Consiliul
Uniunii Europene

Bruxelles, 22 martie 2022
(OR. en)

7474/22
ADD 1

Dosar interinstituțional:
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

PROPUNERE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	22 martie 2022
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2022) 122 final - Annexes
Subiect:	ANEXE la Propunerea de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii

În anexă, se pune la dispoziția delegațiilor documentul COM(2022) 122 final - Annexes.

Anexă: COM(2022) 122 final - Annexes

COMISIA
EUROPEANĂ

Bruxelles, 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

ANEXE

la

Propunerea de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii

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

ANEXA I

Domeniile următoare trebuie abordate în cadrul nivelului de referință în materie de securitate cibernetică:

(1) politica de securitate cibernetică, inclusiv obiectivele și prioritățile privind securitatea rețelelor și a sistemelor informatice, în special în ceea ce privește utilizarea serviciilor de cloud computing [în sensul articolului 4 punctul 19 din (propunerea de Directivă NIS 2)] și modalitățile tehnice care să permită telemunca;

(2) organizarea securității cibernetice, inclusiv definirea rolurilor și a responsabilităților;

(3) gestionarea activelor, inclusiv inventarul activelor informatice și cartografierea rețelelor informatice;

(4) controlul accesului;

(5) securitatea operațiunilor;

(6) securitatea comunicațiilor;

(7) achiziționarea, dezvoltarea și întreținerea de sisteme;

(8) relațiile cu furnizorii;

(9) gestionarea incidentelor, inclusiv abordări privind îmbunătățirea gradului de pregătire, a răspunsului la incidente și a capacității de recuperare în urma acestora, precum și cooperarea cu CERT-UE, cum ar fi monitorizarea și jurnalizarea evenimentelor de securitate;

(10) gestionarea continuității activității și gestionarea crizelor și

(11) programe de educație, sensibilizare și formare în materie de securitate cibernetică.

ANEXA II

Instituțiile, organele și agențiile Uniunii abordează cel puțin următoarele măsuri specifice de securitate cibernetică când implementează nivelul de referință în materie de securitate cibernetică și când își concep planurile de securitate cibernetică, în conformitate cu documentele de orientare și recomandările din partea IICB:

(1) pași concreți înspre o arhitectură bazată pe modelul de încredere zero (zero trust), care înseamnă un model de securitate, un set de principii de proiectare a sistemului și o strategie coordonată de gestionare a securității cibernetice și a sistemului, bazată pe recunoașterea faptului că există amenințări atât în interiorul, cât și în afara granițelor tradiționale ale rețelei;

(2) adoptarea autentificării multifactor ca normă pentru toate rețelele și sistemele informatice;

(3) asigurarea securității lanțului de aprovizionare cu software prin criterii de dezvoltare și evaluare securizată a software-ului

(4) consolidarea normelor privind achizițiile publice pentru a facilita un nivel comun ridicat de securitate cibernetică prin:

   (a) eliminarea barierelor contractuale care limitează schimbul de informații între furnizorii de servicii informatice și CERT-UE cu privire la incidente, vulnerabilități și amenințări cibernetice

   (b) obligația contractuală de a raporta incidentele, vulnerabilitățile și amenințările cibernetice, precum și de a institui măsuri adecvate de răspuns la incidente și de monitorizare a acestora.