Raad van de
Europese Unie

Brussel, 22 maart 2022
(OR. en)

7474/22

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
Betreft:	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.

Bijlage: COM(2022) 122 final

EUROPESE
COMMISSIE

Brussel, 22.3.2022
COM(2022) 122 final

2022/0085 (COD)

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}

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

• Motivering en doel van het voorstel

Bij dit voorstel wordt een kader voor gemeenschappelijke voorschriften en maatregelen voor cyberbeveiliging binnen de instellingen, organen en instanties van de Unie opgericht. Het voorstel beoogt de weerbaarheid van alle entiteiten en de responscapaciteit bij incidenten verder te verbeteren. Het sluit aan bij de prioriteiten van de Commissie om Europa klaar te maken voor het digitale tijdperk en een toekomstbestendige economie op te bouwen die werkt voor de mensen. Bovendien is de zorg voor een veilig en veerkrachtig openbaar bestuur een hoeksteen van de digitale transformatie van de samenleving in haar geheel.

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).

Het voorstel moderniseert het bestaande rechtskader van CERT-EU en houdt rekening met de veranderde en toegenomen digitalisering van de instellingen, organen en instanties in de afgelopen jaren, en met de veranderende dreigingen op het gebied van cyberbeveiliging. Beide ontwikkelingen zijn verder versterkt sinds het begin van de COVID-19-crisis, terwijl het aantal incidenten blijft toenemen, met steeds complexere aanvallen vanuit uiteenlopende bronnen.

Het voorstel doopt CERT-EU om van “computercrisisteam” in “cyberbeveiligingscentrum” voor de instellingen, organen en instanties van de Unie, conform de ontwikkelingen in de lidstaten en wereldwijd, waar veel CERT’s worden omgedoopt tot cyberbeveiligingscentra; de korte naam “CERT-EU” blijft vanwege de herkenbaarheid evenwel behouden.

• Samenhang met bestaand beleid op het betrokken gebied

Dit voorstel is erop gericht de cyberbeveiligingsweerbaarheid van de instellingen, organen en instanties van de Unie tegen cyberdreigingen te verbeteren en in overeenstemming te brengen met de bestaande wetgeving:

- Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie. Het is ook in overeenstemming met het voorstel voor een richtlijn (EU) XXX/XXX betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148 [NIS 2-voorstel];
- Verordening (EU) 2019/881 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging) en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie (de cyberbeveiligingsverordening);
- Voorstel voor een verordening (EU) XXX/XXX betreffende informatiebeveiliging in de instellingen, organen en instanties van de Unie;
- de aanbeveling van de Commissie van 23 juni 2021 betreffende de opbouw van een gezamenlijke cybereenheid;
- Aanbeveling (EU) 2017/1584 van de Commissie van 13 september 2017 inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises.

De bijlage bij Aanbeveling (EU) 2017/1584 van de Commissie van 13 september 2017 inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises bevat de blauwdruk

voor een gecoördineerde respons op grensoverschrijdende grootschalige cyberincidenten en -crises.

In zijn resolutie van 9 maart 2021 benadrukte de Raad van de Europese Unie dat cyberbeveiliging essentieel is voor de werking van openbare diensten en instellingen, zowel nationaal als op EU-niveau, en voor onze samenleving en de gehele economie, en hij benadrukte verder het belang van een robuust en consistent beveiligingskader om alle personeel, gegevens, communicatienetwerken en informatiesystemen evenals besluitvormingsprocessen te beschermen. Daartoe moet de EU weerbaarder worden gemaakt tegen cyberdreigingen en moet er een betere veiligheidscultuur komen bij de instellingen, organen en instanties van de Unie. Er moet worden gezorgd voor voldoende beschikbare middelen en capaciteiten, onder meer in het kader van de versterking van het mandaat van CERT-EU.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

• Rechtsgrondslag

De rechtsgrond voor deze verordening is artikel 298 van het Verdrag betreffende de werking van de Europese Unie (VWEU), 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. Met inachtneming van het statuut en de regeling vastgesteld op grond van artikel 336, stellen het Europees Parlement en de Raad volgens de gewone wetgevingsprocedure bij verordeningen toepasselijke bepalingen vast.

Informatietechnologie heeft de instellingen, organen en instanties van de Unie nieuwe manieren geboden om te functioneren, met burgers te communiceren en de algehele werking te verbeteren. Cyberdreigingen evolueren mee met de zich ontwikkelende technologie. De instellingen, organen en instanties van de Unie zijn zeer aantrekkelijke doelwitten van geavanceerde cyberaanvallen geworden. Het opzetten van systemen en vereisten om cyberbeveiliging te waarborgen, lijkt bij te dragen tot de efficiëntie en de onafhankelijkheid van het Europese openbaar bestuur, zodat de instellingen, organen en instanties van de Unie bij de uitvoering van hun taken efficiënter kunnen functioneren in een digitale wereld.

Bovendien vormen de huidige verschillen in opstelling jegens en benadering van cyberbeveiliging tussen de instellingen, organen en instanties van de Unie, zoals uiteengezet in punt 3 hieronder, verdere belemmeringen voor een open, efficiënt en onafhankelijk Europees bestuur. Zonder een gemeenschappelijke aanpak zou de positie ten opzichte van cyberbeveiliging onder de instellingen, organen en instanties van de Unie zich in uiteenlopende richtingen blijven ontwikkelen. De rechtsgrond is derhalve passend, aangezien de verordening tot doel heeft een gemeenschappelijk rechtskader voor cyberbeveiliging te scheppen binnen de instellingen, organen en instanties van de Unie.

• Subsidiariteit

De verordening betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging voor de instellingen, organen en instanties van de Unie valt onder de exclusieve bevoegdheid van de Unie.

• Evenredigheid

De in deze verordening voorgestelde regels gaan niet verder dan nodig is om de specifieke doelstellingen op bevredigende wijze te verwezenlijken. De voorgenomen maatregelen dragen bij tot de verwezenlijking van een hoog gezamenlijk niveau van cyberbeveiliging, zonder

verder te gaan dan wat nodig is om de doelstelling te verwezenlijken, in het licht van de steeds grotere risico's.

- **Keuze van het instrument**

De keuze voor een verordening, die rechtstreeks toepasselijk is, wordt beschouwd als het geschikte rechtsinstrument om de aan de instellingen, organen en instanties van de Unie opgelegde verplichtingen te definiëren en te stroomlijnen. Met het oog op gerichte verbeteringen is een verordening het geschiktste rechtsinstrument.

3. RESULTATEN VAN EX ANTE-EVALUATIES, RAADPLEGINGEN VAN BELANGHEBBENDEN EN EFFECTBEOORDELINGEN

- **Ex ante-evaluaties**

CERT-EU heeft een beoordeling uitgevoerd van de belangrijkste cyberdreigingen waaraan de instellingen, organen en instanties van de Unie momenteel of waarschijnlijk in de nabije toekomst worden blootgesteld.

In de analyse zijn drie categorieën waarnemingen gebruikt:

- pogingen om de IT-infrastructuur van de instellingen, organen en instanties van de Unie binnen te dringen (indien succesvol worden ze als incidenten beschouwd, anders worden ze als opgespoorde pogingen geregistreerd);
- dreigingen die zijn ontdekt in de nabijheid van de instellingen, organen en instanties van de Unie (bijvoorbeeld in gerelateerde sectoren, groepen van belanghebbenden of in Europa);
- grootschalige dreigingen die wereldwijd worden waargenomen.

Verder is geanalyseerd op welke manier huidige grote evoluties van invloed zijn op de wijze waarop de instellingen van de Unie hun IT-infrastructuur en -diensten beheren en gebruiken. Deze evoluties omvatten:

- meer thuiswerk;
- migratie van systemen naar de cloud;
- meer outsourcing van IT-diensten.

Tussen 2019 en 2021 is het aantal door advanced persistent threat-actoren uitgevoerde significante incidenten[1] met gevolgen voor de instellingen, organen en instanties van de Unie, dramatisch gestegen. In de eerste helft van 2021 waren er evenveel significante incidenten als in heel 2020. Dit is goed te zien in het aantal door CERT-EU in 2020 geanalyseerde forensische beelden (snapshots van de inhoud van getroffen systemen of apparaten), dat was verdrievoudigd ten opzichte van 2019, en het aantal significante incidenten is sinds 2018 meer dan vertienvoudigd.

Het CERT-EU-bestuur heeft in 2020 een nieuwe strategische doelstelling voor CERT-EU vastgesteld om te zorgen voor een alomvattend niveau van cyberdefensie voor alle instellingen, organen en instanties van de Unie, met een passend bereik en met voortdurende aanpassing aan huidige of op handen zijnde dreigingen, waaronder aanvallen op mobiele apparatuur, cloudomgevingen en apparaten voor het internet der dingen.

[1] "Significant incident": een incident, tenzij het beperkte gevolgen heeft en de methode of technologie waarschijnlijk al afdoende bekend is.

In aanvulling op de dreigingsanalyse van CERT-EU heeft de Commissie de werking van de cyberbeveiliging van 20 instellingen, organen en instanties van de Unie onderzocht. Dit gaf inzicht in de bestaande cyberbeveiligingspraktijken en de capaciteiten op het gebied van cyberbeveiligingsbeheer, met externe benchmarking van een aantal technische beveiligingscontroles.

Het onderzoek was gebaseerd op vragenlijsten die deze instellingen, organen en instanties hadden ingevuld, openbare gegevens en gegevens die rechtstreeks door de instellingen, organen en instanties van de Unie zelf werden verstrekt. Het bood voldoende inzicht in de huidige situatie om te kunnen concluderen dat:

- de maturiteit op het gebied van cyberbeveiliging, de grootte van de IT-infrastructuur en de capaciteitsniveaus onder de onderzochte instellingen, organen en instanties van de Unie aanzienlijk verschillen;
- hoewel veel instellingen, organen en instanties van de Unie over het algemeen over degelijke opsporings- en responscapaciteiten beschikken, de niveaus van geïntegreerd risicobeheer binnen hun governancevermogens op het gebied van cyberbeveiliging uiteenlopen;
- hoewel de cyberbeveiligingskaders (strategie, beleid en een basis van regels) van de geëvalueerde instellingen, organen en instanties van de Unie over het algemeen op de belangrijkste in bijlage I bij de verordening opgenomen cyberbeveiligingsgebieden aanwezig zijn, een degelijk bedrijfscontinuïteitsbeheer, naleving, audit en voortdurende verbetering bij sommige instellingen, organen en instanties van de Unie ontbreken;
- als beste praktijken beschouwde technische maatregelen door de onderzochte instellingen, organen en instanties van de Unie verschillend bleken te worden toegepast.

Samenvattend blijkt uit de analyse van de 20 instellingen, organen en instanties van de Unie dat hun governance, cyberhygiëne, algehele capaciteit en maturiteit over een breed spectrum uiteenlopen. Daarom is de eis dat alle instellingen, organen en instanties van de Unie een basis van cyberbeveiligingsmaatregelen implementeren, bevorderlijk om dit verschil in maturiteit aan te pakken en alle instellingen, organen en instanties van de Unie naar een hoog gezamenlijk niveau van cyberbeveiliging te tillen.

Er bestaat momenteel nog geen Uniewetgeving die op de cyberbeveiliging van de instellingen, organen en instanties van de Unie gericht is en de dreigingen op het gebied van cyberbeveiliging en de uit de digitalisering voortvloeiende nieuwe IT-risico's alomvattend aanpakt.

- **Raadpleging van belanghebbenden**

De Commissie heeft belanghebbenden uit alle instellingen, organen en instanties van de Unie, alsook vertegenwoordigers van de lidstaten in de Raad en belanghebbenden in het Europees Parlement geraadpleegd. Vertegenwoordigers van de lidstaten en belanghebbenden van de instellingen, organen en instanties van de Unie hebben op 25 juni 2021 deelgenomen aan een door de Commissie georganiseerde workshop om de inhoud van het toekomstige verordeningsvoorstel te bespreken.

- **Effectbeoordeling**

Het onderhavige voorstel heeft gevolgen voor de instellingen, organen en instanties van de Unie. Aangezien het niet van toepassing is op de lidstaten, is een specifieke effectbeoordeling overbodig.

- **Grondrechten**

De EU heeft zich ertoe verbonden hoge normen voor de bescherming van de grondrechten te waarborgen. Het delen van informatie op basis van deze verordening vindt plaats in een betrouwbare omgeving met volledige inachtneming van het recht op bescherming van persoonsgegevens in de zin van artikel 8 van het Handvest van de grondrechten van de Europese Unie en de toepasselijke gegevensbeschermingsregels, met name Verordening (EU) 2018/1725 van het Europees Parlement en de Raad.

4. GEVOLGEN VOOR DE BEGROTING

Uit marktbenchmarks en studies[2] blijkt dat de directe uitgaven voor cyberbeveiliging plegen te variëren van 4 tot 7 % van de totale IT-uitgaven van organisaties. Uit de dreigingsanalyse van CERT-EU ter ondersteuning van dit wetgevingsvoorstel blijkt echter dat internationale organen en politieke organisaties met grotere risico's te kampen hebben en dat een niveau van 10 % van de IT-uitgaven voor cyberbeveiliging derhalve een adequater cijfer is. De precieze kosten van die inspanningen kunnen niet worden bepaald vanwege het gebrek aan nadere informatie over de IT-uitgaven van de instellingen, organen en instanties van de Unie en het relevante deel van de uitgaven aan cyberbeveiliging.

