Publicatieblad
van de Europese Unie

NL
L-serie

2023/2841

18.12.2023

VERORDENING (EU, Euratom) 2023/2841 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 13 december 2023

tot vaststelling van 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 ([1]),

Overwegende hetgeen volgt:

(1) In het digitale tijdperk vormt informatie- en communicatietechnologie een hoeksteen van een open, doeltreffend en onafhankelijk Europees ambtenarenapparaat. Technologische ontwikkelingen en de toegenomen complexiteit en onderlinge verwevenheid van digitale systemen vergroten de cyberbeveiligingsrisico's, waardoor de entiteiten van de Unie kwetsbaarder worden voor cyberdreigingen en cyberincidenten, wat hun bedrijfscontinuïteit en gegevensbeveiligingscapaciteit in gevaar brengt. Het toegenomen gebruik van clouddiensten, het alomtegenwoordige gebruik van informatie- en communicatietechnologie (ICT), de hoge mate van digitalisering, thuiswerk en evoluerende technologie en connectiviteit zijn 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 cyberdreigingen. 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 van dreigingsactoren volgen elkaar steeds sneller op, met steeds geavanceerdere en meer geautomatiseerde campagnes, gericht tegen zwakke plekken, en daarbij worden kwetsbaarheden snel uitgebuit.

(3) De ICT-omgevingen van de entiteiten van de Unie hebben onderlinge afhankelijkheden en geïntegreerde gegevensstromen, en hun gebruikers werken nauw samen. Die 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 kan hebben voor de andere entiteiten van de Unie. Bovendien zijn de ICT-omgevingen van bepaalde entiteiten van de Unie verbonden met de ICT-omgevingen van de lidstaten, zodat een incident in een entiteit van de Unie een cyberbeveiligingsrisico kan vormen voor de ICT-omgevingen van de lidstaten, en omgekeerd. Het delen van incidentspecifieke informatie 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 het niveau en 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 de entiteiten van de Unie nodig dat zij een hoog gezamenlijk niveau van cyberbeveiliging bereiken, door cyberbeveiligingsmaatregelen uit te voeren die in verhouding staan tot de vastgestelde cyberbeveiligingsrisico's, informatie uit te wisselen en samen te werken.

([1]) Standpunt van het Europees Parlement van 21 november 2023 (nog niet bekendgemaakt in het Publicatieblad) en besluit van de Raad van 8 december 2023.

(5) Bij Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad ([2]) wordt beoogd de cyberveerkracht en de responscapaciteit bij incidenten van publieke en private entiteiten, bevoegde autoriteiten en organen alsmede de Unie als geheel verder te verbeteren. Daarom moet ervoor worden gezorgd dat de entiteiten van de Unie hetzelfde doen door regels vast te stellen die in overeenstemming zijn met Richtlijn (EU) 2022/2555 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 (het "kader") opzetten, dat een doeltreffend en prudent beheer van alle cyberbeveiligingsrisico's waarborgt en rekening houdt met bedrijfscontinuïteit en crisisbeheer. Met het kader moet cyberbeveiligingsbeleid, met doelstellingen en prioriteiten, worden vastgesteld voor de beveiliging van netwerk- en informatiesystemen die de gehele niet-gerubriceerde ICT-omgeving omvatten. Het kader moet gebaseerd zijn op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en 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 of betrouwbaarheid van via netwerk- en informatiesystemen opgeslagen, verzonden, verwerkte of toegankelijke gegevens zou kunnen worden gecompromitteerd.

(7) Teneinde de binnen het kader geïdentificeerde cyberbeveiligingsrisico's te beheren, moet elke entiteit van de Unie passende en evenredige technische, operationele en organisatorische maatregelen nemen. Die maatregelen moeten betrekking hebben op in deze verordening genoemde domeinen en maatregelen voor het beheer van cyberbeveiligingsrisico's om de cyberbeveiliging van elke entiteit van de Unie te versterken.

(8) De binnen het kader aangeduide activa en vastgestelde cyberbeveiligingsrisico's en de conclusies van de regelmatig uitgevoerde maturiteitsbeoordelingen van de cyberbeveiliging moeten tot uiting komen in het cyberbeveiligingsplan van elke entiteit van de Unie. Het cyberbeveiligingsplan moet de vastgestelde maatregelen voor het beheer van cyberbeveiligingsrisico's omvatten.

(9) Aangezien cyberbeveiliging een continu proces is, moeten de op grond van deze verordening genomen maatregelen regelmatig op geschiktheid en doeltreffendheid worden getoetst in het licht van de veranderende cyberbeveiligingsrisico's, activa en maturiteit van de cyberbeveiliging van de entiteiten van de Unie. Het kader moet regelmatig en minstens om de vier jaar worden geëvalueerd, en het cyberbeveiligingsplan moet om de twee jaar worden herzien, of vaker indien nodig na de maturiteitsbeoordelingen van de cyberbeveiliging of na een substantiële herziening van het kader.

(10) De door de entiteiten van de Unie genomen maatregelen voor het beheer van cyberbeveiligingsrisico's moeten beleidsmaatregelen omvatten die waar mogelijk beogen de broncode transparant te maken, rekening houdend met de waarborgen voor de rechten van derden of entiteiten van de Unie. Dat beleid moet in verhouding staan tot het cyberbeveiligingsrisico en bedoeld zijn om de analyse van cyberdreigingen te vergemakkelijken, zonder verplichtingen tot openbaarmaking van of rechten op toegang tot een code van derden te creëren die verder gaan dan de toepasselijke contractuele voorwaarden.

(11) Openbroninstrumenten en -toepassingen voor cyberbeveiliging kunnen bijdragen tot een hogere mate van openheid. Open normen bevorderen de interoperabiliteit tussen beveiligingsinstrumenten, wat ten goede komt aan de beveiliging van belanghebbenden. Opensource-instrumenten en -toepassingen voor cyberbeveiliging kunnen een hefboomwerking hebben voor de bredere gemeenschap van ontwikkelaars, waardoor diversificatie van leveranciers mogelijk wordt. Dankzij open bronnen kan het proces voor de verificatie van cyberbeveiligingsinstrumenten transparanter verlopen en kan het proces om kwetsbaarheden te ontdekken, door de gemeenschap worden aangestuurd. Daarom moet het voor de entiteiten van de Unie mogelijk zijn om het gebruik van opensourcesoftware en open normen te bevorderen door beleid te voeren inzake het gebruik van open data en open bronnen als onderdeel van beveiliging door transparantie.

([2]) Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80).

(12) De verschillen tussen de entiteiten van de Unie vereisen flexibiliteit bij de uitvoering van deze verordening. De in deze verordening vervatte 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. Daarom moeten die entiteiten hun eigen kaders opstellen en hun eigen maatregelen voor het beheer van cyberbeveiligingsrisico's en cyberbeveiligingsplannen vaststellen. Bij de uitvoering van die maatregelen moet terdege rekening worden gehouden met bestaande synergieën 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 en samenwerking tussen entiteiten van de Unie onderling alsmede tussen entiteiten van de Unie en hun tegenhangers in de lidstaten.

(13) Met het oog op een optimaal gebruik van middelen moet deze verordening voorzien in de mogelijkheid dat twee of meer entiteiten van de Unie met soortgelijke structuren samenwerken bij de uitvoering van de maturiteitsbeoordelingen van de cyberbeveiliging van hun respectieve entiteiten.

(14) Om te voorkomen dat aan de entiteiten van de Unie onevenredige financiële en administratieve lasten worden opgelegd, moeten de eisen inzake het beheer van cyberbeveiligingsrisico's, rekening houdend met de stand van de techniek, in verhouding staan tot het cyberbeveiligingsrisico voor de netwerk- en informatiesystemen in kwestie. Elke entiteit van de Unie moeten beogen een passend percentage van haar ICT-begroting aan betere cyberbeveiliging te besteden. Op langere termijn moet een indicatief doel van minstens 10 % worden nagestreefd. Bij de maturiteitsbeoordeling van de cyberbeveiliging moet worden nagegaan of de uitgaven voor cyberbeveiliging van de entiteit van de Unie in verhouding staan tot de cyberbeveiligingsrisico's waaraan ze is blootgesteld. Onverminderd de regels betreffende de jaarlijkse begroting van de Unie uit hoofde van de Verdragen moet de Commissie in haar voorstel voor de eerste jaarlijkse begroting die na de inwerkingtreding van deze verordening wordt vastgesteld, bij de beoordeling van de begrotings- en personeelsbehoeften van de entiteiten van de Unie die uit hun uitgavenramingen resulteren, rekening houden met de verplichtingen die uit deze verordening voortvloeien.

(15) Voor een hoog gezamenlijk niveau van cyberbeveiliging is vereist dat cyberbeveiliging onder het toezicht van het hoogste managementniveau van elke entiteit van de Unie wordt geplaatst. Het hoogste managementniveau van de entiteit van de Unie moet verantwoordelijk zijn voor de uitvoering van deze verordening, onder meer voor de vaststelling van het kader, het nemen van maatregelen voor het beheer van cyberbeveiligingsrisico's en de goedkeuring van het cyberbeveiligingsplan. Het aanpakken van de cyberbeveiligingscultuur, dat wil zeggen de dagelijkse cyberbeveiligingspraktijk, maakt integraal deel uit van het kader en de bijbehorende maatregelen voor het beheer van cyberbeveiligingsrisico's binnen alle entiteiten van de Unie.

(16) De beveiliging van netwerk- en informatiesystemen die gerubriceerde EU-informatie (EU classified information — EUCI) verwerken, is van essentieel belang. Entiteiten van de Unie die EUCI verwerken, zijn verplicht de uitgebreide regelgevingskaders voor de bescherming van dergelijke informatie toe te passen, met inbegrip van specifieke governance-, beleids- en risicobeheersprocedures. Netwerk- en informatiesystemen die EUCI verwerken, moeten voldoen aan strengere beveiligingsnormen dan niet-gerubriceerde netwerk- en informatiesystemen. Daarom zijn netwerk- en informatiesystemen die EUCI verwerken, beter bestand tegen cyberdreigingen en -incidenten. Hoewel de noodzaak van een gemeenschappelijk kader in dit verband wordt erkend, mag deze verordening derhalve niet van toepassing zijn op netwerk- en informatiesystemen die EUCI verwerken. Op uitdrukkelijk verzoek van een entiteit van de Unie moet het computercrisisresponsteam voor de instellingen, organen en instanties van de Europese Unie (CERT-EU) die entiteit van de Unie echter bijstand kunnen verlenen bij incidenten in gerubriceerde ICT-omgevingen.

(17) De entiteiten van de Unie moeten de cyberbeveiligingsrisico's betreffende de betrekkingen met leveranciers en dienstverleners, inclusief leveranciers van gegevensopslag- en gegevensverwerkingsdiensten of beheerde beveiligingsdiensten, beoordelen, en daarvoor passende maatregelen nemen. Cyberbeveiligingsmaatregelen moeten 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 relevante Europese en internationale normen, alsook met het relevante Unierecht en -beleid, met inbegrip van cyberbeveiligingsrisicobeoordelingen en aanbevelingen van de op grond van artikel 14 van Richtlijn (EU) 2022/2555 opgerichte samenwerkingsgroep, zoals de gecoördineerde EU-risicobeoordeling van de cyberbeveiliging van 5G-netwerken en de EU-toolbox inzake 5G-cyberbeveiliging. Bovendien kan het, rekening houdend met het cyberdreigingslandschap en het feit dat het belangrijk is de cyberveerkracht van de entiteiten van

de Unie te vergroten, nodig zijn dat relevante ICT-producten, -diensten en -processen worden gecertificeerd volgens op grond van artikel 49 van Verordening (EU) 2019/881 van het Europees Parlement en de Raad ([3]) vastgestelde specifieke Europese cyberbeveiligingscertificeringsregelingen.

