Raad van de
Europese Unie

Brussel, 31 oktober 2022
(OR. en)

14128/22

Interinstitutioneel dossier:
2022/0085(COD)

CYBER 343
TELECOM 428
INST 396
CSC 472
CSCI 157
INF 176
FIN 1158
BUDGET 22
DATAPROTECT 294
CODEC 1617

NOTA I/A-PUNT

van:	het secretariaat-generaal van de Raad
aan:	het Comité van permanente vertegenwoordigers (2e deel)/de Raad
nr. vorig doc.:	10097/5/22 REV 5
nr. Comdoc.:	7474/22 + ADD 1
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 - Algemene oriëntatie

INLEIDING

1. De Commissie heeft op 22 maart 2022 het voorstel aangenomen voor een verordening betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie. Het voorstel was een van de maatregelen in de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk[1], die tot doel heeft de collectieve weerbaarheid van de Unie tegen cyberdreigingen te versterken.

1 Doc. 14133/20.

In zijn conclusies van 22 maart 2021 over deze strategie[2] heeft de Raad benadrukt dat cyberbeveiliging van essentieel belang is voor de werking van openbare diensten en instellingen, zowel op nationaal als op EU-niveau, en voor onze samenleving en de gehele economie.

2. Het voorstel van de Commissie, dat gebaseerd is op artikel 298 van het Verdrag betreffende de werking van de Europese Unie, heeft tot doel het cyberbeveiligingsniveau bij de instellingen, organen en instanties van de Unie te verbeteren door een gemeenschappelijk kader vast te stellen, met inachtneming van de autonomie van elke entiteit van de Unie. Meer in het bijzonder heeft het voorstel de volgende doelstellingen:

   – het versterken van het mandaat en de financiering van CERT-EU (autonoom interinstitutioneel computercrisisresponsteam voor de entiteiten van de Unie);

   – het opzetten van een interinstitutionele structuur (interinstitutionele raad voor cyberbeveiliging - IICB) waarin vertegenwoordigers van alle entiteiten van de Unie bijeenkomen om de correcte uitvoering van de verordening te waarborgen;

   – het invoeren van de verplichting voor de entiteiten van de Unie om met CERT-EU (niet-gerubriceerde) informatie te delen over incidenten, en significante dreigingen, kwetsbaarheden en incidenten te melden; en

   – het bevorderen van de coördinatie en samenwerking in het kader van de respons op significante incidenten.

3. Het Europees Parlement heeft mevrouw Henna Virkkunen (PPE) aangesteld als rapporteur van de bevoegde Commissie ITRE. Het ontwerpverslag werd op 7 oktober 2022 bekendgemaakt.

4. De Europese Toezichthouder voor gegevensbescherming heeft op 17 mei 2022 advies uitgebracht[3].

---

[2] Doc. 6722/21.
[3] Doc. 9252/22.

5. In de Raad is de Horizontale Groep cybervraagstukken tijdens het Franse voorzitterschap op 29 maart 2022 begonnen met de bespreking van het voorstel. Het Franse voorzitterschap heeft de eerste compromistekst opgesteld, die in juni 2022 in de Horizontale Groep cyber-vraagstukken is besproken, en heeft op 21 juni 2022 de Raad een voortgangsverslag[4] voorgelegd.

6. Tijdens het Tsjechische voorzitterschap heeft de Horizontale Groep cybervraagstukken acht vergaderingen[5] gewijd aan besprekingen over het voorstel en over verschillende opeenvolgende compromisteksten.

7. Op 23 mei 2022 heeft het voorzitterschap het Beveiligingscomité (CSC) om advies verzocht over de aspecten van het voorstel die verband houden met informatiebeveiliging en met name gerubriceerde informatie. Het CSC heeft op 19 september 2022 advies uitgebracht[6]. Zoals het CSC voorstelt, is gerubriceerde EU-informatie uitdrukkelijk uitgesloten van het toepassings-gebied van de verordening. De bepalingen met betrekking tot vrijstelling van de verplichtingen tot delen en rapporteren van informatie die van buiten de entiteiten van de Unie is ontvangen, zijn dienovereenkomstig gewijzigd.

8. Op 28 oktober 2022 heeft de Horizontale Groep cybervraagstukken overeenstemming bereikt over de compromistekst van het voorzitterschap in de bijlage.

---

4 Doc. 9719/22.
5 6 en 20 juli, 13, 21 en 28 september, 5, 19 en 28 oktober 2022.
6 Doc. 12603/22 + COR 1.

BELANGRIJKSTE PUNTEN

9. De lidstaten zijn tevreden over dit voorstel, omdat het op het juiste moment komt als aanvulling op de toekomstige richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS 2), en steunen de algemene doelstellingen ervan. Zij pleiten echter voor verdere afstemming op NIS 2, meer wederkerigheid bij de uitwisseling van informatie tussen de entiteiten van de Unie en de lidstaten, en wijzen op het buitensporig vrijwillige karakter van sommige van de voorgestelde maatregelen. De lidstaten geven er ook de voorkeur aan om de gezamenlijke cybereenheid (waarvan het mandaat en de samenstelling nog moeten worden vastgesteld) niet te vermelden.

10. Op basis van de besprekingen in de Horizontale Groep cybervraagstukken worden de volgende punten als belangrijke politieke kwesties aangemerkt.

a) Afstemming op de toekomstige NIS 2-richtlijn

Op verzoek van de lidstaten is er verder afgestemd op de toekomstige NIS 2-richtlijn, namelijk:

- een aantal definities (artikel 3) is afgestemd op die in NIS 2;
- er is een nieuw artikel 7a ingevoegd over vrijwillige collegiale toetsingen, in overeenstemming met NIS 2, aangepast aan de behoeften van Unie-entiteiten;
- de rapportageverplichtingen in artikel 20 zijn afgestemd op die in NIS 2.

b) Samenstelling van de interinstitutionele raad voor cyberbeveiliging (IICB) (artikel 9)

Na de besprekingen over de wijze waarop vertegenwoordigers van de lidstaten passend worden betrokken bij de werkzaamheden van de IICB, is een compromis bereikt in de vorm van een verklaring van de Raad voor de notulen.

c) Institutionele autonomie

Er is een evenwichtige aanpak gevonden tussen de wil van de lidstaten om de nalevingsmechanismen te versterken en de noodzaak om het beginsel van institutionele autonomie te eerbiedigen, met name wat betreft audits en disciplinaire maatregelen (artikel 11).

Tot slot staat in overweging 8 niet langer het specifieke percentage dat van de IT-begroting aan cyberbeveiliging wordt besteed.

CONCLUSIE

11. Het Comité van permanente vertegenwoordigers wordt verzocht:

(a) zijn goedkeuring te hechten aan de compromistekst in de bijlage, die vervolgens het mandaat zal vormen voor onderhandelingen met het Europees Parlement;

(b) de Raad te verzoeken de compromistekst in bijlage dezes in zijn zitting van 18 november 2022 goed te keuren, en de verklaring van de Raad in het addendum bij dit document in de notulen op te nemen.

BIJLAGE

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 de zich ontwikkelende technologie en connectiviteit zijn tegenwoordig kernkenmerken van alle activiteiten van de entiteiten van de Unie, maar digitale weerbaarheid is hier nog onvoldoende ingebouwd.

(2) De [...] **entiteiten** van de Unie hebben te kampen met constant veranderende cyber-dreigingen. 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 [...] **entiteiten** 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 [...] **entiteit** van de Unie, breder kan uitwaaieren en ingrijpende langdurige negatieve gevolgen voor de andere entiteiten kan hebben. Bovendien zijn de IT-omgevingen van bepaalde [...] **entiteiten** 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. **Voorts behandelen entiteiten van de Unie grote hoeveelheden vaak gevoelige informatie van de lidstaten, en kunnen incidenten derhalve ook negatieve gevolgen hebben voor de lidstaten. Daarom is de cyberbeveiliging van de entiteiten van de Unie ook voor de lidstaten van groot belang. Informatie over een specifiek incident kan ertoe leiden dat soortgelijke cyberdreigingen of incidenten waarmee andere lidstaten te kampen hebben, gemakkelijker worden ontdekt.**

(4) De [...] **entiteiten** 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 [...] **entiteiten** van de Unie een hoog gezamenlijk niveau van cyberbeveiliging bereiken, door **cyberbeveiligings-maatregelen uit te voeren**, [...] informatie uit te wisselen en samen te werken.

(5) 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 [...] **entiteiten** van de Unie hetzelfde doen en zorgen voor regels die in overeenstemming zijn met Richtlijn [NIS 2-voorstel] en het ambitieniveau ervan weerspiegelen.

(6) Om een hoog gezamenlijk niveau van cyberbeveiliging te bereiken, moeten de [...] **entiteiten** 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 [...]. **Dat kader moet cyberbeveiligingsbeleid omvatten, inclusief procedures om de doeltreffendheid van uitgevoerde cyberbeveiligingsmaatregelen te evalueren. Het moet gebaseerd zijn op een alle risico's omvattende benadering, die erop gericht is netwerk- en informatiesystemen alsook de fysieke omgeving van die systemen te beschermen tegen gebeurtenissen als diefstal, brand, overstromingen, uitval van telecommunicatie of stroom, of tegen ongeoorloofde fysieke toegang tot en beschadiging en verstoring van informatie en informatieverwerkingsfaciliteiten van entiteiten van de Unie, waardoor de beschikbaarheid, authenticiteit, integriteit en betrouwbaarheid van via netwerk- en informatiesystemen opgeslagen, verzonden, verwerkte of toegankelijke gegevens zouden kunnen worden gecompromitteerd. Het kader moet recht doen aan de bevindingen van de risicoanalyse en rekening houden met alle betrokken technische, operationele en organisatorische risico's op cyberbeveiligingsgebied van de betrokken entiteit van de Unie.**

(6a) Teneinde de door het kader vastgestelde risico's te beheren, moet elke entiteit van de Unie ervoor zorgen dat passende en evenredige technische, operationele en organisatorische maatregelen worden genomen. Die moeten betrekking hebben op de domeinen, waaronder cyberbeveiligingsmaatregelen, die in deze verordening zijn opgenomen om de cyberbeveiliging van elke entiteiten van de Unie te versterken.

