Svet
Evropske unije

Bruselj, 22. marec 2022
(OR. en)

**Medinstitucionalna zadeva:**
**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**

**PREDLOG**

| | |
|---|---|
| Pošiljatelj: | za generalno sekretarko Evropske komisije:<br>direktorica Martine DEPREZ |
| Datum prejema: | 22. marec 2022 |
| Prejemnik: | generalni sekretar Sveta Evropske unije Jeppe TRANHOLM-MIKKELSEN |
| Št. dok. Kom.: | COM(2022) 122 final - Annexes |
| Zadeva: | PRILOGI k predlogu UREDBE EVROPSKEGA PARLAMENTA IN SVETA o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije |

Delegacije prejmejo priloženi dokument COM(2022) 122 final - Annexes.

Priloga: COM(2022) 122 final - Annexes

EVROPSKA
KOMISIJA

Bruselj, 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

**PRILOGI**

**k**

**predlogu UREDBE EVROPSKEGA PARLAMENTA IN SVETA**

**o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije**

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

## PRILOGA I

V osnovnih ukrepih za kibernetsko varnost se obravnavajo naslednja področja:

(1) politika na področju kibernetske varnosti, vključno s cilji in prednostnimi nalogami za varnost omrežij in informacijskih sistemov, zlasti v zvezi z uporabo storitev računalništva v oblaku (smislu člena 4(19) Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov]) in tehničnimi ureditvami za omogočanje dela na daljavo;

(2) organizacija kibernetske varnosti, vključno z opredelitvijo vlog in odgovornosti;

(3) upravljanje sredstev, vključno s popisom sredstev IT in kartografijo omrežja IT;

(4) nadzor dostopa;

(5) varnost operacij;

(6) varnost komunikacij;

(7) nakup, razvoj in vzdrževanje sistemov;

(8) odnosi z dobavitelji;

(9) obvladovanje incidentov, vključno s pristopi za izboljšanje pripravljenosti na incidente, odzivanje nanje in okrevanje po njih, ter s sodelovanjem s CERT-EU, kot je ohranjanje varnostnega spremljanja in vodenja dnevnikov;

(10) upravljanje neprekinjenega poslovanja in krizno upravljanje, ter

(11) izobraževanje, ozaveščanje in programi usposabljanja na področju kibernetske varnosti.

## PRILOGA II

Institucije, organi in agencije Unije pri izvajanju osnovnih ukrepov za kibernetsko varnost in v svojih načrtih za kibernetsko varnost v skladu s smernicami in priporočili IICB obravnavajo vsaj naslednje specifične ukrepe za kibernetsko varnost:

(1) konkretne ukrepe za prehod na arhitekturo ničelnega zaupanja (ki pomeni varnostni model, sklop načel zasnove sistemov ter usklajeno strategijo za kibernetsko varnost in upravljanje sistema na podlagi zavedanja, da grožnje obstajajo znotraj tradicionalnih meja omrežja in zunaj njih);

(2) sprejetje večfaktorske avtentifikacije kot norme v omrežjih in informacijskih sistemih;

(3) vzpostavitev varnosti dobavne verige programske opreme z merili za varni razvoj in oceno programske opreme;

(4) okrepitev pravil o javnem naročanju za omogočanje visoke skupne ravni kibernetske varnosti:

   (a) z odpravo pogodbenih ovir, ki omejujejo izmenjavo informacij med ponudniki storitev IT in CERT-EU o incidentih, šibkih točkah in kibernetskih grožnjah;

   (b) s pogodbenimi obveznostmi glede poročanja o incidentih, šibkih točkah in kibernetskih grožnjah ter glede vzpostavitve ustreznega odzivanja na incidente in njihovega spremljanja.