(18) In mei 2011 hebben de secretarissen-generaal van de instellingen, organen en instanties van de Unie besloten een voorbereidingsteam voor CERT-EU in te stellen, onder toezicht van een interinstitutionele stuurgroep. In juli 2012 bevestigden de secretarissen-generaal de praktische regelingen en kwamen zij overeen CERT-EU te handhaven als permanente entiteit om het algehele niveau van IT-veiligheid van de instellingen, organen en instanties van de EU verder te helpen verbeteren, als voorbeeld van zichtbare interinstitutionele samenwerking op het gebied van cyberveiligheid. In september 2012 is CERT-EU opgericht als permanente taskforce van de 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 ([4]). In deze verordening moet een uitgebreide reeks voorschriften worden vastgesteld betreffende de organisatie, het functioneren en de werking van CERT-EU. De bepalingen van deze verordening hebben voorrang op de in december 2017 gesloten interinstitutionele regeling betreffende de organisatie en het functioneren van CERT-EU.

(19) CERT-EU moet worden omgedoopt tot cyberbeveiligingsdienst voor de instellingen, organen en instanties van de Unie, maar de korte naam "CERT-EU" moet vanwege de herkenbaarheid behouden blijven.

(20) Bij deze verordening worden niet enkel meer taken en een grotere rol gegeven aan CERT-EU, maar wordt ook de interinstitutionele raad voor cyberbeveiliging (IICB) opgericht, teneinde een hoog gezamenlijk niveau van cyberbeveiliging onder de entiteiten van de Unie te bevorderen. De IICB moet een exclusieve rol spelen bij het monitoren en ondersteunen van de uitvoering van deze verordening door de entiteiten van de Unie en bij het toezicht op de uitvoering van de algemene prioriteiten en doelstellingen van CERT-EU en het geven van strategische sturing aan CERT-EU. De IICB moet derhalve de vertegenwoordiging van de instellingen van de Unie waarborgen, en moet via het netwerk van agentschappen van de Unie (EUAN) zijn samengesteld uit vertegenwoordigers van organen en instanties van de Unie. De organisatie en werking van de IICB moeten nader worden geregeld door een reglement van orde, dat verdere bijzonderheden met betrekking tot regelmatige vergaderingen van de IICB kan bevatten, waaronder jaarlijkse bijeenkomsten op politiek niveau waar vertegenwoordigers van het hoogste managementniveau van elk IICB-lid de IICB in staat zouden stellen strategische discussies te houden en de IICB strategische richtsnoeren zouden geven. Voorts moet de IICB een uitvoerend comité kunnen oprichten dat de IICB bij zijn werkzaamheden bijstaat en waaraan hij een aantal taken en bevoegdheden kan overdragen, met name taken die een bepaalde expertise van de leden vereisen, bijvoorbeeld de goedkeuring van de dienstencatalogus en actualiseringen daarvan, regelingen voor dienstenniveauovereenkomsten, de evaluatie van documenten en verslagen die de entiteiten van de Unie op grond van 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.

(21) De IICB beoogt entiteiten van de Unie te helpen om hun respectieve cyberbeveiligingspositie te verbeteren door deze verordening uit te voeren. Om de entiteiten van de Unie te ondersteunen, moet de IICB richtsnoeren verstrekken aan het hoofd van CERT-EU, een meerjarige strategie vaststellen om het cyberbeveiligingsniveau in de entiteiten van de Unie te verhogen, de methodologie voor en andere aspecten van vrijwillige collegiale toetsingen vaststellen, en de oprichting faciliteren van een informele groep van lokale cyberbeveiligingsfunctionarissen, ondersteund door het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), met als doel beste praktijken en informatie met betrekking tot de uitvoering van deze verordening uit te wisselen.

([3]) 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).

([4]) Regeling tussen het Europees Parlement, de Europese Raad, de Raad van de Europese Unie, de Europese Commissie, het Hof van Justitie van de Europese Unie, de Europese Centrale Bank, de Europese Rekenkamer, de Europese Dienst voor extern optreden, het Europees Economisch en Sociaal Comité, het Europees Comité van de Regio's en de Europese Investeringsbank betreffende de organisatie en het functioneren van een computercrisisteam voor de instellingen, organen en instanties van de Unie (CERT-EU) (PB C 12 van 13.1.2018, blz. 1).

(22) Om een hoog niveau van cyberbeveiliging bij alle entiteiten van de Unie te bereiken, moeten de belangen van de organen en instanties van de Unie die hun eigen ICT-omgeving beheren, in de IICB worden vertegenwoordigd door drie door het EUAN aangewezen vertegenwoordigers. De beveiliging van de verwerking van persoonsgegevens, en dus ook de cyberbeveiliging daarvan, is een hoeksteen van gegevensbescherming. Gezien de synergieën tussen gegevensbescherming en cyberbeveiliging moet de Europese Toezichthouder voor gegevensbescherming in de IICB worden vertegenwoordigd in zijn hoedanigheid van onder deze verordening vallende entiteit van de Unie met specifieke deskundigheid op het gebied van gegevensbescherming, met inbegrip van de beveiliging van elektronische communicatienetwerken. Gezien het belang van innovatie en concurrentievermogen op het gebied van cyberbeveiliging moet het Europees Kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging in de IICB worden vertegenwoordigd. Gezien de rol van Enisa als expertisecentrum op het gebied van cyberbeveiliging en de steun die Enisa verleent, en gezien het belang van cyberbeveiliging van de ruimtevaartinfrastructuur en -diensten van de Unie, moeten Enisa en het Agentschap van de Europese Unie voor het ruimtevaartprogramma in de IICB worden vertegenwoordigd. Gezien de rol die bij deze verordening aan CERT-EU wordt toegekend, moet het hoofd van CERT-EU door de voorzitter van de IICB worden uitgenodigd op alle vergaderingen van de IICB, behalve wanneer de IICB aangelegenheden bespreekt die rechtstreeks betrekking hebben op het hoofd van CERT-EU.

(23) De IICB moet toezicht houden op de naleving van deze verordening en de uitvoering van richtsnoeren, aanbevelingen en oproepen tot actie. De IICB moet op technisch gebied worden ondersteund door technische adviesgroepen, die de IICB naar eigen inzicht samenstelt. Die technische adviesgroepen moeten waar nodig nauw samenwerken met CERT-EU, de entiteiten van de Unie en andere belanghebbenden.

(24) Indien de IICB vaststelt dat een entiteit van de Unie deze verordening of de op grond van deze verordening vastgestelde richtsnoeren, aanbevelingen en oproepen tot actie niet effectief heeft uitgevoerd, moet de IICB, onverminderd de interne procedures van de entiteit van de Unie in kwestie, nalevingsmaatregelen kunnen nemen. De IICB moet nalevingsmaatregelen stapsgewijs toepassen, met andere woorden, de IICB moet eerst de minst strenge maatregel nemen, namelijk een met redenen omkleed advies, en alleen indien nodig steeds strengere maatregelen, culminerend in de strengste maatregel, namelijk een aanbeveling tot tijdelijke opschorting van de gegevensstromen naar de betrokken entiteit van de Unie. Een dergelijke aanbeveling mag alleen worden toegepast in uitzonderlijke gevallen van langdurige, opzettelijke, herhaalde of ernstige inbreuk op deze verordening door de betrokken entiteit van de Unie.

(25) Het met redenen omkleed advies is de minst strenge nalevingsmaatregel om vastgestelde lacunes in de uitvoering van deze verordening aan te pakken. De IICB moet een met redenen omkleed advies kunnen laten volgen door richtsnoeren om de entiteit van de Unie te helpen ervoor te zorgen dat haar kader, maatregelen voor het beheer van cyberbeveiligingsrisico's, cyberbeveiligingsplan en verslaglegging aan deze verordening voldoen, en vervolgens door een waarschuwing om vastgestelde tekortkomingen van de entiteit van de Unie binnen een bepaalde termijn te verhelpen. Indien de in de waarschuwing genoemde tekortkomingen onvoldoende zijn aangepakt, moet de IICB een met redenen omklede kennisgeving kunnen doen.

(26) De IICB moet kunnen aanbevelen dat er een audit van een entiteit van de Unie wordt uitgevoerd. De entiteit van de Unie moet hiervoor haar interne auditfunctie kunnen gebruiken. De IICB moet ook kunnen vragen dat een audit door een derde partij wordt uitgevoerd, onder meer door een gezamenlijk overeengekomen dienstverlener uit de particuliere sector.

(27) In uitzonderlijke gevallen van langdurige, opzettelijke, herhaalde of ernstige inbreuken op deze verordening door een entiteit van de Unie moet de IICB in laatste instantie alle lidstaten en entiteiten van de Unie een tijdelijke opschorting van de gegevensstromen naar de entiteit van de Unie kunnen aanbevelen, die van kracht moet zijn totdat de entiteit van de Unie de inbreuk tot een einde heeft gebracht. Een dergelijke aanbeveling moet worden meegedeeld via passende en beveiligde communicatiekanalen.

(28) Met het oog op de correcte uitvoering van deze verordening moet de IICB, indien hij van oordeel is dat een aanhoudende schending van deze verordening door een entiteit van de Unie rechtstreeks het gevolg is van het handelen of nalaten van een van haar personeelsleden, ook op het hoogste managementniveau, de entiteit van de Unie in kwestie verzoeken passende maatregelen te nemen, met inbegrip van het verzoek te overwegen disciplinaire maatregelen te nemen overeenkomstig de bepalingen en procedures van het Statuut van de ambtenaren van de Europese Unie en de Regeling welke van toepassing is op de andere personeelsleden van de Unie, vastgesteld bij Verordening (EEG, Euratom, EGKS) nr. 259/68 van de Raad ([5]) (het "Statuut") en alle andere toepasselijke regels en procedures.

(29) CERT-EU moet bijdragen tot de beveiliging van de ICT-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 over beleidskwesties ter zake te verstrekken, moet het ervoor zorgen dat dit geen belemmering vormt voor de uitvoering van de andere taken die op grond van deze verordening aan CERT-EU zijn toegewezen. CERT-EU moet handelen namens entiteiten van de Unie als equivalent van de coördinator die is aangewezen met het oog op de gecoördineerde bekendmaking van kwetsbaarheden op grond van artikel 12, lid 1, van Richtlijn (EU) 2022/2555.

(30) 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 nemen. De IICB moet CERT-EU opdragen om een oproep tot actie of een voorstel voor richtsnoeren of voor een aanbeveling uit te vaardigen, in te trekken of te wijzigen.

(31) CERT-EU moet ook de rol vervullen waarin is voorzien in Richtlijn (EU) 2022/2555 inzake samenwerking en informatie-uitwisseling met het op grond van artikel 15 van die richtlijn opgezette netwerk van computer security incident response teams (CSIRT's). Verder moet CERT-EU in lijn met Aanbeveling (EU) 2017/1584 van de Commissie ([6]) samenwerken met de belanghebbende partijen en een respons coördineren. Met het oog op een hoog niveau van cyberbeveiliging in de hele Unie, moet CERT-EU incidentspecifieke informatie delen met tegenhangers in de lidstaten. CERT-EU moet ook samenwerken met andere publieke en private tegenhangers, zoals bij de Noord-Atlantische Verdragsorganisatie, na voorafgaande goedkeuring door de IICB.

(32) Bij de ondersteuning van operationele cyberbeveiliging moet CERT-EU gebruikmaken van de beschikbare deskundigheid van Enisa, door middel van gestructureerde samenwerking zoals bedoeld in Verordening (EU) 2019/881. 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 cyberdreigingsanalyse en zijn dreigingslandschapverslag regelmatig met Enisa delen.

(33) CERT-EU moet kunnen samenwerken en informatie kunnen uitwisselen met relevante cyberbeveiligingsgemeenschappen binnen de Unie en haar lidstaten om operationele samenwerking te bevorderen en de bestaande netwerken hun volledige potentieel voor de bescherming van de Unie te laten ontplooien.

(34) Aangezien de diensten en taken van CERT-EU in het belang van de entiteiten van de Unie zijn, moeten de individuele entiteiten van de Unie met ICT-uitgaven een billijke bijdrage aan die diensten en taken leveren. Die bijdragen laten de budgettaire autonomie van de entiteiten van de Unie onverlet.

([5]) Verordening (EEG, Euratom, EGKS) 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, alsmede van bijzondere maatregelen welke tijdelijk op de ambtenaren van de Commissie van toepassing zijn (PB L 56 van 4.3.1968, blz. 1).

([6]) 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).