(6b) **De in het kader bepaalde activa en risico's en de conclusies van de regelmatig uitgevoerde maturiteitsbeoordelingen moeten tot uiting komen in het cyberbeveiligingsplan van elke entiteit van de Unie. Het cyberbeveiligingsplan moet de aangenomen cyberbeveiligingsplannen bevatten, teneinde de algemene cyberbeveiliging van de betrokken entiteit van de Unie te vergroten.**

(6c) **Aangezien cyberbeveiliging een continu proces is, moeten alle maatregelen regelmatig op geschiktheid en doeltreffendheid worden getoetst in het licht van veranderende risico's, activa en maturiteit van de entiteiten van de Unie. Het kader moet regelmatig en minstens om de drie jaar worden geëvalueerd; het cyberbeveiligingsplan moet minstens om de twee jaar, na elke maturiteitsbeoordeling of na elke evaluatie van het kader worden herzien.**

(6d) **Entiteiten van de Unie moeten regelmatig ter zake dienende informatie uitwisselen, onder meer over relevante incidenten en cyberdreigingen, en moeten daarbij het vertrouwelijk karakter en de passende bescherming van de door de rapporterende entiteit van de Unie verstrekte informatie garanderen.**

(6e) **Er dient een mechanisme te worden ingevoerd voor doeltreffende informatie-uitwisseling, coördinatie en samenwerking tussen de entiteiten van de Unie, waarbij de rollen en verantwoordelijkheden van de betrokken entiteiten van de Unie duidelijk zijn vastgelegd. Het voor EU-CyCLONe aangewezen contactpunt moet met de uitgewisselde informatie rekening houden wanneer het met EU-CyCLONe relevante informatie deelt als bijdrage tot het gedeelde situatiebewustzijn.**

(7) De verschillen tussen de [...] **entiteiten** 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 [...] **entiteiten** van de Unie, of hun institutionele autonomie aantasten. Die [...] **entiteiten** van de Unie moeten dus hun eigen kaders voor het beheer, de governance en de controle met betrekking tot cyberbeveiligings-risico's opstellen alsook hun eigen **cyberbeveiligingsplannen** [...], en moeten [...] cyberbeveiligings**maatregelen** vaststellen. **Bij de uitvoering van die maatregelen moet terdege rekening worden gehouden met de synergie tussen entiteiten van de Unie, met het oog op een goed beheer van de middelen en kostenoptimalisatie. Tevens moet erop worden toegezien dat de maatregelen geen negatieve gevolgen hebben voor de efficiënte informatie-uitwisseling door de entiteiten van de Unie en voor de operaties met andere entiteiten van de Unie en nationale bevoegde instanties.**

(8) Om te voorkomen dat aan [...] **entiteiten** 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. Elke [...] **entiteit** van de Unie moet beogen een passend percentage van zijn IT-begroting aan betere cyberbeveiliging te besteden [...]. **Tijdens de maturiteitsbeoordeling moet ook worden nagegaan of de uitgaven voor cyberbeveiliging van de entiteit van de Unie in verhouding staan tot de risico's waaraan ze is blootgesteld.**

(9) Voor een hoog gezamenlijk niveau van cyberbeveiliging is vereist dat cyberbeveiliging wordt geplaatst onder het toezicht van het hoogste managementniveau van elke [...] **entiteit** van de Unie. **[...] Het hoogste managementniveau dient toezicht te houden op de uitvoering van deze verordening, waaronder het tot stand brengen van een kader voor beheer, governance en controle met betrekking tot cyberbeveiligings-risico's, van cyberbeveiligingsplannen en alomvattende cyberbeveiligingsmaatregelen.** Het aanpakken van de cyberbeveiligingscultuur, dat wil zeggen de dagelijkse cyber-beveiligingspraktijk, maakt in elke [...] **entiteit** van de Unie integraal deel uit van een cyberbeveiliging**skader** [...].

(10) [...] [...] **Cyberbeveiligings**maatregelen moeten deel uitmaken van het cyber-beveiliging[...]**plan** en nader worden gespecificeerd in richtsnoeren of aanbevelingen van CERT-EU. Bij het vaststellen van maatregelen en richtsnoeren moet terdege rekening worden gehouden **met de laatste stand van de techniek en, indien van toepassing, de betrokken Europese en internationale normen**, met de Uniewetgeving en -beleidsmaatregelen ter zake, 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 krachtens artikel 49 van Verordening (EU) 2019/881 vastgestelde specifieke EU-cyberbeveiligings-certificeringsregelingen. **Waar mogelijk moet CERT-EU samenwerken met Enisa.**

(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 Unie verder te helpen verbeteren, als voorbeeld van zichtbare interinstitutionele samenwerking op het gebied van cyberbeveiliging. 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[7]. Deze [...] **verordening** moet **voorzien in een uitgebreide reeks voorschriften over de organisatie, het functioneren en de werking van CERT-EU. De bepalingen van deze verordening hebben voorrang op de in december 2017 gesloten inter-institutionele regeling betreffende de organisatie en het functioneren van CERT-EU.**

[...]

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

(13) Veel cyberaanvallen zijn onderdeel van bredere campagnes die gericht zijn tegen groepen [...] **entiteit**en van de Unie of belangengemeenschappen die [...] **entiteiten** van de Unie omvatten. Om proactief opsporings-, incidentrespons- of beperkende maatregelen te kunnen treffen, moeten de [...] **entiteiten** van de Unie CERT-EU in kennis stellen van dreigingen, [...] kwetsbaarheden, **bijna-ongelukken en** [...] incidenten op het gebied van cyberveiligheid, en moeten zij passende technische details delen, op grond waarvan opsporings-, incidentrespons- of beperkende maatregelen kunnen worden getroffen tegen vergelijkbare dreigingen, **kwetsbaarheden, bijna-ongelukken** en incidenten op het gebied van cyberveiligheid binnen andere [...] **entiteiten** van de Unie. Op basis van dezelfde aanpak als die van Richtlijn [NIS 2-voorstel] moeten entiteiten **van de Unie** worden verplicht binnen 24 uur nadat zij van een significant incident kennis hebben gekregen, CERT-EU [...] **een vroegtijdige waarschuwing** te verstrekken. Aan de hand van die informatie-uitwisseling moet CERT-EU de informatie kunnen verspreiden onder andere [...] **entiteiten** 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 [...].

(13a) Deze richtlijn voorziet in een meerfasige aanpak voor het melden van significante incidenten, om het juiste evenwicht te vinden tussen enerzijds een snelle melding die de potentiële verspreiding van significante incidenten helpt te beperken en entiteiten van de Unie in staat stelt steun te zoeken, en anderzijds een uitvoerige melding die waardevolle lessen trekt uit individuele incidenten en mettertijd de veerkracht van individuele entiteiten van de Unie ten aanzien van cyberdreigingen verbetert. Deze verordening moet daarom de melding omvatten van incidenten die op basis van een eerste beoordeling door de entiteit van de Unie, de werking van de entiteit van de Unie ernstig zouden kunnen verstoren of voor de betrokken entiteit tot financiële verliezen zou kunnen leiden dan wel andere natuurlijke of rechtspersonen aanzienlijke materiële of immateriële schade zou kunnen berokkenen. Bij die eerste beoordeling moet onder andere rekening worden gehouden met de getroffen netwerk- en informatiesystemen, in het bijzonder met hun belang voor de werking van de entiteit van de Unie, de ernst en de technische kenmerken van een cyberdreiging, de achterliggende kwetsbaarheden die worden uitgebuit en de ervaring die de entiteit van de Unie met soortgelijke incidenten heeft. Indicatoren zoals de mate waarin de werking van de entiteit van de Unie is aangetast, de duur van het incident of het aantal getroffen natuurlijke of rechtspersonen, kunnen een belangrijke rol spelen bij het bepalen of de operationele verstoring ernstig is.

(13b) Aangezien de infrastructuur en de netwerken van de betrokken entiteit van de Unie en die van de lidstaat waar die is gevestigd, onderling verbonden zijn, is het voor die lidstaat van cruciaal belang dat hij onmiddellijk wordt geïnformeerd over een significant incident in die entiteit van de Unie. Daarom moet de getroffen entiteit van de Unie daarvan kennis geven aan de nationale tegenhanger van CERT-EU, die door de lidstaat is aangewezen overeenkomstig Richtlijn [NIS 2-voorstel], binnen dezelfde termijn als die welke voor het melden van een significant incident aan CERT-EU geldt. Ook CERT-EU moet die nationale tegenhanger informeren wanneer het kennis krijgt van een significant incident, tenzij de getroffen entiteit van de Unie dat al heeft gedaan.

