2024/3144

19.12.2024

KOMISJONI RAKENDUSMÄÄRUS (EL) 2024/3144,

18. detsember 2024,

millega muudetakse rakendusmäärust (EL) 2024/482 kohaldatavate rahvusvaheliste standardite osas ja parandatakse seda rakendusmäärust

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrust (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus), ([1]) eriti selle artikli 49 lõiget 7,

ning arvestades järgmist:

(1) Komisjoni rakendusmäärusega (EL) 2024/482 ([2]) määratakse kindlaks Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kavaga (EUCC) ette nähtud rollid, eeskirjad ja kohustused ning kava struktuur vastavalt määruses (EL) 2019/881 kindlaks määratud küberturvalisuse sertifitseerimise raamistikule.

(2) Rakendusmäärus (EL) 2024/482 põhineb väljakujunenud rahvusvahelistel standarditel, st Rahvusvahelise Standardiorganisatsiooni (ISO) ja Rahvusvahelise Elektrotehnikakomisjoni (IEC) hallatavatel ühiskriteeriumidel ja ühisel hindamismetoodikal. Rakendusmääruses (EL) 2024/482 viidatakse ISO/IEC standarditele, kuid ei täpsustata nende standardite kohaldatavat versiooni. Seepärast tuleks täpsustada, millist standardite versiooni EUCC alusel välja antud sertifikaatide suhtes kohaldatakse.

(3) Valitsusorganisatsioonid, kes aitasid IT-turbe valdkonna ühiskriteeriumide sertifikaatide tunnustamise kokkuleppe (CCRA) kaudu kaasa ühiskriteeriumide ja ühise hindamismetoodika väljatöötamisele, on koos ISO/IECga nende autoriõiguste ühisomanikud. Neile valitsusorganisatsioonidele jääb õigus neid kasutada. Võttes arvesse CCRAst tulenevate dokumentide tähtsust, peaksid need olema ka EUCC kohase sertifitseerimise aluseks.

(4) CCRA sisaldab ühiskriteeriumide ja ühise hindamismetoodika standardite tõlgendusi, mis hõlbustavad nende rakendamist ning mida infotehnoloogia turvalisuse hindamise üksused ja sertifitseerimisasutused võivad arvesse võtta.

(5) Ühiskriteeriumidega seotud rahvusvahelisi standardeid võidakse ajakohastada. Nõuetekohase ja õigeaegse ülemineku tagamiseks on asjakohane määrata kindlaks üleminekueeskirjad, et anda müüjatele, infotehnoloogia turvalisuse hindamise üksustele ja sertifitseerimisasutustele ning muudele asjaomastele osalejatele piisavalt aega vajalike kohanduste tegemiseks. Sellised üleminekueeskirjad peaksid olema asjakohasel määral kooskõlas ülemaailmsete tavadega, sealhulgas CCRAs määratletud tavadega.

([1]) ELT L 151, 7.6.2019, lk 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) Komisjoni 31. jaanuari 2024. aasta rakendusmäärus (EL) 2024/482, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 rakenduseeskirjad seoses Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava (EUCC) vastuvõtmisega (ELT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(6) Rakendusmääruses (EL) 2024/482 ei ole täpsustatud, kui kaua võib IKT-toote sertifitseerimine põhineda ühiskriteeriumide ja ühise hindamismetoodika standardite varasematel versioonidel. Nimetatud rakendusmääruse I, II ja III lisas loetletud tehnilised valdkonnad ja kaitseprofiilid põhinevad standardite ISO/IEC 15408 ja 18045 varasematel versioonidel. Seepärast tuleks rakendusmääruses (EL) 2024/482 täpsustada, millistel asjaoludel kohaldatakse endiselt ühiskriteeriumide ja ühise hindamismetoodika eelmist versiooni ning kuidas toimub üleminek rahvusvaheliste standardite uusimale versioonile.

