Euroopa Liidu
Nõukogu

Brüssel, 22. märts 2022
(OR. en)

Institutsioonidevaheline dokument: 2022/0085(COD)

7474/22
ADD 3

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

SAATEMÄRKUSED

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Martine DEPREZ, direktor
Kättesaamise kuupäev:	22. märts 2022
Saaja:	Jeppe TRANHOLM-MIKKELSEN, Euroopa Liidu Nõukogu peasekretär
Komisjoni dok nr:	SWD(2022) 68 final
Teema:	KOMISJONI TALITUSTE TÖÖDOKUMENT MÕJUANALÜÜSI KOKKUVÕTE Lisatud dokumendile: Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, millega nähakse ette meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes

Käesolevaga edastatakse delegatsioonidele dokument SWD(2022) 68 final.

Lisatud: SWD(2022) 68 final

EUROOPA
KOMISJON

Brüssel, 22.3.2022
SWD(2022) 68 final

KOMISJONI TALITUSTE TÖÖDOKUMENT

MÕJUANALÜÜSI KOKKUVÕTE

Lisatud dokumendile:

Ettepanek:
EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

millega nähakse ette meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes

{COM(2022) 122 final} - {SWD(2022) 67 final}

1. Sissejuhatus

2020. aastal suurenes järsult selliste liidu institutsioone, organeid ja asutusi mõjutanud oluliste intsidentide arv, mille panid toime kinnisründeohu (*advanced persistent threat*) subjektid. See kajastub ka CERT-EU poolt 2020. aastal analüüsitud ekspertiisitõmmiste arvus, mis 2019. aastaga võrreldes enam kui kolmekordistus, samal ajal kui oluliste intsidentide arv suurenes alates 2018. aastast rohkem kui kümme korda.

Liidu institutsioonide, organite ja asutuste küberturvalisusalane suutlikkus ja kulutused IT turvalisusele on mõnel juhul silmatorkavalt ebavõrdsed, mistõttu on liidu institutsioonide, organite ja asutuste küberturvalisuse küpsuse tase väga erinev. Lisaks näitavad ohtude analüüs ja IT turvalisuse intsidentide statistika, et liidu institutsioonide, organite ja asutuste kokkupuude küberohtudega üksnes suureneb.

2. Eesmärgid

Tuvastatud puudused toovad lõpuks kaasa ebapiisava kübervastupidavusvõime liidu institutsioonides, organites ja asutustes, IT turvalisusele ressursside killustatud eraldamise ja IT valdkonna tasakaalustamata riskiseisundi.

Seadusandliku akti eesmärk oleks näha ette meetmed, millega tagada küberturvalisuse ühtlaselt kõrge tase liidu institutsioonides, organites ja asutustes. See soodustaks ja tagaks, et küberturvalisuse küpsus peab sammu liidu institutsioonide, organite ja asutuste kiireneva digiüleminekuga.

3. Institutsioonidevaheline küberturvalisuse nõukogu ja küberturvalisuse raamistik

Institutsioonidevahelise küberturvalisuse nõukogu ja küberturvalisuse raamistiku ettepanekuga pakutakse välja meetmed, et tagada küberturvalisuse ühtlaselt kõrge tase liidu institutsioonides, organites ja asutustes, võimaldades kooskõlastamist sellise raamistiku alusel, mis käsitleb kõigi liidu institutsioonide, organite ja asutuste küberturvalisusega seotud ohte, ning nähakse ette järelevalve ja intsidentidest teatamine institutsioonidevahelisele küberturvalisuse nõukogule.

Ettepanekuga soovitakse ajakohastada CERT-EU volitusi ja ülesandeid, võttes arvesse viimastel aastatel toimunud liidu institutsioonide, organite ja asutuste muutunud ja suurenenud digiüleminekut ja küberturvalisusega seotud muutuvat ohumaastikku.

Otsest mõju või eelarvelisi tagajärgi liikmesriikidele või ELi kodanikele ei ole.

Määruse õiguslik alus on Euroopa Liidu toimimise lepingu artikkel 298, millega on ette nähtud, et liidu institutsioone, organeid ja asutusi abistab nende ülesannete täitmisel avatud, tõhus ja sõltumatu Euroopa halduskorraldus.

Käesolev ettepanek tugineb ELi julgeolekuliidu strateegiale (COM(2020) 605 final) ja ELi küberturvalisuse strateegiale digikümnendi jaoks (JOIN(2020) 18 final).

4. Kokkuvõte

Institutsioonidevahelise küberturvalisuse nõukogu tööga ja küberturvalisuse raamistikuga saavutatakse enamik kavandatud eesmärke suhteliselt tulemuslikult, tõhusalt ja muude liidu poliitikavaldkondadega sidusalt ning sidusrühmade kõige ulatuslikuma toetusega. See valitud lahendus on kõige paremini teostatav, arvestades kehtivaid õiguslikke piire, mille raames me tegutseme, ning kuna kõigile sobiv lähenemisviis ei vastaks liidu institutsioonide, organite ja

asutuste praegusele ebaühtlasele küpsusele ning nende ees seisvate tehnoloogiliste riskide ja intsidentide keerukuse erinevustele.