb komisjoni ettepaneku alusel.

Artikkel 37

Lähetatud riiklikud eksperdid ja muud töötajad

1. ENISA võib kasutada lähetatud riiklikke eksperte või muid ENISA-väliseid töötajaid. Sellise töötajate suhtes ei kohaldata personalieeskirju ega muude teenistujate teenistustingimusi.

2. Haldusnõukogu võtab vastu otsuse, milles sätestatakse riiklike ekspertide ENISAsse lähetamist käsitlevad normid.

VI PEATÜKK

Üldsätted

Artikkel 38

ENISA õiguslik seisund

1. ENISA on liidu asutus ja juriidiline isik.

2. ENISA-l on igas liikmesriigis kõige laialdasem õigusvõime, mis vastavalt liikmesriigi õigusele on juriidilistel isikutel. Eelkõige võib ENISA omandada ja võõrandada vallas- ja kinnisvara ning olla kohtus menetlusosaliseks.

3. ENISAt esindab tegevdirektor.

Artikkel 39

ENISA vastutus

1. ENISA lepingulist vastutust reguleerib asjaomase lepingu suhtes kohaldatav õigus.

2. ENISA sõlmitud lepingus sisalduva vahekohtuklausli alusel kohtuotsuste tegemine kuulub Euroopa Liidu Kohtu pädevusse.

3. Lepinguvälise vastutuse korral heastab ENISA vastavalt liikmesriikide õiguse ühistele üldpõhimõtetele kõik kahjud, mida ENISA või tema töötajad on oma ülesannete täitmisel tekitanud.

4. Lõikes 3 osutatud kahjude hüvitamisega seotud vaidluste lahendamine kuulub Euroopa Liidu Kohtu pädevusse.

5. ENISA töötajate isiklikku vastutust ENISA ees reguleeritakse ENISA töötajate suhtes kohaldatavate sätetega.

Artikkel 40

Kasutatavad keeled

1. ENISA suhtes kohaldatakse nõukogu määrust nr 1 ([32]). Liikmesriigid ja nende poolt määratud asutused võivad pöörduda ENISA poole ja saada vastuse nende poolt valitud liidu institutsioonide ametlikus keeles.

2. ENISA toimimiseks vajalikke tõlketeenuseid osutab Euroopa Liidu Asutuste Tõlkekeskus.

Artikkel 41

Isikuandmete kaitse

1. ENISA kohaldab isikuandmete töötlemise suhtes määrust (EL) 2018/1725.

2. Haldusnõukogu võtab vastu määruse (EL) 2018/1725 artikli 45 lõikes 3 osutatud rakenduseeskirja. Haldusnõukogu võib võtta vastu täiendavaid meetmeid, mis on vajalikud ENISA poolt määruse (EL) 2018/1725 kohaldamiseks.

([32]) Nõukogu määrus nr 1, millega määratakse kindlaks Euroopa Majandusühenduses kasutatavad keeled (EÜT 17, 6.10.1958, lk 385/58).

Artikkel 42

Koostöö kolmandate riikide ja rahvusvaheliste organisatsioonidega

1. Niivõrd kui see on vajalik käesoleva määruse eesmärkide saavutamiseks, võib ENISA teha koostööd kolmandate riikide pädevate asutuste ja rahvusvaheliste organisatsioonidega. Selleks võib ENISA komisjoni eelneval nõusolekul leppida kolmandate riikide asutuste ja rahvusvaheliste organisatsioonidega kokku koostöökorras. Kõnealune koostöökord ei too liidule ega selle liikmesriikidele kaasa õiguslikke kohustusi.

2. ENISA on osalemiseks avatud nendele kolmandatele riikidele, kes on sõlminud liiduga vastavad lepingud. Kõnealuste lepingute asjakohaste sätete alusel lepitakse kokku koostöökorras, milles täpsustatakse eelkõige nende kolmandate riikide poolt ENISA töös osalemise olemus, ulatus ja viis, sealhulgas sätted, mis käsitlevad ENISA käivitatud algatustes osalemist, rahalist osalust ja töötajaid. Personaliküsimustes peab kõnealune koostöökord olema igal juhul kooskõlas personalieeskirjade ja muude teenistujate teenistustingimustega.

3. Haldusnõukogu võtab vastu strateegia, mis käsitleb suhteid kolmandate riikide ja rahvusvaheliste organisatsioonidega ENISA pädevusse kuuluvates küsimustes. Komisjon tagab, et ENISA tegutseb oma volituste piires ja olemasolevas institutsioonilises raamistikus, leppides tegevdirektoriga kokku asjakohases töökorras.

Artikkel 43

Julgeolekunormid salastamata tundliku teabe ja salastatud teabe kaitse kohta

Pärast komisjoniga konsulteerimist võtab ENISA vastu julgeolekunormid, mille abil kohaldatakse julgeolekupõhimõtteid, mis sisalduvad komisjoni julgeolekunormides, mis käsitlevad salastamata tundliku teabe ja salastatud teabe kaitset, nagu on sätestatud otsustes (EL, Euratom) 2015/443 ja 2015/444. ENISA julgeolekunormid hõlmavad muu hulgas sätteid sellise teabe vahetamise, töötlemise ja säilitamise kohta.

Artikkel 44

Peakorterileping ja tegutsemistingimused

1. Vajalikud kokkulepped, milles käsitletakse ENISA-le asukohaliikmesriigis antavaid ruume ja pakutavat taristut ning ENISA asukohaliikmesriigis tegevdirektori, haldusnõukogu liikmete, ENISA töötajate ja nende pereliikmete suhtes kohaldatavaid erinorme, sätestatakse ENISA ja vastuvõtva liikmesriigi vahelises peakorterilepingus, mis sõlmitakse pärast haldusnõukogu heakskiidu saamist.

2. ENISA asukohaliikmesriik tagab ENISA-le parimad võimalikud tegutsemistingimused, et tagada ENISA nõuetekohane toimimine, võttes arvesse asukoha ligipääsetavust, sobivate haridusasutuste olemasolu töötajate laste jaoks, töötajate laste ja abikaasade piisavat juurdepääsu tööturule, sotsiaalkindlustusele ja arstiabile.

Artikkel 45

Halduskontroll

ENISA tegevuse üle teeb järelevalvet Euroopa ombudsman ELi toimimise lepingu artikli 228 kohaselt.

III JAOTIS

KÜBERTURVALISUSE SERTIFITSEERIMISE RAAMISTIK

Artikkel 46

Euroopa küberturvalisuse sertifitseerimise raamistik

1. Kehtestatakse Euroopa küberturvalisuse sertifitseerimise raamistik, et parandada siseturu toimimise tingimusi, suurendades liidus küberturvalisuse taset ja võimaldades liidu tasandil ühtlustatud lähenemisviisi Euroopa küberturvalisuse sertifitseerimise kavadele, eesmärgiga luua IKT-toodete, -teenuste ja -protsesside jaoks digitaalne ühtne turg.

2. Euroopa küberturvalisuse sertifitseerimise raamistik näeb ette mehhanismi, et kehtestada Euroopa küberturvalisuse sertifitseerimise kavad ning kinnitada, et selliste kavade kohaselt hinnatud IKT-tooted, -teenused ja -protsessid vastavad kindlaksmääratud turvanõuetele eesmärgiga kaitsta salvestatud, edastatud või töödeldud andmete või kõnealuste toodete, protsesside ja teenuste funktsioonide või nende poolt pakutavate või nende kaudu juurdepääsetavate teenuste käidelda-vust, autentsust, terviklust ja konfidentsiaalsust kogu nende olelusringi kestel.

Artikkel 47

Euroopa küberturvalisuse sertifitseerimise liidu jooksev tööprogramm

1. Komisjon avaldab Euroopa küberturvalisuse sertifitseerimise liidu jooksva tööprogrammi („liidu jooksev tööprogramm"), milles määratakse kindlaks tulevaste Euroopa küberturvalisuse sertifitseerimise kavade strateegilised prioriteedid.

2. Eelkõige sisaldab liidu jooksev tööprogramm IKT-toodete, -teenuste ja -protsesside või nende kategooriate loetelu, mis võivad saada kasu Euroopa küberturvalisuse sertifitseerimise kava kohaldamisalasse kuulumisest.