(35) Veel cyberaanvallen zijn onderdeel van bredere campagnes die gericht zijn tegen groepen entiteiten van de Unie of belangengemeenschappen die de entiteiten van de Unie omvatten. Om proactief opsporings-, incidentrespons- of beperkende maatregelen te kunnen nemen en van incidenten te kunnen herstellen, moeten de entiteiten van de Unie CERT-EU onverwijld in kennis kunnen stellen van incidenten, cyberdreigingen, kwetsbaarheden en bijna-incidenten en passende technische details delen, op grond waarvan opsporings-, incidentrespons- of beperkende maatregelen kunnen worden getroffen tegen soortgelijke incidenten, cyberdreigingen, kwetsbaarheden en bijna-incidenten op het gebied van cyberveiligheid binnen andere entiteiten van de Unie. Op basis van dezelfde aanpak als in Richtlijn (EU) 2022/2555 moeten entiteiten van de Unie CERT-EU een vroegtijdige waarschuwing toezenden binnen 24 uur nadat zij kennis hebben gekregen van significante incidenten. 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 ICT-omgevingen van de entiteiten van de Unie en die van de tegenhangers van de entiteiten van de Unie te helpen beschermen tegen soortgelijke incidenten.

(36) Deze verordening voorziet in een aanpak in meerdere fasen van de melding 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 om hulp te vragen, en anderzijds een grondige melding die het mogelijk maakt waardevolle lessen te trekken uit afzonderlijke incidenten en mettertijd de veerkracht van afzonderlijke entiteiten van de Unie verbetert en hun algemene cyberveiligheidspositie helpt versterken. Deze verordening moet daarom voorzien in de melding 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 van de Unie tot financiële verliezen zouden kunnen leiden, dan wel andere natuurlijke of rechtspersonen aanzienlijke materiële of immateriële schade zouden kunnen berokkenen. Bij die eerste beoordeling moet onder andere rekening worden gehouden met de getroffen netwerk- en informatiesystemen, en met name 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.

(37) Aangezien de infrastructuur en de netwerk- en informatiesystemen van de betrokken entiteit van de Unie en die van de lidstaat waar die entiteit van de Unie is gevestigd, onderling verbonden zijn, is het voor die lidstaat van cruciaal belang dat hij onmiddellijk in kennis wordt gesteld van een significant incident in die entiteit van de Unie. Daartoe moet de getroffen entiteit van de Unie alle relevante op grond van de artikelen 8 en 10 van Richtlijn (EU) 2022/2555 aangewezen of opgerichte tegenhangers in de lidstaten in kennis stellen als zich een significant incident voordoet waarover zij aan CERT-EU rapporteert. Indien CERT-EU kennis krijgt van een significant incident dat zich in een lidstaat voordoet, moet het de relevante tegenhangers in die lidstaat op de hoogte brengen.

(38) Er moet een mechanisme worden ingesteld voor doeltreffende informatie-uitwisseling, coördinatie en samenwerking tussen de entiteiten van de Unie in geval van ernstige incidenten, waarbij de rollen en verantwoordelijkheden van de betrokken entiteiten van de Unie duidelijk zijn vastgelegd. De vertegenwoordiger van de Commissie in de IICB moet, onder voorbehoud van het cybercrisisbeheersplan, het contactpunt zijn om het voor de IICB gemakkelijker te maken relevante informatie over ernstige incidenten te delen met het Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe), als bijdrage aan het gedeelde situationele bewustzijn. De rol van de vertegenwoordiger van de Commissie in de IICB als contactpunt mag geen afbreuk doen aan de afzonderlijke en onderscheiden rol van de Commissie in EU-CyCLONe op grond van artikel 16, lid 2, van Richtlijn (EU) 2022/2555.

(39) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([7]) is van toepassing op de verwerking van persoonsgegevens op grond van deze verordening. De verwerking van persoonsgegevens kan plaatsvinden in verband met maatregelen die zijn vastgesteld in het kader van het beheer van cyberbeveiligingsrisico's, de behandeling van kwetsbaarheden en incidenten, het delen van informatie over incidenten, cyberdreigingen en kwetsbaarheden, en coördinatie en samenwerking bij de respons op incidenten. Dergelijke maatregelen kunnen de verwerking van bepaalde categorieën persoonsgegevens vereisen, zoals IP-adressen, uniform resource locators (URL's), domeinnamen, e-mailadressen, organisatorische rollen van de betrokkene, tijdstempels, onderwerpen van

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

e-mails of bestandsnamen. Alle maatregelen die op grond van deze verordening worden genomen, moeten in overeenstemming zijn met het kader voor gegevensbescherming en privacy, en de entiteiten van de Unie, CERT-EU en, in voorkomend geval, de IICB moeten alle relevante technische en organisatorische garanties inbouwen om die naleving op verantwoordelijke wijze te waarborgen.

(40) Bij deze verordening wordt de rechtsgrondslag vastgesteld voor de verwerking van persoonsgegevens door entiteiten van de Unie, CERT-EU en, in voorkomend geval, de IICB met het oog op het vervullen van hun taken en verplichtingen op grond van deze verordening, overeenkomstig artikel 5, lid 1, punt b), van Verordening (EU) 2018/1725. CERT-EU kan optreden als verwerker of verwerkingsverantwoordelijke, afhankelijk van de taak die het op grond van Verordening (EU) 2018/1725 vervult.

(41) In bepaalde gevallen kan het noodzakelijk zijn dat entiteiten van de Unie en CERT-EU bijzondere categorieën persoonsgegevens als bedoeld in artikel 10, lid 1, van Verordening (EU) 2018/1725 verwerken om te voldoen aan hun verplichtingen uit hoofde van deze verordening om een hoog niveau van cyberbeveiliging te waarborgen, en met name bij de behandeling van kwetsbaarheden en incidenten. Bij deze verordening wordt de rechtsgrondslag vastgesteld voor de verwerking van bijzondere categorieën persoonsgegevens door entiteiten van de Unie en CERT-EU overeenkomstig artikel 10, lid 2, punt g), van Verordening (EU) 2018/1725. De verwerking van bijzondere categorieën persoonsgegevens in het kader van deze verordening moet strikt in verhouding staan tot het beoogde doel. Met inachtneming van de voorwaarden van artikel 10, lid 2, punt g), van die verordening mogen de entiteiten van de Unie en CERT-EU dergelijke gegevens alleen kunnen verwerken voor zover dat noodzakelijk is en indien daar uitdrukkelijk in wordt voorzien in deze verordening. Wanneer zij bijzondere categorieën persoonsgegevens verwerken, moeten de entiteiten van de Unie en CERT-EU de essentie van het recht op gegevensbescherming eerbiedigen en voorzien in passende en specifieke maatregelen om de grondrechten en de belangen van de betrokkenen te beschermen.

(42) Op grond van artikel 33 van Verordening (EU) 2018/1725 moeten de entiteiten van de Unie en CERT-EU, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, passende technische en organisatorische maatregelen nemen om een passend niveau van beveiliging van persoonsgegevens te waarborgen, zoals het verlenen van beperkte toegangsrechten op "need-to-know"-basis, de toepassing van controlespoorbeginselen, de vaststelling van een bewakingsketen, de opslag van inactieve gegevens in een gecontroleerde en controleerbare omgeving, gestandaardiseerde operationele procedures en privacybeschermingsmaatregelen zoals pseudonimisering of versleuteling. Die maatregelen mogen niet worden uitgevoerd op een wijze die afbreuk doet aan het doel van incidentenbehandeling en de integriteit van bewijsmateriaal. Wanneer een entiteit van de Unie of CERT-EU voor de toepassing van deze verordening persoonsgegevens in verband met een incident, met inbegrip van bijzondere categorieën persoonsgegevens, doorgeeft aan een tegenhanger of partner, moeten die doorgiften in overeenstemming zijn met Verordening (EU) 2018/1725. Wanneer bijzondere categorieën persoonsgegevens aan een derde partij worden doorgegeven, moeten de entiteiten van de Unie en CERT-EU ervoor zorgen dat de derde partij maatregelen ter bescherming van persoonsgegevens toepast op een niveau dat gelijkwaardig is aan dat van Verordening (EU) 2018/1725.

(43) Persoonsgegevens die voor de toepassing van deze verordening worden verwerkt, mogen niet langer worden bewaard dan nodig is overeenkomstig Verordening (EU) 2018/1725. Wanneer zij als verwerkingsverantwoordelijke optreden, moeten de entiteiten van de Unie en, indien van toepassing, CERT-EU bewaringstermijnen vaststellen die beperkt blijven tot wat nodig is om de gespecificeerde doelstellingen te verwezenlijken. Met name met betrekking tot persoonsgegevens die worden verzameld voor incidentenbehandeling moeten de entiteiten van de Unie en CERT-EU een onderscheid maken tussen persoonsgegevens die worden verzameld voor het opsporen van een cyberdreiging in hun ICT-omgevingen om een incident te voorkomen, en persoonsgegevens die worden verzameld met het oog op de beperking van, de respons op en het herstel van een incident. Voor het opsporen van een cyberdreiging is het belangrijk ermee rekening te houden hoelang een dreigingsactor in een systeem onopgemerkt kan blijven. Met het oog op de beperking van, de respons op en het herstel van een incident is het belangrijk na te gaan of de persoonsgegevens noodzakelijk zijn om een terugkerend incident of een incident van vergelijkbare aard waarvoor een correlatie zou kunnen worden aangetoond, op te sporen en te behandelen.

(44) De entiteiten van de Unie en CERT-EU moeten informatie verwerken in overeenstemming met de toepasselijke regels inzake informatiebeveiliging. Ook als personele middelen worden beveiligd als maatregel voor het beheer van cyberbeveiligingsrisico's, moet dat geschieden in overeenstemming met de toepasselijke regels.

(45) Voor het delen van informatie worden zichtbare markeringen gebruikt om aan te geven dat de ontvanger van informatie ten aanzien van het delen van informatie beperkingen in acht moet nemen op basis van, met name, niet-openbaarmakingsovereenkomsten of informele niet-openbaarmakingsovereenkomsten zoals het verkeerslicht-protocol of andere duidelijke indicaties door de bron. Onder het verkeerslichtprotocol moet worden verstaan een middel om informatie te verstrekken over beperkingen ten aanzien van de verdere verspreiding van informatie. Het wordt gebruikt door nagenoeg alle CSIRT's en door een aantal centra voor informatie-uitwisseling en -analyse.

(46) Deze verordening moet regelmatig worden geëvalueerd in het licht van toekomstige onderhandelingen over meerjarige financiële kaders, zodat verdere beslissingen kunnen worden genomen over de werking en de institutionele rol van CERT-EU, waaronder de mogelijke aanduiding van CERT-EU als bureau van de Unie.

(47) De IICB moet, met de hulp van CERT-EU, de uitvoering van deze verordening evalueren en beoordelen en verslag over zijn bevindingen 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. In dat verslag moet, met de input van de IICB, worden beoordeeld of het passend is netwerk- en informatiesystemen waarin EUCI wordt verwerkt, in het toepassingsgebied van deze verordening op te nemen, met name omdat de entiteiten van de Unie geen gemeenschappelijke regels inzake informatiebeveiliging hebben.

(48) Overeenkomstig het evenredigheidsbeginsel is het, teneinde de fundamentele doelstelling het bereiken van een hoog gezamenlijk niveau van cyberbeveiliging binnen de entiteiten van de Unie te verwezenlijken, noodzakelijk en passend de cyberbeveiliging voor de entiteiten van de Unie te regelen. Deze verordening gaat overeenkomstig artikel 5, lid 4, van het Verdrag betreffende de Europese Unie niet verder dan nodig is om de beoogde doelstelling te verwezenlijken.

(49) In deze verordening wordt rekening gehouden met het feit dat de entiteiten van de Unie verschillen in omvang en capaciteit, onder meer wat financiële en personele middelen betreft.

(50) Overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 is de Europese Toezichthouder voor gegevensbescherming geraadpleegd, en op 17 mei 2022 heeft hij een advies uitgebracht ([8]),

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp

Bij deze verordening worden maatregelen vastgesteld met als doel in entiteiten van de Unie een hoog gezamenlijk niveau van cyberbeveiliging te verwezenlijken met betrekking tot:

a) de vaststelling door elke entiteit van de Unie van een intern kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's op grond van artikel 6;

b) het beheer van, rapportage over en het delen van informatie op het gebied van cyberbeveiligingsrisico's;

c) de organisatie, het functioneren en de werking van de op grond van artikel 10 opgerichte interinstitutionele raad voor cyberbeveiliging, alsook de organisatie, het functioneren en de werking van de cyberbeveiligingsdienst voor de instellingen, organen en instanties van de Unie (CERT-EU);

d) het toezicht op de tenuitvoerlegging van deze verordening.