(14) Naast meer taken en een grotere rol voor CERT-EU, moet een interinstitutionele raad voor cyberbeveiliging (IICB) worden opgericht die, **om een hoog gezamenlijk niveau van cyberbeveiliging onder de** [...] **entiteiten** van de Unie te bevorderen**, een exclusieve rol moet hebben in** [...] [...] het toezicht op de uitvoering van deze verordening door de [...] **entiteiten** van de Unie en **in** het toezicht op de uitvoering van de algemene prioriteiten en doelstellingen door CERT-EU, en die CERT-EU strategische leiding moet bieden. De IICB moet **derhalve** de vertegenwoordiging van de instellingen waarborgen, en moet via het netwerk van agentschappen van de Unie zijn samengesteld uit vertegenwoordigers van instanties en organen. **De organisatie en werking van de IICB moeten nader worden geregeld door zijn reglement van orde, dat verdere bijzonderheden met betrekking tot regelmatige vergaderingen van de IICB kan bevatten, waaronder jaarlijkse bijeenkomsten op politiek niveau waar de IICB via vertegenwoordigers van het hoogste managementniveau van elk IICB-lid een strategische bespreking kan voeren en strategische sturing kan krijgen. Daarnaast kan de IICB een uitvoerend comité oprichten dat de IICB in zijn taken bijstaat en waaraan hij een aantal taken en bevoegdheden kan overdragen, vooral taken die een bepaalde expertise van de leden vereisen, bijvoorbeeld de goedkeuring van de dienstencatalogus en actualiseringen daarvan, de voorwaarden voor dienstenniveauovereenkomsten, de evaluatie van documenten en verslagen die de entiteiten van de Unie overeenkomstig deze verordening aan de IICB voorleggen, of taken in verband met de voorbereiding van besluiten over nalevingsmaatregelen van de IICB en het toezicht op de uitvoering daarvan. De IICB moet het reglement van orde van het uitvoerend comité vaststellen, met inbegrip van de taken en bevoegdheden daarvan.**

(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 [...] **entiteiten** van de Unie binnen een bepaalde termijn met klem wordt aangeraden te treffen. **De IICB kan CERT-EU opdragen om een oproep tot actie, of een voorstel voor richtsnoeren of een aanbeveling, uit te vaardigen, in te trekken of te wijzigen.**

(16) De IICB moet toezicht houden op de naleving van deze verordening en gevolg geven aan de richtsnoeren, aanbevelingen en oproepen tot actie [...]. 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 [...] **entiteiten** van de Unie en andere belanghebbenden. [...] **Indien de IICB vaststelt dat de entiteiten van de Unie deze verordening of de krachtens deze verordening vastgestelde richtsnoeren, aanbevelingen en oproepen tot actie niet toepassen of uitvoeren, kan hij, onverminderd de interne procedures van de entiteit van de Unie in kwestie, overgaan tot nalevingsmaatregelen. Het stelsel van nalevingsmaatregelen moet volgens toenemende mate van ernst worden gebruikt, wat betekent dat de IICB bij het nemen van nalevingsmaatregelen begint bij een waarschuwing, als minst ernstige maatregel, en zo nodig opschuift naar de meest ernstige maatregel, namelijk het afgeven van een advies tot tijdelijke opschorting van de gegevensstromen naar de entiteit van de Unie in kwestie, zulks slechts in uitzonderlijke gevallen, wanneer de betrokken entiteit van de Unie langdurig, bewust en/of in ernstige mate de verplichtingen uit hoofde van deze verordening niet nakomt.**

(16a) Een waarschuwing is de minst ernstige nalevingsmaatregel, heeft betrekking op bij de entiteit van de Unie vastgestelde tekortkomingen en omvat aanbevelingen om de cyberbeveiligingsdocumenten binnen een bepaalde termijn te wijzigen. Alle entiteiten van de Unie kunnen een waarschuwing krijgen, tenzij zulks op passende wijze overeenkomstig deze verordening wordt beperkt.

(16b) De IICB kan voorts aanbevelen dat de entiteit van de Unie aan een audit wordt onderworpen. De entiteiten van de Unie kunnen hiervoor gebruikmaken van de eigen interne auditfunctie. De IICB kan ook voorschrijven dat de audit door een derde partij wordt uitgevoerd, onder meer door een wederzijds overeengekomen dienstverlener uit de private sector.

(16c) Op basis van de resultaten van een op aanbeveling of verzoek van de IICB uitgevoerde audit, kan de IICB de entiteit van de Unie vervolgens verzoeken om het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's in overeenstemming te brengen met de bepalingen van deze verordening.

(16d) Aangezien de lidstaten met betrokken entiteiten van de Unie mogelijk gevoelige informatie uitwisselen, is de cyberbeveiliging van de geadresseerde van die informatie van cruciaal belang voor de lidstaten. Daarom kan de IICB, in uitzonderlijke gevallen wanneer de entiteit van de Unie langdurig, bewust en/of in ernstige mate haar verplichtingen niet nakomt, als uiterste redmiddel alle lidstaten en entiteiten van de Unie een advies afgeven met een aanbeveling om de gegevensstromen naar de entiteit van de Unie tijdelijk op te schorten; de opschorting blijft van kracht totdat de cyberbeveiligingssituatie van deze entiteit is gecorrigeerd. Dit advies moet via de gepaste beveiligde communicatiekanalen aan alle lidstaten en entiteiten van de Unie worden meegedeeld.

(16e) **Om de correcte uitvoering van deze verordening te garanderen moet de IICB, wanneer zij vaststelt dat een aanhoudende inbreuk op deze verordening door een entiteit van de Unie rechtstreeks wordt veroorzaakt door handelen of nalaten van een personeelslid van die entiteit, ook op het hoogste managementniveau, de betrokken entiteit van de Unie verzoeken om gepaste maatregelen te nemen ten aanzien van dat personeelslid, overeenkomstig het Statuut van de ambtenaren of andere gelijkwaardige, in sommige entiteiten van de Unie toepasselijke voorschriften. Deze maatregelen kunnen, bijvoorbeeld, tuchtprocedures omvatten en zo nodig in het specifieke geval van Unieagentschappen, een verzoek aan de bevoegde autoriteit om de nodig stappen zetten opdat de mogelijke verantwoordelijke voor de aanhoudende inbreuk op deze verordening uit zijn functies wordt ontheven.**

(17) Het moet de missie van CERT-EU zijn om bij te dragen tot de beveiliging van de IT-omgeving van alle [...] **entiteiten** van de Unie. **Wanneer CERT-EU overweegt om op verzoek van een entiteit van de Unie technisch advies of technische input voor beleidskwesties ter zake te verstrekken, moet het ervoor zorgen dat dit de uitvoering van zijn andere in deze verordening bepaalde taken niet belemmert.**

(17a) CERT-EU moet optreden als het equivalent van de aangewezen coördinator voor de [...] **entiteiten** 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], **en moet beleid inzake het beheer van kwetsbaarheden ontwikkelen waarin ruimte is voor het bevorderen en faciliteren van vrijwillige gecoördineerde bekendmaking van kwetsbaarheden.**

[...]

(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 (CSIRT's). Verder moet CERT-EU overeenkomstig Aanbeveling (EU) 2017/1584 van de Commissie[8] 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.

[8] 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).

(20) Bij de ondersteuning van operationele cyberbeveiliging moet CERT-EU gebruikmaken van de beschikbare deskundigheid van het Agentschap van de Europese Unie voor cyberbeveiliging (**Enisa**), door middel van gestructureerde samenwerking zoals bedoeld in Verordening (EU) 2019/881 van het Europees Parlement en de Raad[9]. 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 [...] **Enisa** samenwerken inzake dreigingsanalyse en zijn dreigingslandschapverslag regelmatig met het agentschap delen.

[...][10]

(22) **De activiteiten van en de informatieverwerking door CERT-EU in het kader van deze verordening, kunnen de verwerking van persoonsgegevens omvatten.** Alle overeenkomstig deze verordening verwerkte persoonsgegevens moeten overeenkomstig de gegevensbeschermingswetgeving, met inbegrip van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad[11], worden verwerkt. **Indien krachtens deze verordening persoonsgegevens worden verstrekt aan in de Unie gevestigde ontvangers die geen entiteiten van de Unie zijn, dient dit te gebeuren overeenkomstig artikel 9 van Verordening (EU) 2018/1725.**

---

9 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).

~~**10**~~

11 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).

(23) CERT-EU en de [...] **entiteiten** van de Unie moeten informatie verwerken overeenkomstig de **toepasselijke** regels [...] inzake informatiebeveiliging [...] [...].

(23a) Voor het delen van informatie worden zichtbare markeringen gebruikt om aan te geven dat de ontvanger van de informatie ten aanzien van het delen van informatie beperkingen in acht moet nemen op basis van, met name, niet-openbaarmakings-overeenkomsten of informele niet-openbaarmakingsovereenkomsten zoals het verkeerslichtprotocol of andere duidelijke indicaties door de bron. Onder het verkeerslichtprotocol moet worden verstaan een middel om informatie te verstrekken over beperkingen in verband met de verdere verspreiding van informatie. Het wordt gebruikt door nagenoeg elk computer security incident response team (CSIRT) en door sommige centra voor informatie-uitwisseling en -analyse.

(24) **Deze verordening en de nieuwe aan CERT-EU toegewezen taken zullen geen gevolgen hebben voor de totale uitgaven in het meerjarig financieel kader.** Aangezien de diensten en taken van CERT-EU in het belang van alle [...] **entiteiten** van de Unie zijn, moet elke [...] **entiteit** van de Unie met IT-uitgaven een billijke bijdrage aan die diensten en taken leveren. Die bijdragen laten de budgettaire autonomie van de [...] **entiteiten** van de Unie onverlet. **Alle entiteiten van de Unie en hun bestuur moeten ervoor zorgen dat hun middelen op het huidige niveau optimaal worden aangewend en dat de efficiëntiewinst toeneemt doordat zij onder meer de interinstitutionele samenwerking op het gebied van cyberbeveiliging verdiepen. Derhalve moet een gezamenlijke aanpak bij het bundelen van administratieve uitgaven voorrang krijgen boven individuele uitgaven van entiteiten van de Unie.**

(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. **Voorts wordt de Europese Rekenkamer verzocht om het functioneren van CERT-EU op regelmatig te evalueren,**

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

Hoofdstuk I
ALGEMENE BEPALINGEN

Artikel 1

Onderwerp

1. Bij deze verordening worden **maatregelen vastgesteld met als doel in entiteiten van de Unie een hoog gezamenlijk niveau van cyberbeveiliging te bereiken** [...]**.**

2. Daartoe voorziet deze verordening in:

(c) verplichtingen voor **elke** [...] **entiteit** van de Unie om een [...] kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's op te zetten;

(d) verplichtingen voor [...] entiteiten van de Unie inzake risicobeheer [...]**,** rapportage **en het delen van informatie** op het gebied van cyberbeveiliging;

(e) voorschriften inzake de organisatie, **het functioneren** en de werking van het [...] **autonoom interinstitutioneel computercrisisresponsteam** voor de [...] **entiteiten** van de Unie (CERT-EU), en inzake de organisatie, **het functioneren** en de werking van de interinstitutionele raad voor cyberbeveiliging **(IICB)**;

(f) voorschriften met betrekking tot het toezicht op de uitvoering van deze verordening.