3. IKT-toote, -teenuse ja -protsessi või nende kategooria liidu jooksvasse tööprogrammi lisamine peab olema põhjen-datud ühel järgneval alusel:

a) on olemas konkreetset IKT-toote, -teenuse või -protsessi kategooriat hõlmavad riiklikud küberturvalisuse sertifitsee-rimise kavad, eeskätt seoses killustatuse ohuga, ja neid arendatakse;

b) asjakohane liidu või liikmesriigi õigus või poliitikameede;

c) nõudlus turul;

d) areng küberohtude vallas;

e) taotlus Euroopa küberturvalisuse sertifitseerimise rühma poolt välja pakutud konkreetse ettevalmistava kava koostami-seks.

4. Komisjon võtab arvesse Euroopa küberturvalisuse sertifitseerimise rühma ja sidusrühmade küberturvalisuse sertifit-seerimise rühma esitatud arvamusi liidu jooksva tööprogrammi kavandi kohta.

5. Esimene liidu jooksev tööprogramm avaldatakse hiljemalt 28. juuniks 2020. Liidu jooksvat tööprogrammi ajako-hastatakse vähemalt iga kolme aasta järel ja vajaduse korral sagedamini.

Artikkel 48

Euroopa küberturvalisuse sertifitseerimise kava taotlemine

1. Komisjon võib esitada ENISA-le taotluse koostada liidu jooksva tööprogrammi alusel ettevalmistav kava või vaadata olemasolev Euroopa küberturvalisuse sertifitseerimise kava liidu jooksva tööprogrammi alusel läbi.

2. Põhjendatud juhtudel võib komisjon või Euroopa küberturvalisuse sertifitseerimise rühm esitada ENISA-le taotluse koostada ettevalmistav kava või vaadata läbi liidu jooksvasse tööprogrammi mitte kuuluv olemasolev Euroopa küberturvalisuse sertifitseerimise kava. Vastavalt sellele ajakohastatakse liidu jooksvat tööprogrammi.

Artikkel 49

Euroopa küberturvalisuse sertifitseerimise kavade koostamine, vastuvõtmine ja läbivaatamine

1. Artikli 48 kohase komisjoni taotluse põhjal koostab ENISA ettevalmistava kava, mis vastab artiklites 51, 52 ja 54 sätestatud tingimustele.

2. Artikli 48 lõike 2 kohase Euroopa küberturvalisuse sertifitseerimise rühma taotluse põhjal võib ENISA koostada ettevalmistava kava, mis vastab artiklites 51, 52 ja 54 sätestatud nõuetele. Kui ENISA jätab taotluse rahuldamata, peab ta seda põhjendama. Taotluse rahuldamata jätmise otsuse teeb haldusnõukogu.

3. Ettevalmistavat kava koostades konsulteerib ENISA kõigi asjaomaste sidusrühmadega ametlikul, avatud, läbipaistval ja kaasaval viisil.

4. Iga ettevalmistava kava puhul moodustab ENISA kooskõlas artikli 20 lõikega 4 ajutise töörühma, et pakkuda ENISA-le spetsiifilist nõu ja oskusteavet.

5. ENISA teeb tihedat koostööd Euroopa küberturvalisuse sertifitseerimise rühmaga. Euroopa küberturvalisuse sertifitseerimise rühm pakub ENISA-le abi ja eksperdinõu seoses ettevalmistava kava koostamisega ning võtab ettevalmistava kava kohta vastu arvamuse.

6. ENISA võtab enne lõigete 3, 4 ja 5 kohaselt koostatud ettevalmistava kava edastamist komisjonile võimalikult suurel määral arvesse Euroopa küberturvalisuse sertifitseerimise rühma arvamust. Euroopa küberturvalisuse sertifitseerimise rühma arvamus ei ole ENISA-le siduv ja selle arvamuse puudumine ei takista ENISA-l edastada ettevalmistavat kava komisjonile.

7. Komisjon võib ENISA koostatud ettevalmistava kava põhjal võtta vastu rakendusaktid, millega nähakse ette artiklites 51, 52 ja 54 sätestatud nõuetele vastavad Euroopa küberturvalisuse sertifitseerimise kavad IKT-toodete, -teenuste ja -protsesside jaoks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 66 lõikes 2 osutatud kontrollimenetlusega.

8. ENISA hindab vähemalt iga viie aasta järel iga vastuvõetud Euroopa küberturvalisuse sertifitseerimise kava, võttes arvesse huvitatud isikutelt saadud tagasisidet. Vajaduse korral võib komisjon või Euroopa küberturvalisuse sertifitseerimise rühm taotleda, et ENISA alustaks kooskõlas artikliga 48 ja käesoleva artikliga muudetud ettevalmistava kava koostamist.

Artikkel 50

Euroopa küberturvalisuse sertifitseerimise kavade veebisait

1. ENISA haldab spetsiaalset veebisaiti, mis pakub teavet Euroopa küberturvalisuse sertifitseerimise kavade, Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide, kaasa arvatud kehtetute Euroopa küberturvalisuse sertifitseerimise kavade ning kehtetuks tunnistatud ja lõppenud kehtivusajaga Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonide kohta, ja tutvustab neid, ning sisaldab linke artikli 55 kohasele küberturvalisuse alasele teabele.

2. Kui see on asjakohane, märgitakse lõikes 1 osutatud veebisaidil ära ka riiklikud küberturvalisuse sertifitseerimise kavad, mis on asendatud Euroopa küberturvalisuse sertifitseerimise kavaga.

Artikkel 51

Euroopa küberturvalisuse sertifitseerimise kavade turvalisusega seotud eesmärgid

Euroopa küberturvalisuse sertifitseerimise kava peab olema koostatud nii, et saavutada asjakohasel juhul vähemalt järgmised turvalisusega seotud eesmärgid:

a) kaitsta salvestatud, edastatud või muul moel töödeldud andmeid juhusliku või volitamata salvestamise, töötlemise, juurdepääsu või avalikustamise eest kogu IKT-toote, -teenuse või -protsessi olelusringi kestel;

b) kaitsta salvestatud, edastatud või muul moel töödeldud andmeid juhusliku või volitamata hävitamise, kaotsimineku või muutmise või ebapiisava kättesaadavuse eest kogu IKT-toote, -teenuse või -protsessi olelusringi kestel;

c) volitatud kasutajatel, programmidel ja masinatel on juurdepääs üksnes neile andmetele, teenustele või funktsioonidele, millele neil on juurdepääsuõigused;

d) teha kindlaks ja dokumenteerida teadaolevad sõltuvusseosed ja turvanõrkused;

e) salvestada teave selle kohta, millal ja kes on pääsenud juurde millistele andmetele, teenustele või funktsioonidele, on neid kasutanud või muul viisil töödelnud;

f) on võimalik kontrollida, millal ja kes on pääsenud juurde millistele andmetele, teenustele või funktsioonidele, on neid kasutanud või muul viisil töödelnud;

g) kontrollida, et IKT-toodetel, -teenustel ja -protsessidel ei ole teadaolevaid turvanõrkuseid;

h) taastada füüsilise või tehnilise intsidendi korral õigeaegselt andmete, teenuste ja funktsioonide käideldavus ja neile juurdepääs;

i) IKT-tooted, -teenused ja -protsessid on vaikimisi ja sisseprojekteeritult turvalised;

j) IKT-toodetele, -teenustele ja -protsessidele pakutakse ajakohastatud tark- ja riistvara, mis ei sisalda avalikult teadaolevaid turvanõrkuseid, ning et olemas on mehhanismid turvaliseks uuendamiseks.

Artikkel 52

Euroopa küberturvalisuse sertifitseerimise kavade usaldusväärsuse tasemed

1. Euroopa küberturvalisuse sertifitseerimise kavas võidakse määrata IKT-toodetele, -teenustele ja -protsessidele üks või mitu järgmist usaldusväärsuse taset: baastase, märkimisväärne tase või kõrge tase. Usaldusväärsuse tase peab vastama IKT-toote, -teenuse või-protsessi ettenähtud kasutamisega seotud riskitasemele, võttes arvesse intsidendi tõenäosust ja mõju.

2. Euroopa küberturvalisuse sertifikaadid ja ELi vastavusdeklaratsioonid osutavad sellise Euroopa küberturvalisuse sertifitseerimise kavas määratud usaldusväärsuse tasemele, mille alusel Euroopa küberturvalisuse sertifikaat või ELi vastavusdeklaratsioon välja anti.

3. Euroopa küberturvalisuse sertifitseerimise kavas määratakse kindlaks igale usaldusväärsuse tasemele vastavad turvanõuded, sealhulgas turvafunktsioonid ja IKT-toote, -teenuse või -protsessi hindamise rangus ja põhjalikkus.