([8]) PB C 258 van 5.7.2022, blz. 10.

Artikel 2

Toepassingsgebied

1. Deze verordening is van toepassing op de entiteiten van de Unie, op de op grond van artikel 10 opgerichte interinstitutionele raad voor cyberbeveiliging en op CERT-EU.

2. Deze verordening laat de institutionele autonomie op grond van de Verdragen onverlet.

3. Met uitzondering van artikel 13, lid 8, is deze verordening niet van toepassing op netwerk- en informatiesystemen die gerubriceerde EU-informatie (EUCI) 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 (VWEU) of het Verdrag tot oprichting van de Europese Gemeenschap voor Atoomenergie;

2) "netwerk- en informatiesysteem": een netwerk- en informatiesysteem zoals gedefinieerd in artikel 6, punt 1), van Richtlijn (EU) 2022/2555;

3) "beveiliging van netwerk- en informatiesystemen": beveiliging van netwerk- en informatiesystemen zoals gedefinieerd in artikel 6, punt 2), van Richtlijn (EU) 2022/2555;

4) "cyberbeveiliging": cyberbeveiliging zoals gedefinieerd in artikel 2, punt 1, van Verordening (EU) 2019/881;

5) "hoogste managementniveau": een leidinggevende, een leidinggevend orgaan of een coördinatie- en toezichtorgaan dat op het hoogste bestuurlijke niveau verantwoordelijk is voor het functioneren van een entiteit van de Unie, met een mandaat om besluiten vast te stellen of hiervoor toestemming te verlenen in overeenstemming met de bestuursregelingen op hoog niveau van die entiteit van de Unie, onverminderd de formele verantwoordelijkheden van andere managementniveaus voor naleving en het beheer van cyberbeveiligingsrisico's op hun respectieve bevoegdheidsgebieden;

6) "bijna-incident": een bijna-incident zoals gedefinieerd in artikel 6, punt 5), van Richtlijn (EU) 2022/2555;

7) "incident": een incident zoals gedefinieerd in artikel 6, punt 6), van Richtlijn (EU) 2022/2555;

8) "ernstig incident": een incident dat een mate van verstoring veroorzaakt die 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) "grootschalig cyberbeveiligingsincident": een grootschalig cyberbeveiligingsincident zoals gedefinieerd in artikel 6, punt 7), van Richtlijn (EU) 2022/2555;

10) "incidentenbehandeling": incidentenbehandeling zoals gedefinieerd in artikel 6, punt 8), van Richtlijn (EU) 2022/2555;

11) "cyberdreiging": een cyberdreiging zoals gedefinieerd in artikel 2, punt 8, van Verordening (EU) 2019/881;

12) "significante cyberdreiging": een significante cyberdreiging zoals gedefinieerd in artikel 6, punt 11), van Richtlijn (EU) 2022/2555;

13) "kwetsbaarheid": kwetsbaarheid zoals gedefinieerd in artikel 6, punt 15), van Richtlijn (EU) 2022/2555;

14) "cyberbeveiligingsrisico": een risico zoals gedefinieerd in artikel 6, punt 9), van Richtlijn (EU) 2022/2555;

15) "cloudcomputingdienst": een cloudcomputingdienst zoals gedefinieerd in artikel 6, punt 30), van Richtlijn (EU) 2022/2555.

Artikel 4

Verwerking van persoonsgegevens

1. De verwerking van persoonsgegevens door CERT-EU, de op grond van artikel 10 opgerichte interinstitutionele raad voor cyberbeveiliging en de entiteiten van de Unie in het kader van deze verordening geschiedt overeenkomstig Verordening (EU) 2018/1725.

2. Wanneer zij taken of verplichtingen op grond van deze verordening vervullen, mogen CERT-EU, de op grond van artikel 10 opgerichte interinstitutionele raad voor cyberbeveiliging en de entiteiten van de Unie persoonsgegevens slechts verwerken en uitwisselen voor zover dat noodzakelijk is en alleen met het oog op het vervullen van die taken of verplichtingen.

3. De verwerking van bijzondere categorieën persoonsgegevens als bedoeld in artikel 10, lid 1, van Verordening (EU) 2018/1725 wordt noodzakelijk geacht om redenen van zwaarwegend algemeen belang op grond van artikel 10, lid 2, punt g), van die verordening. Dergelijke gegevens mogen alleen worden verwerkt voor zover dat noodzakelijk is voor de uitvoering van de in de artikelen 6 en 8 bedoelde maatregelen voor het beheer van cyberbeveiligingsrisico's, voor de verlening van diensten door CERT-EU op grond van artikel 13, voor het delen van incidentspecifieke informatie op grond van artikel 17, lid 3, en artikel 18, lid 3, voor het delen van informatie op grond van artikel 20, voor de rapportageverplichtingen op grond van artikel 21, voor coördinatie en samenwerking bij incidentenbehandeling op grond van artikel 22 en voor het beheer van ernstige incidenten op grond van artikel 23 van deze verordening. Wanneer de entiteiten van de Unie en CERT-EU optreden als verwerkingsverantwoordelijken, passen zij technische maatregelen toe om te voorkomen dat bijzondere categorieën persoonsgegevens voor andere doeleinden worden verwerkt en voorzien zij in passende en specifieke maatregelen om de grondrechten en de belangen van de betrokkenen te beschermen.

HOOFDSTUK II

MAATREGELEN VOOR EEN HOOG GEZAMENLIJK NIVEAU VAN CYBERBEVEILIGING

Artikel 5

Uitvoering van maatregelen

1. Uiterlijk op 8 september 2024 verstrekt de op grond van artikel 10 opgerichte interinstitutionele raad voor cyberbeveiliging, na raadpleging van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) en na advies van CERT-EU, richtsnoeren aan de entiteiten van de Unie met het oog op de uitvoering van een initiële cyberbeveiligingsevaluatie en de vaststelling van een intern kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's op grond van artikel 6, de uitvoering van maturiteitsbeoordelingen van de cyberbeveiliging op grond van artikel 7, het nemen van maatregelen voor het beheer van cyberbeveiligingsrisico's op grond van artikel 8 en de vaststelling van het cyberbeveiligingsplan op grond van artikel 9.

2. Bij de uitvoering van de artikelen 6 tot en met 9 houden de entiteiten van de Unie rekening met de in lid 1 van dit artikel bedoelde richtsnoeren alsook met relevante richtsnoeren en aanbevelingen die zijn vastgesteld op grond van de artikelen 11 en 14.

Artikel 6

Kader voor risicobeheer, governance en toezicht op het gebied van cyberbeveiliging

1. Uiterlijk op 8 april 2025 stelt elke entiteit van de Unie, na een initiële evaluatie van de cyberbeveiliging, zoals een audit, te hebben uitgevoerd, een intern kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's (het "kader") op. De vaststelling van het kader geschiedt onder toezicht van en onder de verantwoordelijkheid van het hoogste managementniveau van de entiteit van de Unie.

2. Het kader omvat de gehele niet-gerubriceerde ICT-omgeving van de entiteit van de Unie in kwestie, met inbegrip van de ICT-omgeving ter plaatse, het operationele technologienetwerk ter plaatse, uitbestede activa en diensten in cloudcomputingomgevingen of gehost door derden, mobiele apparatuur, bedrijfsnetwerken, zakelijke netwerken die niet met het internet verbonden zijn en met die omgevingen verbonden apparaten ("ICT-omgeving"). Het kader is gebaseerd op een alle risico's omvattende aanpak.

3. Het kader waarborgt een hoog niveau van cyberbeveiliging. In het kader wordt het interne cyberbeveiligingsbeleid, met inbegrip van doelstellingen en prioriteiten, vastgesteld voor de beveiliging van netwerk- en informatiesystemen, en de taken en verantwoordelijkheden van het personeel van de entiteit van de Unie dat belast is met het waarborgen van de effectieve uitvoering van deze verordening. Het kader omvat ook mechanismen om de effectiviteit van de uitvoering te meten.

4. Het kader wordt regelmatig, en ten minste om de vier jaar, geëvalueerd in het licht van de veranderende cyberbeveiligingsrisico's. In voorkomend geval en na een verzoek van de op grond van artikel 10 opgerichte interinstitutionele raad voor cyberbeveiliging kan het kader van een entiteit van de Unie worden geactualiseerd op basis van richtsnoeren van CERT-EU met betrekking tot vastgestelde incidenten of mogelijk geconstateerde lacunes in de uitvoering van deze verordening.

5. Het hoogste managementniveau van elke entiteit van de Unie is verantwoordelijk voor de uitvoering van deze verordening en houdt toezicht op de naleving door zijn organisatie van de verplichtingen in verband met het kader.

6. Indien nodig en onverminderd zijn verantwoordelijkheid voor de uitvoering van deze verordening, kan het hoogste managementniveau van elke entiteit van de Unie specifieke verplichtingen uit hoofde van deze verordening delegeren aan hoger leidinggevend personeel in de zin van artikel 29, lid 2, van het Statuut of andere functionarissen op gelijkwaardig niveau binnen de betrokken entiteit van de Unie. Ongeacht een dergelijke delegatie kan het hoogste managementniveau aansprakelijk worden gesteld voor inbreuken op deze verordening door de betrokken entiteit van de Unie.

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

8. Elke entiteit van de Unie stelt elk 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 op regelmatige basis rechtstreeks aan het hoogste managementniveau 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 dienstenniveauovereenkomst 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 delegeren, of kunnen die taken door meerdere entiteiten van de Unie worden gedeeld. Indien die taken aan CERT-EU zijn gedelegeerd, besluit de op grond van artikel 10 opgerichte interinstitutionele raad voor cyberbeveiliging of die dienstverlening onderdeel dient uit te maken van de basisdienstverlening van CERT-EU, rekening houdend met de personele en financiële middelen van de betrokken entiteit van de Unie. Elke entiteit van de Unie geeft CERT-EU onverwijld kennis van de aangewezen lokale cyberbeveiligingsfunctionaris en iedere wijziging daarvan.

CERT-EU stelt een lijst van aangewezen lokale cyberbeveiligingsfunctionarissen op en houdt deze actueel.

9. Het hoger leidinggevend personeel in de zin van artikel 29, lid 2, van het Statuut of andere functionarissen op gelijkwaardig niveau binnen de betrokken entiteit van de Unie, alsmede alle relevante personeelsleden die belast zijn met de uitvoering van de in deze verordening vastgelegde maatregelen en met de naleving van verplichtingen voor het beheer van cyberbeveiligingsrisico's volgen regelmatig specifieke opleidingen om voldoende kennis en vaardigheden op te doen om risico- en beheerspraktijken op het gebied van cyberbeveiliging en de gevolgen daarvan op de activiteiten van de entiteit van de Unie te begrijpen en te beoordelen.

Artikel 7

Maturiteitsbeoordelingen van de cyberbeveiliging

1. Uiterlijk op 8 juli 2025 en daarna ten minste om de twee jaar voert elke entiteit van de Unie een maturiteitsbeoordeling van de cyberbeveiliging uit die alle elementen van haar ICT-omgeving omvat.

2. De maturiteitsbeoordelingen van de cyberbeveiliging worden zo nodig uitgevoerd met bijstand van een gespecialiseerde derde partij.

3. Entiteiten van de Unie met soortgelijke structuren kunnen samenwerken bij de uitvoering van maturiteitsbeoordelingen van de cyberbeveiliging van hun respectieve entiteiten.

4. Op basis van een verzoek van de op grond van artikel 10 opgerichte interinstitutionele raad voor cyberbeveiliging en met de uitdrukkelijke toestemming van de betrokken entiteit van de Unie kunnen de resultaten van een maturiteitsbeoordeling van de cyberbeveiliging worden besproken in die raad of in de informele groep van lokale cyberbeveiligingsfunctionarissen, om lering te trekken uit ervaringen en beste praktijken te delen.