Hoewel het daarom waarschijnlijk is dat veel instellingen, organen en instanties van de Unie minder aan cyberbeveiliging uitgeven dan zou moeten, zal deze verordening als zodanig niet leiden tot een verhoging van de huidige uitgaven. Ook zonder de verordening moet iedere entiteit een passend niveau van cyberbeveiliging waarborgen. De verordening bestendigt de eerdere samenwerking binnen het CERT-EU-bestuur, en formaliseert een momenteel al ten dele bestaande informatie-uitwisseling. Zoals beschreven in het financieel memorandum, heeft CERT-EU extra middelen nodig om zijn uitgebreide rol te vervullen, en die middelen moeten worden geheroriënteerd van de instellingen, organen en instanties van de Unie die van de diensten van CERT-EU profiteren.

5. ANDERE ELEMENTEN

- **Uitvoering en regelingen betreffende controle, evaluatie en rapportage**

De interinstitutionele raad voor cyberbeveiliging (IICB) moet, met de hulp van CERT-EU, de werking van deze verordening evalueren, beoordelingen uitvoeren en daarover verslag uitbrengen aan de Commissie. De Commissie moet zorgen voor regelmatige verslaggeving aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's.

CERT-EU kan een voorstel voor richtsnoeren of een aanbeveling opstellen, dat de IICB kan besluiten aan te nemen. Richtsnoeren zijn een advies, gericht tot alle of een aantal van de instellingen, organen en instanties van de Unie, en aanbevelingen zijn gericht tot individuele instellingen, organen en instanties van de Unie. Een oproep tot actie is een advies van CERT-EU betreffende dringende veiligheidsmaatregelen die instellingen, organen en instanties van de Unie binnen een bepaalde termijn met klem wordt aangeraden te treffen.

- **Uitgebreide toelichting bij de specifieke bepalingen van het voorstel**

[2] Bron: Gartner, "Identifying the Real Information Security Budget" (2016). Die kosten komen bovenop de indirecte uitgaven voor IT-beveiliging, zoals netwerkbeveiliging (firewalls, antivirus), en verantwoordelijkheden van systeembeheerders, waaronder risicobeoordeling en de implementatie van beveiligingscontroles. Een paper uit 2020 stelt dat uitgaven voor cyberbeveiliging bij financiële instellingen rond 10-11 % van de IT-uitgaven bedragen, zie: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

Algemene bepalingen

De verordening bevat maatregelen ter waarborging van een hoog gezamenlijk niveau van cyberbeveiliging en geldt voor de instellingen, organen en instanties van de Unie, zodat zij hun respectieve taken op een open, efficiënte en onafhankelijke wijze kunnen uitvoeren (artikelen 1-3, 23-25).

Maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging

De instellingen, organen en instanties van de Unie moeten een intern kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's opzetten dat een doeltreffend en prudent beheer van alle cyberbeveiligingsrisico's waarborgt. Verder stellen de instellingen, organen en instanties van de Unie een basisniveau van cyberbeveiliging vast om de in het kader vastgestelde risico's aan te pakken, regelmatig maturiteitsbeoordeling van de cyberbeveiliging uit te voeren en een cyberbeveiligingsbasis vast te stellen (artikelen 4-8).

Interinstitutionele raad voor cyberbeveiliging

Er wordt een Interinstitutionele raad voor cyberbeveiliging opgericht die verantwoordelijk is voor het toezicht op de uitvoering van deze verordening door de instellingen, organen en instanties van de Unie, en het toezicht op de uitvoering van de algemene prioriteiten en doelstellingen door CERT-EU, en voor de strategische leiding van CERT-EU (artikelen 9-11).

CERT-EU

CERT-EU draagt bij tot de beveiliging van de IT-omgeving van de instellingen, organen en instanties van de Unie door ze advies te geven, te helpen incidenten te voorkomen, die op te sporen en daarop te reageren, en door op te treden als knooppunt voor informatie-uitwisseling inzake cyberbeveiliging en responscoördinatie bij incidenten (artikelen 12-17).

Samenwerking en verslagleggingsverplichtingen

De verordening waarborgt de samenwerking en de uitwisseling van informatie tussen CERT-EU en de instellingen, organen en instanties van de Unie, om vertrouwen te kweken. Daartoe kan CERT-EU, zonder toestemming van het betrokken constituerende deel, de instellingen, organen en instanties van de Unie verzoeken relevante informatie te verstrekken, en incidentspecifieke informatie uitwisselen met de instellingen, organen en instanties van de Unie om de opsporing van soortgelijke cyberdreigingen of -incidenten te vergemakkelijken. Incidentspecifieke informatie die de identiteit van het doelwit van het cyberbeveiligingsincident onthult, mag door CERT-EU alleen met toestemming van het betrokken constituerende deel worden uitgewisseld.

De instellingen, organen en instanties van de Unie stellen CERT-EU met name onverwijld en in ieder geval binnen 24 uur nadat zij daarvan kennis hebben gekregen, op de hoogte van significante cyberdreigingen, significante kwetsbaarheden en significante incidenten (artikelen 18-22).

2022/0085 (COD)

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

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 298,

Gezien het Verdrag tot oprichting van de Europese Gemeenschap voor Atoomenergie, en met name artikel 106 bis,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) In het digitale tijdperk vormt informatie- en communicatietechnologie een hoeksteen van een open, efficiënt en onafhankelijk openbaar bestuur van de Unie. Technologische ontwikkelingen en toegenomen complexiteit en onderlinge verwevenheid van digitale systemen vergroten de risico's op het gebied van cyberbeveiliging, waardoor het openbaar bestuur van de Unie kwetsbaarder wordt voor cyberdreigingen en cyberincidenten, wat uiteindelijk de bedrijfscontinuïteit en de gegevensbeveiligingscapaciteit in gevaar brengt. Het toegenomen gebruik van clouddiensten, een alomtegenwoordig gebruik van IT, een hoge graad van digitalisering, thuiswerk en technologische ontwikkelingen en connectiviteit zijn tegenwoordig kernkenmerken van alle activiteiten van de entiteiten van de Unie, maar digitale weerbaarheid is hier nog onvoldoende ingebouwd.

(2) De instellingen, organen en instanties van de Unie hebben te kampen met constant veranderende dreigingen op het gebied van cyberveiligheid. De tactieken, technieken en procedures van dreigingsactoren evolueren constant, maar de voornaamste motieven voor die aanvallen blijven dezelfde: die gaan van diefstal van waardevolle niet openbaar gemaakte informatie tot geld verdienen, het manipuleren van de publieke opinie en het ondermijnen van de digitale infrastructuur. Cyberaanvallen volgen elkaar steeds sneller op, met steeds geavanceerdere en meer geautomatiseerde campagnes, gericht tegen zwakke plekken, en daarbij worden kwetsbaarheden snel uitgebuit.

(3) De IT-omgevingen van de instellingen, organen en instanties van de Unie hebben onderlinge afhankelijkheden en geïntegreerde gegevensstromen, en hun gebruikers werken nauw samen. Deze onderlinge afhankelijkheid betekent dat elke verstoring, zelfs als die in eerste instantie beperkt is tot één instelling, orgaan of instantie van de Unie, breder kan uitwaaieren en ingrijpende langdurige negatieve gevolgen voor de andere entiteiten kan hebben. Bovendien zijn de IT-omgevingen van bepaalde instellingen, organen en instanties van de Unie verbonden met de IT-omgevingen van

de lidstaten, zodat een incident in één entiteit van de Unie een risico kan vormen voor de cyberbeveiliging van de IT-omgevingen van de lidstaten, en omgekeerd.

(4) De instellingen, organen en instanties van de Unie zijn aantrekkelijke doelwitten die worden geconfronteerd met hooggekwalificeerde en goed toegeruste dreigingsactoren en andere dreigingen. Tegelijkertijd lopen de maturiteit van cyberveerkracht en het vermogen om kwaadwillige cyberactiviteiten op te sporen, aanzienlijk uiteen tussen deze entiteiten. Daarom is het voor de werking van het Europese openbaar bestuur nodig dat de instellingen, organen en instanties van de Unie een hoog gezamenlijk niveau van cyberbeveiliging bereiken, door tot een basisniveau van cyberbeveiliging te komen (minimumregels inzake cyberbeveiliging waaraan netwerk- en informatiesystemen en hun beheerders en gebruikers moeten voldoen om cyberbeveiligingsrisico's tot een minimum te beperken), informatie uit te wisselen en samen te werken.

(5) De richtlijn [NIS 2-voorstel] betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie beoogt de weerbaarheid op het gebied van cyberbeveiliging en de responscapaciteit bij incidenten van publieke en private entiteiten, nationale bevoegde autoriteiten en organen alsmede de Unie als geheel verder te verbeteren. Daarom moeten de instellingen, organen en instanties van de Unie hetzelfde doen en zorgen voor regels die in overeenstemming zijn met de richtlijn [NIS 2-voorstel] en het ambitieniveau ervan weerspiegelen.

(6) Om een hoog gezamenlijk niveau van cyberbeveiliging te bereiken, moeten de instellingen, organen en instanties van de Unie elk een intern kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's opzetten, dat een doeltreffend en prudent beheer van alle cyberbeveiligingsrisico's waarborgt en rekening houdt met bedrijfscontinuïteit en crisisbeheer.

(7) De verschillen tussen de instellingen, organen en instanties van de Unie vereisen flexibiliteit bij de uitvoering, omdat een uniforme aanpak niet mogelijk is. De maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging mogen geen verplichtingen omvatten die rechtstreeks ingrijpen in de uitoefening van de missie van de instellingen, organen en instanties van de Unie, of hun institutionele autonomie aantasten. Die instellingen, organen en instanties van de Unie moeten dus hun eigen kaders voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's opstellen en hun eigen basisniveau van cyberbeveiliging en cyberbeveiligingsplannen vaststellen.

(8) Om te voorkomen dat aan de instellingen, organen en instanties van de Unie onevenredige financiële en administratieve lasten worden opgelegd, moeten de eisen inzake risicobeheer op het gebied van cyberbeveiliging, rekening houdend met de stand van de techniek, in verhouding staan tot het risico dat verbonden is aan het netwerk- en informatiesysteem in kwestie. De instellingen, organen en instanties van de Unie moeten beogen een passend percentage van hun IT-begroting aan betere cyberbeveiliging te besteden; op langere termijn moet een doel van ongeveer 10 % worden nagestreefd.

(9) Voor een hoog gezamenlijk niveau van cyberbeveiliging is vereist dat cyberbeveiliging wordt geplaatst onder het toezicht van het hoogste managementniveau van de individuele instellingen, organen en instanties van de Unie, dat een basisniveau van cyberbeveiliging moet goedkeuren om de risico's aan te pakken die in het door de afzonderlijke instellingen, organen en instanties van de Unie

op te stellen kader zijn aangeduid. Het aanpakken van de cyberbeveiligingscultuur, dat wil zeggen de dagelijkse cyberbeveiligingspraktijk, maakt integraal deel uit van een basisniveau van cyberbeveiliging binnen de instellingen, organen en instanties van de Unie.

(10) De instellingen, organen en instanties van de Unie moeten de risico's betreffende de betrekkingen met leveranciers en dienstverleners, inclusief leveranciers van gegevensopslag- en gegevensverwerkingsdiensten of beheerde beveiligingsdiensten, beoordelen, en daarvoor passende maatregelen treffen. Deze maatregelen moeten deel uitmaken van het basisniveau van cyberbeveiliging en nader worden gespecificeerd in richtsnoeren of aanbevelingen van CERT-EU. Bij het definiëren van maatregelen en richtsnoeren moet terdege rekening worden gehouden met de toepasselijke Uniewetgeving en -beleidsmaatregelen, met inbegrip van risicobeoordelingen en aanbevelingen van de NIS-samenwerkingsgroep, zoals de gecoördineerde EU- risicobeoordeling en de EU-toolbox inzake 5G-cyberbeveiliging. Bovendien kan het noodzakelijk zijn dat relevante ICT-systemen, diensten en processen worden gecertificeerd op grond van artikel 49 van Verordening (EU) 2019/881 vastgestelde specifieke EU-cyberbeveiligingscertificeringsregelingen.

(11) In mei 2011 hebben de secretarissen-generaal van de instellingen, organen en instanties van de Unie besloten een preconfiguratieteam voor een computercrisisteam voor de instellingen, organen en instanties van de Unie (CERT-EU) in te stellen, onder toezicht van een interinstitutionele stuurgroep. In juli 2012 bevestigden de secretarissen-generaal de praktische regelingen en kwamen zij overeen CERT-EU te handhaven als permanente entiteit om het algehele niveau van IT-veiligheid van de instellingen, organen en instanties van de EU verder te helpen verbeteren, als voorbeeld van zichtbare interinstitutionele samenwerking op het gebied van cyberveiligheid. In september 2012 is CERT-EU opgericht als taskforce van de Europese Commissie, met een interinstitutioneel mandaat. In december 2017 zijn de instellingen, organen en instanties van de Unie een interinstitutionele regeling overeengekomen over de organisatie en de werking van CERT-EU[3]. Deze regeling moet doorlopend evolueren ter ondersteuning van de uitvoering van deze verordening.

