EUROPESE
COMMISSIE

Brussel, 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Voorstel voor een

RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148

(Voor de EER relevante tekst)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

TOELICHTING

1. CONTEXT VAN HET VOORSTEL

• Redenen en doelstellingen van het voorstel

Dit voorstel maakt deel uit van een pakket maatregelen om de veerkracht en de responscapaciteit bij incidenten van openbare en particuliere entiteiten, de bevoegde autoriteiten en de Unie als geheel op het gebied van cyberbeveiliging en de bescherming van kritieke infrastructuur verder te verbeteren. Het is in overeenstemming met de prioriteiten van de Commissie om Europa klaar te maken voor het digitale tijdperk en een economie op te bouwen die klaar is voor de toekomst en die werkt voor de mensen. Cyberbeveiliging is een prioriteit in de respons van de Commissie op de COVID-19-crisis. Het pakket omvat een nieuwe strategie inzake cyberbeveiliging met als doel de strategische autonomie van de Unie te versterken om haar veerkracht en collectieve respons te verbeteren en een open en mondiaal internet op te bouwen. Tot slot bevat het pakket een voorstel voor een richtlijn betreffende de veerkracht van kritieke aanbieders van essentiële diensten, die tot doel heeft de fysieke bedreigingen tegen dergelijke aanbieders te beperken.

Dit voorstel bouwt voort op en strekt tot intrekking van Richtlijn (EU) 2016/1148 betreffende de beveiliging van netwerk- en informatiesystemen (NIS-richtlijn), die het eerste stuk EU-wetgeving over cyberbeveiliging is en voorziet in wettelijke maatregelen om het algemene niveau van cyberbeveiliging in de Unie te verhogen. De NIS-richtlijn heeft (1) bijgedragen aan de verbetering van de cyberbeveiligingscapaciteiten op nationaal niveau door de lidstaten te verplichten nationale cyberbeveiligingsstrategieën vast te stellen en cyberbeveiligingsautoriteiten aan te wijzen; (2) de samenwerking tussen de lidstaten op het niveau van de Unie versterkt door verschillende fora op te richten die de uitwisseling van strategische en operationele informatie vergemakkelijken; en (3) de cyberveerkracht van publieke en private entiteiten verbeterd in zeven specifieke sectoren (energie, vervoer, bankwezen, infrastructuur van de financiële markt, gezondheidszorg, drinkwatervoorziening en -distributie, en digitale infrastructuur) en bij drie digitale diensten (elektronische marktplaatsen, onlinezoekmachines en cloudcomputerdiensten) door van de lidstaten te eisen dat zij ervoor zorgen dat aanbieders van essentiële diensten en digitaledienstverleners cyberbeveiligingseisen stellen en incidenten melden.

Het voorstel moderniseert het bestaande rechtskader, rekening houdend met de toegenomen digitalisering van de interne markt in de afgelopen jaren en een zich ontwikkelend bedreigingslandschap voor cyberbeveiliging. Beide ontwikkelingen zijn sinds het begin van de COVID-19-crisis verder versterkt. Het voorstel pakt ook een aantal zwakke punten aan die de NIS-richtlijn hebben belet haar volledige potentieel te ontsluiten.

Niettegenstaande haar opmerkelijke verwezenlijkingen heeft de NIS-richtlijn, die de weg heeft vrijgemaakt voor een belangrijke verandering van de mentaliteit met betrekking tot de institutionele en regelgevende aanpak van cyberbeveiliging in veel lidstaten, ook haar beperkingen bewezen. De digitale transformatie van de maatschappij (nog versterkt door de COVID-19-crisis) heeft het bedreigingslandschap verruimd en leidt tot nieuwe uitdagingen, die een aangepaste, innovatieve reactie vereisen. Het aantal cyberaanvallen blijft toenemen, waarbij steeds geavanceerdere aanvallen uit een groot aantal bronnen binnen en buiten de EU komen.

Bij de evaluatie van de werking van de NIS-richtlijn, die ten behoeve van de effectbeoordeling is uitgevoerd, zijn de volgende punten aan het licht gekomen: 1) de geringe mate van cyberveerkracht van bedrijven die actief zijn in de EU; 2) de inconsistente veerkracht binnen de lidstaten en sectoren; en 3) het lage niveau van gezamenlijk situationeel

bewustzijn en het gebrek aan een gezamenlijke respons op een crisis. Zo vallen bepaalde grote ziekenhuizen in een lidstaat niet onder het toepassingsgebied van de NIS-richtlijn en zijn zij dus niet verplicht de daaruit voortvloeiende beveiligingsmaatregelen uit te voeren, terwijl in een andere lidstaat bijna elke zorgverlener in het land onder de beveiligingseisen voor netwerk- en informatiebeveiliging valt.