(7) Üleminekuperioodil peaks asjaomaste sidusrühmade prioriteet olema vastavate tehniliste valdkondade ja kaitseprofiilide ajakohastamine. Rakendusmääruses (EL) 2024/482 tuleks sätestada, et standardite varasemal versioonil põhinevad turvasihid kiidetakse heaks kuni 31. detsembrini 2027 kooskõlas CCRA üleminekustrateegiaga. Tuleb siiski märkida, et CCRA üleminekustrateegia hõlmab toodete ja kaitseprofiilide esialgset hindamist, mis algab hiljemalt 30. juunil 2024, mil EUCC ei olnud veel kohaldatav. Lisaks tuleks kooskõlas CCRA üleminekustrateegiaga rakendusmääruses (EL) 2024/482 sätestada, et kõnealusele rakendusmäärusele vastavad turvasihid, mille väide vastavuse kohta kaitseprofiilidele põhineb standardite eelmisel versioonil, kiidetakse heaks kuni 31. detsembrini 2027. Kui uus sertifikaat antakse rakendusmääruse (EL) 2024/482 alusel välja riikliku sertifikaadi läbivaatamise käigus kahe aasta jooksul pärast algset sertifikaati, peaks olema võimalik kasutada standardite varasemat versiooni. See ei oleks asjakohane juhul, kui läbivaatamisprotsessi puhul ei nõuta uue sertifikaadi väljaandmist rakendusmääruse (EL) 2024/482 alusel ja sertifikaat jääb kehtima.

(8) Et tagada nõuetekohane üleminek standardite värskeimale versioonile, tuleks rakendusmäärusega (EL) 2024/482 ette näha konkreetsed üleminekueeskirjad ja lubada jätkuvalt väljastada kõnealuse rakendusmääruse alusel sertifikaate, milles väidetakse vastavust kaitseprofiilidele, mis põhinevad CCRA alusel avaldatud standardite varasematel versioonidel, kui selliste kaitseprofiilide kasutamine on liidu õigusaktide kohaselt nõutav. See puudutab komisjoni rakendusmäärust (EL) 2016/799, ([3]) Euroopa Parlamendi ja nõukogu määrust (EL) nr 910/2014 ([4]) ja komisjoni rakendusotsust (EL) 2016/650 ([5]).

(9) Rakendusmääruse (EL) 2024/482 I lisas on loetletud IKT-toodete ja kaitseprofiilide hindamiseks kohaldatavad tehnika taset käsitlevad dokumendid. Selles ei täpsustata aga dokumentide versiooni. Seepärast tuleks täpsustada, millist dokumentide versiooni EUCC alusel välja antud sertifikaatide suhtes kohaldatakse. Need versioonid põhinevad Euroopa küberturvalisuse sertifitseerimise rühma (ECCG) poolt heaks kiidetud dokumentidel, mis on läbi vaadatud, et lisada need EUCCsse. Lisaks tuleks I lisa muuta, et lisada ajakohastatud ja uued tehnika taset käsitlevad dokumendid, mille ECCG on heaks kiitnud, tagades seega vastavushindamisasutuste ühtse akrediteerimise EUCC alusel. Infotehnoloogia turvalisuse hindamise üksuse akrediteerimise nõudeid tuleks ajakohastada, et selgitada sõltumatuse ja erapooletuse kriteeriumide kohaldamist, ning sertifitseerimisasutuste akrediteerimiseks tuleks kehtestada uus tehnika taset käsitlev dokument.

(10) EUCC-le võib lisada tehnika taset käsitlevaid dokumente või neid ajakohastada seoses kava haldamisega. Uute või ajakohastatud tehnika taset käsitlevate dokumentide jaoks võib olla vaja kehtestada asjakohased üleminekueeskirjad, et võimaldada müüjatel, infotehnoloogia turvalisuse hindamise üksustel, sertifitseerimisasutustel ja muudel sidusrühmadel teha vajalikke kohandusi. Infotehnoloogia turvalisuse hindamise üksuste akrediteerimisega seotud tehnika taset käsitleva dokumendi ajakohastamiseks tuleks ajakohastatud dokumenti kohaldada enne 8. juulit 2025 väljastatud akrediteeringute suhtes üksnes siis, kui need vaadatakse läbi, näiteks hindamis- või ümberhindamismenetluse raames. Lisaks tuleks ajakohastatud dokumenti kohaldada kõigi infotehnoloogia turvalisuse hindamise üksuste akrediteeringute suhtes, mis on välja antud pärast 8. juulit 2025.

