Vijeće
Europske unije

Bruxelles, 22. ožujka 2022.
(OR. en)

Međuinstitucijski predmet:
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

PRIJEDLOG

Od:	Glavna tajnica Europske komisije, potpisala direktorica Martine DEPREZ
Datum primitka:	22. ožujka 2022.
Za:	Jeppe TRANHOLM-MIKKELSEN, glavni tajnik Vijeća Europske unije
Br. dok. Kom.:	COM(2022) 122 final - Annexes
Predmet:	PRILOZI Prijedlogu uredbe EUROPSKOG PARLAMENTA I VIJEĆA o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije

Za delegacije se u prilogu nalazi dokument COM(2022) 122 final - Annexes.

Priloženo: COM(2022) 122 final - Annexes

EUROPSKA
KOMISIJA

Bruxelles, 22.3.2022.
COM(2022) 122 final

ANNEXES 1 to 2

PRILOZI

Prijedlogu uredbe EUROPSKOG PARLAMENTA I VIJEĆA

o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije

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

PRILOG I.

Područja kojima se treba posvetiti u osnovnom okviru za kibersigurnost:

(1) politika kibersigurnosti, uključujući ciljeve i prioritete za sigurnost mrežnih i informacijskih sustava, posebno kad je riječ o korištenju usluga računalstva u oblaku (u smislu članka 4. stavka 19. Direktive [prijedlog NIS 2]) i tehničkim rješenjima za omogućivanje rada na daljinu;

(2) organizacija kibersigurnosti, uključujući definiranje uloga i odgovornosti;

(3) upravljanje imovinom, uključujući popis informatičke imovine i kartografiju informatičke mreže;

(4) kontrola pristupa;

(5) sigurnost operacija;

(6) sigurnost komunikacija;

(7) nabava, razvoj i održavanje sustava;

(8) odnosi s dobavljačima;

(9) upravljanje incidentima, uključujući pristupe za poboljšanje pripravnosti, odgovora na incidente i oporavka od njih te suradnju s CERT-EU-om, primjerice održavanje nadzora nad sigurnošću i vođenje evidencije o njoj;

(10) upravljanje kontinuitetom poslovanja i upravljanje krizama; i

(11) programi obrazovanja, informiranja i osposobljavanja u području kibersigurnosti.

PRILOG II.

Pri provedbi osnovnog okvira za kibersigurnost te u svojim planovima za kibersigurnost institucije, tijela i agencije Unije bavit će se barem sljedećim specifičnim kibersigurnosnim mjerama, u skladu sa smjernicama i preporukama IICB-a:

(1) konkretnim koracima prema uspostavi arhitekture nultog povjerenja (što znači sigurnosni model, skup načela za projektiranje sustava te koordinirana strategija za kibersigurnost i upravljanje sustavom koji se temelje na priznavanju postojanja prijetnji unutar i izvan tradicionalnih granica mreže);

(2) primjenom dvostruke autentifikacije kao norme u mrežnim i informacijskim sustavima;

(3) uspostavljanjem sigurnosti lanca opskrbe softverom s pomoću kriterija za siguran razvoj i evaluaciju softvera;

(4) poboljšanjem pravila javne nabave kako bi se olakšalo postizanje visoke zajedničke razine kibersigurnosti:

   (a) uklanjanjem ugovornih prepreka koje pružateljima informatičkih usluga otežavaju razmjenu informacija o incidentima, ranjivostima i kiberprijetnjama s CERT-EU-om;

   (b) ugovornom obvezom prijavljivanja incidenata, ranjivosti i kiberprijetnji te uspostavljanja odgovarajućeg odgovora na incidente i praćenja incidenata.