Het voorstel is een initiatief in het kader van het programma voor gezonde regelgeving (REFIT) en heeft tot doel de regelgevingslast voor de bevoegde autoriteiten en de nalevingskosten voor openbare en particuliere entiteiten te verminderen. Dit wordt met name bereikt door het afschaffen van de verplichting voor de bevoegde autoriteiten om de aanbieders van essentiële diensten te identificeren en door het verhogen van het niveau van de harmonisatie van de beveiligings- en rapportage-eisen om de naleving van de regelgeving voor entiteiten die grensoverschrijdende diensten verlenen, te vergemakkelijken. Tegelijkertijd zullen de bevoegde autoriteiten ook een aantal nieuwe taken krijgen, waaronder het toezicht op entiteiten in sectoren die tot nu toe niet onder de NIS-richtlijn vielen.

- **Samenhang met bestaande beleidsbepalingen op het beleidsterrein**

Dit voorstel maakt deel uit van een breder pakket van bestaande rechtsinstrumenten en ophanden zijnde initiatieven op het niveau van de Unie die erop gericht zijn de veerkracht van openbare en particuliere entiteiten tegen bedreigingen te vergroten.

Op het gebied van cyberbeveiliging gaat het met name om Richtlijn (EU) 2018/1972 tot vaststelling van het Europees wetboek voor elektronische communicatie (waarvan de bepalingen inzake cyberbeveiliging zullen worden vervangen door de bepalingen van het onderhavige voorstel) en om het voorstel voor een verordening betreffende digitale operationele veerkracht voor de financiële sector (COM(2020) 595 final), die als lex specialis van het onderhavige voorstel zal worden beschouwd zodra beide wetteksten in werking zijn getreden.

Op het gebied van de fysieke beveiliging vormt het voorstel een aanvulling op het voorstel voor een richtlijn inzake de veerkracht van kritieke entiteiten, waarin Richtlijn 2008/114/EG inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren (ECI-richtlijn) wordt herzien, waarin een EU-procedure voor de identificatie van Europese kritieke infrastructuren en de aanmerking van infrastructuren als Europese kritieke infrastructuren wordt vastgesteld en waarin een aanpak voor de verbetering van de bescherming van dergelijke infrastructuren wordt uiteengezet. In juli 2020 heeft de Commissie de EU-strategie voor de veiligheidsunie[1] goedgekeurd, waarin de toenemende interconnectie en onderlinge afhankelijkheid tussen fysieke en digitale infrastructuren wordt erkend. Zij benadrukte de noodzaak van een meer coherente en consistente aanpak tussen de ECI-richtlijn en Richtlijn (EU) 2016/1148 betreffende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de hele Unie.

Het voorstel sluit dan ook nauw aan bij het voorstel voor een richtlijn betreffende de veerkracht van kritieke entiteiten, dat tot doel heeft de veerkracht van kritieke entiteiten tegen fysieke bedreigingen in een groot aantal sectoren te vergroten. Het voorstel heeft tot doel ervoor te zorgen dat de bevoegde autoriteiten in het kader van beide rechtshandelingen

[1] COM(2020) 605 final.

aanvullende maatregelen nemen en indien nodig informatie uitwisselen met betrekking tot cyber- en niet-cyberveerkracht, en dat met name kritieke aanbieders in de sectoren die volgens het onderhavige voorstel als "essentieel" worden beschouwd, ook onderworpen zijn aan meer algemene veerkrachtverhogende verplichtingen, met de nadruk op niet-cyberrisico's.

- **Samenhang met ander beleid van de Unie**

Zoals uiteengezet in de mededeling "De digitale toekomst van Europa vormgeven"[2] is het voor Europa van cruciaal belang om alle voordelen van het digitale tijdperk te benutten en zijn industrie en innovatiecapaciteit te versterken, binnen veilige en ethische grenzen. De Europese strategie voor gegevens bevat vier pijlers — gegevensbescherming, grondrechten, veiligheid en cyberbeveiliging — als essentiële voorwaarden voor een samenleving die zich verder ontwikkelt door gegevens te gebruiken.

In een resolutie van 12 maart 2019 heeft het Europees Parlement de "*[...] de Commissie [verzocht] na te gaan of het nodig is het toepassingsgebied van de NIS-richtlijn verder uit te breiden naar andere kritieke sectoren en diensten die niet onder sectorspecifieke wetgeving vallen*".[3] In zijn conclusies van 9 juni 2020 was de Raad ingenomen *"[...] met de plannen van de Commissie om voor consistente regels voor marktdeelnemers te zorgen en beveiligde, robuuste en adequate informatie-uitwisseling over dreigingen en incidenten te faciliteren, onder meer door een evaluatie van de richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIS-richtlijn), zodat kan worden gezocht naar opties voor een betere cyberweerbaarheid en een effectievere respons op cyberaanvallen, met name voor essentiële economische en maatschappelijke activiteiten, met inachtneming van de bevoegdheden van de lidstaten, waaronder de verantwoordelijkheid voor hun nationale veiligheid"*.[4] Voorts laat de voorgestelde rechtshandeling de toepassing van de mededingingsregels van het Verdrag betreffende de werking van de Europese Unie (VWEU) onverlet.