4. Euroopa küberturvalisuse sertifikaadis või ELi vastavusdeklaratsioonis osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk on vähendada küberturvalisuse intsidentide riski või ennetada küberturvalisuse intsidente.

5. Euroopa küberturvalisuse sertifikaat või ELi vastavusdeklaratsioon, mis osutab usaldusväärsuse baastasemele, annab kindluse, et IKT-tooted, -teenused ja -protsessid, mille kohta kõnealune sertifikaat või ELi vastavusdeklaratsioon on välja antud, täidavad vastavaid turvanõudeid, sealhulgas turvafunktsioone, ning et neid on hinnatud tasemel, mille eesmärk on minimeerida küberintsidentide ja küberrünnete teadaolevaid põhilisi riske. Hindamine hõlmab vähemalt tehnilise dokumentatsiooni läbivaatamist. Kui tehnilise dokumentatsiooni läbivaatamine ei ole asjakohane, tuleb selle asemel kasutada muud samaväärse mõjuga hindamist.

6. Euroopa küberturvalisuse sertifikaat, mis osutab märkimisväärsele usaldusväärsuse tasemele, annab kindluse, et IKT-tooted, -teenused ja -protsessid, mille kohta kõnealune sertifikaat on välja antud, täidavad vastavaid turvanõudeid, sealhulgas turvafunktsioone, ning et neid on hinnatud tasemel, mille eesmärk on minimeerida teadaolevaid küberturvalisuse riske ning piiratud oskuste ja vahenditega isikute poolt toimepandavate küberintsidentide ja küberrünnete riske. Hindamine hõlmab vähemalt järgmist: kontrollimine, et ei esine avalikult teadaolevaid turvanõrkuseid, ning testimine, et IKT-tooted, -teenused ja -protsessid rakendavad korrektselt vajalikke turvafunktsioone. Kui selline hindamine ei ole asjakohane, tuleb selle asemel kasutada muud samaväärse mõjuga hindamist.

7. Euroopa küberturvalisuse sertifikaat, mis osutab kõrgele usaldusväärsuse tasemele, annab kindluse, et IKT-tooted, -teenused ja -protsessid, mille kohta kõnealune sertifikaat on välja antud, täidavad vastavaid turvanõudeid, sealhulgas turvafunktsioone, ning et neid on hinnatud tasemel, mille eesmärk on minimeerida märkimisväärsete oskuste ja vahenditega isikute poolt toimepandavate tipptasemel küberrünnete riski. Hindamine hõlmab vähemalt järgmist: kontrollimine, et ei esine avalikult teadaolevaid turvanõrkuseid, ning testimine, et IKT-tooted, -teenused ja -protsessid rakendavad korrektselt vajalikke turvafunktsioone tipptasemel, ning nende oskuslikele häkkeritele vastupanemise võime hindamine läbistustestimise kaudu. Kui selline hindamine ei ole asjakohane, tuleb selle asemel kasutada muud samaväärse mõjuga hindamist.

8. Euroopa küberturvalisuse sertifitseerimise kavas võidakse määratleda mitmeid hindamistasemeid, sõltuvalt kasutatava hindamismetoodika rangusest ja põhjalikkusest. Iga hindamistase vastab ühele usaldusväärsuse tasemele ja see määratakse kindlaks usaldusväärsuse komponentide asjakohase kombinatsiooni kaudu.

Artikkel 53

Vastavuse enesehindamine

1. Euroopa küberturvalisuse sertifitseerimise kavas võidakse lubada vastavuse enesehindamise läbiviimist IKT-toodete, -teenuste või -protsesside tootja või pakkuja ainuvastutusel. Vastavuse enesehindamine on lubatud üksnes madala riskiga IKT-toodete, -teenuste ja -protsesside suhtes, mis vastavad usaldusväärsuse baastasemele.

2. IKT-toodete, -teenuste või -protsesside tootja või pakkuja võib anda välja ELi vastavusdeklaratsiooni, milles kinnitatakse, et kavas esitatud nõuded on täidetud. ELi vastavusdeklaratsiooni väljaandmisega võtab IKT-toodete, -teenuste või -protsesside tootja või pakkuja vastutuse IKT-toote, -teenuse või -protsessi vastavuse eest kõnealuses kavas sätestatud nõuetele.

3. IKT-toodete, -teenuste või -protsesside tootja või pakkuja hoiab ELi vastavusdeklaratsiooni, tehnilist dokumentatsiooni ja muud asjaomast teavet, mis puudutab IKT-toodete või -teenuste vastavust kavale, asjaomases Euroopa küberturvalisuse sertifitseerimise kavas kindlaks määratud tähtaja jooksul kättesaadavana artiklis 58 osutatud riikliku küberturvalisuse sertifitseerimise asutusele. ELi vastavusdeklaratsiooni koopia esitatakse riiklikule küberturvalisuse sertifitseerimise asutusele ja ENISA-le.

4. ELi vastavusdeklaratsiooni väljaandmine on vabatahtlik, kui liidu ega liikmesriikide õiguses ei ole sätestatud teisiti.

5. ELi vastavusdeklaratsioone tunnustatakse kõikides liikmesriikides.

Artikkel 54

Euroopa küberturvalisuse sertifitseerimise kavade elemendid

1. Euroopa küberturvalisuse sertifitseerimise kava sisaldab vähemalt järgmisi elemente:

a) sertifitseerimiskava sisu ja ulatus, sealhulgas hõlmatud IKT-toodete, -teenuste ja -protsesside liik või kategooria;

b) kava eesmärgi selge kirjeldus ja kirjeldus selle kohta, kuidas valitud standardid, hindamismeetodid ja usaldusväärsuse tasemed vastavad kava kavandatud kasutajate vajadustele;

c) viide hindamises kohaldatud rahvusvahelistele, Euroopa või riiklikele standarditele, või kui sellised standardid ei ole kättesaadavad või asjakohased, siis viide tehnilisele kirjeldusele, mis vastab määruse (EL) nr 1025/2012 II lisas sätestatud nõuetele, või kui selline kirjeldus ei ole kättesaadav, siis viide Euroopa küberturvalisuse sertifitseerimise kavas kindlaks määratud tehnilisele kirjeldusele või muudele küberturvalisuse nõuetele;

d) asjakohasel juhul üks või mitu usaldusväärsuse taset;

e) märge selle kohta, kas vastavuse enesehindamine on kava puhul lubatud;

f) asjakohasel juhul vastavushindamisasutuste suhtes kohaldatavad eri- või täiendavad nõuded, et tagada nende tehniline pädevus hinnata küberturvalisuse nõudeid;

g) konkreetsed hindamiskriteeriumid ja meetodid, sealhulgas hindamise liigid, tõendamaks, et artiklis 51 osutatud turvalisusega seotud eesmärgid on täidetud;

h) asjakohasel juhul sertifitseerimiseks vajalik teave, mille taotleja peab vastavushindamisasutustele esitama või muul viisil kättesaadavaks tegema;

i) kui kava näeb ette märgi või märgistuse, tingimused märgi või märgistuse kasutamiseks;

j) eeskiri IKT-toodete, -teenuste ja -protsesside Euroopa küberturvalisuse sertifikaatide nõuete või ELi vastavusdeklaratsiooni nõuete täitmise kontrollimiseks, sealhulgas mehhanismid tõestamaks konkreetsete küberturvalisuse nõuete jätkuvat täitmist;

k) asjakohasel juhul tingimused Euroopa küberturvalisuse sertifikaatide väljaandmiseks, säilitamiseks, jätkamiseks ja kehtivuse pikendamiseks ning tingimused sertifitseerimise ulatuse laiendamiseks või kitsendamiseks;

l) eeskiri sertifitseeritud või ELi vastavusdeklaratsiooni saanud IKT-toodete, -teenuste ja -protsesside kava nõuetele mittevastavuse tagajärgede kohta;

m) eeskiri selle kohta, kuidas tuleks IKT-toodete, -teenuste ja -protsesside varem avastamata küberturvalisuse nõrkustest teada anda ja kuidas neid menetleda;

n) asjakohasel juhul eeskiri andmete säilitamise kohta vastavushindamisasutuste poolt;

o) teave sama liiki või samasse kategooriasse kuuluvaid IKT-tooteid, -teenuseid ja -protsesse, turvanõudeid, hindamiskriteeriumeid ja -meetodeid ning usaldusväärsuse tasemeid hõlmavate riiklike või rahvusvaheliste küberturvalisuse sertifitseerimise kavade kohta;