Artikel 8

Maatregelen voor het beheer van cyberbeveiligingsrisico's

1. Elke entiteit van de Unie neemt onverwijld en in elk geval uiterlijk op 8 september 2025, onder het toezicht van haar hoogste managementniveau, passende en evenredige technische, operationele en organisatorische maatregelen voor het beheer van de binnen het kader geïdentificeerde cyberbeveiligingsrisico's, en voor het voorkomen of tot een minimum beperken van de gevolgen van incidenten. Rekening houdend met de stand van de techniek en, in voorkomend geval, de relevante Europese en internationale normen waarborgen die maatregelen een beveiligingsniveau van netwerk- en informatiesystemen in de gehele ICT-omgeving dat in verhouding staat tot de cyberbeveiligingsrisico's die zich voordoen. Bij het beoordelen van de evenredigheid van die maatregelen wordt terdege rekening gehouden met de mate waarin de entiteit van de Unie aan cyberbeveiligingsrisico's is blootgesteld, de omvang van de entiteit van de Unie en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke, economische en interinstitutionele gevolgen daarvan.

2. Bij de uitvoering van de maatregelen voor het beheer van cyberbeveiligingsrisico's behandelen de entiteiten van de Unie ten minste de volgende gebieden:

a) cyberbeveiligingsbeleid, met inbegrip van de maatregelen die nodig zijn om de in artikel 6 en lid 3 van dit artikel bedoelde doelstellingen en prioriteiten te verwezenlijken;

b) beleid inzake cyberbeveiligingsrisicoanalyse en beveiliging van informatiesystemen;

c) beleidsdoelstellingen met betrekking tot het gebruik van cloudcomputingdiensten;

d) in voorkomend geval een cyberbeveiligingsaudit, die een beoordeling van het cyberbeveiligingsrisico, de kwetsbaarheid en de cyberdreiging kan omvatten, en penetratietests die regelmatig door een betrouwbare particuliere aanbieder worden uitgevoerd;

e) de uitvoering van aanbevelingen die voortvloeien uit de in punt d) bedoelde cyberbeveiligingsaudits door middel van cyberbeveiligings- en beleidsupdates;

f) de organisatie van cyberbeveiliging, inclusief de vaststelling van rollen en verantwoordelijkheden;

g) activabeheer, inclusief een inventaris van ICT-activa en ICT-netwerkarchitectuur;

h) beveiliging van personele middelen en toegangscontrole;

i) operationele beveiliging;

j) communicatiebeveiliging;

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

l) indien mogelijk, beleid inzake de transparantie van de broncode;

m) beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten van de betrekkingen tussen elke entiteit van de Unie en haar rechtstreekse leveranciers of dienstverleners;

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

o) bedrijfscontinuïteitsbeheer, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer, en

p) bevordering en ontwikkeling van programma's betreffende onderwijs, vaardigheden, bewustmaking, oefeningen en opleiding op het gebied van cyberbeveiliging.

Voor de toepassing van de eerste alinea, punt m), houden entiteiten van de Unie rekening met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener, en met de algehele kwaliteit van de producten en cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, veilige ontwikkelingsprocessen inbegrepen.

3. Entiteiten van de Unie nemen ten minste de volgende specifieke maatregelen voor het beheer van cyberbeveiligingsrisico's:

a) technische regelingen om telewerken mogelijk te maken en te ondersteunen;

b) concrete stappen in de richting van zero trust-beginselen;

c) het gebruik van multifactorauthenticatie als norm in alle netwerk- en informatiesystemen;

d) het gebruik van cryptografie en versleuteling, en met name eind-tot-eindversleuteling, alsook beveiligde digitale ondertekening;

e) waar passend, beveiligde spraak-, beeld- en tekstcommunicatie, en beveiligde noodcommunicatiesystemen binnen de entiteit van de Unie;

f) proactieve maatregelen voor het opsporen en verwijderen van malware en spyware;

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

h) de opstelling en vaststelling van opleidingsprogramma's op het gebied van cyberbeveiliging die in verhouding staan tot de voorgeschreven taken en verwachte capaciteiten, voor het hoogste managementniveau en voor de personeelsleden van de entiteit van de Unie die belast zijn met het waarborgen van de effectieve uitvoering van deze verordening;

i) de regelmatige opleiding van personeelsleden op het gebied van cyberbeveiliging;

j) in voorkomend geval de deelname aan risicoanalyses van de interconnectiviteit tussen de entiteiten van de Unie;

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

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

   ii) contractueel te bepalen dat incidenten, kwetsbaarheden en cyberdreigingen moeten worden gemeld, en dat er mechanismen voor een passende respons en passend toezicht op incidenten voorhanden moeten zijn.

Artikel 9

Cyberbeveiligingsplannen

1. Na de afronding van de op grond van artikel 7 uitgevoerde maturiteitsbeoordeling van de cyberbeveiliging en rekening houdend met de binnen het kader aangeduide activa en vastgestelde cyberbeveiligingsrisico's en de op grond van artikel 8 genomen maatregelen voor het beheer van cyberbeveiligingsrisico's, keurt het hoogste managementniveau van elke entiteit van de Unie onverwijld en in elk geval uiterlijk op 8 januari 2026 een cyberbeveiligingsplan goed. Het cyberbeveiligingsplan beoogt de algehele cyberbeveiliging van de entiteit van de Unie te versterken en aldus bij te dragen tot de verhoging van een hoog gezamenlijk niveau van cyberbeveiliging in de entiteiten van de Unie. Het cyberbeveiligingsplan bevat minstens de op grond van artikel 8 genomen maatregelen voor het beheer van cyberbeveiligingsrisico's. Het cyberbeveiligingsplan wordt om de twee jaar herzien, of vaker indien nodig na de op grond van artikel 7 uitgevoerde maturiteitsbeoordelingen van de cyberbeveiliging of na een substantiële herziening van het kader.

2. Het cyberbeveiligingsplan omvat het cybercrisisbeheersplan van de entiteit van de Unie voor ernstige incidenten.

3. De entiteit van de Unie dient het afgeronde cyberbeveiligingsplan in bij de op grond van van artikel 10 opgerichte interinstitutionele raad voor cyberbeveiliging.

HOOFDSTUK III

INTERINSTITUTIONELE RAAD VOOR CYBERBEVEILIGING

Artikel 10

Interinstitutionele raad voor cyberbeveiliging

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

2. De IICB is verantwoordelijk voor:

a) het toezicht op en de ondersteuning van 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 bestaat uit:

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

i) het Europees Parlement;

ii) de Europese Raad;

iii) de Raad van de Europese Unie;

iv) de Commissie;

v) het Hof van Justitie van de Europese Unie;

vi) de Europese Centrale Bank;

vii) de 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;

xiii) Enisa;

xiv) de Europese Toezichthouder voor gegevensbescherming;

xv) het Agentschap van de Europese Unie voor het ruimtevaartprogramma;

b) drie vertegenwoordigers die door het netwerk van EU-agentschappen (EUAN) op basis van een voorstel van zijn adviescomité voor ICT worden aangewezen om de belangen te behartigen van andere dan de in punt a) bedoelde organen en instanties van de Unie die hun eigen ICT-omgeving beheren.

De in de IICB vertegenwoordigde entiteiten van de Unie streven naar genderevenwicht onder de aangewezen vertegenwoordigers.

4. De leden van de IICB kunnen door een plaatsvervanger worden bijgestaan. Andere vertegenwoordigers van de in lid 3 bedoelde entiteiten van de Unie of van andere entiteiten van de Unie kunnen door de voorzitter worden uitgenodigd om zonder stemrecht aan IICB-vergaderingen deel te nemen.

5. Het hoofd van CERT-EU en de voorzitters van de samenwerkingsgroep, het CSIRT-netwerk en EU-CyCLONe, respectievelijk opgericht op grond van de artikelen 14, 15 en 16 van Richtlijn (EU) 2022/2555, of hun plaatsvervangers, kunnen als waarnemer deelnemen aan IICB-vergaderingen. In uitzonderlijke gevallen kan de IICB overeenkomstig zijn reglement van orde anders beslissen.

6. De IICB stelt zijn reglement van orde vast.

7. De IICB wijst overeenkomstig zijn reglement van orde uit zijn leden een voorzitter aan voor een periode van drie jaar. De plaatsvervanger van de voorzitter wordt voor dezelfde duur volwaardig lid van de IICB.

8. De IICB komt ten minste driemaal per jaar bijeen op initiatief van zijn voorzitter, op verzoek van CERT-EU of op verzoek van een van zijn leden.

9. 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 van de IICB heeft uitsluitend stemrecht bij staking van de stemmen; in dat geval geeft de stem van de voorzitter de doorslag.

10. 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.

11. Het secretariaat van de IICB wordt verzorgd door de Commissie en legt verantwoording af aan de voorzitter van de IICB.

12. De door het EUAN benoemde vertegenwoordigers brengen de besluiten van de IICB over aan de leden van het EUAN. Leden van het EUAN mogen iedere kwestie die zij voor de IICB van belang achten, aan die vertegenwoordigers of de voorzitter van de IICB voorleggen.

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

14. Uiterlijk op 8 januari 2025 en vervolgens jaarlijks dient de IICB bij het Europees Parlement en 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 tegenhangers in de lidstaten in elk van de lidstaten wordt gespecificeerd. Het verslag dient als input voor het tweejaarlijkse verslag over de stand van zaken op het gebied van de cyberbeveiliging in de Unie dat op grond van artikel 18 van Richtlijn (EU) 2022/2555 wordt opgesteld.

Artikel 11

Taken van de IICB

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

a) hij verstrekt het hoofd van CERT-EU richtsnoeren;

b) hij houdt effectief toezicht op de uitvoering van deze verordening en ondersteunt de entiteiten van de Unie bij het versterken van hun cyberbeveiliging, onder meer door entiteiten van de Unie en CERT-EU waar passend om ad-hocverslagen te vragen;

c) hij stelt na een strategische discussie een meerjarige strategie vast voor het verhogen van het cyberbeveiligingsniveau in de entiteiten van de Unie, evalueert die strategie regelmatig en in elk geval om de vijf jaar, en wijzigt die strategie indien nodig;

d) hij stelt de methodologie en organisatorische aspecten voor de uitvoering van vrijwillige collegiale toetsingen door entiteiten van de Unie vast om van gedeelde ervaringen te leren, het onderlinge vertrouwen te versterken, een hoog gemeenschappelijk niveau van cyberbeveiliging te bewerkstelligen en de cyberbeveiligingscapaciteiten van de entiteiten van de Unie te verbeteren, waarbij ervoor wordt gezorgd dat dergelijke collegiale toetsingen worden uitgevoerd door cyberbeveiligingsdeskundigen die zijn aangewezen door een andere entiteit van de Unie dan de entiteit van de Unie die wordt geëvalueerd, en dat de methodologie gebaseerd is op artikel 19 van Richtlijn (EU) 2022/2555 en, in voorkomend geval, wordt aangepast aan de entiteiten van de Unie;

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

f) hij hecht zijn goedkeuring aan de CERT-EU -dienstencatalogus en alle bijwerkingen daarvan, op basis van een voorstel van het hoofd van CERT-EU;

g) hij hecht zijn goedkeuring aan de verwachte jaarlijkse ontvangsten en uitgaven, inclusief wat personeel betreft, voor CERT-EU, op basis van een voorstel van het hoofd van CERT-EU;

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

i) 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;

j) hij hecht zijn goedkeuring aan en monitort kernprestatie-indicatoren voor CERT-EU die op basis van een voorstel van het hoofd van CERT-EU worden vastgesteld;

k) hij hecht zijn goedkeuring aan samenwerkingsovereenkomsten en dienstenniveauovereenkomsten of overeenkomsten tussen CERT-EU en andere entiteiten op grond van artikel 18;

l) hij stelt richtsnoeren en aanbevelingen vast op basis van een voorstel van CERT-EU overeenkomstig artikel 14 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;

m) hij stelt technische adviesgroepen met specifieke taken in ter ondersteuning van de werkzaamheden van de IICB, keurt hun mandaat goed en wijst hun voorzitter aan;

n) hij ontvangt en beoordeelt documenten en verslagen die de entiteiten van de Unie uit hoofde van deze verordening indienen, zoals maturiteitsbeoordelingen van de cyberbeveiliging;

o) hij bevordert de oprichting van een informele groep van lokale cyberbeveiligingsfunctionarissen van entiteiten van de Unie, ondersteund door Enisa, teneinde beste praktijken en informatie in verband met de uitvoering van deze verordening uit te wisselen;

p) hij houdt toezicht op de toereikendheid van de interconnectiviteitsregelingen tussen de ICT-omgevingen van de entiteiten van de Unie, rekening houdend met de door CERT-EU verstrekte informatie over de vastgestelde cyberbeveiligingsrisico's en de geleerde lessen, en brengt advies uit over mogelijke verbeteringen;

q) hij stelt een cybercrisisbeheersplan op om op operationeel niveau het gecoördineerde beheer 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 met betrekking tot de gevolgen en de ernst van ernstige incidenten en de mogelijke manieren om de gevolgen ervan te beperken;

r) hij coördineert de vaststelling van de cybercrisisbeheersplannen door de individuele entiteiten van de Unie zoals bedoeld in artikel 9, lid 2;

s) hij stelt aanbevelingen vast in verband met de beveiliging van de toeleveringsketen zoals bedoeld in artikel 8, lid 2, eerste alinea, punt m), rekening houdend met de resultaten van op Unieniveau gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens zoals bedoeld in artikel 22 van Richtlijn (EU) 2022/2555, teneinde de entiteiten van de Unie te ondersteunen bij het doorvoeren van doeltreffende en passende maatregelen voor het beheer van cyberbeveiligingsrisico's.