(12) CERT-EU moet worden omgedoopt van "computercrisisteam" in "cyberbeveiligingscentrum" voor de instellingen, organen en instanties van de Unie, in overeenstemming met de ontwikkelingen in de lidstaten en wereldwijd, waar veel CERT's worden omgedoopt tot cyberbeveiligingscentra, maar de korte naam "CERT-EU" moet vanwege de herkenbaarheid behouden blijven.

(13) Veel cyberaanvallen zijn onderdeel van bredere campagnes die gericht zijn tegen groepen instellingen, organen en instanties van de Unie of belangengemeenschappen die de instellingen, organen en instanties van de Unie omvatten. Om proactief opsporings-, incidentrespons- of beperkende maatregelen te kunnen treffen, moeten de instellingen, organen en instanties van de Unie CERT-EU onverwijld in kennis stellen van significante dreigingen, significante kwetsbaarheden en significante incidenten op het gebied van cyberveiligheid en passende technische details delen, op grond waarvan opsporings-, incidentrespons- of beperkende maatregelen kunnen worden getroffen tegen vergelijkbare dreigingen, kwetsbaarheden en incidenten op het gebied van cyberveiligheid binnen andere instellingen, organen en instanties van de Unie. Op basis van dezelfde aanpak als die voorzien in richtlijn [NIS 2-voorstel] moeten

[3] PB C 12 van 13.1.2018, blz. 1.

entiteiten binnen 24 uur nadat zij daarvan kennis hebben gekregen, CERT-EU initieel van significante incidenten op de hoogte stellen. Aan de hand van die informatie-uitwisseling moet CERT-EU de informatie kunnen verspreiden onder de andere instellingen, organen en instanties van de Unie en aan passende tegenhangers, om de IT-omgevingen van de Unie en die van de tegenhangers van de Unie te helpen beschermen tegen soortgelijke incidenten, dreigingen en kwetsbaarheden.

(14) Naast meer taken en een grotere rol voor CERT-EU, moet een interinstitutionele raad voor cyberbeveiliging (IICB) worden opgericht, die een hoog gezamenlijk niveau van cyberbeveiliging onder de instellingen, organen en instanties van de Unie moet bevorderen, door middel van toezicht op de uitvoering van deze verordening door de instellingen, organen en instanties van de Unie en op de uitvoering van de algemene prioriteiten en doelstellingen door CERT-EU, en via de strategische leiding van CERT-EU. De IICB moet vertegenwoordiging van de instellingen waarborgen, en via het netwerk van agentschappen van de Unie vertegenwoordigers van instanties en organen omvatten.

(15) CERT-EU moet de uitvoering van maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging ondersteunen middels voorstellen voor richtsnoeren en aanbevelingen aan de IICB of oproepen tot actie. Deze richtsnoeren en aanbevelingen moeten door de IICB worden goedgekeurd. Indien nodig moet CERT-EU oproepen tot actie uitvaardigen betreffende dringende veiligheidsmaatregelen die instellingen, organen en instanties van de Unie binnen een bepaalde termijn met klem wordt aangeraden te treffen.

(16) De IICB moet toezicht houden op de naleving van deze verordening en van de richtsnoeren, aanbevelingen en oproepen tot actie van CERT-EU. De IICB moet op technisch gebied worden ondersteund door technische adviesgroepen, die de IICB naar eigen inzicht samenstelt, en die voor zover nodig nauw moeten samenwerken met CERT-EU, de instellingen, organen en instanties van de Unie en andere belanghebbenden. Indien nodig moet de IICB niet-bindende waarschuwingen geven en audits aanbevelen.

(17) Het moet de missie van CERT-EU zijn om bij te dragen tot de beveiliging van de IT-omgeving van de instellingen, organen en instanties van de Unie. CERT-EU moet optreden als het equivalent van de aangewezen coördinator voor de instellingen, organen en instanties van de Unie, met het oog op de gecoördineerde bekendmaking van kwetsbaarheid aan een Europees kwetsbaarheidsregister, als bedoeld in artikel 6 van richtlijn [NIS 2-voorstel].

(18) Het CERT-EU-bestuur heeft in 2020 een nieuwe strategische doelstelling voor CERT-EU vastgesteld, namelijk om te zorgen voor een alomvattend niveau van cyberdefensie voor alle instellingen, organen en instanties van de Unie, met een passend bereik en met voortdurende aanpassing aan huidige of op handen zijnde dreigingen, waaronder aanvallen tegen mobiele apparatuur, cloudomgevingen en apparaten voor het internet der dingen. Het strategische doel omvat op brede basis werkzame operationele beveiligingscentra (SOC's) die continu netwerken monitoren voor zeer ernstige dreigingen. CERT-EU moet de IT-beveiligingsteams van de grotere instellingen, organen en instanties van de Unie ondersteunen, onder meer met continue eerstelijnsmonitoring. Voor kleinere en enkele middelgrote instellingen, organen en instanties van de Unie moet CERT-EU alle diensten verlenen.

(19) CERT-EU moet ook de rol vervullen waarin is voorzien in richtlijn [NIS 2-voorstel] inzake samenwerking en informatie-uitwisseling met het netwerk van computer

security incident response teams (CSIRTs). Verder moet CERT-EU overeenkomstig Aanbeveling (EU) 2017/1584[4] van de Commissie samenwerken met de belanghebbende partijen en de respons coördineren. Met het oog op een hoog niveau van cyberbeveiliging in de hele Unie, moet CERT-EU incidentspecifieke informatie delen met nationale tegenhangers. CERT-EU moet ook samenwerken met andere publieke en private tegenhangers, zoals bij de NAVO, na voorafgaande goedkeuring door de IICB.

(20) Bij de ondersteuning van operationele cyberbeveiliging moet CERT-EU gebruikmaken van de beschikbare deskundigheid van het agentschap van de Europese Unie voor cyberbeveiliging, door middel van gestructureerde samenwerking zoals bedoeld in Verordening (EU) 2019/881[5] van het Europees Parlement en de Raad. Indien passend moeten specifieke regelingen tussen de twee entiteiten worden vastgesteld teneinde de praktische uitvoering van die samenwerking te bepalen en dubbel werk te vermijden. CERT-EU moet met het agentschap van de Europese Unie voor cyberbeveiliging samenwerken inzake dreigingsanalyse en zijn dreigingslandschapverslag regelmatig met het agentschap delen.

(21) Ter ondersteuning van de gezamenlijke cybereenheid die overeenkomstig de aanbeveling van de Commissie van 23 juni 2021[6] is opgezet, moet CERT-EU samenwerken en informatie uitwisselen met belanghebbende partijen om operationele samenwerking te bevorderen en de bestaande netwerken hun volledige potentieel voor de bescherming van de Unie te laten ontplooien.

(22) Alle overeenkomstig deze verordening verwerkte persoonsgegevens moeten overeenkomstig de gegevensbeschermingswetgeving, met inbegrip van Verordening (EU) 2018/1725[7] van het Europees Parlement en de Raad, worden verwerkt.

(23) CERT-EU en de instellingen, organen en instanties van de Unie moeten informatie verwerken overeenkomstig de regels zoals bepaald in verordening [de voorgestelde verordening inzake informatiebeveiliging]. Met het oog op de coördinatie van veiligheidskwesties moeten alle contacten met CERT-EU die door nationale veiligheids- en inlichtingendiensten worden geïnitieerd of beoogd, onverwijld aan het directoraat Beveiliging van de Commissie en de voorzitter van de IICB worden meegedeeld.

(24) Aangezien de diensten en taken van CERT-EU in het belang van alle instellingen, organen en instanties van de Unie zijn, moeten de individuele instellingen, organen en instanties van de Unie met IT-uitgaven een billijke bijdrage aan die diensten en taken leveren. Die bijdragen laten de budgettaire autonomie van de instellingen, organen en instanties van de Unie onverlet.

---

4 Aanbeveling (EU) 2017/1584 van de Commissie van 13 september 2017 inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises (PB L 239 van 19.9.2017, blz. 36).

5 Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15).

6 Aanbeveling van de Commissie C(2021) 4520 van 23 juni 2021 betreffende de opbouw van een gezamenlijke cybereenheid.

7 Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39).

(25) De IICB moet, met de hulp van CERT-EU, de uitvoering van deze verordening evalueren en beoordelen en daarover verslag uitbrengen aan de Commissie. Op basis van die input moet de Commissie regelmatig verslag uitbrengen aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

Hoofdstuk I
INLEIDING

Artikel 1
Onderwerp

Bij deze verordening worden de volgende voorschriften vastgesteld:

(a) verplichtingen voor de instellingen, organen en instanties van de Unie om een intern kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's op te zetten;

(b) verplichtingen voor de instellingen, organen en instanties van de Unie inzake risicobeheer en rapportage op het gebied van cyberbeveiliging;

(c) voorschriften inzake de organisatie en werking van het cyberbeveiligingscentrum voor de instellingen, organen en instanties van de Unie (hierna "CERT-EU" genoemd) en de interinstitutionele raad voor cyberbeveiliging (hierna "IICB" genoemd).

Artikel 2
Toepassingsgebied

Deze verordening is van toepassing op het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's door de instellingen, organen en instanties van de Unie en op de organisatie en de werking van CERT-EU en de interinstitutionele raad voor cyberbeveiliging.

Artikel 3
Definities

Voor de toepassing van deze verordening wordt verstaan onder:

(1) "instellingen, organen en instanties van de Unie": instellingen, organen en instanties van de Unie die zijn opgericht bij of krachtens het Verdrag betreffende de Europese Unie, het Verdrag betreffende de werking van de Europese Unie of het Verdrag tot oprichting van de Europese Gemeenschap voor Atoomenergie;

(2) "netwerk- en informatiesysteem": een netwerk- en informatiesysteem in de zin van artikel 4, punt 1, van richtlijn [NIS 2-voorstel];

(3) "beveiliging van netwerk- en informatiesystemen": beveiliging van netwerk- en informatiesystemen in de zin van artikel 4, punt 2, van richtlijn [NIS 2-voorstel];

(4) "cyberbeveiliging": cyberbeveiliging in de zin van artikel 4, punt 3, van richtlijn [NIS 2-voorstel];

(5) “hoogste managementniveau”: een leidinggevende, een leidinggevend of coördinatie- en toezichtorgaan op het hoogste bestuurlijke niveau, met inachtneming van de bestuursregelingen op hoog niveau binnen de individuele instellingen, organen en instanties van de Unie;

(6) “incident”: een incident in de zin van artikel 4, punt 5, van richtlijn [NIS 2-voorstel];

(7) “significant incident”: een incident, tenzij het beperkte gevolgen heeft en de methode of technologie waarschijnlijk al afdoende bekend is;

(8) “grootscheepse aanval”: een incident waarvoor meer middelen nodig zijn dan beschikbaar bij de getroffen instelling, orgaan of instantie van de Unie en bij CERT-EU;

(9) “incidentenbehandeling”: incidentenbehandeling in de zin van artikel 4, punt 6, van richtlijn [NIS 2-voorstel];

(10) “cyberdreiging”: cyberdreiging in de zin van artikel 2, punt 8, van Verordening (EU) 2019/881;

(11) “significante cyberdreiging”: een cyberdreiging met de bedoeling, de gelegenheid en het vermogen om een significant incident te veroorzaken;

(12) “kwetsbaarheid”: kwetsbaarheid in de zin van artikel 4, punt 8, van richtlijn [NIS 2-voorstel];

(13) “significante kwetsbaarheid”: een kwetsbaarheid die, indien uitgebuit, waarschijnlijk tot een significant incident leidt;

(14) “cyberbeveiligingsrisico”: elke redelijkerwijs vast te stellen omstandigheid of gebeurtenis met een mogelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen;

(15) “gezamenlijke cybereenheid”: een virtueel en fysiek samenwerkingsplatform voor de verschillende cyberbeveiligingsgemeenschappen in de Unie, gericht op operationele en technische coördinatie bij grote grensoverschrijdende cyberdreigingen en incidenten in de zin van de aanbeveling van de Commissie van 23 juni 2021;

(16) “basisniveau van cyberbeveiliging”: minimale voorschriften voor cyberbeveiliging waaraan netwerk- en informatiesystemen en de beheerders en gebruikers ervan moeten voldoen om cyberbeveiligingsrisico’s te beperken.

Hoofdstuk II
MAATREGELEN VOOR EEN HOOG GEZAMENLIJK NIVEAU VAN CYBERBEVEILIGING

Artikel 4
Risicobeheer, governance en toezicht

1. Bij de uitoefening van hun institutionele autonomie zetten de instellingen, organen en instanties van de Unie elk een intern kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico’s op (hierna “het kader” genoemd), ter ondersteuning van de missie van die entiteit. Dit geschiedt onder toezicht van het hoogste managementniveau van die entiteit, om een doeltreffend en prudent beheer van alle cyberbeveiligingsrisico’s te waarborgen. Het kader moet uiterlijk … [15 maanden na de inwerkingtreding van deze verordening] zijn voltooid.