([3]) Komisjoni 18. märtsi 2016. aasta rakendusmäärus (EL) 2016/799, millega rakendatakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 165/2014, millega sätestatakse sõidumeerikute ja nende komponentide konstruktsiooni, katsetamise, paigaldamise, kasutamise ja parandamise nõuded (ELT L 139, 26.5.2016, lk 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([5]) Komisjoni 25. aprilli 2016. aasta rakendusotsus (EL) 2016/650, millega kehtestatakse kvalifitseeritud allkirja andmise ja templi loomise vahendi turvalisuse hindamise standardid vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 30 lõikele 3 ja artikli 39 lõikele 2 (ELT L 109, 26.4.2016, lk 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Rakendusmääruse (EL) 2024/482 artiklite 5, 8, 16, 29 ja 44 ning IV lisa täiendavad parandused aitavad tagada ühtse sõnastuse ja selge õigusliku tõlgenduse.

(12) Vastavushindamisasutustest teatamise eeskirjad tuleks kehtestada horisontaalselt kõigi Euroopa küberturvalisuse sertifitseerimise raamistiku kavade jaoks. Selliseid teatamise eeskirju on käsitletud komisjoni rakendusmääruses (EL) 2024/3143 ([6]). Seetõttu tuleks rakendusmääruse (EL) 2024/482 artiklid 23 ja 24 kustutada alates kuupäevast, mil hakatakse kohaldama rakendusmäärust (EL) 2024/3143.

(13) Seepärast tuleks rakendusmäärust (EL) 2024/482 vastavalt muuta ja parandada.

(14) Käesoleva määrusega ettenähtud meetmed on kooskõlas määruse (EL) 2019/881 artikli 66 kohaselt asutatud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Rakendusmäärust (EL) 2024/482 muudetakse järgmiselt.

1) Artikli 2 punktid 1 ja 2 asendatakse järgmisega:

„1) „Ühiskriteeriumid“ – infotehnoloogia turvalisuse hindamise ühiskriteeriumid, nagu on esitatud standardites ISO/IEC 15408–1:2022, ISO/IEC 15408–2:2022, ISO/IEC 15408–3:2022, ISO/IEC 15408–4:2022 või ISO/IEC 15408–5:2022 või infotehnoloogia turvalisuse hindamise ühiskriteeriumide versiooni CC:2022 1.–5. osas, mille on avaldanud IT-turbe valdkonna ühiskriteeriumide sertifikaatide tunnustamise kokkuleppe osalised;

2) „ühine hindamismetoodika“ – infotehnoloogia turvalisuse hindamise ühine metoodika, nagu on esitatud standardis ISO/IEC 18045:2022, või infotehnoloogia turvalisuse hindamise ühise metoodika versioon CEM:2022, mille on avaldanud IT-turbe valdkonna ühiskriteeriumide sertifikaatide tunnustamise kokkuleppe osalised;“.

2) Artikkel 3 asendatakse järgmisega:

„*Artikkel 3*

Hindamisstandardid

1. EUCC kohaselt tehtavate hindamiste suhtes kohaldatakse järgmisi standardeid:

a) ühiskriteeriumid;

b) ühine hindamismetoodika.

2. Kuni 31. detsembrini 2027 võib sertifikaadi välja anda EUCC alusel, kohaldades üht kahest järgmisest standardist:

a) ISO/IEC 15408–1:2009, ISO/IEC 15408–2:2008 või ISO/IEC 15408–3:2008;

b) infotehnoloogia turvalisuse hindamise ühiskriteeriumid, versioon 3.1, 5. läbivaatamine, mille on avaldanud IT-turbe valdkonna ühiskriteeriumide sertifikaatide tunnustamise kokkuleppe osalised;

([6]) Komisjoni 18. detsembri 2024. aasta rakendusmäärus (EL) 2024/3143, millega nähakse ette teadete esitamise asjaolud, vormingud ja menetlused vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 (mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist) artikli 61 lõikele 5 (ELT L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

c) ISO/IEC 18045:2008;

d) infotehnoloogia turvalisuse hindamise ühine metoodika, 5. läbivaatamine, versioon 3.1, mille on avaldanud IT-turbe valdkonna ühiskriteeriumide sertifikaatide tunnustamise kokkuleppe osalised.

3. Kuni 31. detsembrini 2027 võib EUCC alusel anda lõikes 1 osutatud standardeid kohaldades välja sertifikaadi, milles väidetakse vastavust kaitseprofiilile, mille puhul on kohaldatud lõikes 2 loetletud standardeid.