Artikel 2

Toepassingsgebied

1. Deze verordening is van toepassing op [...] alle **entiteiten** van de Unie en op [...] [...] CERT-EU en de **IICB.**

2. Deze verordening laat de krachtens de Verdragen bepaalde institutionele autonomie onverlet.

3. Met uitzondering van artikel 12, lid 7, is deze verordening niet van toepassing op netwerk- en informatiesystemen die gerubriceerde EU-informatie verwerken.

Artikel 3

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

1. "[...] **entiteiten** 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 [...] **als gedefinieerd in** artikel 4, punt 1, van Richtlijn [NIS 2-voorstel];

3. "beveiliging van netwerk- en informatiesystemen": een netwerk- en informatiesysteem **als gedefinieerd in** artikel 4, punt 2, van Richtlijn [NIS 2-voorstel];

4. "cyberbeveiliging": cyberbeveiliging **als gedefinieerd in artikel 2, punt 21, van Verordening (EU) 2019/881**;

5. "hoogste managementniveau": een leidinggevende, een leidinggevend of coördinatie- en toezichtorgaan op het hoogste bestuurlijke niveau **met beslissingsbevoegdheid**, met inachtneming van de bestuursregelingen op hoog niveau binnen [...] elke **entiteit** van de Unie;

5a. "bijna-ongeluk": een bijna-ongeluk als gedefinieerd in artikel 4, punt 4a, van Richtlijn [NIS 2-voorstel];

6. "incident": een incident **als gedefinieerd in** artikel 4, punt 5, van Richtlijn [NIS 2-voorstel];

[...]

8. "ernstig **incident**": een incident **met een verstoringsniveau dat het responsvermogen van een entiteit van de Unie en CERT-EU overstijgt of dat significante gevolgen heeft voor ten minste twee entiteiten van de Unie;** [...]

9. "incidentenbehandeling": incidentenbehandeling [...] **als gedefinieerd in** artikel 4, punt 6, van Richtlijn [NIS 2-voorstel];

10. "cyberdreiging": cyberdreiging [...] **in de zin van in** artikel 2, punt 8, van Verordening (EU) 2019/881;

[...]

12. "kwetsbaarheid": kwetsbaarheid in de zin van artikel 4, punt 8, van Richtlijn [NIS 2-voorstel];

[...]

14. "[...] risico": risico **in de zin van artikel 4, punt 7b, van Richtlijn [NIS 2-voorstel] [...];**

[...]

[...]

Artikel 3a

Verwerking van persoonsgegevens

1) De verwerking van persoonsgegevens door CERT-EU, de IICB of entiteiten van de Unie in het kader van deze verordening geschiedt overeenkomstig Verordening (EU) 2018/1725.

2) CERT-EU, de IIBC en entiteiten van de Unie verwerken persoonsgegeven en wisselen die uit voor zover dit nodig is en uitsluitend met als doel hun respectieve verplichtingen uit hoofde van deze verordening na te komen.

HOOFSTUK II
MAATREGELEN VOOR EEN HOOG GEZAMENLIJK NIVEAU VAN CYBERBEVEILIGING

Artikel 4

Kader voor het beheer, de governance en de controle met betrekking tot risico's

1. Elke [...] **entiteit** van de Unie zet haar eigen kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's op (hierna "het kader"), ter ondersteuning van de missie van die entiteit. **Het kader** staat 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 niet-geclassificeerde IT-omgeving van de [...] betrokken [...] **entiteit van de Unie**, met inbegrip van de IT-omgeving on site, **operationele technologienetwerken**, 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 **is gebaseerd op een alle risico's omvattende benadering en op een maturiteitsbeoordeling als bedoeld in artikel 6, die alle ter zake dienende technische, operationele en organisatorische risico's bestrijkt die gevolgen zouden kunnen hebben voor de cyberbeveiliging van de betrokken entiteit van de Unie [...].**

2a. Het kader omvat cyberbeveiligingsbeleid, waaronder doelstellingen en prioriteiten voor de beveiliging van netwerk- en informatiesystemen, alsook beleid en procedures om de doeltreffendheid van de uitgevoerde maatregelen voor het beheer van cyberbeveiligings-risico's te evalueren en de rollen en verantwoordelijkheden van personeelsleden te definiëren.

2b. Het kader wordt regelmatig geëvalueerd, en minstens om de drie jaar in het licht van de veranderende risico's, de activa en de maturiteit van de entiteit van de Unie.

3. Het hoogste managementniveau van elke [...] **entiteit** van de Unie houdt toezicht op de nakoming door **de entiteit** van de verplichtingen in verband met het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's, onverminderd de formele verantwoordelijkheden van andere managementniveaus voor naleving en risicobeheer binnen hun respectieve bevoegdheid.

3a. **Het hoogste managementniveau van elke entiteit kan, waar passend en onverminderd zijn verantwoordelijkheid voor de uitvoering van deze verordening, specifieke verplichtingen uit hoofde van deze verordening overdragen aan ander hoger leidinggevend personeel binnen de entiteit. Ongeacht enige overdacht van zijn specifieke verplichtingen, kan het hoogste managementniveau aansprakelijk worden gehouden voor de niet-nakoming door de entiteiten van hun verplichtingen uit hoofde van deze verordening.**

3b. Het hoogste managementniveau van elke entiteit van de Unie zorgt ervoor dat de entiteiten van de Unie het cyberbeveiligingsplan met maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren, overeenkomstig hun risicoanalyse, zodat het kader in overeenstemming met deze verordening wordt uitgevoerd.

[...]

5. Elke [...] **entiteit** van de Unie stelt een lokale cyberbeveiligingsfunctionaris of een gelijkwaardige functionaris aan, die fungeert als het centrale contactpunt voor alle cyberbeveiligingsaspecten.

De lokale cyberbeveiligingsfunctionaris faciliteert de uitvoering van deze verordening en brengt aan het hoogste managementniveau regelmatig rechtstreeks verslag uit over de stand van de uitvoering.

Ongeacht of in elke entiteit van de Unie de lokale cyberbeveiligingsfunctionaris het centrale contactpunt is, kan een entiteit van de Unie, op basis van een dienstenniveau-overeenkomst tussen die entiteit van de Unie en CERT-EU, bepaalde aan de uitvoering van deze verordening gerelateerde taken van de lokale cyberbeveiligingsfunctionaris aan CERT-EU overdragen. De IICB besluit of deze dienstverlening onderdeel is van de basisdienstverlening van CERT-EU, met inachtneming van de personele en financiële middelen van de betrokken entiteit van de Unie. Elke entiteit van de Unie geeft aan CERT-EU onmiddellijk kennis van de aanwijzing van een lokale cyberbeveiligings-functionaris en van alle latere wijzigingen daarvan. CERT-EU houdt de lijst bij van aangewezen lokale cyberbeveiligingsfunctionarissen, die regelmatig wordt geactualiseerd.

6. Het hoger leidinggevend personeel in de zin van artikel 29, lid 2, van het Statuut van de ambtenaren[12] of een andere ambtenaar van gelijkwaardig niveau van elke entiteit 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 voor de activiteiten van de organisatie te begrijpen en te beoordelen.

---

12 **Verordening nr. 259/68 van de Raad van 29 februari 1968 tot vaststelling van het Statuut van de ambtenaren van de Europese Gemeenschappen en de Regeling welke van toepassing is op de andere personeelsleden van deze Gemeenschappen, (PB L 56 van 4.3.1968, blz. 1)**.

7. Elke entiteit van de Unie beschikt over doeltreffende mechanismen om te waarborgen dat een passend percentage van de IT-begroting aan cyberbeveiliging wordt besteed. Bij het vaststellen van dit percentage wordt terdege rekening gehouden met het kader.

Artikel 5

Maatregelen voor het beheer van cyberbeveiligingsrisico's [...]

1. [...] **Elke entiteit van de Unie zorgt ervoor, onder het toezicht van haar** hoogste managementniveau, [...] [...] **dat passende en evenredige technische, operationele en organisatorische maatregelen worden genomen voor het beheer van de risico's die worden genoemd in het in artikel 4, lid 1, bedoelde kader, en voor het voorkomen en/of tot een minimum beperken van de gevolgen van incidenten. Rekening houdend met de stand van de techniek en, indien van toepassing, de betrokken Europese en internationale normen, alsook met de kosten van de uitvoering, zorgen die maatregelen ervoor dat het beveiligingsniveau van netwerk- en informatiesystemen in verhouding staat tot de risico's. Bij het beoordelen van de evenredigheid van deze maatregelen wordt terdege rekening gehouden met de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit, de waarschijnlijkheid van incidenten en de ernst, alsook de maatschappelijke en economische gevolgen daarvan.**

[...]