Artikel 12

Naleving

1. De IICB houdt op grond van artikel 10, lid 2, en artikel 11 effectief toezicht op de uitvoering van deze verordening en de door de entiteiten van de Unie vastgestelde richtsnoeren, aanbevelingen en oproepen tot actie. De IICB kan de daartoe benodigde informatie of documentatie opvragen bij de entiteiten van de Unie. Voor de vaststelling van nalevingsmaatregelen uit hoofde van dit artikel heeft de betrokken entiteit van de Unie geen stemrecht indien die entiteit rechtstreeks vertegenwoordigd is in de IICB.

2. Indien de IICB vaststelt dat een entiteit van de Unie deze verordening of de op grond van deze verordening vastgestelde richtsnoeren, aanbevelingen of oproepen tot actie niet doeltreffend heeft uitgevoerd, kan hij, onverminderd de interne procedures van de betrokken entiteit van de Unie, en na de betrokken entiteit van de Unie de gelegenheid te hebben gegeven opmerkingen te maken:

a) de betrokken entiteit van de Unie een met redenen omkleed advies doen toekomen inzake de geconstateerde lacunes in de uitvoering van deze verordening;

b) na raadpleging van CERT-EU de betrokken entiteit van de Unie richtsnoeren verstrekken om ervoor te zorgen dat haar kader, maatregelen voor het beheer van cyberbeveiligingsrisico's, cyberbeveiligingsplan en verslaglegging binnen een bepaalde termijn in overeenstemming zijn met deze verordening;

c) een waarschuwing doen uitgaan om vastgestelde tekortkomingen binnen een bepaalde termijn te verhelpen, met inbegrip van aanbevelingen tot wijziging van maatregelen die de betrokken entiteit van de Unie op grond van deze verordening heeft getroffen;

d) een met redenen omklede kennisgeving doen uitgaan aan de betrokken entiteit van de Unie indien de in een waarschuwing op grond van punt c) vastgestelde tekortkomingen niet voldoende werden verholpen binnen de vermelde termijn;

e) het volgende doen uitgaan:

i) een aanbeveling om een audit uit te voeren, of

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

f) in voorkomend geval de Rekenkamer, binnen de grenzen van haar mandaat, in kennis stellen van de vermeende niet-naleving;

g) een aanbeveling aan alle lidstaten en entiteiten van de Unie doen uitgaan om gegevensstromen naar de betrokken entiteit van de Unie tijdelijk op te schorten.

Voor de toepassing van de eerste alinea, punt c), wordt de waarschuwing gericht tot een op passende wijze beperkt publiek, indien nodig met het oog op het cyberbeveiligingsrisico.

Op grond van de eerste alinea uitgebrachte waarschuwingen en aanbevelingen worden gericht aan het hoogste managementniveau van de betrokken entiteit van de Unie.

3. Indien de IICB maatregelen heeft genomen op grond van lid 2, eerste alinea, punten a) tot en met g), verstrekt de betrokken entiteit van de Unie nadere informatie over de maatregelen en acties die zijn genomen om de door de IICB vastgestelde vermeende tekortkomingen te verhelpen. De entiteit van de Unie dient deze nadere informatie 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 schending 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 van de Unie passende maatregelen te nemen, met inbegrip van het verzoek te overwegen om maatregelen van disciplinaire aard te nemen, overeenkomstig de bepalingen en procedures van het Statuut en alle andere toepasselijke regels en procedures. Daartoe draagt de IICB de nodige informatie over aan de betrokken entiteit van de Unie.

5. Indien entiteiten van de Unie er kennis van geven dat zij niet in staat zijn om de in artikel 6, lid 1, en artikel 8, lid 1, vastgestelde termijnen te halen, kan de IICB, in naar behoren gemotiveerde gevallen en rekening houdend met de omvang van de entiteit van de Unie, toestemming geven om die termijnen te verlengen.

HOOFDSTUK IV

CERT-EU

Artikel 13

Missie en taken van CERT-EU

1. De missie van CERT-EU bestaat erin bij te dragen tot de beveiliging van de niet-gerubriceerde ICT-omgeving van de entiteiten van de Unie door ze te adviseren over cyberbeveiliging, door ze te helpen incidenten te voorkomen, op te sporen, te behandelen, te beperken, daarop te reageren en daarvan te herstellen, en door op te treden als knooppunt voor hun informatie-uitwisseling inzake cyberbeveiliging en responscoördinatie bij incidenten.

2. CERT-EU verzamelt, beheert, analyseert en deelt informatie met de entiteiten van de Unie over cyberdreigingen, kwetsbaarheden en incidenten in 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.

3. CERT-EU verricht de volgende taken om de entiteiten van de Unie bij te staan:

a) het ondersteunt ze bij de uitvoering van deze verordening en draagt bij tot de coördinatie van de uitvoering van deze verordening door middel van de in artikel 14, lid 1, vermelde maatregelen of via door de IICB gevraagde ad-hocverslagen;

b) het biedt standaard CSIRT-diensten aan de entiteiten van de Unie door middel van een in zijn dienstencatalogus beschreven pakket cyberbeveiligingsdiensten (basisniveaudiensten);

c) het onderhoudt een netwerk van soortgelijke organisaties en partners ter ondersteuning van de in de artikelen 17 en 18 bedoelde diensten;

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

e) het draagt op basis van de in lid 2 bedoelde informatie bij tot het situatiebewustzijn van de Unie op het gebied van cyberbeveiliging, in nauwe samenwerking met Enisa;

f) het coördineert het beheer van ernstige incidenten;

g) het handelt namens entiteiten van de Unie als equivalent van de coördinator die is aangewezen met het oog op de gecoördineerde bekendmaking van kwetsbaarheden op grond artikel 12, lid 1, van Richtlijn (EU) 2022/2555;

h) het gaat op verzoek van een entiteit van de Unie over tot het proactief en niet-intrusief scannen van openbaar toegankelijke netwerk- en informatiesystemen van die entiteit van de Unie.

De in de eerste alinea, punt e), bedoelde informatie wordt, indien van toepassing en gepast, gedeeld met de IICB, het CSIRT-netwerk en het Inlichtingen- en situatiecentrum van de Europese Unie (EU-Intcen); daarbij worden passende geheimhoudingsvoorwaarden in acht genomen.

4. CERT-EU kan overeenkomstig artikel 17 of artikel 18, naargelang het geval, samenwerken met relevante cyberbeveiligingsgemeenschappen binnen de Unie en haar lidstaten, onder meer op de volgende gebieden:

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

b) operationele samenwerking inzake het CSIRT-netwerk, ook betreffende wederzijdse bijstand;

c) inlichtingen inzake cyberdreigingen, inclusief situatiebewustzijn;

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

5. Binnen het kader van zijn bevoegdheid onderhoudt CERT-EU gestructureerde samenwerking met Enisa met betrekking tot capaciteitsopbouw, operationele samenwerking en strategische langetermijnanalyses van cyberdreigingen, overeenkomstig Verordening (EU) 2019/881. CERT-EU kan samenwerken en informatie uitwisselen met het Europees Centrum voor de bestrijding van cybercriminaliteit van Europol.

6. CERT-EU kan de volgende diensten aanbieden die niet in de dienstencatalogus zijn beschreven (aangerekende diensten):

a) andere dan de in lid 3 bedoelde diensten ter ondersteuning van de cyberbeveiliging van de ICT-omgeving van de entiteiten van de Unie, op basis van dienstenniveauovereenkomsten en afhankelijk van de beschikbaarheid van middelen, met name brede netwerkmonitoring, met inbegrip van continue eerstelijnsmonitoring voor zeer ernstige cyberdreigingen;

b) andere diensten dan diensten ter bescherming van de ICT-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) op verzoek, het proactief scannen van de netwerk- en informatiesystemen van de betrokken entiteit van de Unie om kwetsbaarheden met mogelijk aanzienlijke gevolgen op te sporen;

d) diensten ter ondersteuning van de beveiliging van de ICT-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 uit hoofde van Unierecht vervullen, op basis van schriftelijke overeenkomsten en met voorafgaande goedkeuring van de IICB.

Met betrekking tot de eerste alinea, punt d), kan CERT-EU bij wijze van uitzondering met voorafgaande toestemming van de IICB dienstenniveauovereenkomsten sluiten met andere entiteiten dan de entiteiten van de Unie.

7. CERT-EU organiseert cyberbeveiligingsoefeningen en kan eraan deelnemen of deelname aan bestaande oefeningen aanbevelen, in voorkomend geval in nauwe samenwerking met Enisa, om het cyberbeveiligingsniveau van de entiteiten van de Unie te testen.

8. CERT-EU kan de entiteiten van de Unie bijstaan bij incidenten in netwerk- en informatiesystemen die EUCI verwerken, indien de betrokken entiteiten van de Unie daar uitdrukkelijk om verzoeken overeenkomstig hun respectieve procedures. Het verlenen van bijstand door CERT-EU uit hoofde van dit lid laat de toepasselijke regels inzake de bescherming van gerubriceerde informatie onverlet.

9. CERT-EU informeert de entiteiten van de Unie over zijn procedures en processen voor incidentenbehandeling.

10. CERT-EU draagt, met een hoog niveau van vertrouwelijkheid en betrouwbaarheid, via de passende samenwerkingsmechanismen en rapportagelijnen bij tot relevante en geanonimiseerde informatie over ernstige incidenten en de wijze waarop deze werden afgehandeld. Die informatie wordt opgenomen in het in artikel 10, lid 14, bedoelde verslag.

11. Bij de aanpak van incidenten die leiden tot inbreuken in verband met persoonsgegevens, ondersteunt CERT-EU de betrokken entiteiten van de Unie, in samenwerking met de Europese Toezichthouder voor gegevensbescherming, onverminderd de bevoegdheid en taken van die Toezichthouder als toezichthoudende autoriteit uit hoofde van Verordening (EU) 2018/1725.

12. 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.

Artikel 14

Richtsnoeren, aanbevelingen en oproepen tot actie

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

a) oproepen tot actie, die dringende beveiligingsmaatregelen omvatten die de entiteiten van de Unie binnen een bepaalde termijn met klem wordt aangeraden te nemen;

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.

Met betrekking tot de eerste alinea, punt a), stelt de betrokken entiteit van de Unie CERT-EU onverwijld na ontvangst van de oproep tot actie in kennis van de wijze waarop de dringende beveiligingsmaatregelen zijn toegepast.