p) väljaantavate Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsiooni sisu ja vorming;

q) ELi vastavusdeklaratsiooni, tehnilise dokumentatsiooni ning IKT-toodete, -teenuste või -protsesside tootja või pakkuja poolt kättesaadavaks tehtava muu asjaomase teabe kättesaadavuse tähtaeg;

r) kava kohaselt välja antud Euroopa küberturvalisuse sertifikaatide maksimaalne kehtivusaeg;

s) kava kohaselt välja antud, muudetud ja kehtetuks tunnistatud Euroopa küberturvalisuse sertifikaatide avalikustamispoliitika;

t) sertifitseerimise kavade kolmandate riikidega vastastikuse tunnustamise tingimused;

u) asjakohasel juhul kavas kehtestatud vastastikuse hindamise mehhanismi käsitlev eeskiri asutuste jaoks, kes annavad kooskõlas artikli 56 lõikega 6 välja Euroopa küberturvalisuse sertifikaate kõrge usaldusväärsuse taseme jaoks. See mehhanism ei piira artiklis 59 ette nähtud vastastikust hindamist;

v) vorming ja menetlused, mida kasutavad IKT-toodete, -teenuste või -protsesside tootjad või pakkujad täiendava küberturvalisuse alase teabe esitamisel ja ajakohastamisel kooskõlas artikliga 55.

2. Euroopa küberturvalisuse sertifitseerimise kavas kirjeldatud nõuded peavad olema kooskõlas kohaldatavate õiguslike nõuetega, eelkõige liidu ühtlustatud õigusnormidest tulenevate nõuetega.

3. Kui konkreetses liidu õigusaktis on nii sätestatud, võib Euroopa küberturvalisuse sertifitseerimise kava kohaselt välja antud sertifikaati või ELi vastavusdeklaratsiooni kasutada kõnealuse õigusakti nõuetele vastavuse eelduse tõendamiseks.

4. Liidu ühtlustatud õigusnormide puudumisel võib liikmesriik oma õiguses sätestada, et Euroopa küberturvalisuse sertifitseerimise kava võib kasutada selleks, et luua õiguslikele nõuetele vastavuse eeldus.

Artikkel 55

Täiendav küberturvalisuse alane teave sertifitseeritud IKT-toodete, -teenuste ja -protsesside kohta

1. Sertifitseeritud või ELi vastavusdeklaratsiooni saanud IKT-toodete, -teenuste ja -protsesside tootja või pakkuja teeb avalikkusele kättesaadavaks järgmise täiendava küberturvalisuse alase teabe:

a) suunised ja soovitused, mis aitavad lõppkasutajal IKT-tooteid või -teenuseid turvaliselt konfigureerida, paigaldada, kasutusele võtta ning neid käitada ja hooldada;

b) ajavahemik, mille jooksul pakutakse lõppkasutajatele turvalisuse alast tuge, eelkõige võimaldades saada küberturvalisuse alaseid uuendusi;

c) tootja või pakkuja kontaktandmed ja aktsepteeritavad viisid lõppkasutajatelt ja küberturvalisusega tegelevatelt teadlastelt turvanõrkuste kohta teabe saamiseks;

d) viited internetis asuvatele andmebaasidele, kus on loetletud IKT-toote, -teenuse või -protsessiga seotud avalikult teada antud turvanõrkused ja asjakohased küberturvalisuse alased nõuanded.

2. Lõikes 1 osutatud teave peab olema kättesaadav elektroonilisel kujul ning see peab olema kättesaadav ja seda tuleb ajakohastada vajaduse korral vähemalt kuni vastava Euroopa küberturvalisuse sertifikaadi või ELi vastavusdeklaratsiooni kehtivuse lõppemiseni.

Artikkel 56

Küberturvalisuse sertifitseerimine

1. Kui IKT-tooted, -teenused ja -protsessid on sertifitseeritud Euroopa küberturvalisuse sertifitseerimise kava kohaselt, mis on vastu võetud kooskõlas artikliga 49, eeldatakse, et nad vastavad kõnealuse kava nõuetele.

2. Küberturvalisuse sertifitseerimine on vabatahtlik, kui liidu või liikmesriikide õiguses ei ole sätestatud teisiti.

3. Komisjon hindab regulaarselt vastuvõetud Euroopa küberturvalisuse sertifitseerimise kavade tõhusust ja kasutamist ning seda, kas konkreetne Euroopa küberturvalisuse sertifitseerimise kava tuleb teha asjakohase liidu õigusaktiga kohustuslikuks, et tagada liidus IKT-toodete, -teenuste ja -protsesside küberturvalisuse piisav tase ning parandada siseturu toimimist. Hindamine tuleb läbi viia hiljemalt 31. detsembriks 2023 ja seejärel vähemalt iga kahe aasta järel. Komisjon teeb hindamise tulemuste põhjal kindlaks olemasoleva sertifitseerimiskavaga hõlmatud IKT-tooted, -teenused ja -protsessid, mis peavad olema kohustusliku sertifitseerimiskavaga hõlmatud.

Esmajärjekorras keskendub komisjon direktiivi (EL) 2016/1148 II lisas loetletud sektoritele, mida hinnatakse hiljemalt kahe aasta möödumisel esimese Euroopa küberturvalisuse sertifitseerimise kava vastuvõtmisest.

Hinnangu koostamisel teeb komisjon järgmist:

a) võtab arvesse mõju, mida avaldavad meetmed kõnealuste IKT-toodete, -teenuste või -protsesside tootjatele või pakkujatele ja kasutajatele kulude seisukohast, ning sotsiaalset ja majanduslikku kasu, mis tuleneb hinnatud IKT-toodete, -teenuste või -protsesside turvalisuse taseme eeldatavast paranemisest;

b) võtab arvesse asjaomase liikmesriikide ja kolmandate riikide õiguse olemasolu ja rakendamist;

c) konsulteerib kõigi asjaomaste sidusrühmade ja liikmesriikidega avatud, läbipaistval ja kaasaval viisil;

d) võtab arvesse rakendamise tähtpäevi, üleminekumeetmeid ja -tähtaegu, eelkõige meetme võimalikku mõju osas IKT-toodete, -teenuste või -protsesside tootjatele ja pakkujatele, kaasa arvatud VKEdele;

e) pakub välja võimalusi, kuidas minna kõige kiiremini ja tõhusamalt vabatahtlikelt sertifitseerimiskavadelt üle kohustuslikele sertifitseerimiskavadele.

4. Käesoleva artikli kohase Euroopa küberturvalisuse sertifikaadi, milles osutatakse kas usaldusväärsuse baastasemele või märkimisväärsele tasemele, annavad välja artiklis 60 osutatud vastavushindamisasutused artikli 49 kohaselt komisjoni poolt vastu võetud Euroopa küberturvalisuse sertifitseerimise kavas sisalduvate kriteeriumide alusel.

5. Erandina lõikest 4 võib põhjendatud juhtudel Euroopa küberturvalisuse sertifitseerimise kavas ette näha, et nimetatud kavast tuleneva Euroopa küberturvalisuse sertifikaadi võib välja anda üksnes avaliku sektori asutus. Selleks asutuseks võib olla:

a) artikli 58 lõikes 1 osutatud riiklik küberturvalisuse sertifitseerimise asutus või

b) artikli 60 lõike 1 kohaselt vastavushindamisasutusena akrediteeritud avaliku sektori asutus.

6. Kui artikli 49 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kava nõuab kõrget usaldusväärsuse taset, võib Euroopa küberturvalisuse sertifikaadi välja anda üksnes riiklik küberturvalisuse sertifitseerimise asutus või järgmistel juhtudel vastavushindamisasutus:

a) riiklik küberturvalisuse sertifitseerimise asutus annab eelneva heakskiidu igale vastavushindamisasutuse poolt välja antud Euroopa küberturvalisuse sertifikaadile või

b) riiklik küberturvalisuse sertifitseerimise asutus delegeerib Euroopa küberturvalisuse sertifikaatide väljaandmise eelnevalt vastavushindamisasutusele.

7. Füüsiline või juriidiline isik, kes esitab oma IKT-tooted, -teenused või -protsessid sertifitseerimiseks, peab tegema artiklis 58 osutatud riiklikule küberturvalisuse sertifitseerimise asutusele, juhul kui nimetatud asutus on Euroopa küberturvalisuse sertifikaati väljaandev asutus, või artiklis 60 osutatud vastavushindamisasutusele kättesaadavaks kogu sertifitseerimise läbiviimiseks vajaliku teabe.