3. Entiteiten van de Unie behandelen in hun cyberbeveiligingsplannen ten minste de volgende specifieke domeinen bij de uitvoering van de maatregelen voor het beheer van cyberbeveiligingsrisico's, conform de richtsnoeren en aanbevelingen van de IICB:

a) cyberbeveiligingsbeleid, bij de specificatie van de instrumenten en maatregelen die nodig zijn om de in de artikel 4 en artikel 5, lid 4, genoemde doelstellingen en prioriteiten te bereiken;

b) risicoanalyse en beleid inzake informatiesysteembeveiliging;

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

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

e) beveiliging van personele middelen en toegangscontrole;

f) beveiliging van operaties;

g) communicatiebeveiliging;

h) aankoop, ontwikkeling en onderhoud van systemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;

i) beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten van de betrekkingen tussen elke entiteit van de Unie en haar rechtstreekse leveranciers of dienstverlener. Entiteiten van de Unie houden rekening met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener, en met de algehele kwaliteit van de producten en cyberbeveiligings-praktijken van hun leveranciers en dienstverleners, veilige ontwikkelingsprocessen inbegrepen;

j) incidentenbehandeling en samenwerking met CERT-EU, zoals monitoring en registratie van de beveiliging;

k) bedrijfscontinuïteitsbeheer, zoals back-upbeheer en herstel na rampen, en crisisbeheer; en

l) bevorderen en ontwikkelen van programma's betreffende onderwijs, vaardigheden, bewustmaking, oefeningen en opleiding op het gebied van cyberbeveiliging.

4. Entiteiten van de Unie behandelen in hun cyberbeveiligingsplannen ten minste de volgende specifieke maatregelen voor het beheer van cyberbeveiligingsrisico's bij de uitvoering van de maatregelen voor het beheer van cyberbeveiligingsrisico's, conform de richtsnoeren en aanbevelingen van de IICB:

a) doelen en prioriteiten inzake het gebruik van cloudcomputingdiensten in de zin van artikel 4, punt 19, van Richtlijn [NIS 2-voorstel] en technische regelingen om thuiswerken mogelijk te maken;

b) concrete stappen om in de toekomst Zero Trust-beginselen te hanteren, waaronder een beveiligingsmodel, en een gecoördineerde strategie voor cyberbeveiliging en systeembeheer op basis van de onderkenning dat er zowel binnen als buiten de traditionele netwerkgrenzen dreigingen bestaan;

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

d) de totstandbrenging van veiligheid van softwaretoeleveringsketens door middel van criteria voor de ontwikkeling en evaluatie van veilige software;

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

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

ii) contractueel te bepalen dat incidenten, kwetsbaarheden en cyberdreigingen moeten worden gemeld, en door voor een passende respons en monitoring van incidenten te zorgen;

f) het gebruik van cryptografie en encryptie, in het bijzonder eind-tot-eindencryptie;

g) beveiligde communicatiesystemen binnen de organisatie.

Artikel 6

Maturiteitsbeoordelingen

1. Elke [...] **entiteit** van de Unie voert, **zo nodig bijgestaan door een gespecialiseerde derde partij**, ten minste om de drie jaar **een** [...] maturiteitsbeoordeling [...] 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.

2. Op aanbeveling van CERT-EU en na raadpleging van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) neemt de IICB binnen vier maanden na de inwerkingtreding van deze verordening richtsnoeren aan over de bij maturiteitsbeoordelingen te volgen methode.

3. Nadat de maturiteitsbeoordeling is voltooid, [...] legt de entiteit van de Unie die voor aan de IICB. De eerste maturiteitsbeoordeling wordt uiterlijk [12 maanden na de inwerkingtreding van deze verordening] uitgevoerd.

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 elke [...]**entiteit** van de Unie, na de opstelling van het [...] kader, na de vaststelling van de maatregelen voor het [...] beheer van **cyberbeveiligingsrisico's, [...] na de uitvoering van de maturiteitsbeoordeling, en niet later dan 21 maanden na de inwerkingtreding van deze verordening,** onverwijld een cyberbeveiligingsplan goed. Het **cyberbeveiligings**plan beoogt de algehele cyberbeveiliging van de **betrokken** entiteit [...] van de **Unie** te versterken en aldus bij te dragen tot [...] een hoog gezamenlijk niveau van cyberbeveiliging bij alle [...] **entiteiten** van de Unie. [...] **Het cyberbeveiligingsplan** bevat minstens de **maatregelen voor het beheer van cyberbeveiligingsrisico'sals bedoeld in artikel 5** [...]. Het **cyberbeveiligings-**plan wordt ten minste om de **twee** [...] jaar geëvalueerd, **of** na [...] **elke** [...] overeenkomstig artikel 6 uitgevoerde maturiteitsbeoordeling **of na elke evaluatie van het kader uit hoofde van artikel 4.**

2. [...]

3. Het cyberbeveiligingsplan **houdt rekening met** [...] de overeenkomstig **artikel 13** afgegeven toepasselijke richtsnoeren en aanbevelingen van CERT-EU.

4. **Nadat de maturiteitsbeoordeling is voltooid, legt de entiteit van de Unie die voor aan de IICB.**

Artikel 7a

Collegiale toetsing

1. Op aanbeveling van CERT-EU en na raadpleging van Enisa stelt de IICB uiterlijk … [24 maanden na de inwerkingtreding van deze verordening], aan de hand van de methode voor collegiale toetsing en de methode voor zelfbeoordeling overeenkomstig artikel 16 van Richtlijn [NIS 2-voorstel], indien nodig aangepast aan de behoeften van de entiteiten van de Unie, de methode en organisatorische aspecten van een collegiale toetsing vast om van gedeelde ervaringen te leren, het onderlinge vertrouwen te versterken, een hoog gezamenlijk niveau van cyberbeveiliging te bewerkstelligen en de cyberbeveiligingscapaciteiten van de entiteiten van de Unie en het nodige beleid voor de uitvoering van deze verordening te verbeteren. Deelname aan de collegiale toetsing is vrijwillig. Vertegenwoordigers van de lidstaten kunnen als waarnemers aan de collegiale toetsing deelnemen. De collegiale toetsingen worden uitgevoerd door cyberbeveiligings-deskundigen die zijn aangewezen door ten minste twee entiteiten van de Unie, verschillend van de entiteiten van de Unie die worden getoetst, en omvatten ten minste een van de volgende aspecten:

(i) het niveau van uitvoering van de maatregelen voor het beheer van cyber-beveiligingsrisico's en de rapportageverplichtingen bedoeld in de artikelen 5 en 20;

(ii) het niveau van de capaciteiten, met inbegrip van de beschikbare financiële, technische en personele middelen;

(iii) het niveau van uitvoering van het in artikel 19 bedoelde kader voor de uitwisseling van informatie;

(iv) specifieke kwesties van sectoroverschrijdende aard.

2. Entiteiten van de Unie kunnen vaststellen welke in lid 1, punt iv), genoemde specifieke kwesties moeten worden getoetst. De reikwijdte van de toetsing, met inbegrip van de vastgestelde kwesties, wordt vóór de aanvang van de collegiale toetsing aan de deelnemende entiteiten van de Unie meegedeeld.

3. Voordat de collegiale toetsing begint, kunnen entiteiten van de Unie een zelfbeoordeling van de getoetste aspecten uitvoeren en die zelfbeoordeling aan de aangewezen deskundigen verstrekken.

4. De intercollegiale toetsingen omvatten fysieke of virtuele bezoeken ter plaatse en uitwisselingen elders. Gelet op het beginsel van goede samenwerking verstrekken de aan collegiale toetsing onderworpen entiteiten van de Unie de aangewezen deskundigen de voor de beoordeling benodigde informatie, onverminderd de nationale of Uniewetgeving inzake de bescherming van gevoelige of gerubriceerde informatie. Alle informatie die via de collegiale toetsing wordt verkregen, wordt uitsluitend voor dat doel gebruikt. De deskundigen die aan de collegiale toetsing deelnemen, maken geen gevoelige of gerubriceerde informatie die zij in het kader van die toetsing hebben verkregen, bekend aan derden.

5. Zodra ze aan een collegiale toetsing zijn onderworpen, worden dezelfde aspecten die in de entiteiten van de Unie zijn beoordeeld, gedurende de twee jaar na de voltooiing van de collegiale toetsing niet meer onderworpen aan verdere collegiale toetsing in die entiteiten van de Unie, tenzij daarom wordt verzocht door de entiteiten van de Unie of anders is overeengekomen na een voorstel van de IICB.

6. De entiteiten van de Unie zorgen ervoor dat elk risico van belangenconflicten met betrekking tot de aangewezen deskundigen vóór de aanvang van de collegiale toetsing ter kennis van de andere entiteiten van de Unie en de IICB wordt gebracht. De aan de collegiale toetsing onderworpen entiteiten van de Unie kunnen tegen de aanwijzing van bepaalde deskundigen bezwaar maken om naar behoren gemotiveerde redenen die aan de aanwijzende entiteiten van de Unie worden meegedeeld.

7. **Deskundigen die deelnemen aan collegiale toetsingen stellen verslagen op over de bevindingen en conclusies van de toetsingen. De entiteiten van de Unie mogen over hun respectieve ontwerpverslagen opmerkingen maken, die bij de verslagen worden gevoegd. De verslagen bevatten aanbevelingen om de aspecten die onder de collegiale toetsing vallen te kunnen verbeteren. De verslagen worden, indien relevant, voorgelegd aan de IICB en het CSIRT-netwerk. Entiteiten van de Unie die worden beoordeeld, kunnen besluiten hun verslag of een bewerkte versie daarvan openbaar te maken.**

Artikel 8

Uitvoering

1. [...]

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

3. **Op verzoek van de IICB brengen de entiteiten van de Unie verslag uit over specifieke aspecten 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 **entiteiten** [...] **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 is als volgt samengesteld:

   a) één vertegenwoordiger aangewezen door elk van de volgende partijen:

      i) het Europees Parlement;

      ii) de Europese Raad

      iii) de Raad van de Europese Unie;

      iv) de Europese Commissie;

      v) het Hof van Justitie van de Europese Unie;

      vi) de Europese Centrale Bank;

vii) de Europese Rekenkamer;

viii) de Europese Dienst voor extern optreden;

ix) het Europees Economisch en Sociaal Comité;

x) het Europees Comité van de Regio's;

xi) de Europese Investeringsbank;

xii) het Europees Kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging; en

xiii) het Agentschap van de Europese Unie voor cyberbeveiliging.

b) drie vertegenwoordigers die door het netwerk van EU-agentschappen (EUAN) op voorstel van zijn adviescomité voor ICT worden [...] **aangewezen** om de belangen te behartigen van de organen en instanties die hun eigen IT-omgeving beheren. [...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

3a. De leden kunnen door een plaatsvervanger worden bijgestaan. Andere vertegenwoordigers van de hierboven vermelde **entiteiten** [...], of andere [...] **entiteiten** 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 [...] **twee** jaar. Zijn of haar plaatsvervanger wordt voor dezelfde duur volwaardig lid van de IICB.