2. Richtsnoeren en aanbevelingen kunnen het volgende omvatten:

a) gemeenschappelijke methoden en een model voor de beoordeling van de maturiteit van de entiteiten van de Unie op het gebied van cyberbeveiliging, met inbegrip van de bijbehorende schalen of kernprestatie-indicatoren, die als referentie dienen ter ondersteuning van de voortdurende verbetering van de cyberbeveiliging in alle entiteiten van de Unie en die de prioritering van cyberbeveiligingsdomeinen en -maatregelen vergemakkelijken, rekening houdend met de positie van de entiteiten ten opzichte van cyberbeveiliging;

b) de regelingen voor of verbetering van het beheer van cyberbeveiligingsrisico's en de maatregelen voor het beheer van cyberbeveiligingsrisico's;

c) de regelingen voor maturiteitsbeoordelingen van de cyberbeveiliging en cyberbeveiligingsplannen;

d) indien van toepassing, het gebruik van algemene technologie, architectuur, open bronnen 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;

e) in voorkomend geval, informatie om het gebruik van instrumenten voor gemeenschappelijke aanbestedingen voor de aankoop van relevante cyberbeveiligingsdiensten en -producten van derde leveranciers te vergemakkelijken;

f) regelingen voor informatie-uitwisseling op grond van artikel 20.

Artikel 15

Hoofd van CERT-EU

1. De Commissie benoemt met goedkeuring door een tweederdemeerderheid van de leden van de IICB het hoofd van CERT-EU. De IICB wordt geraadpleegd in alle stadia van de benoemingsprocedure, in het bijzonder bij het opstellen van vacatureberichten, de beoordeling van de sollicitaties en de benoeming van de selectiecomités voor de functie. De selectieprocedure, met inbegrip van de definitieve shortlist van kandidaten waaruit het hoofd van CERT-EU zal worden benoemd, zorgt voor een eerlijke vertegenwoordiging van elk gender, rekening houdend met de ingediende sollicitaties.

2. Het hoofd van CERT-EU is verantwoordelijk voor het goed functioneren van CERT-EU en handelt binnen de grenzen van zijn of haar rol, onder de leiding van de IICB. Het hoofd van CERT-EU brengt regelmatig verslag uit aan de voorzitter van de IICB en dient desgevraagd ad-hocverslagen in bij de IICB.

3. Het hoofd van CERT-EU verleent de bevoegde gedelegeerd ordonnateur bijstand bij het opstellen van het overeenkomstig artikel 74, lid 9, van Verordening (EU, Euratom) 2018/1046 van het Europees Parlement en de Raad ([9]) opgestelde jaarlijks activiteitenverslag, dat financiële en beheersinformatie, inclusief de resultaten van controles, bevat, en brengt regelmatig verslag uit aan de bevoegde gedelegeerd ordonnateur over de uitvoering van maatregelen waarvoor aan het hoofd van CERT-EU 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, een voorgesteld jaarlijks werkprogramma, een voorgestelde dienstencatalogus voor CERT-EU, voorgestelde herzieningen van de dienstencatalogus, voorgestelde regelingen voor dienstenniveauovereenkomsten en voorgestelde kernprestatie-indicatoren voor CERT-EU, die overeenkomstig artikel 11 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 ten minste eenmaal per jaar verslag uit aan de IICB en de voorzitter ervan over de activiteiten en de prestaties van CERT-EU gedurende de referentieperiode, onder meer met betrekking tot de uitvoering van de begroting, gesloten dienstenniveauovereenkomsten en schriftelijke overeenkomsten, de samenwerking met tegenhangers en partners, en de dienstreizen van personeel, met inbegrip van de in artikel 11 bedoelde verslagen. Die verslagen bevatten een werkprogramma voor de volgende periode, de financiële planning van ontvangsten en uitgaven, met inbegrip van personeel, geplande actualiseringen van de dienstencatalogus van CERT-EU en een beoordeling van het verwachte effect dat dergelijke actualiseringen kunnen hebben op het gebied van financiële en personele middelen.

Artikel 16

Financiële en personeelszaken

1. CERT-EU wordt 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, met behoud van zijn status als autonome interinstitutionele dienstverlener voor alle entiteiten van de Unie. De Commissie stelt de IICB in kennis van de administratieve vestiging van CERT-EU en van eventuele wijzigingen daarvan. De Commissie evalueert de administratieve regelingen met betrekking tot CERT-EU regelmatig en in elk geval vóór de vaststelling van een meerjarig financieel kader op grond van artikel 312 VWEU, zodat passende actie kan worden ondernomen. De evaluatie omvat de mogelijkheid om CERT-EU als bureau van de Unie aan te duiden.

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

([9]) 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 de 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).

3. De taken en activiteiten van CERT-EU, inclusief de diensten die CERT-EU op grond van artikel 13, leden 3, 4, 5 en 7, en artikel 14, 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. De voor CERT-EU gereserveerde posten worden gespecificeerd in een voetnoot bij de personeelsformatie van de Commissie.

4. Andere dan de in lid 3 van dit artikel bedoelde entiteiten van de Unie leveren een jaarlijkse financiële bijdrage aan CERT-EU ter dekking van de door CERT-EU op grond van dat lid verleende diensten. De bijdragen worden gebaseerd op richtsnoeren van de IICB en in dienstenniveauovereenkomsten tussen elke entiteit van de Unie en CERT-EU bepaald. De bijdragen vertegenwoordigen een billijk en evenredig deel van de totale kosten van de verleende diensten. Deze worden als interne bestemmingsontvangsten in de zin van artikel 21, lid 3, punt c), van Verordening (EU, Euratom) 2018/1046 via de in lid 3 van dit artikel bedoelde afzonderlijke begrotingslijn ontvangen.

5. De kosten van de in artikel 13, lid 6, bedoelde diensten 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.

Artikel 17

Samenwerking van CERT-EU met tegenhangers in de lidstaten

1. CERT-EU werkt onverwijld samen en wisselt informatie uit met tegenhangers in de lidstaten, met name de op grond van artikel 10 van Richtlijn (EU) 2022/2555 aangewezen of ingestelde CSIRT's of, indien van toepassing, de op grond van artikel 8 van die richtlijn aangewezen of ingestelde bevoegde autoriteiten en centrale contactpunten, met betrekking tot incidenten, cyberdreigingen, kwetsbaarheden, bijna-incidenten, mogelijke tegenmaatregelen en beste praktijken, en doet dat voor alle onderwerpen die relevant zijn voor een betere bescherming van de ICT-infrastructuur van de entiteiten van de Unie, onder meer via het op grond van artikel 15 van Richtlijn (EU) 2022/2555 opgerichte CSIRT-netwerk. CERT-EU ondersteunt de Commissie in het op grond van artikel 16 van Richtlijn (EU) 2022/2555 opgerichte EU-CyCLONe bij het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en -crises.

2. Indien CERT-EU kennis krijgt van een significant incident dat zich voordoet op het grondgebied van een lidstaat, stelt het overeenkomstig lid 1 onverwijld de betrokken tegenhangers in die lidstaat in kennis.

3. Op voorwaarde dat persoonsgegevens worden beschermd overeenkomstig het toepasselijk Unierecht inzake gegevensbescherming, wisselt CERT-EU onverwijld, zonder toestemming van de getroffen entiteit van de Unie, relevante incidentspecifieke informatie uit met tegenhangers in de lidstaten teneinde de opsporing van soortgelijke cyberdreigingen of -incidenten te vergemakkelijken of bij te dragen aan de analyse van een incident. CERT-EU wisselt enkel in de volgende gevallen incidentspecifieke informatie uit die de identiteit van het doelwit van het incident onthult:

a) de getroffen entiteit van de Unie verleent toestemming;

b) de getroffen entiteit van de Unie verleent weliswaar geen toestemming als bepaald in punt a), maar bekendmaking van de identiteit van de getroffen entiteit van de Unie zou de waarschijnlijkheid vergroten dat elders incidenten worden voorkomen of beperkt, of

c) de getroffen entiteit van de Unie heeft reeds bekendgemaakt dat zij getroffen werd.

Besluiten om op grond van de eerste alinea, punt b), incidentspecifieke informatie uit te wisselen die de identiteit van het doelwit van het incident onthult, worden bekrachtigd door het hoofd van CERT-EU. Alvorens een dergelijk besluit te nemen, neemt CERT-EU schriftelijk contact op met de getroffen entiteit van de Unie, waarbij duidelijk wordt uitgelegd hoe de bekendmaking van haar identiteit elders incidenten zou helpen voorkomen of beperken. Het hoofd van CERT-EU verstrekt de uitleg en verzoekt de entiteit van de Unie uitdrukkelijk om aan te geven of zij binnen een bepaalde termijn toestemming verleent. Het hoofd van CERT-EU deelt de entiteit van de Unie tevens mee dat hij of zij zich, in het licht van de verstrekte uitleg, het recht voorbehoudt om de informatie ook bekend te maken als er geen toestemming wordt verleend. De getroffen entiteit van de Unie wordt in kennis gesteld voordat de informatie wordt bekendgemaakt.

Artikel 18

Samenwerking van CERT-EU met andere tegenhangers

1. CERT-EU kan met andere tegenhangers in de Unie samenwerken dan de in artikel 17 bedoelde tegenhangers die onderworpen zijn aan cyberbeveiligingsvereisten van de Unie, met inbegrip van bedrijfstakspecifieke tegenhangers, inzake instrumenten en methoden, zoals technieken, tactiek, procedures en beste praktijken, en cyberdreigingen en kwetsbaarheden. Voor iedere samenwerking met dergelijke tegenhangers verzoekt CERT-EU per geval vooraf om de goedkeuring van de IICB. Wanneer CERT-EU met dergelijke tegenhangers een samenwerking aangaat, informeert het de in artikel 17, lid 1, bedoelde tegenhangers in de lidstaat waar de instantie is gevestigd. Waar dit toepasselijk en gepast is, worden die samenwerking en de voorwaarden daarvan, onder meer met betrekking tot cyberbeveiliging, gegevensbescherming en informatieverwerking, vastgelegd in specifieke geheimhoudingsregelingen zoals overeenkomsten of administratieve regelingen. Voor de geheimhoudingsregelingen is geen voorafgaande goedkeuring van de IICB nodig, maar de voorzitter van de IICB wordt ervan op de hoogte gebracht. Indien het dringend noodzakelijk is om informatie over cyberbeveiliging uit te wisselen in het belang van entiteiten van de Unie of een andere partij, kan CERT-EU dit doen met een entiteit waarvan de specifieke bevoegdheid, capaciteit en deskundigheid aantoonbaar vereist zijn om bijstand te verlenen bij een dergelijke dringende noodzaak, ook al heeft CERT-EU geen geheimhoudingsregeling met die entiteit. In dergelijke gevallen brengt CERT-EU de voorzitter van de IICB onmiddellijk op de hoogte en brengt het verslag uit aan de IICB door middel van regelmatige verslagen of vergaderingen.

2. CERT-EU kan samenwerken met partners, zoals commerciële entiteiten, met inbegrip van bedrijfstakspecifieke entiteiten, internationale organisaties en nationale entiteiten van buiten de Unie of individuele deskundigen, om informatie te verzamelen over algemene en specifieke cyberdreigingen, bijna-incidenten, 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, met toestemming van de door een incident getroffen entiteit van de Unie en op voorwaarde dat er met de betrokken tegenhanger of partner een geheimhoudingsregeling of -overeenkomst is gesloten, informatie over het specifieke incident verstrekken aan de in de leden 1 en 2 bedoelde tegenhangers of partners, louter om hen te helpen bij hun analyse.

HOOFDSTUK V

SAMENWERKING EN VERSLAGLEGGINGSVERPLICHTINGEN

Artikel 19

Informatieverwerking

1. De entiteiten van de Unie en CERT-EU nemen de geheimhoudingsplicht in acht overeenkomstig artikel 339 VWEU of gelijkwaardige toepasselijke kaders.

2. Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad ([10]) is van toepassing op verzoeken om toegang van het publiek tot documenten die berusten bij CERT-EU, met inbegrip van de verplichting uit hoofde van die verordening om andere entiteiten van de Unie of, in voorkomend geval, de lidstaten te raadplegen indien een verzoek betrekking heeft op hun documenten.

3. De entiteiten van de Unie en CERT-EU verwerken informatie in overeenstemming met de toepasselijke regels inzake informatiebeveiliging.