Aangezien een significant deel van de cyberbeveiligingsbedreigingen hun oorsprong vinden buiten de EU, is een coherente aanpak van de internationale samenwerking nodig. Deze richtlijn vormt een referentiemodel dat moet worden bevorderd in het kader van de samenwerking van de EU met derde landen, met name bij het verlenen van externe technische bijstand.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

- **Rechtsgrondslag**

De rechtsgrondslag voor de NIS-richtlijn is artikel 114 van het Verdrag betreffende de werking van de Europese Unie, dat tot doel heeft de interne markt tot stand te brengen en te laten functioneren door de maatregelen voor de onderlinge aanpassing van de nationale regels te versterken. Zoals het Hof van Justitie van de EU in zijn arrest in zaak C-58/08 Vodafone e.a. heeft geoordeeld, is de toepassing van artikel 114 VWEU gerechtvaardigd wanneer er verschillen zijn tussen de nationale voorschriften die rechtstreeks van invloed zijn op de werking van de interne markt. Het Hof heeft ook geoordeeld dat wanneer een op artikel 114

[2] COM(2020) 67 final.
[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_NL.html
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/nl/pdf

VWEU gebaseerde handeling reeds elke handelsbelemmering op het door haar geharmoniseerde gebied heeft weggenomen, de Uniewetgever niet de mogelijkheid kan worden ontzegd om die handeling aan te passen aan elke wijziging van de omstandigheden of ontwikkeling van de kennis in het licht van zijn door het Verdrag erkende taak om de algemene belangen te vrijwaren. Ten slotte heeft het Hof geoordeeld dat de maatregelen voor de in artikel 114 VWEU bedoelde onderlinge aanpassing bedoeld zijn om, afhankelijk van de algemene context en de specifieke omstandigheden van de te harmoniseren materie, een beoordelingsmarge te laten ten aanzien van de methode van onderlinge aanpassing die het meest geschikt is om het gewenste resultaat te bereiken. De voorgestelde wetshandeling zou de belemmeringen voor de totstandbrenging en de werking van de interne markt voor essentiële en belangrijke entiteiten wegnemen en verbeteren door duidelijke, algemeen toepasselijke regels vast te stellen over het toepassingsgebied van de NIS-richtlijn en de regels die van toepassing zijn op het gebied van het beheer van risico's inzake cyberbeveiliging en de rapportage van incidenten te harmoniseren. De huidige verschillen op dit gebied, op zowel wetgevend en toezichthoudend niveau als op nationaal en EU-niveau, zijn belemmeringen voor de interne markt omdat entiteiten die grensoverschrijdende activiteiten ontplooien, te maken hebben met verschillende en mogelijk overlappende regelgevingsvereisten en/of de toepassing daarvan, hetgeen ten koste gaat van de uitoefening van hun vrijheid van vestiging en van dienstverlening. Verschillende regels hebben ook een negatief effect op de concurrentievoorwaarden in de interne markt wanneer het gaat om entiteiten van hetzelfde type in verschillende lidstaten.

- **Subsidiariteit (voor niet-exclusieve bevoegdheid)**

Cyberbeveiligingsveerkracht in de hele Unie kan niet effectief zijn als deze op een ongelijke manier wordt benaderd via nationale of regionale silo's. De NIS-richtlijn heeft deze tekortkoming gedeeltelijk verholpen door een kader voor de beveiliging van netwerk- en informatiesystemen op nationaal en Unieniveau vast te stellen. Bij de omzetting en uitvoering van de richtlijn zijn echter ook inherente tekortkomingen en beperkingen van bepaalde bepalingen of benaderingen aan het licht gekomen, zoals de onduidelijke afbakening van het toepassingsgebied van de richtlijn, wat leidt tot aanzienlijke verschillen in de omvang en diepgang van het feitelijke EU-optreden op het niveau van de lidstaten. Bovendien is de Europese economie sinds de COVID-19-crisis nog afhankelijker geworden van netwerk- en informatiesystemen dan ooit tevoren en zijn sectoren en diensten steeds meer met elkaar verbonden. Het optreden van de EU dat verder gaat dan de huidige maatregelen van de NIS-richtlijn is vooral gerechtvaardigd door: (i) het in toenemende mate grensoverschrijdende karakter van de bedreigingen en uitdagingen op het gebied van netwerk- en informatiebeveiliging; (ii) het potentieel van het optreden van de Unie om doeltreffend en gecoördineerd nationaal beleid te verbeteren en te vergemakkelijken; en (iii) de bijdrage van gecoördineerde en gezamenlijke beleidsacties aan een doeltreffende bescherming van de gegevensbescherming en de persoonlijke levenssfeer.