2. Het kader omvat de gehele IT-omgeving van de instelling, het orgaan of de instantie, met inbegrip van de IT-omgeving on site, uitbestede activa en diensten in cloudcomputingomgevingen of gehost door derden, mobiele apparatuur, bedrijfsnetwerken, zakelijke netwerken die niet met het internet verbonden zijn, en met de IT-omgeving verbonden apparaten. Het kader houdt rekening met bedrijfscontinuïteit en crisisbeheer, de beveiliging van de toeleveringsketen en het beheer van menselijke risico's die gevolgen kunnen hebben voor de cyberbeveiliging van de instellingen, organen en instanties van de Unie.

3. Het hoogste managementniveau van de individuele instellingen, organen en instanties van de Unie houdt toezicht op de naleving door hun organisatie van de verplichtingen in verband met het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's, onverminderd de formele verantwoordelijkheden van andere managementlagen voor naleving en risicobeheer binnen hun respectieve bevoegdheid.

4. De instellingen, organen en instanties van de Unie beschikken over doeltreffende mechanismen om te waarborgen dat een passend percentage van de IT-begroting aan cyberbeveiliging wordt besteed.

5. De instellingen, organen en instanties van de Unie stellen elk een lokale cyberbeveiligingsfunctionaris of een gelijkwaardige functionaris aan, die fungeert als het centrale contactpunt voor alle cyberbeveiligingsaspecten.

Artikel 5

Basisniveau van cyberbeveiliging

1. Het hoogste managementniveau van de individuele instellingen, organen en instanties van de Unie keurt voor de eigen entiteit een basisniveau van cyberbeveiliging goed om de in het kader van de in artikel 4, lid 1, bedoelde risico's aan te pakken. Dit geschiedt ter ondersteuning van de missie en bij de uitoefening van hun institutionele autonomie. Het basisniveau van cyberbeveiliging is uiterlijk … [18 maanden na de inwerkingtreding van deze verordening] van kracht en heeft betrekking op de in bijlage I vermelde domeinen en de in bijlage II vermelde maatregelen.

2. Het hogere management van de instellingen, organen en instanties van de Unie volgt regelmatig specifieke opleidingen om voldoende kennis en vaardigheden op te doen om risico- en beheerspraktijken op het gebied van cyberbeveiliging en de gevolgen daarvan op de activiteiten van de organisatie te begrijpen en te beoordelen.

Artikel 6

Maturiteitsbeoordelingen

De individuele instellingen, organen en instanties van de Unie voeren ten minste om de drie jaar een maturiteitsbeoordeling van de cyberbeveiliging uit die alle elementen van hun IT-omgeving zoals beschreven in artikel 4 omvat, met inachtneming van de overeenkomstig artikel 13 vastgestelde toepasselijke richtsnoeren en aanbevelingen.

Artikel 7

Cyberbeveiligingsplannen

1. Naar aanleiding van de conclusies uit de maturiteitsbeoordeling en met inachtneming van de uit hoofde van artikel 4 aangeduide activa en risico's keurt het hoogste

managementniveau van de individuele instellingen, organen en instanties van de Unie na de opstelling van het kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's en van het basisniveau van cyberbeveiliging onverwijld een cyberbeveiligingsplan goed. Het plan beoogt de algehele cyberbeveiliging van de betrokken entiteit te versterken en aldus bij te dragen tot de verwezenlijking of verhoging van een hoog gezamenlijk niveau van cyberbeveiliging bij de instellingen, organen en instanties van de Unie. Ter ondersteuning van de missie van de entiteit en in de uitoefening van hun institutionele autonomie, omvat het plan ten minste de in bijlage I vermelde domeinen en de in bijlage II vermelde maatregelen, en de maatregelen in verband met de paraatheid bij, het reageren op en het herstel van incidenten, zoals toezicht op en registratie van de beveiliging. Het plan wordt ten minste om de drie jaar herzien naar aanleiding van de overeenkomstig artikel 6 uitgevoerde maturiteitsbeoordelingen.

2. Het cyberbeveiligingsplan omvat de rollen en verantwoordelijkheden van het personeel voor de uitvoering ervan.

3. Het cyberbeveiligingsplan houdt rekening met de toepasselijke richtsnoeren en aanbevelingen van CERT-EU.

Artikel 8
Uitvoering

1. Na voltooiing van de maturiteitsbeoordelingen zenden de instellingen, organen en instanties van de Unie die naar de interinstitutionele raad voor cyberbeveiliging. Na voltooiing van de cyberbeveiligingsplannen stellen de instellingen, organen en instanties van de Unie de interinstitutionele raad voor cyberbeveiliging daarvan in kennis. Op verzoek van de raad brengen zij verslag uit over specifieke aspecten betreffende dit hoofdstuk.

2. Overeenkomstig artikel 13 uitgevaardigde richtsnoeren en aanbevelingen ondersteunen de uitvoering van dit hoofdstuk.

Hoofdstuk III
INTERINSTITUTIONELE RAAD VOOR CYBERBEVEILIGING

Artikel 9
Interinstitutionele raad voor cyberbeveiliging

1. Er wordt een interinstitutionele raad voor cyberbeveiliging (IICB) opgericht.

2. De IICB is verantwoordelijk voor:

   (a) het toezicht op de uitvoering van deze verordening door de instellingen, organen en instanties van de Unie;

   (b) het toezicht op de uitvoering van de algemene prioriteiten en doelstellingen door CERT-EU en het geven van strategische leiding aan CERT-EU.

3. De IICB bestaat uit drie vertegenwoordigers die door het netwerk van EU-agentschappen (EUAN) op voorstel van zijn adviescomité voor ICT worden benoemd om de belangen te behartigen van de organen en instanties die hun eigen IT-omgeving beheren, en één vertegenwoordiger, aangewezen door ieder van de volgende:

(a) het Europees Parlement;

(b) de Raad van de Europese Unie;

(c) de Europese Commissie;

(d) het Hof van Justitie van de Europese Unie;

(e) de Europese Centrale Bank;

(f) de Europese Rekenkamer,

(g) de Europese Dienst voor extern optreden;

(h) het Europees Economisch en Sociaal Comité;

(i) het Europees Comité van de Regio's;

(j) de Europese Investeringsbank;

(k) het agentschap van de Europese Unie voor cyberbeveiliging.

De leden kunnen door een plaatsvervanger worden bijgestaan. Andere vertegenwoordigers van de hierboven vermelde organisaties, of andere instellingen, organen en instanties van de Unie kunnen door de voorzitter worden uitgenodigd om zonder stemrecht aan IICB-vergaderingen deel te nemen.

4. De IICB stelt zijn reglement van orde vast.

5. De IICB wijst overeenkomstig zijn reglement van orde uit zijn leden een voorzitter aan voor een periode van vier jaar. Zijn of haar plaatsvervanger wordt voor dezelfde duur volwaardig lid van de IICB.

6. De IICB komt bijeen op initiatief van zijn voorzitter, op verzoek van CERT-EU of van een van zijn leden.

7. Elk lid van de IICB heeft één stem. Tenzij in deze verordening anders is bepaald, worden de besluiten van de IICB genomen met gewone meerderheid. De voorzitter stemt uitsluitend bij staking van de stemmen; dan geeft zijn stem de doorslag.

8. De IICB kan handelen door middel van een vereenvoudigde schriftelijke procedure conform zijn reglement van orde. Op grond van die procedure wordt het desbetreffende besluit geacht binnen de door de voorzitter vastgestelde termijn te zijn goedgekeurd, tenzij een lid bezwaar maakt.

9. Het hoofd van CERT-EU of zijn plaatsvervanger neemt deel aan IICB-vergaderingen, tenzij de IICB anders beslist.

10. Het secretariaat van de IICB wordt verzorgd door de Commissie.

11. De op voorstel van het adviescomité voor ICT door het EUAN benoemde vertegenwoordigers brengen de besluiten van de IICB over aan de organen en gemeenschappelijke ondernemingen van de Unie. Organen en instanties van de Unie mogen iedere kwestie die zij voor de IICB van belang achten, aan de vertegenwoordigers of de voorzitter van de IICB voorleggen.

12. De IICB kan handelen door middel van een door de voorzitter ingestelde vereenvoudigde schriftelijke procedure, op grond waarvan het desbetreffende besluit wordt geacht binnen de door de voorzitter vastgestelde termijn te zijn goedgekeurd, tenzij een lid bezwaar maakt.

13. De IICB kan een uitvoerend comité benoemen om hem bij zijn werkzaamheden bij te staan, en een aantal van zijn taken en bevoegdheden daaraan delegeren. De IICB stelt het reglement van orde van het uitvoerend comité vast, met inbegrip van de taken en bevoegdheden en de ambtstermijn van de leden daarvan.

Artikel 10
Taken van de IICB

Bij de uitoefening van zijn verantwoordelijkheden vervult de IICB de volgende taken:

(a) hij beoordeelt de verslagen van CERT-EU over de stand van de uitvoering van deze verordening door de instellingen, organen en instanties van de Unie;

(b) hij hecht zijn goedkeuring aan het jaarlijkse werkprogramma voor CERT-EU op basis van een voorstel van het hoofd van CERT-EU en ziet toe op de uitvoering ervan;

(c) hij hecht zijn goedkeuring aan de CERT-EU-dienstencatalogus, op basis van een voorstel van het hoofd van CERT-EU;

(d) hij hecht zijn goedkeuring aan de verwachte jaarlijkse ontvangsten en uitgaven, inclusief personeel, voor CERT-EU, op basis van ramingen opgesteld door het hoofd van CERT-EU;

(e) hij hecht zijn goedkeuring aan de voorwaarden voor de dienstenniveauovereenkomst, op basis van een voorstel van het hoofd van CERT-EU;

(f) het controleert en hecht zijn goedkeuring aan het door het hoofd van CERT-EU opgestelde jaarverslag over de activiteiten van en het beheer van de middelen door CERT-EU;

(g) hij hecht zijn goedkeuring aan en monitort prestatie-indicatoren voor CERT-EU die op voorstel van het hoofd van CERT-EU worden vastgesteld;

(h) hij hecht zijn goedkeuring aan samenwerkingsovereenkomsten en dienstverleningsregelingen of -overeenkomsten tussen CERT-EU en andere entiteiten op grond van artikel 17;

(i) hij stelt naar behoefte technische adviesgroepen in ter ondersteuning van de werkzaamheden van de IICB, keurt hun mandaat goed en wijst hun voorzitter aan.

Artikel 11
Naleving

De IICB houdt toezicht op de uitvoering van deze verordening en de door de instellingen, organen en instanties van de Unie vastgestelde richtsnoeren, aanbevelingen en oproepen tot actie. Indien de IICB vaststelt dat de instellingen, organen of instanties van de Unie deze verordening of de krachtens deze verordening vastgestelde richtsnoeren, aanbevelingen en oproepen tot actie niet doeltreffend hebben toegepast, kan hij, onverminderd de interne procedures van de instelling, het orgaan of de instantie van de Unie in kwestie, de volgende maatregelen treffen:

(a) een waarschuwing doen uitgaan; indien nodig met het oog op een overtuigend cyberbeveiligingsrisico, de waarschuwing richten tot een op passende wijze beperkt publiek;

(b) een betreffende auditdienst aanbevelen een audit uit te voeren.

Hoofdstuk IV
CERT-EU

Artikel 12
Missie en taken van CERT-EU

1. De missie van CERT-EU, het autonome interinstitutionele cyberbeveiligingscentrum voor de instellingen, organen en instanties van de Unie, bestaat erin bij te dragen tot de beveiliging van de niet-geclassificeerde IT-omgeving van de instellingen, organen en instanties van de Unie door ze te adviseren over cyberbeveiliging, te helpen incidenten te voorkomen, die op te sporen en daarop te reageren, en door op te treden als knooppunt voor hun informatie-uitwisseling inzake cyberbeveiliging en responscoördinatie bij incidenten.

2. CERT-EU is voor de instellingen, organen en instanties van de Unie belast met de volgende taken:

   (a) het ondersteunt ze bij de uitvoering van deze verordening en draagt bij tot de coördinatie van de toepassing van deze verordening door middel van de in artikel 13, lid 1, vermelde maatregelen, of via door de IICB verzochte ad-hocverslagen;

   (b) het ondersteunt ze met een in zijn dienstencatalogus beschreven pakket cyberbeveiligingsdiensten, de zogenaamde basisniveaudiensten;

   (c) het onderhoudt een netwerk van soortgelijke organisaties en partners ter ondersteuning van de in de artikelen 16 en 17 bedoelde diensten;

   (d) het brengt kwesties betreffende de uitvoering van deze verordening en van de uitvoering van richtsnoeren, aanbevelingen en oproepen tot actie onder de aandacht van de IICB;

   (e) het brengt verslag uit over de cyberdreigingen waaraan de instellingen, organen en instanties van de Unie blootstaan en draagt bij tot het situatiebewustzijn van de EU op het gebied van cyberbeveiliging.