8. Euroopa küberturvalisuse sertifikaadi omanik teavitab lõikes 7 osutatud asutust igast hiljem avastatud turvanõrkusest või nõuete rikkumisest, mis puudutab sertifitseeritud IKT-toote, -teenuse või -protsessi turvalisust ja millel võib olla mõju sertifitseerimisega seotud nõuete täitmisele. Kõnealune asutus edastab selle teabe põhjendamatu viivituseta asjaomasele riiklikule küberturvalisuse sertifitseerimise asutusele.

9. Euroopa küberturvalisuse sertifikaat antakse Euroopa küberturvalisuse sertifitseerimise kavas kindlaks määratud tähtajaks ja selle kehtivust võib pikendada, kui asjakohased nõuded on täidetud.

10. Käesoleva artikli kohaselt välja antud Euroopa küberturvalisuse sertifikaati tunnustatakse kõigis liikmesriikides.

Artikkel 57

Riiklikud küberturvalisuse sertifitseerimise kavad ja sertifikaadid

1. Ilma et see piiraks käesoleva artikli lõike 3 kohaldamist, lõpeb riiklike küberturvalisuse sertifitseerimise kavade ja Euroopa küberturvalisuse sertifitseerimise kavaga hõlmatud IKT-toodete, -teenuste ja -protsessidega seotud menetluste õiguslik toime artikli 49 lõike 7 kohaselt vastu võetud rakendusaktis sätestatud kuupäeval. Riiklikud küberturvalisuse sertifitseerimise kavad ja Euroopa küberturvalisuse sertifitseerimise kavaga hõlmamata IKT-toodete, -teenuste ja -protsessidega seotud menetlused kehtivad edasi.

2. Liikmesriigid ei kehtesta kehtiva Euroopa küberturvalisuse sertifitseerimise kavaga hõlmatud IKT-toodetele, -teenustele ja -protsessidele uusi riiklikke küberturvalisuse sertifitseerimise kavasid.

3. Riiklike küberturvalisuse sertifitseerimise kavade alusel väljastatud sertifikaadid, mis on hõlmatud Euroopa küberturvalisuse sertifitseerimise kavaga, jäävad kehtima kuni oma kehtivusaja lõpuni.

4. Et vältida siseturu killustatust, teatavad liikmesriigid komisjonile ja Euroopa küberturvalisuse sertifitseerimise rühmale oma kavatsusest koostada uued riiklikud küberturvalisuse sertifitseerimise kavad.

Artikkel 58

Riiklikud küberturvalisuse sertifitseerimise asutused

1. Iga liikmesriik määrab oma territooriumil ühe või mitu riiklikku küberturvalisuse sertifitseerimise asutust või vastastikusel kokkuleppel teise liikmesriigiga ühe või mitu riiklikku küberturvalisuse sertifitseerimise asutust, mis asub nimetatud teises liikmesriigis ja mis vastutab järelevalveülesannete eest määravas liikmesriigis.

2. Iga liikmesriik teatab komisjonile määratud riiklike küberturvalisuse sertifitseerimise asutuste andmetest. Kui liikmesriik määrab rohkem kui ühe asutuse, teatab ta komisjonile ka igale asutusele määratud ülesannetest.

3. Ilma et see piiraks artikli 56 lõike 5 punkti a ja artikli 56 lõike 6 kohaldamist, peab iga riiklik küberturvalisuse sertifitseerimise asutus olema oma organisatsiooni, rahastamisotsuste, õigusliku struktuuri ja otsuste tegemise poolest sõltumatu üksustest, mille järele ta valvab.

4. Liikmesriigid tagavad, et riikliku küberturvalisuse sertifitseerimise asutuste tegevus on seoses artikli 56 lõike 5 punktis a ja artikli 56 lõikes 6 osutatud Euroopa küberturvalisuse sertifikaatide väljaandmisega rangelt lahus käesolevas artiklis sätestatud järelevalvetegevustest ning et nimetatud tegevusi viiakse ellu üksteisest sõltumatult.

5. Liikmesriigid tagavad, et riiklikel küberturvalisuse sertifitseerimise asutustel on piisavad ressursid oma volituste rakendamiseks ning oma ülesannete tulemuslikuks ja tõhusaks täitmiseks.

6. Käesoleva määruse tõhusaks rakendamiseks on asjakohane, et riiklikud küberturvalisuse sertifitseerimise asutused osaleksid aktiivselt, tõhusalt, tulemuslikult ja turvaliselt Euroopa küberturvalisuse sertifitseerimise rühma töös.

7. Riiklik küberturvalisuse sertifitseerimise asutus:

a) teeb koostöös teiste asjaomaste turujärelevalveasutustega järelevalvet artikli 54 lõike 1 punkti j kohaselt Euroopa küberturvalisuse sertifitseerimise kavades sisalduva eeskirja üle, mille kohaselt kontrollitakse IKT-toodete, -teenuste ja -protsesside vastavust selliste Euroopa küberturvalisuse sertifikaatide nõuetele, mis on välja antud tema liikmesriigi territooriumil, ja tagab selle eeskirja täitmise;

b) jälgib tema liikmesriigi territooriumil asuvate ja vastavuse enesehindamist tegevate IKT-toodete, -teenuste või -protsesside tootjate või pakkujate kohustuste täitmist, eriti artikli 53 lõigetes 2 ja 3 ning vastavas Euroopa küberturvalisuse sertifitseerimise kavas sätestatud kohustuste täitmist, ja tagab nende kohustuste täitmise;

c) aktiivselt aitab ja toetab riiklikke akrediteerimisasutusi vastavushindamisasutuste poolt käesoleva määruse kohaldamiseks läbi viidava tegevuse jälgimisel ja järelevalvel, ilma et see piiraks artikli 60 lõike 3 kohaldamist;

d) jälgib ja kontrollib artikli 56 lõikes 5 osutatud avaliku sektori asutuste tegevust;

e) annab kooskõlas artikli 60 lõikega 3 vastavushindamisasutustele loa, kui see on asjakohane, ning piirab olemasolevat luba, peatab selle kehtivuse või tunnistab selle kehtetuks, kui vastavushindamisasutused rikuvad käesoleva määruse nõudeid;

f) käsitleb füüsiliste või juriidiliste isikute kaebusi seoses Euroopa küberturvalisuse sertifikaatidega, mille on välja andnud riiklikud küberturvalisuse sertifitseerimise asutused või kooskõlas artikli 56 lõikega 6 vastavushindamisasutused, või seoses artikli 53 kohaselt välja antud ELi vastavusdeklaratsioonidega, ning uurib asjakohasel määral nende kaebuste sisu ja teavitab kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest;

g) esitab ENISA-le ja Euroopa küberturvalisuse sertifitseerimise rühmale iga-aastase kokkuvõtliku aruande käesoleva lõike punktide b, c ja d ning lõike 8 kohaselt läbi viidud tegevuste kohta;

h) teeb koostööd teiste riiklike küberturvalisuse sertifitseerimise asutuste ja muude avaliku sektori asutustega, sealhulgas jagades teavet IKT-toodete, -teenuste ja -protsesside võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade nõuetele, ning

i) jälgib küberturvalisuse sertifitseerimise valdkonna asjakohast arengut.

8. Igal riiklikul küberturvalisuse sertifitseerimise asutusel on vähemalt järgmised volitused:

a) anda vastavushindamisasutustele, Euroopa küberturvalisuse sertifikaadi omanikele ja ELi vastavusdeklaratsiooni väljaandjatele korraldus esitada teavet, mis on vajalik tema ülesannete täitmiseks;

b) uurida auditi vormis vastavushindamisasutusi, Euroopa küberturvalisuse sertifikaadi omanikke ja ELi vastavusdeklaratsiooni väljaandjaid, et kontrollida nende poolt käesoleva jaotise järgimist;

c) võtta asjakohaseid meetmeid vastavalt liikmesriigi õigusele tagamaks, et vastavushindamisasutused, Euroopa küberturvalisuse sertifikaadi omanikud ja ELi vastavusdeklaratsiooni väljaandjad järgivad käesoleva määruse ja Euroopa küberturvalisuse sertifitseerimise kava nõudeid;

d) saada juurdepääs kõigile vastavushindamisasutuste ja Euroopa küberturvalisuse sertifikaadi omanike ruumidele, et toimetada uurimisi kooskõlas liidu või liikmesriigi menetlusõigusega;

e) tunnistada liikmesriigi õiguse kohaselt kehtetuks Euroopa küberturvalisuse sertifikaadid, mille on välja andnud riiklikud küberturvalisuse sertifitseerimise asutused või kooskõlas artikli 56 lõikega 6 vastavushindamisasutused, kui need sertifikaadid ei vasta käesolevale määrusele või Euroopa küberturvalisuse sertifitseerimise kavale;

f) määrata liikmesriigi õiguse kohaselt artiklis 65 osutatud karistusi ning nõuda käesolevas määruses sätestatud kohustuste rikkumise viivitamatut lõpetamist.