6. De IICB komt **ten minste driemaal per jaar** bijeen op initiatief van zijn voorzitter **en/of** op verzoek van CERT-EU **en/**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**, de voorzitter van de NIS-samenwerkingsgroep, de voorzitter van EU-CyCLONe en de voorzitter van het CSIRT-netwerk,** of **hun** plaatsvervanger**s** [...] **kunnen als waarnemers** deel**nemen** aan IICB-vergaderingen, tenzij de IICB anders beslist.

10. Het secretariaat van de IICB wordt verzorgd door **Enisa** [...] **en legt verantwoording af aan de voorzitter van de IICB**.

11. De op voorstel van het adviescomité voor ICT door het EUAN benoemde vertegenwoordigers brengen de besluiten van de IICB over aan de **leden van het EUAN** [...]. 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. [...]

13. De IICB kan een uitvoerend comité **instellen** [...] om hem bij zijn werkzaamheden bij te staan, en een aantal van zijn taken en bevoegdheden daaraan delegeren**, in het bijzonder die van artikel 10, punten c) en e)**. 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.

14. De IICB dient om de 12 maanden bij de Raad een verslag in over de vooruitgang die bij de uitvoering van deze verordening is geboekt, waarin met name de mate van samenwerking van CERT-EU met zijn nationale tegenhangers in elk van de lidstaten wordt gespecificeerd. Dat verslag dient als input voor het tweejaarlijkse verslag over de cyberbeveiligingssituatie in de Unie gedurende dezelfde periode overeenkomstig artikel 15 van Richtlijn [NIS 2-voorstel].

Artikel 10

Taken van de IICB

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

(a) [...] **hij houdt doeltreffend toezicht op de toepassing** van deze verordening [...] en **ondersteunt de entiteiten** van de Unie **bij het versterken van hun cyberbeveiliging**; **daartoe kan de IICB verzoeken om ad-hocverslagen van CERT-EU en entiteiten van de Unie;**

aa) **hij stelt na een strategische discussie een meerjarige strategie vast voor het verhogen van het cyberbeveiligingsniveau in de entiteiten van de Unie, evalueert ze regelmatig en ten minste om de vijf jaar, en wijzigt ze indien nodig;**

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 **en alle bijwerkingen daarvan**, op basis van een voorstel van het hoofd van CERT-EU;

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

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

f) hij 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 dienst**enniveau-overeenkomsten** [...] of overeenkomsten tussen CERT-EU en andere entiteiten op grond van artikel 17;

i) hij stelt [...] technische adviesgroepen in ter ondersteuning van de werkzaamheden van de IICB, keurt hun mandaat goed en wijst hun voorzitter aan;

j) **hij stelt richtsnoeren en aanbevelingen vast op basis van een voorstel van CERT-EU overeenkomstig artikel 13 en draagt CERT-EU op om een oproep tot actie, of een voorstel voor richtsnoeren of aanbevelingen, uit te vaardigen, in te trekken of te wijzigen;**

k) hij ontvangt en beoordeelt documenten en verslagen die de entiteiten van de Unie uit hoofde van deze verordening indienen;

l) hij ondersteunt de oprichting van een informele groep van de lokale cyber-beveiligingsfunctionarissen van alle entiteiten en vergemakkelijkt zo de uitwisseling van beste praktijken en informatie in verband met de uitvoering van deze verordening;

m) hij werkt een cybercrisisbeheersplan uit om het gecoördineerde beheer op operationeel niveau van ernstige incidenten met gevolgen voor entiteiten van de Unie te ondersteunen en bij te dragen tot de regelmatige uitwisseling van relevante informatie, met name over de gevolgen en de ernst van ernstige incidenten en de mogelijke manieren om die te beperken.

Artikel 11

Naleving

1. De IICB houdt **in overeenstemming met artikel 9, lid 2, en artikel 10 daadwerkelijk** toezicht op de uitvoering van deze verordening en de door de [...] **entiteiten** van de Unie vastgestelde richtsnoeren, aanbevelingen en oproepen tot actie. **Daartoe kan de IICB om informatie of documentatie verzoeken die nodig is om de correcte toepassing van de bepalingen van de verordening door de entiteiten van de Unie te beoordelen. Voor de vaststelling van nalevingsmaatregelen uit hoofde van dit artikel heeft de betrokken entiteit van de Unie geen stemrecht.**

2. Indien de IICB vaststelt dat **entiteiten** [...] 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 [...] **entiteit** van de Unie in kwestie, **en na de betrokken entiteit of persoon de gelegenheid te hebben gegeven hun standpunt bekend te maken**:

a) een waarschuwing doen uitgaan **om vastgestelde tekortkomingen binnen een bepaalde termijn te verhelpen, met inbegrip van aanbevelingen tot wijziging van cyberveiligheidsdocumenten die de entiteiten van de Unie op basis van deze verordening hebben opgesteld**; indien nodig met het oog op een overtuigend cyberbeveiligingsrisico, de waarschuwing richten tot een op passende wijze beperkt publiek;

aa) een met redenen omklede kennisgeving doen uitgaan aan een entiteit van de Unie indien de in de eerdere waarschuwing vastgestelde tekortkomingen niet voldoende binnen een bepaalde termijn zijn verholpen, en dat advies formeel ter kennis brengen van de Raad, het Europees Parlement en de Commissie;

b) **met name het volgende doen uitgaan:** [...]

i. een aanbeveling dat de entiteit van de Unie aan een audit wordt onderworpen;

ii. een verzoek om een derde partij een audit te laten uitvoeren;

c) de entiteit van de Unie verzoeken het beheer, de governance en de controle van cyberbeveiligingsrisico's in overeenstemming te brengen met de bepalingen van deze verordening, in voorkomend geval op een gespecificeerde wijze en binnen een bepaalde termijn;

d) een advies uitvaardigen aan alle lidstaten en entiteiten van de Unie waarin wordt aanbevolen gegevensstromen naar de entiteit van de Unie tijdelijk op te schorten.

3. Indien de IICB maatregelen heeft genomen op grond van lid 2, punten a) tot en met d), verstrekt de betrokken entiteit van de Unie een gedetailleerd overzicht van de maatregelen en acties die zijn genomen om de door de IICB vastgestelde vermeende tekortkomingen te verhelpen. De entiteit van de Unie dient dit overzicht binnen een met de IICB overeen te komen redelijke termijn in.

4. **Wanneer de IICB van oordeel is dat er sprake is van een aanhoudende inbreuk op de bepalingen van deze verordening door een entiteit van de Unie als rechtstreeks gevolg van het handelen of nalaten van een ambtenaar of ander personeelslid van de Unie, ook op het hoogste managementniveau, verzoekt de IICB de betrokken entiteit passende maatregelen te nemen, ook van disciplinaire aard, overeenkomstig met name de regels van het Statuut van de ambtenaren en de Regeling welke van toepassing is op de andere personeelsleden van de Unie. Daartoe draagt de IICB de nodige informatie over aan de betrokken entiteit.**

Hoofdstuk IV
CERT-EU

Artikel 12

Missie en taken van CERT-EU

1. De missie van CERT-EU [...] bestaat erin bij te dragen tot de beveiliging van de niet-geclassificeerde IT-omgeving van alle [...] **entiteiten** van de Unie door ze te adviseren over cyberbeveiliging, te helpen incidenten te voorkomen, die op te sporen, te beperken en daarop te reageren, en door op te treden als knooppunt voor hun informatie-uitwisseling inzake cyberbeveiliging en responscoördinatie bij incidenten.

1a. CERT-EU verzamelt, beheert, analyseert en deelt informatie met de entiteiten van de Unie over dreigingen, kwetsbaarheden en incidenten met betrekking tot niet-gerubriceerde ICT-infrastructuur. Het coördineert de respons op incidenten op interinstitutioneel niveau en op het niveau van de entiteiten van de Unie, onder meer door gespecialiseerde operationele bijstand te verlenen of te coördineren.

2. CERT-EU is voor de […] **entiteiten** 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 **bepalingen** […], of via door de IICB gevraagde ad-hocverslagen;

b) […] **het biedt standaard CSIRT-diensten aan alle entiteiten van de Unie door middel van** 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 draagt op basis van de in lid 1a bedoelde informatie** […] bij tot het situatie-bewustzijn van de EU op het gebied van cyberbeveiliging**, in nauwe samenwerking met Enisa. Deze informatie wordt gedeeld met de IICB, het CSIRT-netwerk en EU-Intcen;**

f) het fungeert als het equivalent van de aangewezen coördinator voor de entiteiten van de Unie, als bedoeld in artikel 6 van Richtlijn [NIS 2-voorstel].

[...]

[...]

[...]

[...]

[...]

4. **In het kader van de bevoegdheden** onderhoudt CERT-EU gestructureerde samenwerking met […] **Enisa** 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 **entiteiten** […] van de Unie, op basis van dienstenniveau-overeenkomsten en afhankelijk van de beschikbaarheid van middelen;

   b) andere diensten dan diensten ter bescherming van de IT-omgeving van de **entiteiten** […] 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 **entiteiten** […] van de Unie, die nauw met de **entiteiten** […] 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 […] **Enisa**, cyberbeveiligingsoefeningen organiseren **of eraan deelnemen** of deelname aan bestaande oefeningen aanbevelen, indien van toepassing, om het cyberbeveiligingsniveau van de **entiteiten** […] van de Unie te testen.