4. EUCC alusel võib lõikes 1 osutatud standardeid kohaldades välja anda ka sertifikaadi, milles väidetakse vastavust kaitseprofiilile, mille puhul on kohaldatud üht kahest järgmisest standardist, tingimusel et sellise kaitseprofiili kasutamine on nõutav vastavalt komisjoni rakendusmäärusele (EL) 2016/799, (*) Euroopa Parlamendi ja nõukogu määrusele (EL) nr 910/2014 (**) või komisjoni rakendusotsusele (EL) 2016/650 (***):

a) infotehnoloogia turvalisuse hindamise ühiskriteeriumid, versioon 3.1, 1.–4. läbivaatamine, mille on avaldanud IT-turbe valdkonna ühiskriteeriumide sertifikaatide tunnustamise kokkuleppe osalised;

b) infotehnoloogia turvalisuse hindamise ühine metoodika, versioon 3.1, 1.–4. läbivaatamine, mille on avaldanud IT-turbe valdkonna ühiskriteeriumide sertifikaatide tunnustamise kokkuleppe osalised.

_____

(*) Komisjoni 18. märtsi 2016. aasta rakendusmäärus (EL) 2016/799, millega rakendatakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 165/2014, millega sätestatakse sõidumeerikute ja nende komponentide konstruktsiooni, katsetamise, paigaldamise, kasutamise ja parandamise nõuded (ELT L 139, 26.5.2016, lk 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) 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, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Komisjoni 25. aprilli 2016. aasta rakendusotsus (EL) 2016/650, millega kehtestatakse kvalifitseeritud allkirja andmise ja templi loomise vahendi turvalisuse hindamise standardid vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 30 lõikele 3 ja artikli 39 lõikele 2 (ELT L 109, 26.4.2016, lk 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).“

3) IV peatükki lisatakse artikkel 20a järgmises sõnastuses:

„*Artikkel 20a*

Vastavushindamisasutuste akrediteerimise nõuete täpsustamine

Vastavushindamisasutuste akrediteerimisel võetakse arvesse sertifitseerimisasutuste ja infotehnoloogia turvalisuse hindamise üksuste akrediteerimise erinõudeid, mis on kehtestatud I lisa punktis 2 loetletud kohaldatavates tehnika taset käsitlevates dokumentides.“

4) Artiklid 23 ja 24 jäetakse välja.

5) Artiklisse 48 lisatakse lõige 4 järgmises sõnastuses:

„4. Kui I või II lisas ei ole sätestatud teisiti, kohaldatakse tehnika taset käsitlevaid dokumente alates selle muutmisakti kohaldamise kuupäevast, millega need I või II lisasse inkorporeeriti.“

6) Artiklisse 49 lisatakse lõige 4 järgmises sõnastuses:

„4. Kui lõikes 3 osutatud läbivaatamine viiakse läbi kahe aasta jooksul alates esialgse sertifikaadi väljastamisest ja kui sellise läbivaatamise tulemusel väljastatakse kooskõlas käesoleva määrusega uus sertifikaat, võib kohaldada artikli 3 lõikes 2 loetletud standardeid. Algse sertifikaadi väljaandmise kuupäevana käsitatakse kuupäeva, mil anti välja viimane sertifikaat IKT-tootele või kaitseprofiilile, millel kehtiv sertifikaat põhineb.“

7) I lisa asendatakse käesoleva määruse I lisas esitatud tekstiga.

8) IV lisa muudetakse vastavalt käesoleva määruse II lisale.

Artikkel 2

Rakendusmäärust (EL) 2024/482 parandatakse järgmiselt.

1) Artikli 5 lõike 1 punkt b asendatakse järgmisega:

„b) mida väidetakse IKT-protsessi osana sertifitseeritud kaitseprofiilile vastavaks, kui IKT-toode kuulub selle kaitseprofiiliga hõlmatud IKT-tootekategooriasse.“

2) Artiklit 8 parandatakse järgmiselt.

a) Pealkiri asendatakse järgmisega:

„Sertifitseerimiseks ja hindamiseks vajalik teave“;

b) lõige 1 asendatakse järgmisega:

„1. EUCC kohase sertifitseerimise taotleja esitab sertifitseerimisasutusele ja infotehnoloogia turvalisuse hindamise üksusele kogu sertifitseerimis- ja hindamistoiminguteks vajaliku teabe või teeb selle muul viisil kättesaadavaks.“

3) Artikkel 16 asendatakse järgmisega:

„*Artikkel 16*

Kaitseprofiili sertifitseerimiseks ja hindamiseks vajalik teave

Kaitseprofiili sertifitseerimise taotleja esitab sertifitseerimisasutusele ja infotehnoloogia turvalisuse hindamise üksusele kogu sertifitseerimis- ja hindamistoiminguteks vajaliku teabe täielikul ja õigel kujul või teeb selle muul viisil kättesaadavaks. Artikli 8 lõikeid 2, 3, 4 ja 7 kohaldatakse *mutatis mutandis*.“

4) Artikli 17 lõige 1 jäetakse välja.