9. Riiklikud küberturvalisuse sertifitseerimise asutused teevad omavahel ja komisjoniga koostööd, eelkõige vahetavad teavet, kogemusi ja häid tavasid seoses küberturvalisuse sertifitseerimisega ning IKT-toodete, -teenuste ja -protsesside küberturvalisust puudutavate tehniliste küsimustega.

Artikkel 59

Vastastikune eksperdihinnang

1. Et saavutada kogu liidus võrdväärsed standardid seoses välja antud Euroopa küberturvalisuse sertifikaatide ja ELi vastavusdeklaratsioonidega, rakendatakse riiklike küberturvalisuse sertifitseerimise asutuste suhtes vastastikust hindamist.

2. Vastastikune hindamine toimub mõistlike ja läbipaistvate kriteeriumide ja menetluste alusel, mis käsitlevad eelkõige struktuuridele, inimressurssidele ja menetlustele kohaldatavaid nõudeid, konfidentsiaalsust ja kaebusi.

3. Vastastikuse hindamise puhul hinnatakse järgmist:

a) kas riikliku küberturvalisuse sertifitseerimise asutuse tegevus, mis on seotud artikli 56 lõike 5 punktis a ja artikli 56 lõikes 6 osutatud Euroopa küberturvalisuse sertifikaatide väljaandmisega, on rangelt lahus artiklis 58 sätestatud järelevalvetegevusest ning kas nimetatud tegevusi viiakse ellu üksteisest sõltumatult, kui see on asjakohane;

b) IKT-toodete, -teenuste ja -protsesside Euroopa küberturvalisuse sertifikaatide nõuetele vastavuse kontrollimise eeskirja artikli 58 lõike 7 punkti a kohase järelevalve ja täitmise tagamise menetlused;

c) artikli 58 lõike 7 punkti b kohaselt toimuva IKT-toodete, -teenuste või -protsesside tootjate ja pakkujate kohustuste täitmise jälgimise ja kohustuste täitmise tagamise menetlused;

d) vastavushindamisasutuste tegevuse jälgimise, selleks loa andmise ja selle üle järelevalve tegemise menetlused;

e) kui see on kohaldatav, siis kas kõrge usaldusväärsuse taseme kohta artikli 56 lõike 6 kohaselt sertifikaate väljaandvate asutuste töötajatel on sobiv oskusteave.

4. Vastastikuse hindamise viivad läbi vähemalt kaks muu liikmesriigi riiklikku küberturvalisuse sertifitseerimise asutust ja komisjon ning see viiakse läbi vähemalt kord viie aasta jooksul. ENISA võib osaleda vastastikuses hindamises.

5. Komisjonil on õigus võtta vastu rakendusakte, millega kehtestatakse vastastikuse hindamise kava vähemalt viieks aastaks, sätestatakse vastastikuse hindamise rühma koosseisu kriteeriumid, hindamismetoodika, hindamiste ajakava, sagedus ja muud vastastikuse hindamisega seotud ülesanded. Nimetatud rakendusaktide vastuvõtmisel võtab komisjon kohaselt arvesse Euroopa küberturvalisuse sertifitseerimise rühma arvamusi. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 66 lõikes 2 osutatud kontrollimenetlusega.

6. Vastastikuse hindamise tulemused vaatab läbi Euroopa küberturvalisuse sertifitseerimise rühm, kes koostab kokkuvõtte, mille võib teha üldsusele kättesaadavaks, ja kes annab vajaduse korral suuniseid ja soovitusi tegevuste või meetmete kohta, mida asjaomased üksused peavad läbi viima või võtma.

Artikkel 60

Vastavushindamisasutused

1. Vastavushindamisasutusi akrediteerivad määruse (EÜ) nr 765/2008 kohaselt nimetatud riiklikud akrediteerimisasutused. Vastavushindamisasutus akrediteeritakse üksnes siis, kui ta vastab käesoleva määruse lisas sätestatud nõuetele.

2. Kui Euroopa küberturvalisuse sertifikaat antakse välja riikliku küberturvalisuse sertifitseerimise asutuse poolt vastavalt artikli 56 lõike 5 punktile a ja artikli 56 lõikele 6, akrediteeritakse käesoleva artikli lõike 1 kohaselt riikliku küberturvalisuse sertifitseerimise asutuse sertifitseerimise organ vastavushindamisasutuseks.

3. Kui Euroopa küberturvalisuse sertifitseerimise kavades on vastavalt artikli 54 lõike 1 punktile f sätestatud konkreetsed või täiendavad nõuded, annab riiklik küberturvalisuse sertifitseerimise asutus nende kavade kohaste ülesannete täitmiseks loa üksnes sellistele vastavushindamisasutustele, kes vastavad nimetatud nõuetele.

4. Lõikes 1 osutatud vastavushindamisasutuste akrediteerimine kehtib maksimaalselt viis aastat ja selle kehtivust võib pikendada samadel tingimustel, kui vastavushindamisasutus vastab jätkuvalt käesolevas artiklis sätestatud nõuetele. Riiklik akrediteerimisasutus võtab mõistliku aja jooksul kõik asjakohased meetmed, et piirata, peatada või tunnistada lõike 1 kohane vastavushindamisasutuse akrediteerimine kehtetuks, kui akrediteerimise tingimused ei ole täidetud või ei ole enam täidetud või kui vastavushindamisasutus rikub käesolevat määrust.

Artikkel 61

Teavitamine

1. Riiklikud küberturvalisuse sertifitseerimise asutused teatavad vastu võetud Euroopa küberturvalisuse sertifitseerimise kava puhul komisjonile, millised akrediteeritud ja asjakohasel juhul artikli 60 lõike 3 kohaselt loa saanud vastavushindamisasutused võivad anda välja artiklis 52 osutatud usaldusväärsuse tasemega sertifikaate. Riiklikud küberturvalisuse sertifitseerimise asutused teatavad põhjendamatu viivituseta komisjonile kõigist hilisematest muudatustest.

2. Üks aasta pärast Euroopa küberturvalisuse sertifitseerimise kava jõustumist avaldab komisjon kõnealuse kava alusel teatatud vastavushindamisasutuste nimekirja *Euroopa Liidu Teatajas*.

3. Kui komisjon saab teate pärast lõikes 2 osutatud tähtaja möödumist, avaldab ta teatatud vastavushindamisasutuste nimekirja muudatused *Euroopa Liidu Teatajas* kahe kuu jooksul alates kõnealuse teate saamise kuupäevast.

4. Riiklik küberturvalisuse sertifitseerimise asutus võib esitada komisjonile taotluse jätta tema poolt teatatud vastavushindamisasutus lõikes 2 osutatud nimekirjast välja. Komisjon avaldab vastavad nimekirja muudatused *Euroopa Liidu Teatajas* ühe kuu jooksul alates riikliku küberturvalisuse sertifitseerimise asutuse taotluse kättesaamise kuupäevast.

5. Komisjon võib vastu võtta rakendusakte, et määrata kindlaks käesoleva artikli lõikes 1 osutatud teavitamise asjaolud, vormingud ja menetlused. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 66 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 62

Euroopa küberturvalisuse sertifitseerimise rühm

1. Moodustatakse Euroopa küberturvalisuse sertifitseerimise rühm.

2. Euroopa küberturvalisuse sertifitseerimise rühm koosneb riiklike küberturvalisuse sertifitseerimise asutuste esindajatest või teiste asjakohaste riiklike asutuste esindajatest. Euroopa küberturvalisuse sertifitseerimise rühma liige võib esindada üksnes kahte liikmesriiki.

3. Sidusrühmi ja asjaomaseid kolmandaid isikuid võidakse kutsuda osalema Euroopa küberturvalisuse sertifitseerimise rühma koosolekutel ning selle töös.