3. CERT-EU draagt bij tot de overeenkomstig de aanbeveling van de Commissie van 23 juni 2021 opgerichte gezamenlijke cybereenheid, onder meer op de volgende gebieden:

   (a) paraatheid, incidentcoördinatie, informatie-uitwisseling en crisisrespons op technisch niveau in gevallen die met de instellingen, organen en instanties van de Unie verband houden;

   (b) operationele samenwerking inzake het netwerk van computer security incident response teams (CSIRT), ook betreffende wederzijdse bijstand, en de bredere cyberbeveiligingsgemeenschap;

   (c) inlichtingen inzake cyberdreigingen, inclusief situatiebewustzijn;

   (d) elk ander onderwerp waarvoor de technische deskundigheid op het gebied van cyberbeveiliging van CERT-EU vereist is.

4. CERT-EU onderhoudt gestructureerde samenwerking met het Agentschap van de Europese Unie voor cyberbeveiliging met betrekking tot capaciteitsopbouw, operationele samenwerking en strategische langetermijnanalyses van cyberdreigingen, overeenkomstig Verordening (EU) 2019/881 van het Europees Parlement en de Raad.

5. CERT-EU kan de volgende diensten aanbieden die niet in de dienstencatalogus zijn beschreven, de zogenaamde aangerekende diensten:

   (a) andere dan de in lid 2 bedoelde diensten, ter ondersteuning van de cyberbeveiliging van de IT-omgeving van de instellingen, organen en instanties van de Unie, op basis van dienstenniveauovereenkomsten en afhankelijk van de beschikbaarheid van middelen;

   (b) andere diensten dan diensten ter bescherming van de IT-omgeving van de instellingen, organen en instanties van de Unie, ter ondersteuning van hun cyberbeveiligingsoperaties of -projecten, op basis van schriftelijke overeenkomsten en met voorafgaande goedkeuring van de IICB;

   (c) diensten ter ondersteuning van de beveiliging van de IT-omgeving van andere organisaties dan de instellingen, organen en instanties van de Unie, die nauw met de instellingen, organen en instanties van de Unie samenwerken, bijvoorbeeld omdat zij taken of verantwoordelijkheden krachtens Unierecht vervullen, op basis van schriftelijke overeenkomsten en met voorafgaande goedkeuring van de IICB.

6. CERT-EU kan, in nauwe samenwerking met het Agentschap van de Europese Unie voor cyberbeveiliging, cyberbeveiligingsoefeningen organiseren of deelname aan bestaande oefeningen aanbevelen, indien van toepassing, om het cyberbeveiligingsniveau van de instellingen, organen en instanties van de Unie te testen.

7. CERT-EU kan de instellingen, organen en instanties van de Unie bijstaan bij incidenten in gerubriceerde IT-omgevingen, indien het betrokken constituerend deel daar uitdrukkelijk om verzoekt.

Artikel 13

Richtsnoeren, aanbevelingen en oproepen tot actie

1. CERT-EU ondersteunt de uitvoering van deze verordening door middel van de volgende activiteiten:

   (a) oproepen tot actie, die dringende veiligheidsmaatregelen omvatten die de instellingen, organen en instanties van de Unie binnen een bepaalde termijn met klem wordt aangeraden te treffen;

   (b) voorstellen aan de IICB voor richtsnoeren die gericht zijn tot alle of een deel van de instellingen, organen en instanties van de Unie;

   (c) voorstellen aan de IICB voor aanbevelingen die gericht zijn tot individuele instellingen, organen en instanties van de Unie.

2. Richtsnoeren en aanbevelingen kunnen het volgende omvatten:

   (a) de voorwaarden voor of verbetering van het beheer van cyberbeveiligingsrisico's en het basisniveau van cyberbeveiliging;

   (b) de voorwaarden voor maturiteitsbeoordelingen en cyberbeveiligingsplannen; en

   (c) indien van toepassing, het gebruik van algemene technologie, architectuur en de bijbehorende beste praktijken, met het oog op interoperabiliteit en gemeenschappelijke normen in de zin van artikel 4, punt 10, van richtlijn [NIS 2-voorstel].

3. De IICB kan op voorstel van CERT-EU richtsnoeren of aanbevelingen vaststellen.

4. De IICB kan CERT-EU opdragen om een oproep tot actie, of een voorstel voor richtsnoeren of aanbevelingen, uit te vaardigen, in te trekken of te wijzigen.

Artikel 14
Hoofd van CERT-EU

Het hoofd van CERT-EU brengt regelmatig verslag uit aan de IICB en de voorzitter ervan over de prestaties van CERT-EU, de financiële planning, inkomsten, de uitvoering van de begroting, en gesloten dienstenniveauovereenkomsten en schriftelijke overeenkomsten, de samenwerking met andere instanties en partners, en de dienstreizen van personeel, met inbegrip van de in artikel 10, lid 1, bedoelde verslagen.

Artikel 15
Financiële en personeelszaken

1. De Commissie benoemt met unanieme goedkeuring van de IICB het hoofd van CERT-EU. De IICB wordt geraadpleegd in alle stadia van de procedure voor de benoeming van het hoofd van CERT-EU, in het bijzonder bij het opstellen van vacatureberichten, de beoordeling van de sollicitaties en de benoeming van de selectiecomités voor deze functie.

2. Voor de toepassing van de administratieve en financiële procedures handelt het hoofd van CERT-EU onder het gezag van de Commissie.

3. De taken en activiteiten van CERT-EU, inclusief de diensten die CERT-EU overeenkomstig artikel 12, leden 2, 3, 4 en 6, en artikel 13, lid 1, verleent aan de uit de rubriek Europees openbaar bestuur van het meerjarige financiële kader gefinancierde instellingen, organen en instanties van de Unie, worden uit een afzonderlijke begrotingslijn van de begroting van de Commissie gefinancierd. Gereserveerde posten van CERT-EU worden gespecificeerd in een voetnoot bij de personeelsformatie.

4. Andere dan de in lid 3 bedoelde instellingen, organen en instanties van de Unie leveren een jaarlijkse financiële bijdrage aan CERT-EU ter dekking van de door CERT-EU overeenkomstig lid 3 verleende diensten. De respectieve bijdragen worden gebaseerd op richtsnoeren van de IICB en in dienstenniveauovereenkomsten tussen elke entiteit en CERT-EU bepaald. De bijdragen vertegenwoordigen een billijk en evenredig deel van de totale kosten van de verleende diensten. Deze worden als bestemmingsontvangsten in de zin van artikel 21, lid 3, punt c), van Verordening (EU, Euratom) 2018/1046 van het Europees Parlement en de Raad[8] via de in lid 3 bedoelde afzonderlijke begrotingslijn ontvangen.

5. De kosten van de in artikel 12, lid 5, bedoelde taken worden verhaald op de instellingen, organen en instanties van de Unie die de diensten van CERT-EU

[8] Verordening (EU, Euratom) 2018/1046 van het Europees Parlement en de Raad van 18 juli 2018 tot vaststelling van de financiële regels van toepassing op de algemene begroting van de Unie, tot wijziging van Verordeningen (EU) nr. 1296/2013, (EU) nr. 1301/2013, (EU) nr. 1303/2013, (EU) nr. 1304/2013, (EU) nr. 1309/2013, (EU) nr. 1316/2013, (EU) nr. 223/2014, (EU) nr. 283/2014 en Besluit nr. 541/2014/EU en tot intrekking van Verordening (EU, Euratom) nr. 966/2012 (PB L 193 van 30.7.2018, blz. 1).

ontvangen. De ontvangsten worden bestemd voor de begrotingsonderdelen die de kosten dragen.

Artikel 16

Samenwerking van CERT-EU met instanties uit de lidstaten

1. CERT-EU werkt samen en wisselt informatie uit met nationale instanties in de lidstaten, met inbegrip van CERT's, nationale cyberbeveiligingscentra, CSIRT's en centrale contactpunten als bedoeld in artikel 8 van richtlijn [het NIS 2-voorstel] over dreigingen, kwetsbaarheden en incidenten op het gebied van cyberveiligheid en over mogelijke tegenmaatregelen, en doet dat voor alle onderwerpen die relevant zijn voor een betere bescherming van de ICT-infrastructuur van de instellingen, organen en instanties van de Unie, onder meer via het CSIRT-netwerk als bedoeld in artikel 13 van richtlijn [NIS 2-voorstel].
2. CERT-EU kan, zonder toestemming van het betrokken constituerende deel, incidentspecifieke informatie uitwisselen met nationale instanties in de lidstaten om de opsporing van soortgelijke cyberdreigingen of -incidenten te vergemakkelijken. CERT-EU kan alleen met toestemming van het betrokken constituerende deel, incidentspecifieke informatie uitwisselen die de identiteit van het doelwit van het cyberbeveiligingsincident onthult.

Artikel 17

Samenwerking van CERT-EU met instanties uit niet-lidstaten

1. CERT-EU kan samenwerken met instanties uit derde landen, met inbegrip van bedrijfstakspecifieke instanties, inzake instrumenten en methoden, zoals technieken, tactiek, procedures en beste praktijken, en cyberdreigingen en -kwetsbaarheden. Voor alle samenwerking met dergelijke instanties, ook in verbanden waar instanties van derde landen samenwerken met de nationale tegenhangers van de lidstaten, verzoekt CERT-EU vooraf de goedkeuring van IICB.
2. CERT-EU kan samenwerken met andere partners, zoals commerciële entiteiten, internationale organisaties en nationale entiteiten van buiten de Europese Unie of individuele deskundigen, om informatie te verzamelen over algemene en specifieke cyberdreigingen, cyberkwetsbaarheden en mogelijke tegenmaatregelen. Voor verdere samenwerking met deze partners verzoekt CERT-EU vooraf de goedkeuring van de IICB.
3. CERT-EU kan, met toestemming van het door een incident getroffen constituerende deel, informatie over een incident verstrekken aan partners die het kunnen helpen analyseren.

Hoofdstuk V
SAMENWERKING EN VERSLAGLEGGINGSVERPLICHTINGEN

Artikel 18

Informatieverwerking

1. CERT-EU en de instellingen, organen en instanties van de Unie nemen het beroepsgeheim in acht overeenkomstig artikel 339 van het Verdrag betreffende de werking van de Europese Unie of gelijkwaardige toepasselijke kaders.

2. Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad[9] is van toepassing op verzoeken om toegang van het publiek tot documenten die berusten bij CERT-EU, met inbegrip van de verplichting overeenkomstig die verordening om andere instellingen, organen en instanties van de Unie te raadplegen indien een verzoek betrekking heeft op hun documenten.

3. Op de verwerking van persoonsgegevens op grond van deze verordening is Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van toepassing.

4. CERT-EU en de instellingen, organen en instanties van de Unie verwerken informatie overeenkomstig de regels zoals opgenomen in [de voorgestelde verordening inzake informatiebeveiliging].

5. Alle contacten met CERT-EU die door nationale veiligheids- en inlichtingendiensten worden geïnitieerd of beoogd, worden onverwijld aan het directoraat Veiligheid van de Commissie en de voorzitter van de IICB meegedeeld.

Artikel 19
Deelverplichtingen

1. Om CERT-EU in staat te stellen het kwetsbaarheidsbeheer en de respons op incidenten te coördineren, kan het de instellingen, organen en instanties van de Unie verzoeken voor CERT-EU-steun relevante informatie uit hun respectieve IT-systeeminventarissen te verstrekken. De aangezochte instellingen, organen en instanties zenden de verlangde informatie en bijbehorende actualiseringen daarvan onverwijld toe.

2. De instellingen, organen en instanties van de Unie delen op verzoek van CERT-EU onverwijld de digitale informatie die is opgesteld door het gebruik van elektronische apparaten die bij de respectieve incidenten betrokken zijn geweest. CERT-EU kan verder verduidelijken welke soort digitale informatie nodig is met het oog op situatiebewustzijn en respons op incidenten.

3. CERT-EU kan alleen met toestemming van de individuele instellingen, organen en instanties van de Unie, incidentspecifieke informatie uitwisselen die de identiteit van de door het incident getroffen entiteit onthult. CERT-EU kan alleen met toestemming van de door het incident getroffen entiteit, incidentspecifieke informatie uitwisselen die de identiteit van het doelwit van het cyberbeveiligingsincident onthult.

4. De deelverplichtingen gelden niet voor gerubriceerde EU-informatie (EUCI), noch voor informatie die een instelling, orgaan of instantie van de Unie van een veiligheids- of inlichtingendienst of een rechtshandhavingsinstantie van een lidstaat heeft ontvangen onder de uitdrukkelijke voorwaarde dat die niet met CERT-EU wordt gedeeld.

[9] Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie (PB L 145 van 31.5.2001, blz. 43).

Artikel 20

Kennisgevingsverplichtingen

1. De instellingen, organen en instanties van de Unie stellen CERT-EU onverwijld en in ieder geval binnen 24 uur nadat zij daarvan kennis hebben gekregen, initieel in kennis van significante cyberdreigingen, significante kwetsbaarheden en significante incidenten.

   In gerechtvaardigde gevallen en in overeenstemming met CERT-EU kunnen de instellingen, organen en instanties van de Unie in kwestie van de in het vorige lid vastgestelde termijn afwijken.

2. De instellingen, organen en instanties van de Unie stellen CERT-EU onverwijld in kennis van passende technische details van dreigingen, kwetsbaarheden en incidenten op het gebied van cyberveiligheid, op grond waarvan opsporings-, incidentrespons- of beperkende maatregelen kunnen worden getroffen. De kennisgeving omvat, indien beschikbaar:

   (a) relevante indicatoren van compromittering;

   (b) relevante opsporingsmechanismen;

   (c) de potentiële impact,

   (d) relevante beperkende maatregelen.

