Raad van de
Europese Unie

Brussel, 22 maart 2022
(OR. en)

7474/22
ADD 1

Interinstitutioneel dossier:
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

VOORSTEL

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
ingekomen:	22 maart 2022
aan:	de heer Jeppe TRANHOLM-MIKKELSEN, secretaris-generaal van de Raad van de Europese Unie
nr. Comdoc.:	COM(2022) 122 final - Annexes
Betreft:	BIJLAGEN bij het Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie

Hierbij gaat voor de delegaties document COM(2022) 122 final - Annexes.

Bijlage: COM(2022) 122 final - Annexes

EUROPESE
COMMISSIE

Brussel, 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

BIJLAGEN

bij het

Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie

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

BIJLAGE I

Het basisniveau van cyberbeveiliging heeft betrekking op de volgende domeinen:

(1) cyberbeveiligingsbeleid, inclusief doelen en prioriteiten voor de beveiliging van netwerk- en informatiesystemen, met name inzake het gebruik van cloudcomputingdiensten (in de zin van artikel 4, punt 19, van richtlijn [NIS 2-voorstel]) en technische regelingen om thuiswerken mogelijk te maken;

(2) de organisatie van cyberbeveiliging, inclusief de definitie van rollen en verantwoordelijkheden;

(3) activabeheer, inclusief een inventaris van IT-activa en IT-netwerkarchitectuur;

(4) toegangscontrole;

(5) operationele beveiliging;

(6) communicatiebeveiliging;

(7) aankoop, ontwikkeling en onderhoud van systemen;

(8) leveranciersrelaties;

(9) incidentbeheer, inclusief benaderingen om de paraatheid bij, het reageren op en het herstel van incidenten en de samenwerking met CERT-EU te verbeteren, zoals het onderhoud van beveiligingsmonitoring en -registratie;

(10) bedrijfscontinuïteitsbeheer en crisisbeheer; en

(11) voorlichting over cyberbeveiliging, bewustmaking en opleidingsprogramma's.

BIJLAGE II

De instellingen, organen en agentschappen van de Unie behandelen ten minste de volgende specifieke cyberbeveiligingsmaatregelen bij de uitvoering van het basisniveau van cyberbeveiliging en in hun cyberbeveiligingsplannen, conform de richtsnoeren en aanbevelingen van de IICB:

(1) concrete stappen in de richting van een Zero Trust-architectuur (een beveiligingsmodel, systeemontwerpbeginselen en een gecoördineerde strategie voor cyberbeveiliging en systeembeheer op basis van de onderkenning dat er zowel binnen als buiten de traditionele netwerkgrenzen dreigingen bestaan);

(2) de invoering van multifactorauthenticatie als norm in alle netwerk- en informatiesystemen;

(3) de totstandbrenging van een veilige toeleveringsketen voor software, door middel van criteria voor de ontwikkeling en evaluatie van veilige software;

(4) betere aanbestedingsregels om een hoog gezamenlijk niveau van cyberbeveiliging te bevorderen door:

  (a) contractuele belemmeringen weg te nemen die informatie-uitwisseling tussen IT-serviceverleners over incidenten, kwetsbaarheden en cyberdreigingen met CERT-EU beperken;

  (b) contractueel te bepalen dat incidenten, kwetsbaarheden en cyberdreigingen moeten worden gemeld, en door een passende respons en passend toezicht op incidenten mogelijk te maken.