7. CERT-EU kan de **entiteiten** […] van de Unie bijstaan bij incidenten in gerubriceerde IT-omgevingen, indien de **betrokken entiteiten van de Unie** […] daar uitdrukkelijk om verzoeken **overeenkomstig hun respectieve procedures. In dat geval zijn de bepalingen van de artikelen 19 tot en met 21 van deze verordening niet van toepassing. Het verlenen van bijstand door CERT-EU uit hoofde van dit lid laat de toepasselijke regels van de lidstaten of de Unie inzake de bescherming van gevoelige of gerubriceerde informatie onverlet.**

8. CERT-EU informeert de entiteiten van de Unie over zijn procedures en processen voor incidentafhandeling.

9. CERT-EU kan het netwerkverkeer van de entiteiten van de Unie monitoren met instemming van de betrokken entiteit van de Unie.

10. CERT-EU kan, indien de beleidsafdelingen van de entiteiten van de Unie daar uitdrukkelijk om verzoeken, technisch advies of technische input verstrekken voor relevante beleidskwesties.

11. CERT-EU ondersteunt, in samenwerking met de Europese Toezichthouder voor gegevensbescherming, de betrokken entiteiten van de Unie bij het behandelen van incidenten die tot inbreuken in verband met persoonsgegevens leiden.

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 entiteiten van de Unie […] binnen een bepaalde termijn met klem wordt aangeraden te treffen. De betrokken entiteit van de Unie stelt CERT-EU na ontvangst van de oproep tot actie onverwijld in kennis van de wijze waarop die maatregelen zijn toegepast;

   b) voorstellen aan de IICB voor richtsnoeren die gericht zijn tot alle of een deel van de **entiteiten** […] van de Unie;

   c) voorstellen aan de IICB voor aanbevelingen die gericht zijn tot individuele **entiteiten** […] van de Unie.

2. Richtsnoeren en aanbevelingen kunnen het volgende omvatten:

   a) de voorwaarden voor of verbetering van het beheer van cyberbeveiligingsrisico's en de **maatregelen voor het beheer van** […] cyberbeveiliging**srisico's**;

   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, **met inbegrip van een gecoördineerde aanpak betreffende de beveiliging van de toeleveringsketen** […]**.**

[...]

[...]

Artikel 14

Hoofd van CERT-EU

1. De Commissie benoemt het hoofd van CERT-EU met de goedkeuring van twee derde van de leden van de IICB. 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. Het hoofd van CERT-EU is verantwoordelijk voor het goed functioneren van CERT-EU, binnen de grenzen van zijn bevoegdheden, onder de leiding van de IICB. Hij of zij is verantwoordelijk voor de implementatie van de door de IICB bepaalde strategische richting, sturing, doelstellingen en prioriteiten, en voor het beheer van CERT-EU, met inbegrip van zijn financiële en personele middelen. Hij of zij brengt regelmatig verslag uit aan de voorzitter van de IICB.

3. Het hoofd van CERT-EU verleent de bevoegde gedelegeerd ordonnateur bijstand bij het opstellen van het jaarlijks activiteitenverslag, overeenkomstig artikel 74, lid 9, van het Financieel Reglement, dat financiële en beheersinformatie, inclusief de resultaten van controles, bevat, en brengt de bevoegde gedelegeerd ordonnateur regelmatig verslag uit over de uitvoering van maatregelen waarvoor aan hem bevoegdheden zijn gesubdelegeerd.

4. Het hoofd van CERT-EU stelt jaarlijks een financiële planning op van de administratieve ontvangsten en uitgaven voor de activiteiten van CERT-EU, het voorstel voor het jaarlijkse werkprogramma, het voorstel voor de dienstencatalogus van CERT-EU en de herziening daarvan, het voorstel inzake de voorwaarden voor dienstenniveau-overeenkomsten en het voorstel voor prestatie-indicatoren voor CERT-EU, die overeenkomstig artikel 10 door de IICB moeten worden goedgekeurd.

Bij de herziening van de lijst van diensten in de dienstencatalogus van CERT-EU houdt het hoofd van CERT-EU rekening met de aan CERT-EU toegewezen middelen.

5. Het hoofd van CERT-EU brengt […] **jaar**verslagen uit aan de IICB […] 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, punt[…]**a)**, bedoelde verslagen.

Artikel 15

Financiële en personeelszaken

[...]

1a. Hoewel opgericht als een autonome interinstitutionele dienstverlener voor alle entiteiten van de Unie, wordt CERT-EU geïntegreerd in de administratieve structuur van een directoraat-generaal van de Commissie zodat het kan profiteren van de ondersteunende structuren van de Commissie op het gebied van administratie, financieel beheer en boekhouding. De Commissie stelt de IICB in kennis van de administratieve vestiging van CERT-EU en van eventuele wijzigingen daarvan. Deze aanpak wordt regelmatig geëvalueerd, uiterlijk vóór het einde van een overeenkomstig artikel 312 VWEU vastgesteld meerjarig financieel kader, zodat passende maatregelen kunnen worden genomen.

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, […] 4 en 6, en artikel 13, lid 1, verleent aan de uit de rubriek Europees openbaar bestuur van het meerjarige financiële kader gefinancierde **entiteiten** […] 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 van de Commissie.

4. Andere dan de in lid 3 bedoelde **entiteiten** […] 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 via de in lid 3 bedoelde afzonderlijke begrotingslijn ontvangen[13].

5. De kosten van de in artikel 12, lid 5, bedoelde taken worden verhaald op de **entiteiten** […] van de Unie die de diensten van CERT-EU ontvangen. De ontvangsten worden bestemd voor de begrotingsonderdelen die de kosten dragen.

[13] 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).

Artikel 16

Samenwerking van CERT-EU met instanties uit de lidstaten

1. CERT-EU werkt **onverwijld** samen en wisselt informatie uit met nationale instanties in de lidstaten, **met name** [...] [...] [...] CSIRT's **als bedoeld in artikel 9 van Richtlijn [NIS 2-voorstel], en/of indien van toepassing nationale bevoegde autoriteiten** en centrale contactpunten als bedoeld in artikel 8 van Richtlijn [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 IT-omgevingen van de [...] **entiteiten** van de Unie, onder meer via het CSIRT-netwerk als bedoeld in artikel 13 van Richtlijn [NIS 2-voorstel].

1a. CERT-EU stelt alle in lid 1 bedoelde relevante nationale instanties in een lidstaat onverwijld in kennis wanneer het kennis krijgt van significante incidenten die zich op het grondgebied van deze lidstaat voordoen, tenzij CERT-EU over informatie beschikt dat de getroffen entiteit van de Unie dit incident reeds heeft gemeld overeenkomstig artikel 20, lid 2a.

2. CERT-EU [...] **wisselt**, zonder **dat** het toestemming van de betrokken **entiteit van de Unie nodig heeft**, **onverwijld** incidentspecifieke informatie uit met nationale instanties in de lidstaten om de opsporing van soortgelijke cyberdreigingen of -incidenten te vergemakkelijken **of om bij de analyse van een incident te helpen**. CERT-EU [...] **wisselt geen** incidentspecifieke informatie uit die de identiteit van het doelwit van het cyberbeveiligingsincident onthult, **tenzij** [...]:

a) de getroffen entiteit van de Unie haar toestemming heeft gegeven;

b) de getroffen entiteit van de Unie reeds heeft bekendgemaakt dat ze werd getroffen;

c) de getroffen entiteit van de Unie weliswaar geen toestemming heeft gegeven maar bekendmaking van de identiteit van de getroffen entiteit van de Unie de waarschijnlijkheid zou vergroten dat elders incidenten worden vermeden of beperkt. Voor dergelijke beslissingen is de goedkeuring van het hoofd van CERT-EU vereist. De getroffen entiteit van de Unie wordt vóór de bekendmaking geïnformeerd.

Artikel 17

Samenwerking van CERT-EU met [...] <u>andere</u> instanties

1. CERT-EU kan **in de Europese Unie** samenwerken met **andere** [...] **dan de in artikel 16 genoemde instanties**, 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 [...] verzoekt CERT-EU **per geval** vooraf om de goedkeuring van de IICB. **Wanneer CERT-EU met dergelijke instanties een samenwerking aangaat, informeert CERT-EU de in artikel 16, lid 1, bedoelde nationale instanties in de lidstaat waar de instantie is gevestigd.**

2. CERT-EU kan samenwerken met andere partners, zoals commerciële entiteiten, internationale organisaties en nationale entiteiten of individuele deskundigen van buiten de Europese Unie, om informatie te verzamelen over algemene en specifieke cyberdreigingen, cyber-kwetsbaarheden en mogelijke tegenmaatregelen. Voor verdere samenwerking met deze partners verzoekt CERT-EU **per geval** vooraf om de goedkeuring van de IICB.

3. CERT-EU kan, **mits er met de betrokken partner een geheimhoudingsregeling of -overeenkomst is gesloten**, met toestemming van de door een incident getroffen **entiteit van de Unie** [...], informatie over het **specifieke** incident verstrekken aan **de in de leden 1 en 2 bedoelde** partners, **louter om hen te helpen** [...] bij hun analyse. **Deze geheimhoudingsregelingen of -overeenkomsten worden wettelijk gecontroleerd overeenkomstig de toepasselijke interne procedures van de Commissie. Voor geheimhoudingsregelingen of -overeenkomsten is geen voorafgaande goedkeuring van de IICB nodig, maar de voorzitter van de IICB wordt ervan op de hoogte gebracht.**

4. **Bij wijze van uitzondering kan CERT-EU met voorafgaande toestemming van de IICB dienstenniveauovereenkomsten sluiten met andere entiteiten dan de entiteiten van de Unie.**

Hoofdstuk V
SAMENWERKING EN RAPPORTAGEVERPLICHTINGEN

Artikel 18
Informatieverwerking

1. CERT-EU en de [...] **entiteiten** 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[14] 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 [...] **entiteiten** van de Unie **en, indien van toepassing, de lidstaten** te raadplegen indien een verzoek betrekking heeft op hun documenten.