3. CERT-EU dient maandelijks bij Enisa een samenvattend verslag in, met geanonimiseerde en geaggregeerde gegevens over significante dreigingen, significante kwetsbaarheden en significante incidenten op het gebied van cyberveiligheid, die overeenkomstig lid 1 ter kennis zijn gegeven.

4. De IICB kan richtsnoeren of aanbevelingen uitbrengen betreffende de randvoorwaarden en de inhoud van de kennisgeving. CERT-EU verspreidt de passende technische details, zodat de instellingen, organen en instanties van de Unie proactief opsporings-, incidentrespons- of beperkende maatregelen kunnen treffen.

5. De kennisgevingsverplichtingen gelden niet voor EUCI, noch voor informatie die instellingen, organen en instanties van de Unie van een veiligheids- of inlichtingendienst of een rechtshandhavingsinstantie van een lidstaat hebben ontvangen onder de uitdrukkelijke voorwaarde dat die niet met CERT-EU wordt gedeeld.

Artikel 21

Coördinatie van respons bij incidenten en samenwerking bij significante incidenten

1. Bij zijn optreden als knooppunt voor informatie-uitwisseling inzake cyberbeveiliging en responscoördinatie bij incidenten faciliteert CERT-EU de uitwisseling van informatie inzake dreigingen, kwetsbaarheden en incidenten op het gebied van cyberveiligheid onder de volgende partijen:

   (a) instellingen, organen en instanties van de Unie;

   (b) de in de artikelen 16 en 17 bedoelde instanties.

2. CERT-EU faciliteert de coördinatie tussen de instellingen, organen en instanties van de Unie inzake de respons bij incidenten, wat het volgende omvat:

   (a) bijdragen tot consequente externe communicatie;

(b) wederzijdse bijstand;

(c) optimaal gebruik van operationele middelen;

(d) coördinatie met andere crisisresponsmechanismen op Unieniveau.

3. CERT-EU ondersteunt de instellingen, organen en instanties van de Unie met betrekking tot het situatiebewustzijn van dreigingen, kwetsbaarheden en incidenten op het gebied van cyberveiligheid.

4. De IICB verstrekt richtsnoeren inzake de respons bij incidenten en samenwerking bij significante incidenten. Wanneer wordt vermoed dat het incident crimineel van aard is, adviseert CERT-EU over de manier waarop het incident aan de rechtshandhavingsinstanties moet worden gemeld.

Artikel 22

Grootscheepse aanvallen

1. CERT-EU coördineert de respons op grootscheepse aanvallen tussen de instellingen, organen en instanties van de Unie. Het houdt een inventaris bij van de technische deskundigheid die nodig is voor de respons op incidenten bij dergelijke aanvallen.

2. De instellingen, organen en instanties van de Unie dragen bij tot de inventaris van technische deskundigheid, en leveren een jaarlijks bijgewerkte lijst van deskundigen die binnen hun respectieve organisaties beschikbaar zijn, inclusief nadere gegevens over hun specifieke technische vaardigheden.

3. Met de goedkeuring van de betrokken instellingen, organen en instanties van de Unie kan CERT-EU de in lid 2 bedoelde deskundigen ook oproepen om te helpen bij de respons op een grootscheepse aanval in een lidstaat, conform de operationele procedures van de gezamenlijke cybereenheid.

Hoofdstuk VI
SLOTBEPALINGEN

Artikel 23

Initiële heroriëntering van begrotingsmiddelen

De Commissie stelt voor de personele en financiële middelen over te hevelen van de instellingen, organen en instanties van de Unie naar de begroting van de Commissie. De heroriëntering valt samen met de eerste begroting die na de inwerkingtreding van deze verordening wordt vastgesteld.

Artikel 24

Evaluatie

1. De IICB brengt, met de hulp van CERT-EU, op gezette tijden verslag uit aan de Commissie over de uitvoering van deze verordening. De IICB kan ook aanbevelingen doen aan de Commissie om wijzigingen van deze verordening voor te stellen.

2. Uiterlijk 48 maanden na de inwerkingtreding van deze verordening en vervolgens om de drie jaar brengt de Commissie verslag uit over de uitvoering van deze verordening aan het Europees Parlement en de Raad.

3. Niet eerder dan vijf jaar na de inwerkingtreding evalueert de Commissie de werking van deze verordening en brengt daarover verslag uit aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's.

Artikel 25
Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel,

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

1.2. Betrokken beleidsterrein(en)

1.3. Het voorstel/initiatief betreft:

1.4. Doelstelling(en)

1.4.1. Algemene doelstelling(en)

1.4.2. Specifieke doelstelling(en)

1.4.3. Verwachte resulta(a)t(en) en gevolg(en)

1.4.4. Prestatie-indicatoren

1.5. Motivering van het voorstel/initiatief

1.5.1. Behoefte(n) waarin op korte of lange termijn moet worden voorzien, met een gedetailleerd tijdschema voor de uitrol van het initiatief

1.5.2. Toegevoegde waarde van de deelname van de Unie (deze kan het resultaat zijn van verschillende factoren, bijvoorbeeld coördinatiewinst, rechtszekerheid, grotere doeltreffendheid of complementariteit). Voor de toepassing van dit punt wordt onder "toegevoegde waarde van de deelname van de Unie" verstaan de waarde die een optreden van de Unie oplevert bovenop de waarde die door een optreden van alleen de lidstaat zou zijn gecreëerd.

1.5.3. Nuttige ervaring die bij soortgelijke activiteiten in het verleden is opgedaan

1.5.4. Verenigbaarheid met het meerjarige financiële kader en eventuele synergie met andere passende instrumenten

1.5.5. Beoordeling van de verschillende beschikbare financieringsopties, waaronder mogelijkheden voor herschikking

1.6. Duur en financiële gevolgen van het voorstel/initiatief

1.7. Beheersvorm(en)

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

2.2. Beheers- en controlesyste(e)m(en)

2.2.1. Rechtvaardiging van de voorgestelde beheersvorm(en), uitvoeringsmechanisme(n) voor financiering, betalingsvoorwaarden en controlestrategie

2.2.2. Informatie over de geïdentificeerde risico's en het (de) systeem (systemen) voor interne controle dat is (die zijn) opgezet om die risico's te beperken

2.2.3. Raming en motivering van de kosteneffectiviteit van de controles (verhouding van de controlekosten tot de waarde van de desbetreffende financiële middelen) en evaluatie van het verwachte foutenrisico (bij betaling en bij afsluiting).

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarige financiële kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

3.2. Geraamde financiële gevolgen van het voorstel inzake kredieten

3.2.1. Samenvatting van de geraamde gevolgen voor de beleidskredieten

3.2.2. Geraamde output, gefinancierd met operationele kredieten

3.2.3. Samenvatting van de geraamde gevolgen voor de administratieve kredieten

3.2.4. Verenigbaarheid met het huidige meerjarige financiële kader

3.2.5. Bijdragen van derden

3.3. Geraamde gevolgen voor de ontvangsten

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

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

1.2. Betrokken beleidsterrein(en)

Europees openbaar bestuur

Het voorstel heeft betrekking op maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie

1.3. Het voorstel/initiatief betreft:

☑een nieuwe actie

☐ een nieuwe actie na een proefproject / voorbereidende actie[10]

☐ de verlenging van een bestaande actie

☑ de samenvoeging of ombuiging van een of meer acties naar een andere/een nieuwe actie

1.4. Doelstelling(en)

1.4.1. Algemene doelstelling(en)

- Een kader oprichten voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie.
- Een nieuwe rechtsgrondslag voor CERT-EU ter versterking van zijn mandaat en financiering.

1.4.2. Specifieke doelstelling(en)

(1) Verplichtingen voor de instellingen, organen en instanties van de Unie vastleggen om een intern kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's op te zetten.

(2) Verplichtingen voor de instellingen, organen en instanties van de Unie vastleggen om verslag uit te brengen over het kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's, alsook over cyberbeveiligingsincidenten.

(3) Voorschriften inzake de organisatie en de werking van het cyberbeveiligingscentrum voor de instellingen, organen en instanties van de Unie (CERT-EU) en de interinstitutionele raad voor cyberbeveiliging (IICB) vastleggen.

(4) Bijdragen tot de gezamenlijke cybereenheid.

[10] In de zin van artikel 58, lid 2, punt a) of b), van het Financieel Reglement.

1.4.3. Verwachte resulta(a)t(en) en gevolg(en)

Vermeld de gevolgen die het voorstel/initiatief zou moeten hebben op de begunstigden/doelgroepen.

- Kaders voor het beheer, de governance en de controle met betrekking tot interne cyberbeveiligingsrisico's, basisniveaus van cyberbeveiliging, regelmatige maturiteitsbeoordelingen en cyberbeveiligingsplannen binnen de instellingen, organen en instanties van de Unie.
- Betere cyberbeveiligingsweerbaarheid en responscapaciteit bij incidenten binnen de instellingen, organen en instanties van de Unie.
- Modernisering van CERT-EU.
- Bijdragen tot de gezamenlijke cybereenheid.

1.4.4. Prestatie-indicatoren

Vermeld de indicatoren voor de monitoring van de voortgang en de beoordeling van de resultaten.

- Kaders en basisniveaus vastgesteld, regelmatige maturiteitsbeoordelingen en cyberbeveiligingsplannen binnen de instellingen, organen en instanties van de Unie uitgevoerd.
- Betere omgang met incidenten.
- Groter bewustzijn van cyberbeveiligingsrisico's bij het hogere management van de instellingen, organen en instanties van de Unie.
- Verhoudingsgewijs gelijke uitgaven voor ICT-beveiliging als percentage van de totale ICT-uitgaven.
- Sterk leiderschap van de IICB en CERT-EU.
- Betere informatiedeling tussen de instellingen, organen en instanties van de Unie en met organen en belanghebbenden in de EU.
- Betere samenwerking inzake cyberbeveiliging met organen en belanghebbenden in de EU, via CERT-EU en Enisa.

1.5. Motivering van het voorstel/initiatief

1.5.1. Behoefte(n) waarin op korte of lange termijn moet worden voorzien, met een gedetailleerd tijdschema voor de uitrol van het initiatief.

Het voorstel beoogt het niveau van cyberweerbaarheid van de instellingen, organen en instanties van de Unie te verhogen, inconsistenties in de weerbaarheid tussen deze entiteiten te verminderen en het niveau van gezamenlijk situatiebewustzijn te verhogen, en het collectieve vermogen om zich voor te bereiden en te reageren, te verbeteren.

Het voorstel is volledig consistent en coherent met andere gerelateerde initiatieven, en met name met het voorstel voor een richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148 [NIS 2-voorstel].

Het voorstel vormt een essentieel onderdeel van de EU-strategie voor de veiligheidsunie en de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk.

De verordening wordt volgens de planning in oktober 2021 door de Europese Commissie voorgesteld en naar verwachting in 2022 door het Europees Parlement en de Raad vastgesteld, en de bepalingen zijn vanaf de inwerkingtreding van de

verordening van toepassing. De in dit financieel memorandum uiteengezette financiële en personele gevolgen beginnen naar verwachting in 2023. Een aanloopperiode is reeds in 2021 begonnen, maar de voorbereidende activiteiten in 2021 en 2022 vallen buiten de financiële gevolgen van het voorstel.

1.5.2. Toegevoegde waarde van de deelname van de Unie (deze kan het resultaat zijn van verschillende factoren, bijvoorbeeld coördinatiewinst, rechtszekerheid, grotere doeltreffendheid of complementariteit). Voor de toepassing van dit punt wordt onder "toegevoegde waarde van de deelname van de Unie" verstaan de waarde die een optreden van de Unie oplevert bovenop de waarde die door een optreden van alleen de lidstaten zou zijn gecreëerd.

Redenen voor maatregelen op EU-niveau (ex ante)

Tussen 2019 en 2021 is het aantal door advanced persistent threat-actoren uitgevoerde significante incidenten met gevolgen voor de instellingen, organen en instanties van de Unie, dramatisch gestegen. In de eerste helft van 2021 waren er evenveel significante incidenten als in heel 2020. Dit is goed te zien in het aantal door CERT-EU in 2020 geanalyseerde forensische beelden (snapshots van de inhoud van getroffen systemen of apparaten), die waren verdrievoudigd ten opzichte van 2019, en het aantal significante incidenten is sinds 2018 meer dan vertienvoudigd.

De maturiteit op het gebied van cyberbeveiliging verschilt aanzienlijk per entiteit[11]. Deze verordening waarborgt dat alle instellingen, organen en instanties van de Unie een basisniveau van beveiligingsmaatregelen toepassen, en samenwerken met het oog op een open en efficiënte werking van het openbaar bestuur van de Unie.

De te beschermen systemen vallen onder de autonomie van en worden beheerd door de instellingen, organen en instanties van de Unie; de voorgestelde activiteiten kunnen niet door de lidstaten worden uitgevoerd.

