Euroopan unionin neuvosto

Bryssel, 22. maaliskuuta 2022
(OR. en)

**7474/22**
**ADD 1**

**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**

**EHDOTUS**

| | |
|---|---|
| Lähettäjä: | Euroopan komission pääsihteeri, allekirjoittajana johtaja Martine DEPREZ |
| Saapunut: | 22. maaliskuuta 2022 |
| Vastaanottaja: | Jeppe TRANHOLM-MIKKELSEN, Euroopan unionin neuvoston pääsihteeri |
| Kom:n asiak. nro: | COM(2022) 122 final – Liitteet |
| Asia: | LIITTEET asiakirjaan Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa |

Valtuuskunnille toimitetaan oheisena asiakirja COM(2022) 122 final – Liitteet.

Liite: COM(2022) 122 final – Liitteet

EUROOPAN
KOMISSIO

Bryssel 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

# LIITTEET

**asiakirjaan**

**Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI**

**toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa**

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

# LIITE I

Kyberturvallisuuden perustasossa otetaan huomioon seuraavat osa-alueet:

(1) kyberturvallisuuspolitiikka, mukaan lukien verkko- ja tietojärjestelmien turvallisuutta koskevat tavoitteet ja painopisteet erityisesti pilvipalvelujen käytön (direktiivin [ehdotus tarkistetuksi verkko- ja tietoturvadirektiiviksi] 4 artiklan 19 kohdan mukaisesti) sekä etätyön mahdollistamiseksi toteutettujen teknisten järjestelyjen osalta;

(2) kyberturvallisuuden organisointi, mukaan lukien tehtävien ja vastuualueiden määrittely;

(3) resurssien hallinta, mukaan lukien tietoteknisten resurssien inventointi ja tietoverkkojen kartoitus;

(4) käyttöoikeuksien hallinta;

(5) operatiivinen turvallisuus;

(6) tietoliikenneturvallisuus;

(7) järjestelmien hankinta, kehittäminen ja ylläpito;

(8) suhteet tavarantoimittajiin;

(9) poikkeamien hallinta, mukaan lukien toimintamallit, joilla parannetaan poikkeamiin varautumista ja reagoimista ja niistä toipumista sekä yhteistyötä CERT-EU:n kanssa, kuten turvallisuuden seurannan ja kirjaamisen ylläpito;

(10) toiminnan jatkuvuuden ja kriisitilanteiden hallinta; ja

(11) kyberturvallisuuteen liittyvät opetus-, tiedotus- ja koulutusohjelmat.

## LIITE II

Unionin toimielimet, elimet ja virastot ottavat IICB:n ohjeasiakirjojen ja suositusten mukaisesti kyberturvallisuuden perustason toteutuksessa ja kyberturvallisuussuunnitelmissaan huomioon ainakin seuraavat erityiset kyberturvallisuustoimenpiteet:

(1) konkreettiset toimet nollaluottamusarkkitehtuuriin (zero trust architecture) siirtymiseksi (eli tietoturvamalli, järjestelmäsuunnittelun periaatteet sekä koordinoitu kyberturvallisuus- ja järjestelmänhallintastrategia, jonka pohjana on se, että uhkia esiintyy sekä perinteisten verkkorajojen sisä- että ulkopuolella);

(2) monivaiheisen tunnistuksen käyttöönotto yleiskäytäntönä kaikissa verkko- ja tietojärjestelmissä;

(3) ohjelmistojen toimitusketjun turvallisuuden varmistaminen ohjelmistokehityksessä ja ohjelmistojen arvioinnissa sovellettavien turvallisuuskriteerien avulla;

(4) julkisia hankintoja koskevien sääntöjen parantaminen yhteisen korkean kyberturvatason edistämiseksi

   (a) sellaisten sopimuksista johtuvien esteiden poistaminen, jotka rajoittavat tietotekniikan palveluntarjoajien mahdollisuuksia jakaa tietoja poikkeamista, haavoittuvuuksista ja kyberuhkista CERT-EU:n kanssa;

   (b) sopimusehdot, jotka velvoittavat raportoimaan poikkeamista, haavoittuvuuksista ja kyberuhkista sekä huolehtimaan siitä, että käytössä on asianmukainen poikkeamiin reagoiminen ja seuranta.