4. Euroopa küberturvalisuse sertifitseerimise rühmal on järgmised ülesanded:

a) nõustada ja abistada komisjoni töös, mille eesmärk on tagada käesoleva jaotise järjepidev rakendamine ja kohaldamine, eelkõige seoses liidu jooksva tööprogrammi, küberturvalisuse sertifitseerimise poliitika küsimuste, poliitika koordineerimise ja Euroopa küberturvalisuse sertifitseerimise kavade koostamisega;

b) abistada ja nõustada ENISAt ja teha temaga koostööd ettevalmistava kava koostamisel kooskõlas artikliga 49;

c) võtta vastu arvamus artikli 49 kohaselt ENISA koostatud ettevalmistava kava kohta;

d) esitada ENISA-le artikli 48 lõike 2 kohaselt taotlus ettevalmistava kava koostamiseks;

e) võtta vastu komisjonile suunatud arvamusi seoses olemasolevate Euroopa küberturvalisuse sertifitseerimise kavade haldamise ja läbivaatamisega;

f) analüüsida olulisi arenguid küberturvalisuse sertifitseerimise valdkonnas ning vahetada teavet ja häid tavasid küberturvalisuse sertifitseerimise kavade kohta;

g) hõlbustada riiklike küberturvalisuse sertifitseerimise asutuste käesoleva jaotise kohast koostööd suutlikkuse suurendamise ja teabevahetuse kaudu, eelkõige töötades välja meetodid tõhusaks teabevahetuseks küberturvalisuse sertifitseerimisega seotud küsimustes;

h) toetada vastastikuse hindamise mehhanismide rakendamist kooskõlas Euroopa küberturvalisuse sertifitseerimise kavas artikli 54 lõike 1 punkti u kohaselt kehtestatud eeskirjaga;

i) hõlbustada Euroopa küberturvalisuse sertifitseerimise kavade kohandamist rahvusvaheliselt tunnustatud standarditega, sealhulgas olemasolevate Euroopa küberturvalisuse sertifitseerimise kavade läbivaatamise abil, ja asjakohasel juhul esitada ENISA-le soovitusi teha koostööd asjaomaste rahvusvaheliste standardiorganisatsioonidega, et kõrvaldada olemasolevate rahvusvaheliselt tunnustatud standardite puudused ja lüngad.

5. Komisjon juhatab ENISA abiga Euroopa küberturvalisuse sertifitseerimise rühma ja osutab sellele sekretariaaditeenust kooskõlas artikli 8 lõike 1 punktiga e.

Artikkel 63

Õigus esitada kaebus

1. Füüsilistel ja juriidilistel isikutel on õigus esitada kaebus Euroopa turvalisuse sertifikaadi väljaandjale või asjaomasele riiklikule Euroopa küberturvalisuse sertifitseerimise asutusele, kui kaebus on seotud artikli 56 lõike 6 kohaselt tegutseva vastavushindamisasutuse välja antud sertifikaadiga.

2. Asutus, kellele kaebus esitatakse, teavitab kaebuse esitajat kaebuse menetlemise käigust ja tehtud otsusest, samuti artiklis 64 osutatud õigusest tõhusale kohtulikule õiguskaitsevahendile.

Artikkel 64

Õigus tõhusale kohtulikule õiguskaitsevahendile

1. Olenemata halduslikest ja muudest kohtuvälistest õiguskaitsevahenditest on füüsilistel ja juriidilistel isikutel õigus tõhusale kohtulikule õiguskaitsele seoses järgmisega:

a) artikli 63 lõikes 1 osutatud asutuse otsused, kaasa arvatud seoses Euroopa küberturvalisuse sertifikaadi ebaõige väljaandmise, välja andmata jätmise ja nende füüsiliste ja juriidiliste isikute omatavate Euroopa küberturvalisuse sertifikaatide tunnustamisega, kui see on kohaldatav;

b) artikli 63 lõikes 1 osutatud asutusele esitatud kaebusele reageerimata jätmine.

2. Käesoleva artikli kohased menetlused algatatakse selle liikmesriigi kohtus, kus asub asutus, mille suhtes kohtulikku õiguskaitsevahendit taotletakse.

Artikkel 65

Karistused

Liikmesriigid kehtestavad käesoleva jaotise ja Euroopa küberturvalisuse sertifitseerimise kavade rikkumise korral kohaldatavad karistusnormid, ning võtavad kõik vajalikud meetmed nende rakendamise tagamiseks. Kehtestatud karistused peavad olema tõhusad, proportsionaalsed ja hoiatavad. Liikmesriigid teavitavad komisjoni viivitamata nimetatud normidest ja meetmetest ning kõikidest nende hilisematest muudatustest.

IV JAOTIS

LÕPPSÄTTED

Artikkel 66

Komiteemenetlus

1. Komisjoni abistab komitee. Nimetatud komitee on komitee määruse (EL) nr 182/2011 tähenduses.

2. Käesolevale lõikele viitamisel kohaldatakse määruse (EL) nr 182/2011 artikli 5 lõike 4 punkti b.

Artikkel 67

Hindamine ja läbivaatamine

1. Hiljemalt 28. juuniks 2024 ja seejärel iga viie aasta tagant hindab komisjon ENISA ja selle töökorralduse mõju, tulemuslikkust ja tõhusust ning võimalikku vajadust muuta ENISA volitusi ja kõigi selliste muudatuste finantsmõju. Hindamisel arvestatakse tagasisidet, mida ENISA on oma tegevuse kohta saanud. Kui komisjon leiab, et ENISA tegevuse jätkamine ei ole ENISA-le seatud eesmärke, volitusi ja ülesandeid arvestades enam põhjendatud, võib ta teha ettepaneku käesolevat määrust ENISAga seotud sätete osas muuta.

2. Hindamise käigus analüüsitakse ka käesoleva määruse III jaotise sätete mõju, tulemuslikkust ja tõhusust seoses eesmärgiga tagada IKT-toodete, -teenuste ja -protsesside piisav küberturvalisuse tase liidus ja parandada siseturu toimimist.

3. Hindamise käigus analüüsitakse, kas on vaja küberturvalisusega seotud siseturule pääsu käsitlevaid olulisi nõudeid, et vältida selliste IKT-toodete, -teenuste ja -protsesside liidu turule jõudmist, mis ei vasta põhilistele küberturvalisuse nõuetele.

4. Hiljemalt 28. juuniks 2024 ja seejärel iga viie aasta tagant edastab komisjon hindamisaruande koos oma järeldustega Euroopa Parlamendile, nõukogule ja haldusnõukogule. Hindamistulemused avalikustatakse.

Artikkel 68

Kehtetuks tunnistamine ja õigusjärglus

1. Määrus (EL) nr 526/2013 tunnistatakse kehtetuks alates 27. juunist 2019.

2. Viiteid määrusele (EL) nr 526/2013 ja kõnealuse määrusega asutatud ENISA-le käsitatakse viidetena käesolevale määrusele ja käesoleva määrusega asutatud ENISA-le.

3. Käesoleva määrusega asutatud ENISA on omandiõiguse, lepingute, õiguslike kohustuste, töölepingute, finantskohustuste ja vastutuse osas määrusega (EL) nr 526/2013 asutatud ENISA õigusjärglane. Kõik määruse (EL) nr 526/2013 kohaselt vastu võetud haldusnõukogu ja juhatuse otsused jäävad kehtima, tingimusel et nad on kooskõlas käesoleva määrusega.

4. ENISA asutatakse määramata ajaks alates 27. juunist 2019.

5. Määruse (EL) nr 526/2013 artikli 24 lõike 4 alusel ametisse nimetatud tegevdirektor jääb ametisse ja täidab käesoleva määruse artiklis 20 osutatud tegevdirektori ülesandeid oma ametiaja lõpuni. See ei mõjuta tegevdirektoriga sõlmitud lepingu tingimusi.

6. Määruse (EL) nr 526/2013 artikli 6 alusel ametisse nimetatud haldusnõukogu liikmed ja nende asendusliikmed jäävad ametisse ja täidavad käesoleva määruse artiklis 15 osutatud haldusnõukogu liikmete ülesandeid oma ametiaja lõpuni.

Artikkel 69

Jõustumine

1. Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas.*

2. Artikleid 58, 60, 61, 63, 64 ja 65 kohaldatakse alates 28. juunist 2021.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Strasbourg, 17. aprill 2019

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*
A. TAJANI	G. CIAMBA

LISA

VASTAVUSHINDAMISASUTUSTE SUHTES KEHTIVAD NÕUDED

Akrediteerimist taotlevad vastavushindamisasutused peavad vastama järgmistele nõuetele.

