Euroopa Liidu
Nõukogu

Brüssel, 22. märts 2022
(OR. en)

Institutsioonidevaheline dokument: 2022/0085(COD)

7474/22
ADD 1

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

ETTEPANEK

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Martine DEPREZ, direktor
Kättesaamise kuupäev:	22. märts 2022
Saaja:	Jeppe TRANHOLM-MIKKELSEN, Euroopa Liidu Nõukogu peasekretär
Komisjoni dok nr:	COM(2022) 122 final - Annexes
Teema:	LISAD järgmise dokumendi juurde: Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, millega nähakse ette meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes

Käesolevaga edastatakse delegatsioonidele dokument COM(2022) 122 final - Annexes.

Lisatud: COM(2022) 122 final - Annexes

EUROOPA
KOMISJON

Brüssel, 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

LISAD

järgmise dokumendi juurde:

Ettepanek:
EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

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

{SWD(2022) 67 final} - {SWD(2022) 68 final}

I LISA

Küberturvalisuse baastase puudutab järgmisi valdkondi:

(1) küberturvalisuse poliitika, sh võrgu- ja infosüsteemide turvalisuse eesmärgid ja prioriteedid, eeskätt seoses pilvandmetöötlusteenuste kasutamisega (direktiivi [küberturvalisuse 2. direktiivi ettepanek] artikli 4 lõike 19 tähenduses) ja kaugtöö võimaldamise tehnilise korraldusega;

(2) küberturvalisuse korraldamine, sh ülesannete ja kohustuste määratlemine;

(3) varade haldamine, sh IT-varade inventeerimine ja IT-võrgu kaardistamine;

(4) juurdepääsukontroll;

(5) tegevuse turvalisus;

(6) teabeedastuse turvalisus;

(7) süsteemi soetamine, arendamine ja hooldamine;

(8) suhted pakkujatega;

(9) intsidentide haldamine, sh lähenemisviisid, et parandada intsidentideks valmisolekut, neile reageerimist ja neist taastumist, ning koostöö CERT-EUga, nt turvaseire ja logimise käigushoidmine;

(10) toimepidevuse haldamine ja kriisiohje ning

(11) küberturvalisuse alane haridus, teadlikkuse suurendamine ja koolitusprogrammid.

II LISA

Liidu institutsioonid, organid ja asutused käsitlevad küberturvalisuse baastaseme rakendamisel ja oma küberturvalisuse kavades vähemalt järgmisi konkreetseid küberturvalisuse meetmeid kooskõlas IICB juhenddokumentide ja soovitustega:

(1) konkreetsed sammud, et liikuda nullusaldusega arhitektuuri suunas (s.o turvalisuse mudel, süsteemi projekteerimise põhimõtted ja küberturvalisuse ja süsteemihalduse koordineeritud strateegia, mis põhinevad tõdemusel, et ohud eksisteerivad nii sees- kui ka väljaspool tavapäraseid võrgupiire);

(2) mitmeteguriline autentimise kui normi kasutuselevõtt võrgu- ja infosüsteemides;

(3) tarkvara tarneahela turvalisuse tagamine tarkvara turvalise arendamise ja hindamise kriteeriumidega;

(4) hanke-eeskirjade tõhustamine, et soodustada küberturvalisuse ühtlaselt kõrget taset järgmiste vahenditega:

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

   (b) lepinguline kohustus teatada intsidentidest, nõrkustest ja küberohtudest ning tagada asjakohane reageerimine intsidentidele ja seire.