Raad van de
Europese Unie

Brussel, 22 maart 2022
(OR. en)

7474/22
ADD 3

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

BEGELEIDENDE NOTA

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.:	SWD(2022) 68 final
Betreft:	WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE SAMENVATTING VAN DE EFFECTBEOORDELING 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 SWD(2022) 68 final.

Bijlage: SWD(2022) 68 final

EUROPESE
COMMISSIE

Brussel, 22.3.2022
SWD(2022) 68 final

WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE

SAMENVATTING VAN DE EFFECTBEOORDELING

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

{COM(2022) 122 final} - {SWD(2022) 67 final}

1. Inleiding

In 2020 is het aantal door advanced persistent threat-actoren uitgevoerde significante incidenten met gevolgen voor de instellingen, organen en instanties van de Unie dramatisch gestegen. Dit is goed te zien aan het aantal door CERT-EU in 2020 geanalyseerde forensische beelden, dat meer dan verdrievoudigd was ten opzichte van 2019, en het aantal significante incidenten, dat sinds 2018 meer dan vertienvoudigd is.

De uitgaven voor cyberbeveiligingscapaciteit en IT-beveiliging in de instellingen, organen en instanties van de Unie lopen in sommige gevallen echter sterk uiteen, wat leidt tot een breed spectrum van maturiteitsniveaus op het gebied van cyberbeveiliging tussen de instellingen, organen en instanties van de Unie. Bovendien blijkt uit de dreigingslandschapsanalyse en de statistieken over IT-beveiligingsincidenten dat de cyberblootstelling van de instellingen, organen en instanties van de Unie alleen maar zal toenemen.

2. Doelstellingen

De vastgestelde tekortkomingen leiden uiteindelijk tot een ontoereikend niveau van cyberweerbaarheid in de instellingen, organen en instanties van de Unie, tot gefragmenteerde middelen voor IT-beveiliging en tot onevenwichtige IT-beveiligingsposities.

De wetgevingshandeling beoogt in maatregelen te voorzien voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie. Dit waarborgt en bevordert dat de maturiteit op het gebied van cyberbeveiliging gelijke tred houdt met de versnellende digitalisering van de instellingen, organen en instanties van de Unie.

3. Een interinstitutionele raad voor cyberbeveiliging en een cyberbeveiligingskader

Met het voorstel voor een interinstitutionele raad voor cyberbeveiliging en een cyberbeveiligingskader worden maatregelen ingevoerd voor een hoog gezamenlijk niveau van cyberbeveiliging binnen de instellingen, organen en instanties van de Unie, waardoor afstemming mogelijk wordt rond een kader dat de cyberdreigingen van de instellingen, organen en instanties van de Unie aanpakt; ook worden met het voorstel monitoring en rapportage aan een interinstitutionele raad voor cyberbeveiliging ingesteld.

Het voorstel moderniseert de missie en de taken van CERT-EU en houdt rekening met de veranderde en toegenomen digitalisering van de instellingen, organen en instanties van de Unie in de afgelopen jaren, en met het veranderende dreigingslandschap op het gebied van cyberbeveiliging.

Er zijn geen rechtstreekse of budgettaire gevolgen voor de lidstaten of de EU-burgers.

De rechtsgrondslag voor de verordening is artikel 298 van het Verdrag betreffende de werking van de Europese Unie, dat bepaalt dat de instellingen, organen en instanties van de Unie bij de vervulling van hun taken steunen op een open, doeltreffend en onafhankelijk Europees ambtenarenapparaat.

Dit voorstel bouwt voort op de EU-strategie voor de veiligheidsunie (COM(2020) 605 final) en de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk (JOIN(2020) 18 final).

4. Conclusie

Middels een interinstitutionele raad voor cyberbeveiliging en een cyberbeveiligingskader worden de meeste van de beoogde doelstellingen op een verhoudingsgewijs doeltreffende,

efficiënte en met andere beleidsmaatregelen van de Unie samenhangende wijze bereikt, met de ruimste steun van de belanghebbenden. Deze gekozen oplossing is de best haalbare optie, gezien de bestaande juridische grenzen waarbinnen wij handelen; verder zou een uniforme aanpak noch tegemoetkomen aan de huidige uiteenlopende maturiteit van de instellingen, organen en instanties van de Unie, noch aan de verschillen in technologische risico's en complexiteit waarmee zij worden geconfronteerd.