1. Vastavushindamisasutus peab olema asutatud liikmesriigi õiguse kohaselt ning olema juriidiline isik.

2. Vastavushindamisasutus peab olema kolmandast isikust asutus, kes on sõltumatu organisatsioonist ja IKT-tootest, -teenusest või -protsessist, mida ta hindab.

3. Asutust, mis kuulub ettevõtjate ühendusse või kutseliitu, mis esindab ettevõtjaid, kes on seotud tema hinnatavate IKT-toodete, -teenuste või -protsesside projekteerimise, tootmise, tarnimise, monteerimise, kasutamise või hooldamisega, võib pidada vastavushindamisasutuseks tingimusel, et tõendatud on tema sõltumatus ning huvide konflikti puudumine.

4. Vastavushindamisasutus, selle kõrgem juhtkond ja vastavushindamisülesannete täitmise eest vastutavad töötajad ei tohi olla hinnatava IKT-toote, -teenuse või -protsessi projekteerija, tootja, tarnija, paigaldaja, ostja, omanik, kasutaja, hooldaja ega ühegi nimetatud isiku volitatud esindaja. Keeld ei välista vastavushindamisasutuse tegevuseks vajalike hinnatavate IKT-toodete kasutamist ega nende IKT-toodete kasutamist isiklikul otstarbel.

5. Vastavushindamisasutus, selle kõrgem juhtkond ja vastavushindamisülesannete täitmise eest vastutavad töötajad ei tohi olla otseselt seotud hinnatavate IKT-toodete, -teenuste või -protsesside projekteerimise, tootmise või konstrueerimise, turustamise, paigaldamise, kasutamise või hooldusega ega esindada ühtegi isikut, kes nimetatud tegevustega tegeleb. Vastavushindamisasutus, selle kõrgem juhtkond ja vastavushindamisülesannete täitmise eest vastutavad töötajad ei tohi osaleda tegevuses, mis võib seada kahtluse alla nende otsuste sõltumatuse ja usaldusväärsuse nende tehtavates vastavushindamistoimingutes. Keeld kehtib eelkõige nõustamisteenuste puhul.

6. Kui vastavushindamisasutus kuulub avaliku sektori üksusele või asutusele või on selle hallatav asutus, tuleb tagada selle sõltumatus ning riikliku küberturvalisuse sertifitseerimise asutuse ja vastavushindamisasutuse vahelise huvide konflikti puudumine ning see dokumenteerida.

7. Vastavushindamisasutused peavad tagama, et nende tütarettevõtjate ja lepingupartnerite tegevus ei mõjuta vastavushindamistoimingute konfidentsiaalsust, objektiivsust ega erapooletust.

8. Vastavushindamisasutused ja nende töötajad peavad tegema vastavushindamistoiminguid suurima erialase usaldusväärsuse ja nõutava erialase tehnilise pädevusega ning nad ei tohi alluda ühelegi surveavaldusele ega ahvatlusele, sealhulgas rahalisele, mis võib nende otsuseid või vastavushindamistoimingute tulemusi mõjutada, see on eriti oluline selliste isikute või isikute rühmade puhul, kes on huvitatud nimetatud toimingute tulemustest.

9. Vastavushindamisasutus peab olema võimeline täitma kõiki talle käesoleva määrusega pandud vastavushindamisülesandeid olenemata sellest, kas vastavushindamisasutus täidab neid ülesandeid ise või neid täidetakse tema nimel ja vastutusel. Alltöövõtt ja konsulteerimine asutuseväliste töötajatega peab olema nõuetekohaselt dokumenteeritud ja ellu viidud ilma vahendajateta ning selle kohta tuleb sõlmida kirjalik leping, milles käsitletakse muu hulgas konfidentsiaalsust ja huvide konflikti küsimusi. Täidetud ülesannete eest vastutab täiel määral asjaomane vastavushindamisasutus.

10. Vastavushindamisasutuse käsutuses peavad olema alati ja kõigile IKT-toodete, -teenuste või -protsesside tüüpidele, kategooriatele või alamkategooriatele ning kõigile vastavushindamismenetlustele vastavad järgmised vahendid:

    a) töötajad, kellel on tehnilised teadmised ning piisav asjakohane kogemus vastavushindamisülesannete täitmiseks;

    b) menetluste kirjeldused, mille kohaselt vastavushindamist tehakse ning mis tagavad nende menetluste läbipaistvuse ja kordamise võimaluse. Asutusel peavad olema asjakohased tegevuspõhimõtted ja menetlused, milles eristatakse ülesandeid, mida ta täidab artikli 61 kohaselt teatatud vastavushindamisasutusena, ja muud tegevust;

c) menetlused toimingute tegemiseks, mis võtavad asjakohaselt arvesse ettevõtja suurust, tegutsemisvaldkonda, tema struktuuri, IKT-toote, -teenuse või -protsessi tehnoloogia keerukuse astet ning seda, kas tegemist on mass- või seeriatootmisega.

11. Vastavushindamisasutusel peavad olema vajalikud vahendid vastavushindamistoimingute nõuetekohase teostamisega seotud tehniliste ja haldusülesannete täitmiseks ning juurdepääs vajalikule varustusele ja vahenditele.

12. Vastavushindamistoimingute teostamise eest vastutavatel töötajatel peavad olema:

a) heal tasemel tehniline ja kutsealane väljaõpe, mis hõlmab kõiki vastavushindamistegevusi;

b) piisavad teadmised nende poolt tehtavate vastavushindamistoimingute nõuetest ning piisav pädevus nimetatud hindamistoimingute läbiviimiseks;

c) sobilikud teadmised ja arusaam kehtivatest nõuetest ja katsestandarditest;

d) oskus koostada sertifikaate, protokolle ja aruandeid, mis tõendavad vastavushindamistoimingute läbiviimist.

13. Tagatud peab olema vastavushindamisasutuste, nende kõrgema juhtkonna, vastavushindamistoimingute teostamise eest vastutavate töötajate ja alltöövõtjate erapooletus.

14. Vastavushindamisasutuse kõrgema juhtkonna ja vastavushindamistoimingute teostamise eest vastutavate töötajate tasu suurus ei tohi sõltuda tehtud vastavushindamiste arvust ega nimetatud hindamiste tulemustest.

15. Vastavushindamisasutus peab sõlmima vastutuskindlustuslepingu, välja arvatud juhul, kui vastutust kannab liikmesriigi õiguse kohaselt liikmesriik või kui vastavushindamine on liikmesriigi enda otsene ülesanne.

16. Vastavushindamisasutus ja selle töötajad, komiteed, allüksused, alltöövõtjad ning sellega seotud asutused ja välised töötajad peavad tagama konfidentsiaalsuse ja hoidma ametisaladust teabe osas, mis on saadud käesoleva määruse või selle täitmise tagamiseks vastuvõetud liikmesriigi õigusaktide kohaselt täidetud vastavushindamisülesannete käigus, välja arvatud juhul, kui teabe avalikustamist nõuab nendele isikutele kohaldatav liidu või liikmesriigi õigus, samuti välja arvatud teabevahetus selle liikmesriigi pädevate asutustega, kus asutus tegutseb. Intellektuaalomandiõiguste kaitse peab olema tagatud. Vastavushindamisasutusel peavad olema käesoleva punkti nõuete täitmiseks kehtestatud dokumenteeritud menetlused.

17. Käesoleva lisa nõuded, välja arvatud punkti 16 nõuded, ei takista tehnilise teabe ja regulatiivsete suuniste vahetamist vastavushindamisasutuse ja sertifikaati taotleva või selle taotlemist kaaluva isiku vahel.

18. Vastavushindamisasutus tegutseb vastavalt sidusatele, õiglastele ja mõistlikele tingimustele, võttes tasude puhul arvesse VKEde huve.

19. Vastavushindamisasutus peab vastama asjakohase standardi nõuetele, mis on ühtlustatud määruse (EÜ) nr 765/2008 kohaselt IKT-toodete, -teenuste või -protsesside sertifitseerimist läbiviivate vastavushindamisasutuste akrediteerimiseks.

20. Vastavushindamisasutus peab tagama, et vastavushindamiseks kasutatavad katselaborid vastavad asjakohase standardi nõuetele, mis on ühtlustatud määruse (EÜ) nr 765/2008 alusel katselaborite akrediteerimiseks.