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

Artikel 20

Informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging

1. De entiteiten van de Unie kunnen CERT-EU op vrijwillige basis in kennis stellen van en informatie verstrekken over incidenten, cyberdreigingen, bijna-incidenten en kwetsbaarheden met gevolgen voor hen. CERT-EU zorgt ervoor dat het over efficiënte communicatiemiddelen met een hoge mate van traceerbaarheid, vertrouwelijkheid en betrouwbaarheid beschikt om informatie-uitwisseling met de entiteiten van de Unie te vergemakkelijken. Bij het verwerken van kennisgevingen kan CERT-EU voorrang geven aan de verwerking van verplichte boven vrijwillige kennisgevingen. Onverminderd artikel 12 mag vrijwillige kennisgeving er niet toe leiden dat de kennisgevende entiteit van de Unie aanvullende verplichtingen worden opgelegd waaraan zij niet onderworpen zou zijn geweest indien zij de kennisgeving niet had gedaan.

2. Om zijn missie en taken op grond van artikel 13 uit te voeren, kan CERT-EU entiteiten van de Unie verzoeken informatie uit hun respectieve ICT-systeeminventarissen te verstrekken, met inbegrip van informatie over cyberdreigingen, bijna-incidenten, kwetsbaarheden, indicatoren voor aantasting, cyberbeveiligingswaarschuwingen en aanbevelingen betreffende de configuratie van cyberbeveiligingsinstrumenten om incidenten te detecteren. De aangezochte entiteit van de Unie zendt de verlangde informatie en bijbehorende actualiseringen daarvan onverwijld toe.

3. CERT-EU kan met entiteiten van de Unie incidentspecifieke informatie uitwisselen die de identiteit van de door het incident getroffen entiteit van de Unie onthult, mits de getroffen entiteit van de Unie daarin toestemt. Wanneer een entiteit van de Unie haar toestemming weigert, verstrekt zij CERT-EU de redenen voor dat besluit.

4. De entiteiten van de Unie wisselen op verzoek informatie uit met het Europees Parlement en de Raad over de voltooiing van de cyberbeveiligingsplannen.

5. De IICB of CERT-EU, naargelang het geval, deelt op verzoek richtsnoeren, aanbevelingen en oproepen tot actie met het Europees Parlement en de Raad.

6. De in dit artikel vastgestelde deelverplichtingen gelden niet voor:

a) EUCI;

b) informatie waarvan de verdere verspreiding is uitgesloten door middel van een zichtbare markering, tenzij het delen daarvan met CERT-EU uitdrukkelijk is toegestaan.

Artikel 21

Rapportageverplichtingen

1. Een incident wordt als significant beschouwd als het:

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

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

2. De entiteiten van de Unie verstrekken aan CERT-EU:

a) onverwijld en in elk geval binnen 24 uur nadat zij kennis hebben gekregen van het significante incident, een vroegtijdige waarschuwing, waarin, indien van toepassing, wordt aangegeven dat het significante incident vermoedelijk door een onwettige of kwaadwillige handeling is veroorzaakt, dan wel entiteitoverstijgende of grensoverschrijdende gevolgen zou kunnen hebben;

b) onverwijld en in elk geval binnen 72 uur nadat zij kennis hebben gekregen van het significante incident, een incidentmelding met, indien van toepassing, een update van de in punt a) bedoelde informatie, een initiële beoordeling van het significante incident, met inbegrip van de ernst en de gevolgen ervan, alsook, indien beschikbaar, de indicatoren voor aantasting;

c) een tussentijds verslag met relevante updates van de situatie, indien CERT-EU daarom verzoekt;

d) uiterlijk één maand na de indiening van de in punt b) bedoelde incidentmelding, een eindverslag waarin het volgende is opgenomen:

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

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

iii) toegepaste en lopende beperkende maatregelen;

iv) in voorkomend geval de grensoverschrijdende of entiteitoverstijgende gevolgen van het incident;

e) indien het incident nog aan de gang is op het moment dat het in punt d) bedoelde eindverslag wordt ingediend, op dat moment een voortgangsverslag en uiterlijk één maand nadat zij het incident hebben afgehandeld, een eindverslag.

3. Een entiteit van de Unie stelt onverwijld en in elk geval binnen 24 uur nadat zij kennis heeft gekregen van een significant incident, alle in artikel 17, lid 1, bedoelde relevante tegenhangers in de lidstaat waar zij is gevestigd, in kennis van het feit dat zich een significant incident heeft voorgedaan.

4. De entiteiten van de Unie verstrekken onder meer alle informatie die CERT-EU in staat stelt om alle mogelijke entiteitoverstijgende gevolgen, gevolgen voor de lidstaat van vestiging of grensoverschrijdende gevolgen van een significant incident in kaart te brengen. Onverminderd artikel 12 leidt het louter doen van een melding niet tot een verhoogde aansprakelijkheid voor de entiteit van de Unie.

5. In voorkomend geval informeren de entiteiten van de Unie de gebruikers van de getroffen netwerk- en informatiesystemen of van andere onderdelen van de ICT-omgeving die mogelijkerwijs door een significant incident of een significante cyberdreiging worden getroffen en in voorkomend geval beperkende maatregelen moeten nemen, onverwijld over alle maatregelen of middelen die zij kunnen nemen of inzetten in antwoord op dat incident of die dreiging. Indien nodig informeren de entiteiten van de Unie die gebruikers over de significante cyberdreiging zelf.

6. Indien een significant incident of een significante cyberdreiging gevolgen heeft voor een netwerk- en informatiesysteem of een onderdeel van de ICT-omgeving van een entiteit van de Unie waarvan bekend is dat het verbonden is met de ICT-omgeving van een andere entiteit van de Unie, doet CERT-EU een cyberbeveiligingswaarschuwing daaromtrent uitgaan.

7. 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 nadere bijzonderheden verstrekken betreffende het soort informatie dat nodig is met het oog op situatiebewustzijn en respons op incidenten.

8. CERT-EU dient om de drie maanden bij de IICB, Enisa, het EU-Intcen en het CSIRT-netwerk een samenvattend verslag in met geanonimiseerde en geaggregeerde gegevens over significante incidenten, incidenten, cyberdreigingen, bijna-incidenten en kwetsbaarheden op grond van artikel 20 en significante incidenten die op grond van lid 2 van dit artikel ter kennis zijn gegeven. Het samenvattend verslag dient als input voor het tweejaarlijkse verslag over de stand van zaken op het gebied van de cyberbeveiliging in de Unie dat op grond van artikel 18 van Richtlijn (EU) 2022/2555 wordt opgesteld.

9. Uiterlijk op 8 juli 2024 brengt de IICB richtsnoeren of aanbevelingen uit waarin de regelingen voor, en de vorm en inhoud van de rapportage op grond van dit artikel nader worden beschreven. Bij het opstellen van dergelijke richtsnoeren of aanbevelingen houdt de IICB rekening met op grond van artikel 23, lid 11, van Richtlijn (EU) 2022/2555 vastgestelde uitvoeringshandelingen waarin het soort informatie, de vorm en de procedure van kennisgevingen nader worden gespecificeerd. CERT-EU verspreidt de passende technische details, zodat de entiteiten van de Unie proactief opsporings-, incidentrespons- of beperkende maatregelen kunnen nemen.

10. De in dit artikel vastgestelde rapportageverplichtingen gelden niet voor:

a) EUCI;

b) informatie waarvan de verdere verspreiding is uitgesloten door middel van een zichtbare markering, tenzij het delen daarvan met CERT-EU uitdrukkelijk is toegestaan.

Artikel 22

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 incidenten, cyberdreigingen, kwetsbaarheden en bijna-incidenten onder de volgende partijen:

a) entiteiten van de Unie;

b) de in de artikelen 17 en 18 bedoelde tegenhangers.

2. CERT-EU faciliteert, zo nodig in nauwe samenwerking met Enisa, de coördinatie tussen de entiteiten van de Unie inzake de respons bij incidenten, wat het volgende omvat:

a) bijdragen tot consequente externe communicatie;

b) wederzijdse ondersteuning, zoals het delen van informatie die relevant is voor entiteiten van de Unie, of het verlenen van bijstand, in voorkomend geval rechtstreeks ter plaatse;

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 incidenten, cyberdreigingen, kwetsbaarheden en bijna-incidenten, en het delen van relevante ontwikkelingen op het gebied van cyberbeveiliging.

4. Uiterlijk op 8 januari 2025 stelt de IICB, 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 onverwijld over de manier waarop het incident aan de rechtshandhavingsinstanties moet worden gemeld.

5. Op specifiek verzoek van een lidstaat en met de goedkeuring van de betrokken entiteiten van de Unie kan CERT-EU een beroep doen op deskundigen van de in artikel 23, lid 4, bedoelde lijst om bij te dragen aan de respons op een ernstig incident dat gevolgen heeft in die lidstaat, of op een grootschalig cyberbeveiligingsincident overeenkomstig artikel 15, lid 3, punt g), van Richtlijn (EU) 2022/2555. De specifieke regels met betrekking tot de toegang tot en de inzet van technische deskundigen van de entiteiten van de Unie worden door de IICB op basis van een voorstel van CERT-EU goedgekeurd.

Artikel 23

Beheer van ernstige incidenten

1. Om op operationeel niveau het gecoördineerde beheer van ernstige incidenten 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, stelt de IICB op grond van artikel 11, punt q), op basis van de in artikel 22, lid 2, bedoelde activiteiten een cybercrisisbeheersplan op, dit in nauwe samenwerking met CERT-EU en Enisa. Het cybercrisisbeheersplan bevat ten minste de volgende elementen:

a) regelingen betreffende de coördinatie en de informatiedoorstroming 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.

2. De vertegenwoordiger van de Commissie in de IICB is, onder voorbehoud van het op grond van lid 1 van dit artikel opgestelde cybercrisisbeheersplan en onverminderd artikel 16, lid 2, eerste alinea, van Richtlijn (EU) 2022/2555, het contactpunt voor het delen van relevante informatie over ernstige incidenten met EU-CyCLONe.

3. CERT-EU coördineert het beheer van ernstige incidenten tussen de entiteiten van de Unie. Het houdt een inventaris bij van de beschikbare technische deskundigheid die nodig is voor de respons op ernstige incidenten, en het ondersteunt de IICB bij de coördinatie van de cybercrisisbeheersplannen van de entiteiten van de Unie voor ernstige incidenten als bedoeld in artikel 9, lid 2.

4. De entiteiten van de Unie dragen bij tot de inventaris van technische deskundigheid door een jaarlijks bijgewerkte lijst te leveren van deskundigen die binnen hun respectieve organisaties beschikbaar zijn, inclusief nadere gegevens over hun specifieke technische vaardigheden.

HOOFDSTUK VI

SLOTBEPALINGEN

Artikel 24

Initiële heroriëntering van begrotingsmiddelen

Om de goede en stabiele werking van CERT-EU te waarborgen, kan de Commissie voorstellen om personele en financiële middelen over te hevelen naar de begroting van de Commissie ten behoeve van de activiteiten van CERT-EU. De heroriëntering valt samen met de eerste jaarlijkse begroting van de Unie die na de inwerkingtreding van deze verordening wordt vastgesteld.

Artikel 25

Evaluatie

1. Uiterlijk op 8 januari 2025 en daarna jaarlijks brengt de IICB, met de hulp van CERT-EU, verslag uit aan de Commissie over de uitvoering van deze verordening. De IICB kan aanbevelingen doen aan de Commissie om deze verordening te evalueren.

2. Uiterlijk op 8 januari 2027 en vervolgens om de twee jaar beoordeelt de Commissie de uitvoering van deze verordening en de ervaring die op strategisch en operationeel niveau is opgedaan en brengt zij hierover verslag uit aan het Europees Parlement en de Raad.

Het in de eerste alinea van dit lid bedoelde verslag bevat de in artikel 16, lid 1, bedoelde evaluatie van de mogelijkheid om CERT-EU als bureau van de Unie aan te duiden.

3. Uiterlijk op 8 januari 2029 evalueert de Commissie de werking van deze verordening en brengt zij daarover verslag uit aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's. De Commissie beoordeelt ook of het passend is netwerk- en informatiesystemen waarin EUCI wordt verwerkt, in het toepassingsgebied van deze verordening op te nemen, rekening houdend met andere wetgevingshandelingen van de Unie die op die systemen van toepassing zijn. Dat verslag gaat zo nodig vergezeld van een wetgevingsvoorstel.

Artikel 26

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 Straatsburg, 13 december 2023.

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*
R. METSOLA	P. NAVARRO RÍOS