1.5.3. Nuttige ervaring die bij soortgelijke activiteiten in het verleden is opgedaan

De NIS-richtlijn was het eerste horizontale internemarktinstrument dat tot doel had de weerbaarheid van netwerken en systemen in de Unie tegen cyberbeveiligingsrisico's te verbeteren. Vanaf de inwerkingtreding in 2016 heeft de richtlijn in grote mate bijgedragen tot een hoger gemeenschappelijk niveau van cyberbeveiliging onder de lidstaten. Het voorstel voor de NIS 2-richtlijn beoogt deze maatregelen verder te verbeteren.

De verordening is gericht op gelijkaardige maatregelen voor de instellingen, organen en instanties van de Unie.

1.5.4. Verenigbaarheid met het meerjarige financiële kader en eventuele synergie met andere passende instrumenten

Het voorstel is in overeenstemming met het meerjarig financieel kader en vormt een essentieel onderdeel van de EU-strategie voor de veiligheidsunie en de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk.

Het voorstel beoogt maatregelen toe te passen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie. Het voorstel is

[11] Referentie: [Speciaal verslag van de ERK over cyberbeveiliging in de instellingen, organen en instanties van de Unie].

in overeenstemming met het voorstel voor een richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148 [NIS 2-voorstel].

1.5.5. Beoordeling van de verschillende beschikbare financieringsopties, waaronder mogelijkheden voor herschikking

Het beheer van de taken van CERT-EU vereist specifieke profielen en brengt extra werkbelasting mee die niet kan worden geabsorbeerd zonder een verhoging van de personele en financiële middelen.

1.6. Duur en financiële gevolgen van het voorstel/initiatief

☐ **beperkte geldigheidsduur**

– ☐ van kracht vanaf [DD/MM]JJJJ tot en met [DD/MM]JJJJ

– ☐ financiële gevolgen vanaf JJJJ tot en met JJJJ voor vastleggingskredieten en vanaf JJJJ tot en met JJJJ voor betalingskredieten.

☑ **onbeperkte geldigheidsduur**

– De financiële gevolgen moeten beginnen met de eerste begroting die na de inwerkingtreding van deze verordening wordt vastgesteld. Een heroriëntering van middelen van de instellingen en de belangrijkste organen van de Unie naar de Commissie zal plaatsvinden in het eerste jaar, dat als overgangsjaar wordt beschouwd; deze en andere heroriënteringen van middelen vinden plaats in het kader van de jaarlijkse begrotingen. Indien de verordening in 2022 wordt vastgesteld, is financieel jaar 2023 de overgangsperiode en is het stelsel in 2024 volledig operationeel.

1.7. Beheersvorm(en)[12]

☑ **Rechtstreeks beheer** door de Commissie en de individuele instellingen, organen en instanties van de Unie

– ☑ door haar diensten, waaronder het personeel in de delegaties van de Unie;

– ☐ door de uitvoerende agentschappen

☐ **Gedeeld beheer** met de lidstaten

☐ **Indirect beheer** door begrotingsuitvoeringstaken te delegeren aan:

– ☐ derde landen of de door hen aangewezen organen;

– ☐ internationale organisaties en hun agentschappen (geef aan welke);

– ☐ de EIB en het Europees Investeringsfonds;

– ☐ de in de artikelen 70 en 71 van het Financieel Reglement bedoelde organen;

– ☐ publiekrechtelijke organen;

– ☐ privaatrechtelijke organen met een openbaredienstverleningstaak, voor zover zij voldoende financiële garanties bieden;

– ☐ privaatrechtelijke organen van een lidstaat, waaraan de uitvoering van een publiek-privaat partnerschap is toevertrouwd en die voldoende financiële garanties bieden;

– ☐ personen aan wie de uitvoering van specifieke maatregelen op het gebied van het GBVB in het kader van titel V van het VEU is toevertrouwd en die worden genoemd in de betrokken basishandeling.

– *Verstrek, indien meer dan een beheersvorm is aangekruist, extra informatie onder "Opmerkingen".*

Opmerkingen

[12] Nadere gegevens over de beheersvormen en verwijzingen naar het Financieel Reglement zijn beschikbaar op BudgWeb: https://myintracomm.ec.europa.eu/budgweb/NL/man/budgmanag/Pages/budgmanag.aspx

Voor de toepassing van de administratieve en financiële procedures handelt CERT-EU onder het gezag van de Commissie.

Extra middelen die voortvloeien uit de ontwerpverordening:

de uitvoering van de artikelen 12 en 13 van de ontwerpverordening leidt tot een grotere dienstencatalogus met aanvullende basisdiensten. Bij volledige werking zijn (tot het einde van het MFK eind 2027) de volgende extra middelen nodig: 21 vte en 14,05 miljoen EUR.

De verdeling van de aanvullende middelen binnen de begroting over de verschillende taken is als volgt:

(a) voor de in artikel 12, lid 2, punten a), b), c), en e), beschreven taken voor de instellingen, organen en instanties van de Unie: 13,75 vte en 11,275 miljoen EUR;

(b) voor de in artikel 12, lid 3 (bijdragen voor de gezamenlijke cybereenheid) beschreven taken: 2 vte en 381 000 EUR;

(c) voor de in artikel 12, lid 4 (gestructureerde samenwerking met Enisa) beschreven taken: 0,25 vte en 236 000 EUR;

(d) voor de in artikel 12, lid 6 (cyberbeveiligingsoefeningen) beschreven taken: 0,25 vte en 79 000 EUR;

(e) voor de in artikel 12, lid 2, punt d), en artikel 13 (analyse van en verslaglegging over de uitvoering van de verordening, voorbereiding van richtsnoeren, aanbevelingen en oproepen tot actie) beschreven taken: 3,75 vte en 2,079 miljoen EUR;

(f) voor de uitvoering van de taken ter ondersteuning van het secretariaat van de interinstitutionele raad voor cyberbeveiliging: 1 vte.

Overzicht van de huidige middelen en de overgang naar volledige werking:

in september 2021 functioneerde CERT-EU met de volgende middelen:

- vaste en gedetacheerde ambten: 14 vte,

- op grond van dienstenniveauovereenkomsten gefinancierde arbeidscontractanten: 24 vte,

- totaal 38 vte.

De begroting van CERT-EU in 2020 bedroeg: 250 000 EUR gefinancierd uit de begroting van de Commissie, 3,5 miljoen EUR uit bestemmingsontvangsten uit de dienstenniveauovereenkomsten. Totaal: 3,75 miljoen EUR. Dit vormde de volledige CERT-EU-begroting en omvatte opleidingen, hardware en software, dienstreizen, ondersteuning, arbeidscontractanten en conferenties.

Nadat de verordening in werking is getreden, worden de toekomstige middelen van CERT-EU geraamd op:

- vaste ambten: 34 vte,

- arbeidscontractanten: 15 vte,

- totaal 49 vte, ofwel een nettostijging van 11 vte.

De verschuiving in de verhouding tussen vaste posten en arbeidscontractanten pakt het permanente struikelblok voor het aanwerven en behouden van ervaren cyberbeveiligingsprofessionals vanwege hun schaarste op de arbeidsmarkt aan.

Verder is 1 vte arbeidscontractant vereist binnen het directoraat-generaal Informatica van de Commissie ter ondersteuning van de IICB.

Er zijn dus 21 vte extra nodig voor de uitvoering van de verordening (20 vte voor CERT-EU en 1 voor het directoraat-generaal Informatica van de Commissie). Dit wordt gecompenseerd door een gelijktijdige inkrimping van 9 vte arbeidscontractanten in CERT-EU die voordien werden gefinancierd met bestemmingsontvangsten uit dienstenniveauovereenkomsten.

De begroting van CERT-EU voor niet-personele middelen in 2024 zal na de overgangsperiode de onder a) tot en met e) genoemde taken omvatten en wordt naar verwachting als volgt gefinancierd:

- 8 921 miljoen EUR per jaar van de instellingen, organen en instanties van de Unie die worden gefinancierd op grond van rubriek 7,

- 2 459 miljoen EUR van de instellingen, organen en instanties van de Unie die worden gefinancierd op grond van de rubrieken 1 tot en met 6,

- 2 670 miljoen EUR van zichzelf financierende instellingen, organen en instanties van de Unie.

- Totale CERT-EU-begroting: 14,05 miljoen EUR.

De in artikel 12, lid 5, vermelde taken, de zogenaamde aangerekende diensten, zijn niet in de dienstencatalogus beschreven. Die diensten zijn aanvullend, betreffen tamelijk lage bedragen, zijn meestal tijdelijk, en de kosten ervan worden op de begunstigden van de diensten verhaald door middel van dienstenniveauovereenkomsten of schriftelijke overeenkomsten.

Ten aanzien van de bijdragen aan het personeel van CERT-EU: de instellingen en de belangrijkste organen van de Unie dragen een billijk aandeel bij, evenredig aan het respectieve aandeel vaste AD-posten van de organisatie. Onderzocht moet worden of de ECB en de EIB ook een billijke bijdrage kunnen leveren door de detachering van vast personeel.

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

Vermeld frequentie en voorwaarden.

De Commissie evalueert met de hulp van de IICB en CERT-EU op gezette tijden de werking van deze verordening en brengt daarover verslag uit aan het Europees Parlement, de Raad, uiterlijk 48 maanden na de inwerkingtreding van deze verordening en vervolgens om de drie jaar.

De voor de evaluaties gebruikte gegevensbronnen zijn voornamelijk afkomstig van de IICB en CERT-EU. Daarnaast kunnen waar nodig specifieke instrumenten voor het verzamelen van gegevens worden gebruikt, bijvoorbeeld onderzoeken van de instellingen, organen en instanties van de Unie, Enisa of het CSIRT-netwerk.

2.2. Beheers- en controlesyste(e)m(en)

2.2.1. Rechtvaardiging van de voorgestelde beheersvorm(en), uitvoeringsmechanisme(n) voor financiering, betalingsvoorwaarden en controlestrategie

Uit de verordening voortvloeiende acties worden binnen de individuele instellingen, organen en instanties van de Unie beheerd overeenkomstig de toepasselijke voorschriften en regels.

Het administratieve en financiële beheer van CERT-EU-activiteiten is in de administratie van de Commissie ingebed en volgt de toepasselijke beheers- en uitvoeringsmechanismen, betalingsvoorwaarden en controles.

De interne controleur van de Commissie heeft ten aanzien van CERT-EU dezelfde bevoegdheden als ten aanzien van de diensten van de Commissie.

2.2.2. Informatie over de geïdentificeerde risico's en het (de) systeem (systemen) voor interne controle dat is (die zijn) opgezet om die risico's te beperken

Zeer laag risico, aangezien CERT-EU al als taskforce van de Commissie administratief is verbonden aan de directeur-generaal voor Informatica, en de IICB naar het huidige CERT-EU-bestuur gemodelleerd is. Het ecosysteem voor financieel beheer en interne controle is dus reeds aanwezig.

2.2.3. Raming en motivering van de kosteneffectiviteit van de controles (verhouding van de controlekosten tot de waarde van de desbetreffende financiële middelen) en evaluatie van het verwachte foutenrisico (bij betaling en bij afsluiting).

De procedures voor aankopen, financieel beheer en controle zijn al aanwezig en beproefd. De kosteneffectiviteit van de controles en de foutenrisiconiveaus komen overeen met die in individuele instellingen, organen of instanties van de Unie en die van de Commissie voor CERT-EU-activiteiten.

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

Vermeld de bestaande en geplande preventie- en beschermingsmaatregelen, bijvoorbeeld in het kader van de fraudebestrijdingsstrategie.

De systemen van de Commissie voor financieel beheer en interne controle van de Commissie zijn van toepassing op CERT-EU-activiteiten.

Ter bestrijding van fraude, corruptie en andere onwettige activiteiten is Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad van 11

september 2013 betreffende onderzoeken door het Europees Bureau voor fraudebestrijding (OLAF) onverkort van toepassing.

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarige financiële kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

- Bestaande begrotingsonderdelen

In volgorde van de rubrieken van het meerjarige financiële kader en de begrotingsonderdelen.

Rubriek van het meerjarige financiële kader	Begrotingsonderdeel	Soort krediet	Bijdrage			
	Nummer	GK/NGK[13]	van EVA-landen[14]	van kandidaat-lidstaten[15]	van derde landen	in de zin van artikel 21, lid 2, punt b), van het Financieel Reglement
1 tot en met 6	Begrotingsonderdelen waar de bijdragen van de Unie aan gedecentraliseerde agentschappen onder vallen	GK	NEE	NEE	NEE	NEE
7	Begrotingsonderdelen waar de bezoldigingen van het personeel, IT-uitgaven en andere administratieve uitgaven in de verschillende afdelingen van de EU-begroting onder vallen	NGK	NEE	NEE	NEE	NEE

- Te creëren nieuwe begrotingsonderdelen

In volgorde van de rubrieken van het meerjarige financiële kader en de begrotingsonderdelen.

Rubriek van het meerjarige financiële kader	Begrotingsonderdeel	Soort uitgaven	Bijdrage			
	Aantal	GK/ NGK	van EVA-landen	van kandidaat-lidstaten	van derde landen	in de zin van artikel 21, lid 2, punt b), van het Financieel Reglement
	Geen		JA/NEE	JA/NEE	JA/NEE	JA/NEE

[13] GK = gesplitste kredieten / NGK = niet-gesplitste kredieten.
[14] EVA: Europese Vrijhandelsassociatie.
[15] Kandidaat-lidstaten en, in voorkomend geval, potentiële kandidaat-lidstaten van de Westelijke Balkan.