[...]

4. CERT-EU en de [...] **entiteiten** van de Unie verwerken informatie overeenkomstig de **toepasselijke** regels [...] inzake informatiebeveiliging [...].

[...]

Artikel 19

[...] ***Delen van cyberbeveiligingsinformatie***

-1. Entiteiten van de Unie kunnen CERT-EU vrijwillig informatie verstrekken over dreigingen, incidenten, bijna-ongelukken en kwetsbaarheden op het gebied van cyberveiligheid die hen aangaan. CERT-EU zorgt ervoor dat er efficiënte communicatie-middelen beschikbaar zijn om de informatie-uitwisseling met de entiteiten van de Unie te vergemakkelijken. CERT-EU kan voorrang geven aan de verwerking van verplichte meldingen boven vrijwillige meldingen.

[14] 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).

1. Om [...] **zijn missie en taken als omschreven in artikel 12 uit te voeren**, kan CERT-EU [...] **entiteiten** van de Unie verzoeken informatie uit hun respectieve IT-systeeminventarissen te verstrekken, **met inbegrip van informatie over cyberdreigingen, bijna-ongevallen, kwetsbaarheden, indicatoren van compromittering, cyberbeveiligingswaarschuwingen en aanbevelingen met betrekking tot de configuratie van cyberbeveiligingsinstrumenten voor het opsporen van cyberincidenten** [...]. De aangezochte [...] **entiteit** van de Unie zendt de verlangde informatie en bijbehorende actualiseringen daarvan onverwijld toe.

2. De [...] **entiteiten** 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 **met de entiteiten van de Unie** alleen incidentspecifieke informatie uitwisselen die de identiteit van de door het incident getroffen [...] **entiteit** van de Unie onthult als het de toestemming van die entiteit heeft gekregen. **Wanneer de toestemming wordt geweigerd, deelt de betrokken entiteit aan CERT-EU haar naar behoren gemotiveerde redenen mee.** [...]

4. De deelverplichtingen gelden niet voor gerubriceerde EU-informatie, noch voor informatie **waarvan de informatiebron de verspreiding buiten de ontvangende entiteit van de Unie door middel van een zichtbare markering heeft uitgesloten, tenzij de informatiebron** [...] **uitdrukkelijk toestaat dat deze informatie met CERT-EU wordt gedeeld.** [...]

Artikel 20

[...] ***Rapportageverplichtingen***

-1. Een incident wordt als significant beschouwd als:

a) het de werking van de entiteit van de Unie ernstig heeft verstoord of kan verstoren dan wel voor de betrokken entiteit tot financiële verliezen heeft geleid of kan leiden;

b) het andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

1. Alle [...] **entiteiten** van de Unie **zenden** [...] **het volgende aan CERT-EU**: [...]

[...].

(a) onverwijld en in ieder geval binnen 24 uur nadat het significante incident bekend is geworden, een vroegtijdige waarschuwing waarin, indien van toepassing, wordt aangegeven of het significante incident vermoedelijk door een onwettige of kwaadwillige handeling is veroorzaakt, en of het grensoverschrijdende gevolgen heeft of kan hebben;

(b) onverwijld en in ieder geval binnen 72 uur nadat het significante incident bekend is geworden, een melding van incident waarin, indien van toepassing, de in punt a) bedoelde informatie wordt bijgewerkt en een eerste beoordeling wordt gegeven van het significante incident, de ernst en de gevolgen ervan, alsook, indien beschikbaar, de indicatoren van compromittering;

(c) op verzoek van CERT-EU, een tussentijds verslag over relevante updates van de situatie;

(d) uiterlijk één maand na de indiening van de in punt b) bedoelde melding van het significante incident, een eindverslag waarin ten minste het volgende is opgenomen:

i) een gedetailleerde beschrijving van het significante incident, de ernst en de gevolgen ervan;

ii) het soort dreiging of de grondoorzaak die waarschijnlijk tot het significante incident heeft geleid;

iii) toegepaste en lopende beperkende maatregelen;

iv) indien van toepassing, de grensoverschrijdende gevolgen van het significante incident.

(e) bij aanhoudende significante incidenten op het tijdstip van de indiening van het in punt d) bedoelde eindverslag, een voortgangsverslag op dat tijdstip en een eindverslag uiterlijk één maand nadat het incident is behandeld.

[...]

(g) [...]

(h) [...]

(i) [...]

(j) [...]

2a. Waar zij gevestigd zijn, delen alle entiteiten van de Unie de overeenkomstig lid 1 gerapporteerde informatie binnen dezelfde termijn met de in artikel 16, lid 1, bedoelde nationale instanties.

3. CERT-EU dient **om de drie maanden** [...] bij **de IICB, EU-Intcen en het CSIRT-netwerk** [...] een samenvattend verslag in met geanonimiseerde en geaggregeerde gegevens over [...] cyberdreigingen, [...] kwetsbaarheden **in de zin van artikel 19, de antwoorden van entiteiten van de Unie op oproepen tot actie in de zin van artikel 13, lid 1, punt a),** en significante incidenten die overeenkomstig lid 1 zijn gemeld. **Dat verslag dient als input voor het tweejaarlijkse verslag over de stand van zaken op het gebied van de cyberbeveiliging in de Unie in de zin van artikel 15 van Richtlijn [NIS 2-voorstel].**

4. Het IICB **brengt** [...] **uiterlijk [6 maanden na de datum van inwerkingtreding van deze verordening]** richtsnoeren of aanbevelingen uit waarin [...] de randvoorwaarden**, de vorm** en de inhoud van de rapportage [...] **nader worden beschreven**. **In de richtsnoeren of aanbevelingen wordt naar behoren rekening gehouden met de bepalingen die door middel van uitvoeringshandelingen overeenkomstig artikel 20, lid 11, van Richtlijn [NIS 2-voorstel] worden uitgevoerd**. CERT-EU verspreidt de passende technische details, zodat de [...] **entiteiten** van de Unie proactief opsporings-, incidentrespons- of beperkende maatregelen kunnen treffen.

5. De [...] **rapportage**verplichtingen gelden niet voor gerubriceerde EU-informatie, noch voor informatie **waarvan de informatiebron de verspreiding buiten de ontvangende entiteit van de Unie door middel van een zichtbare markering heeft uitgesloten, tenzij de informatiebron** [...] **uitdrukkelijk toestaat dat deze informatie met CERT-EU wordt gedeeld.** [...]

Artikel 21

Coördinatie van respons bij incidenten en samenwerking [...]

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) [...] **entiteiten** van de Unie;

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

2. CERT-EU faciliteert, [...] **in voorkomend geval in nauwe samenwerking met Enisa overeenkomstig artikel 7, lid 7, punt d), van de cyberbeveiligingsverordening**[15], de coördinatie tussen de [...] **entiteiten** van de Unie inzake de respons bij incidenten, wat het volgende omvat:

   a) bijdragen tot consequente externe communicatie;

   [...]

   c) optimaal gebruik van operationele middelen;

   d) coördinatie met andere crisisresponsmechanismen op Unieniveau.

3. CERT-EU ondersteunt, **in nauwe samenwerking met Enisa** de [...] **entiteiten** van de Unie met betrekking tot het situatiebewustzijn van dreigingen, kwetsbaarheden en incidenten op het gebied van cyberveiligheid

---

15 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).

4. De IICB [...] **stelt uiterlijk [12 maanden na de datum van inwerkingtreding van deze verordening] en op basis van een voorstel van CERT-EU** richtsnoeren **of aanbevelingen** inzake de respons bij incidenten en samenwerking bij significante incidenten **vast**. 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

Beheer van ernstige incidenten [...]

-1. Om het gecoördineerde beheer van ernstige incidenten op operationeel niveau die gevolgen hebben voor entiteiten van de Unie te ondersteunen en bij te dragen tot de regelmatige uitwisseling van relevante informatie tussen entiteiten van de Unie en met de lidstaten, komt de IICB met een cybercrisisbeheersplan op basis van de in artikel 21, lid 2, bedoelde activiteiten, dit in nauwe samenwerking met CERT-EU en Enisa, dat ten minste de volgende elementen bevat:

a) coördinatie van en randvoorwaarden voor de informatiestroom tussen entiteiten van de Unie voor het beheer van ernstige incidenten op operationeel niveau;

b) gemeenschappelijke standaardwerkwijzen;

c) een gemeenschappelijke taxonomie met betrekking tot de ernst van ernstige incidenten en crisistriggerpunten;

d) regelmatige oefeningen;

e) te gebruiken beveiligde communicatiekanalen;

f) een contactpunt voor EU-CyCLONe, dat met EU-CyCLONe relevante informatie deelt als input voor gedeeld situationeel bewustzijn.

1. CERT-EU coördineert tussen de [...] **entiteiten** van de Unie de respons op ernstige **incidenten** [...]. Het houdt een inventaris bij van de technische deskundigheid die nodig is voor de respons bij dergelijke **ernstige incidenten** [...].

2. De [...] **entiteiten** 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. Naar aanleiding van een specifiek verzoek van een lidstaat waar de getroffen entiteit van de Unie is gevestigd en met [...] de goedkeuring van de **getroffen** [...] **entiteit** [...] van de Unie [...], kan CERT-EU de in lid 2 bedoelde deskundigen ook oproepen om te helpen bij de respons op een ernstig **incident** [...] **in** [...] **die entiteit van de Unie** [...]**.**

Hoofdstuk VI
SLOTBEPALINGEN

Artikel 23

Initiële heroriëntering van begrotingsmiddelen

De Commissie stelt voor de personele en financiële middelen over te hevelen van de [...] **entiteiten** 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 [...] deze verordening te **evalueren**.

2. Uiterlijk [...] **36** 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. **Uiterlijk** [...] 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. **Dat verslag gaat zo nodig vergezeld van een wetgevingsvoorstel.**

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*

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

BIJLAGE II

[...]

[...]

[...]

[...]

[...]

[...]

[...]