5) Artikli 29 lõige 2 asendatakse järgmisega:

„2. Kui EUCC sertifikaadi omanik ei tee lõikes 1 osutatud ajavahemiku jooksul ettepanekut asjakohaste parandusmeetmete võtmiseks, siis sertifikaat peatatakse vastavalt artiklile 30 või tunnistatakse kehtetuks vastavalt artiklile 14 või artiklile 20.“

Artikkel 3

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

Artikli 1 lõiget 4 kohaldatakse alates 8. jaanuarist 2025.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 18. detsember 2024

Komisjoni nimel
president
Ursula VON DER LEYEN

I LISA

„„*I LISA*

Tehnilisi valdkondi toetavad tehnika taset käsitlevad dokumendid ja muud tehnika taset käsitlevad dokumendid

1. Tehnika taset käsitlevad dokumendid, mis toetavad tehnilisi valdkondi tasemetel AVA_VAN.4 ja AVA_VAN.5:

   a) järgmised tehnilise valdkonna „Kiipkaardid ja samalaadsed seadmed“ ühtlustatud hindamisega seotud dokumendid:

      1) „Infotehnoloogia turvalisuse hindamise üksuse miinimumnõuded kiipkaartide ja samalaadsete seadmete turvalisuse hindamiseks“, versioon 1.1;

      2) „Minimaalsed kohapealsed turvanõuded“, versioon 1.1;

      3) „Ühiskriteeriumide kohaldamine kiipide suhtes“, versioon 1.1;

      4) „Turvaarhitektuuri nõuded (ADV_ARC) kiipkaartidele ja samalaadsetele seadmetele“, versioon 1.1;

      5) „Avatud kiipkaarditoodete sertifitseerimine“, versioon 1.1;

      6) „Liittoodete hindamine kiipkaartide ja samalaadsete seadmete puhul“, versioon 1.1;

      7) „Ründepotentsiaali rakendamine kiipkaartide ja samalaadsete seadmete suhtes“, versioon 1.2.

   b) järgmised tehnilise valdkonna „Turvaümbrisega riistvaraseadmed“ ühtlustatud hindamisega seotud dokumendid:

      1) „Infotehnoloogia turvalisuse hindamise üksuse miinimumnõuded turvaümbrisega riistvaraseadmete turvalisuse hindamiseks“, versioon 1.1;

      2) „Minimaalsed kohapealsed turvanõuded“, versioon 1.1;

      3) „Ründepotentsiaali rakendamine turvaümbrisega riistvaraseadmete suhtes“, versioon 1.2.

2. Vastavushindamisasutuste ühtlustatud akrediteerimisega seotud tehnika taset käsitlevad dokumendid:

   a) „Infotehnoloogia turvalisuse hindamise üksuse akrediteerimine EUCC jaoks“, versioon 1.1, akrediteeringute puhul, mis on välja antud enne 8. juulit 2025.

   b) „Infotehnoloogia turvalisuse hindamise üksuse akrediteerimine EUCC jaoks“, versioon 1.6c, akrediteeringute puhul, mis on uued või läbi vaadatud pärast 8. juulit 2025.

   c) „Sertifitseerimisasutuste akrediteerimine EUCC jaoks“, versioon 1.6b.““

II LISA

Rakendusmääruse (EL) 2024/482 IV lisa IV.3 jao punktid 5 ja 6 asendatakse järgmisega:

„5. Kui sertifitseerimisasutus on kinnitanud, et muudatus on väike, ei anta muudetud IKT-tootele välja uut sertifikaati ja koostatakse algse sertifitseerimisaruande haldusaruanne.

Haldusaruanne lisatakse mõjuanalüüsi aruande alajaotisena, mis sisaldab järgmisi jaotisi:

a) sissejuhatus,

b) muudatuste kirjeldus,

c) mõjutatud arendaja tõendid.

6. Punktis 5 osutatud haldusaruanne esitatakse ENISA-le avaldamiseks küberturvalisuse sertifitseerimise veebisaidil.“