Euroopan unionin neuvosto

Bryssel, 22. maaliskuuta 2022
(OR. en)

7474/22
ADD 3

Toimielinten välinen asia:
2022/0085(COD)

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

SAATE

Lähettäjä:	Euroopan komission pääsihteeri, allekirjoittajana johtaja Martine DEPREZ
Saapunut:	22. maaliskuuta 2022
Vastaanottaja:	Jeppe TRANHOLM-MIKKELSEN, Euroopan unionin neuvoston pääsihteeri
Kom:n asiak. nro:	SWD(2022) 68 final
Asia:	KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA TIIVISTELMÄ VAIKUTUSTENARVIOINNISTA Oheisasiakirja ehdotukseen EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa

Valtuuskunnille toimitetaan oheisena asiakirja SWD(2022) 68 final.

Liite: SWD(2022) 68 final

EUROOPAN
KOMISSIO

Bryssel 22.3.2022
SWD(2022) 68 final

KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA

TIIVISTELMÄ VAIKUTUSTENARVIOINNISTA

Oheisasiakirja

ehdotukseen EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI

toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa

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

1. Johdanto

Kohdistettuja hyökkäyksiä (APT) suorittavien toimijoiden toteuttamien, unionin toimielimiin, elimiin ja virastoihin vaikuttaneiden merkittävien poikkeamien määrä kasvoi merkittävästi vuonna 2020. Tämä näkyi myös CERT-EU:n vuonna 2020 analysoimien forensisten peilikuvatiedostojen määrässä, joka yli kolminkertaistui vuodesta 2019. Samalla merkittävien poikkeamien määrä yli kymmenkertaistui vuodesta 2018.

Unionin toimielinten, elinten ja virastojen kyberturvallisuusvalmiudet ja tietotekniikan turvallisuuteen osoitetut määrärahat ovat joissakin tapauksissa hyvin eritasoisia, minkä seurauksena kyberturvallisuuden kehitystasot vaihtelevat laajasti unionin toimielimissä, elimissä ja virastoissa. Lisäksi uhkaympäristöä koskeva analyysi ja tietotekniikan turvapoikkeamia koskevat tilastot osoittavat, että kyberuhkille altistuminen unionin toimielimissä, elimissä ja virastoissa tulee vain kasvamaan jatkossa.

2. Tavoitteet

Havaittujen puutteiden seurauksena on lopulta se, että kyberuhkien sietokyky unionin toimielimissä, elimissä ja virastoissa on riittämätöntä, tietotekniikan turvallisuuden resursointi on pirstaloitunutta ja tietotekniikan turvallisuustasot ovat epätasapainossa.

Säädöksen tavoitteena on saada aikaan toimenpiteitä, joilla voidaan varmistaa yhteinen korkea kyberturvataso unionin toimielimissä, elimissä ja virastoissa. Tämä edistäisi kyberturvallisuuden kehitystasoa ja varmistaisi, että se pysyy unionin toimielinten, elinten ja virastojen kiihtyvän digitalisaation tahdissa.

3. Toimielinten välinen kyberturvallisuuslautakunta ja kyberturvallisuuskehys

Ehdotetulla asetuksella, joka koskee toimielinten välistä kyberturvallisuuslautakuntaa ja kyberturvallisuuskehystä, otetaan käyttöön toimenpiteitä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja virastoissa. Tavoitteena on mahdollistaa kyberturvallisuuden yhdenmukaistaminen kaikkien unionin toimielinten, elinten ja virastojen kyberuhat kattavan kehyksen puitteissa. Lisäksi ehdotetussa asetuksessa säädetään seurannasta ja raportoinnista toimielinten väliselle kyberturvallisuuslautakunnalle.

Ehdotuksella nykyaikaistetaan CERT-EU:n toimeksiantoa ja tehtäviä ottaen huomioon unionin toimielinten, elinten ja virastojen digitalisaatiossa viime vuosina tapahtuneet muutokset ja edistyminen sekä alati muuttuva kyberuhkaympäristö.

Ehdotuksella ei ole suoria tai talousarviovaikutuksia jäsenvaltioihin tai EU:n kansalaisiin.

Asetuksen oikeusperusta on Euroopan unionin toiminnasta tehdyn sopimuksen 298 artikla, jossa määrätään, että ”unionin toimielimet, elimet ja laitokset tukeutuvat tehtäviään hoitaessaan avoimeen, tehokkaaseen ja riippumattomaan eurooppalaiseen hallintoon”.

Ehdotus perustuu EU:n turvallisuusunionistrategiaan (COM(2020) 605 final) ja EU:n kyberturvallisuusstrategiaan digitaaliselle vuosikymmenelle (JOIN(2020) 18 final).

4. Päätelmät

Toimielinten välisellä kyberturvallisuuslautakunnalla ja kyberturvallisuuskehyksellä saavutetaan suurin osa asetetuista tavoitteista suhteellisen vaikuttavalla, tehokkaalla ja muiden unionin toimintapolitiikkojen kanssa johdonmukaisella tavalla sekä laajimmalla sidosryhmien tuella. Valittu ratkaisu on toteuttamiskelpoisin vaihtoehto vallitsevien oikeudellisten rajojen puitteissa. Lisäksi yhdellä yhteisellä toimintamallilla ei voitaisi puuttua

unionin toimielinten, elinten ja virastojen nykyisiin eri kehitystasoihin tai eroihin niihin kohdistuvissa teknologiariskeissä ja monimutkaisuuden tasoissa.