3.2. Geraamde financiële gevolgen van het voorstel inzake kredieten

3.2.1. Samenvatting van de geraamde gevolgen voor de beleidskredieten

– ☐ Voor het voorstel/initiatief zijn geen beleidskredieten nodig

– ☑ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

miljoen EUR (tot op drie decimalen)

Rubriek van het meerjarig financieel kader	1 tot en met 6	Rubrieken waar de bijdragen aan gedecentraliseerde agentschappen onder vallen

DG: Verscheidene			Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**TOTAAL**
○ Beleidskredieten								
Begrotingsonderdelen waar de bijdragen van de Unie aan gedecentraliseerde agentschappen onder vallen (xx 10 xx xx)[16]	Vastleggingen	1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Betalingen	2a)	2,459	2,459	2,459	2,459	2,459	12,293
Uit het budget van specifieke programma's gefinancierde administratieve kredieten[17]								
Begrotingsonderdeel		3)						
TOTAAL kredieten Voor DG: Verscheidene	Vastleggingen	=1a+1b +3	2,459	2,459	2,459	2,459	2,459	12,293
	Betalingen	=2a+2b +3	2,459	2,459	2,459	2,459	2,459	12,293

[16] Volgens de officiële begrotingsnomenclatuur.

[17] Technische en/of administratieve bijstand en uitgaven ter ondersteuning van de uitvoering van programma's en/of acties van de EU (vroegere "BA"-onderdelen), onderzoek door derden, eigen onderzoek.

○ TOTAAL beleidskredieten	Vastleggingen	4)	2,459	2,459	2,459	2,459	2,459	12,293
	Betalingen	5)	2,459	2,459	2,459	2,459	2,459	12,293
○ TOTAAL uit het budget van specifieke programma's gefinancierde administratieve kredieten		6)						
TOTAAL kredieten onder de RUBRIEKEN 1 tot en met 6 van het meerjarige financiële kader	Vastleggingen	=4+6	2,459	2,459	2,459	2,459	2,459	12,293
	Betalingen	=5+6	2,459	2,459	2,459	2,459	2,459	12,293

Wanneer het voorstel/initiatief gevolgen heeft voor meerdere beleidsrubrieken, herhaal bovenstaand deel:

○ TOTAAL beleidskredieten (alle beleidsrubrieken)	Vastleggingen	4)	2,459	2,459	2,459	2,459	2,459	12,293
	Betalingen	5)	2,459	2,459	2,459	2,459	2,459	12,293
TOTAAL uit het budget van specifieke programma's gefinancierde administratieve kredieten (alle beleidsrubrieken)		6)						
TOTAAL kredieten onder de RUBRIEKEN 1 tot en met 6 van het meerjarige financiële kader (referentiebedrag)	Vastleggingen	=4+6	2,459	2,459	2,459	2,459	2,459	12,293
	Betalingen	=5+6	2,459	2,459	2,459	2,459	2,459	12,293

Rubriek van het meerjarig financieel kader	**7**	"Administratieve uitgaven"

Dit deel moet worden ingevuld aan de hand van de "administratieve begrotingsgegevens", die eerst moeten worden opgenomen in de bijlage bij het financieel memorandum (Bijlage V bij de interne voorschriften), te uploaden in DECIDE met het oog op overleg tussen de diensten.

miljoen EUR (tot op drie decimalen)

		Jaar **2023**	Jaar **2024**	Jaar **2025**	Jaar **2026**	**Jaar 2027**	**TOTAAL**
DG: DIGIT (CERT-EU)							
○ Personele middelen		1,184	2,126	2,754	3,225	3,225	12,514
○ Andere administratieve uitgaven		7,938	8,921	8,921	8,921	8,921	43,622
TOTAAL DG DIGIT (CERT-EU)	Kredieten	9,122	11,047	11,675	12,146	12,146	56,136

TOTAAL kredieten onder RUBRIEK 7 van het meerjarige financiële kader	(Totaal vastleggingen = totaal betalingen)	9,122	11,047	11,675	12,146	12,146	**56,136**

miljoen EUR (tot op drie decimalen)

		Jaar 2023	Jaar 2024	Jaar 2025	Jaar 2026	Jaar 2027	**TOTAAL**
TOTAAL kredieten onder de RUBRIEKEN 1 tot en met 7 van het meerjarige financiële kader (*)	Vastleggingen	11,581	13,506	14,134	14,605	14,605	68,429
	Betalingen	11,581	13,506	14,134	14,605	14,605	68,429

(*) Bijdragen van zichzelf financierende instellingen, organen en instanties van de Unie worden geraamd op 2 670 miljoen EUR per jaar (totaal voor de vijf jaar: 13 350 miljoen EUR). De bijdragen vormen bestemmingsontvangsten voor CERT-EU. De bovenstaande tabellen bevatten alleen de geraamde totale gevolgen voor de begroting van de Unie en omvatten die bijdragen niet.

3.2.2. Geraamde output, gefinancierd met operationele kredieten

Vastleggingskredieten, in miljoenen euro's (tot op drie decimalen)

Vermeld doelstellingen en outputs ⇩			Jaar **N**		Jaar **N+1**		Jaar **N+2**		Jaar **N+3**		Vul zoveel jaren in als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)						**TOTAAL**	
	OUTPUTS																	
	Soort [18]	Gem. kosten	aantal	Kosten	aantal	Kosten	aantal	Kosten	aantal	Kosten	aantal	Kosten	aantal	Kosten	aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 1[19]…																		
- Output																		
- Output																		
- Output																		
Subtotaal voor specifieke doelstelling nr. 1																		
SPECIFIEKE DOELSTELLING NR. 2…																		
- Output																		
Subtotaal voor specifieke doelstelling nr. 2																		
TOTAAL																		

[18] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen enz.).

[19] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

3.2.3. Samenvatting van de geraamde gevolgen voor de administratieve kredieten

– ☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

– ☑ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

miljoen EUR (tot op drie decimalen)

	Jaar 2023	Jaar 2024	Jaar 2025	Jaar 2026	Jaar 2027	**TOTAAL**
RUBRIEK 7 van het meerjarige financiële kader						
Personele middelen						
Vast personeel (AD-rangen)	1,099	2,041	2,669	3,14	3,14	12,089
Arbeidscontractanten	0,085	0,085	0,085	0,085	0,085	0,425
Andere administratieve uitgaven	7,938	8,921	8,921	8,921	8,921	43,622
Subtotaal RUBRIEK 7 van het meerjarige financiële kader	9,122	11,047	11,675	12,146	12,146	56,136

Buiten RUBRIEK 7[20] van het meerjarige financiële kader						
Personele middelen						
Andere administratieve uitgaven						
Subtotaal buiten RUBRIEK 7 van het meerjarige financiële kader						

TOTAAL	9,122	11,047	11,675	12,146	12,146	56,136

De benodigde kredieten voor personele middelen en andere administratieve uitgaven zullen worden gefinancierd uit de kredieten van het DG die reeds voor het beheer van deze actie zijn toegewezen en/of binnen het DG zijn herverdeeld, eventueel aangevuld met middelen die in het kader van de jaarlijkse toewijzingsprocedure met inachtneming van de budgettaire beperkingen aan het beherende DG kunnen worden toegewezen.

[20] Technische en/of administratieve bijstand en uitgaven ter ondersteuning van de uitvoering van programma's en/of acties van de EU (vroegere "BA"-onderdelen), onderzoek door derden, eigen onderzoek.

3.2.3.1. Geraamde personeelsbehoeften

– ☐ Voor het voorstel/initiatief zijn geen personele middelen nodig

– ☑ Voor het voorstel/initiatief zijn personele middelen nodig, zoals hieronder nader wordt beschreven:

Raming in voltijdequivalenten

		Jaar 2023	Jaar 2024	Jaar 2025	Jaar 2026	Jaar 2027		
O Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)								
20 01 02 01 (zetel en vertegenwoordigingen van de Commissie)		7	13	17	20	20		
20 01 02 03 (delegaties)								
01 01 01 01 (onderzoek door derden)								
01 01 01 11 (eigen onderzoek)								
Ander begrotingsonderdeel (te vermelden)								
O Extern personeel (in voltijdequivalenten: VTE)[21]								
20 02 01 (AC, END, INT van de "totale financiële middelen")		1	1	1	1	1		
20 02 03 (AC, AL, END, INT en JPD in de delegaties)								
XX 01 xx **yy zz** [22]	zetel							
	delegaties							
01 01 01 02 (AC, END, INT — onderzoek door derden)								
01 01 01 12 (AC, END, INT — eigen onderzoek)								
Ander begrotingsonderdeel (te vermelden)								
TOTAAL		**8**	**14**	**18**	**21**	**21**		

XX is het desbetreffende beleidsterrein of de begrotingstitel.

Voor de benodigde personele middelen zal een beroep worden gedaan op het personeel van het DG dat reeds voor het beheer van deze actie is toegewezen en/of binnen het DG is herverdeeld, eventueel aangevuld met middelen die in het kader van de jaarlijkse toewijzingsprocedure met inachtneming van de budgettaire beperkingen aan het beherende DG kunnen worden toegewezen.

Beschrijving van de uit te voeren taken:

Ambtenaren en tijdelijk personeel	Ambtenaren voeren de taken en activiteiten van CERT-EU uit overeenkomstig de verordening, met name de hoofdstukken IV en V.
Extern personeel	De arbeidscontractant ondersteunt de secretariaatsfuncties van de Interinstitutionele Raad voor cyberbeveiliging.

[21] AC= Agent Contractuel (arbeidscontractant); AL= Agent Local (plaatselijk functionaris); END= Expert National Détaché (gedetacheerd nationaal deskundige); INT = Intérimaire (uitzendkracht); JPD = Jeune Professionnel en Délégation (jonge professional in delegaties).

[22] Subplafond voor extern personeel uit beleidskredieten (vroegere "BA"-onderdelen).

3.2.4. Verenigbaarheid met het huidige meerjarige financiële kader

Het voorstel/initiatief:

– ☑ kan volledig worden gefinancierd door middel van herschikking binnen de relevante rubriek van het meerjarig financieel kader (MFK).

Zet uiteen welke herprogrammering nodig is, onder vermelding van de betrokken begrotingsonderdelen en de desbetreffende bedragen. Verstrek een Excel-tabel in het geval van een omvangrijke herprogrammeringsexercitie.

– ☐ hiervoor moet een beroep worden gedaan op de niet-toegewezen marge in de desbetreffende rubriek van het MFK en/of op de speciale instrumenten zoals gedefinieerd in de MFK-verordening.

Zet uiteen wat nodig is, onder vermelding van de betrokken rubrieken en begrotingsonderdelen, de desbetreffende bedragen en de voorgestelde instrumenten.

– ☐ hiervoor is een herziening van het MFK nodig.

Zet uiteen wat nodig is, onder vermelding van de betrokken rubrieken en begrotingsonderdelen en de desbetreffende bedragen.

3.2.5. Bijdragen van derden

Het voorstel/initiatief:

– ☑ voorziet niet in medefinanciering door derden[23]

– ☐ voorziet in medefinanciering door derden, zoals hieronder wordt geraamd:

Kredieten in miljoen EUR (tot op drie decimalen)

	Jaar **N**[24]	Jaar **N+1**	Jaar **N+2**	Jaar **N+3**	Vul zoveel jaren in als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)			Totaal
Medefinancieringsbron								
TOTAAL medegefinancierde kredieten								

[23] De bestemmingsontvangsten uit de sporadische dienstverlening aan niet-constituerende organisaties in de zin van artikel 12, lid 5, punt c), zijn niet geraamd omdat zij onbetekenend zijn.

[24] Het jaar N is het jaar waarin met de uitvoering van het voorstel/initiatief wordt begonnen. Vervang "N" door het verwachte eerste jaar van uitvoering (bijvoorbeeld: 2021). Hetzelfde voor de volgende jaren.

3.3. Geraamde gevolgen voor de ontvangsten

– ☑ Het voorstel/initiatief heeft geen financiële gevolgen voor de ontvangsten.

– ☐ Het voorstel/initiatief heeft de hieronder beschreven financiële gevolgen:

  – ☐ voor de eigen middelen

  – ☐ voor overige ontvangsten

  – Geef aan of de ontvangsten worden toegewezen aan de begrotingsonderdelen voor uitgaven ☐

miljoen EUR (tot op drie decimalen)

Begrotingsonderdeel voor ontvangsten:	Voor het lopende begrotingsjaar beschikbare kredieten	Gevolgen van het voorstel/initiatief[25]						
		Jaar **N**	Jaar **N+1**	Jaar **N+2**	Jaar **N+3**	Vul zoveel jaren in als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)		
Artikel ….								

Vermeld voor de toegewezen ontvangsten het (de) betrokken begrotingsonderde(e)l(en) voor uitgaven.

Andere opmerkingen (bijv. over de methode/formule voor de berekening van de gevolgen voor de ontvangsten of andere informatie).

[25] Voor traditionele eigen middelen (douanerechten en suikerheffingen) moeten nettobedragen worden vermeld, d.w.z. brutobedragen na aftrek van 20 % aan inningskosten.