- **Evenredigheid**

De in deze richtlijn voorgestelde regels gaan niet verder dan wat nodig is om de specifieke doelstellingen op bevredigende wijze te verwezenlijken. De beoogde afstemming en stroomlijning van de beveiligingsmaatregelen en de rapportageverplichtingen hebben betrekking op de verzoeken van de lidstaten en het bedrijfsleven om het huidige kader te verbeteren.

Het voorstel houdt rekening met de reeds bestaande praktijken in de lidstaten. Een hoger beschermingsniveau dat door dergelijke gestroomlijnde en gecoördineerde eisen wordt bereikt, staat in verhouding tot de steeds grotere risico's die worden gelopen, met inbegrip van de risico's met een grensoverschrijdend element; zij zijn redelijk en komen over het algemeen overeen met het belang dat de betrokken entiteiten hebben bij het waarborgen van de continuïteit en de kwaliteit van hun diensten. De kosten voor het waarborgen van systematische samenwerking tussen de lidstaten zouden niet opwegen tegen de economische en maatschappelijke verliezen en schade die door cyberbeveiligingsincidenten worden veroorzaakt. Bovendien blijkt uit de raadplegingen van belanghebbenden in het kader van de herziening van de NIS-richtlijn, met inbegrip van de resultaten van de openbare raadpleging en de gerichte enquêtes, dat de herziening van de NIS-richtlijn in de bovengenoemde zin wordt gesteund.

- **Keuze van het instrument**

Het voorstel zal de verplichtingen voor het bedrijfsleven verder stroomlijnen en zorgen voor een hoger niveau van harmonisatie. Tegelijkertijd beoogt het voorstel de lidstaten de nodige flexibiliteit te bieden om rekening te houden met specifieke nationale kenmerken (zoals de mogelijkheid om aanvullende essentiële of belangrijke entiteiten te identificeren die verder gaan dan het in de rechtshandeling vastgestelde basisniveau). Het toekomstige rechtsinstrument moet daarom een richtlijn zijn, aangezien dit rechtsinstrument een gerichte verbeterde harmonisatie en een zekere mate van flexibiliteit voor de bevoegde autoriteiten mogelijk maakt.

3. RESULTATEN VAN EVALUATIES ACHTERAF, RAADPLEGINGEN VAN BELANGHEBBENDEN EN EFFECTBEOORDELINGEN

- **Evaluaties/geschiktheidscontroles achteraf van bestaande wetgeving**

De Commissie heeft de werking van de NIS-richtlijn geëvalueerd.[5] Zij heeft de relevantie, de toegevoegde waarde voor de EU, de samenhang, de doeltreffendheid en de efficiëntie ervan geanalyseerd. De belangrijkste bevindingen van deze analyse zijn:

- Het toepassingsgebied van de NIS-richtlijn is te beperkt wat betreft de sectoren die onder de richtlijn vallen, voornamelijk als gevolg daarvan: (i) de toegenomen digitalisering in de afgelopen jaren en een hogere mate van onderlinge verbondenheid, (ii) het toepassingsgebied van de NIS-richtlijn dat niet langer alle gedigitaliseerde sectoren die essentiële diensten aan de economie en de samenleving als geheel leveren, weerspiegelt.
- De NIS-richtlijn is niet duidelijk genoeg als het gaat om het toepassingsgebied voor aanbieders van essentiële diensten en de bepalingen ervan bieden onvoldoende duidelijkheid over de nationale bevoegdheid voor digitaledienstverleners. Dit heeft geleid tot een situatie waarin bepaalde soorten entiteiten niet in alle lidstaten zijn geïdentificeerd en dus niet verplicht zijn om beveiligingsmaatregelen te treffen en incidenten te melden.
- De NIS-richtlijn liet de lidstaten een ruime beoordelingsmarge bij het vaststellen van de eisen inzake beveiliging en het melden van incidenten voor aanbieders van essentiële diensten. Uit de evaluatie blijkt dat de lidstaten deze eisen in sommige

[5] [Bijlage 5 van de effectbeoordeling]

gevallen op sterk uiteenlopende wijze hebben uitgevoerd, wat een extra belasting vormt voor bedrijven die in meer dan één lidstaat actief zijn.

- Het toezichts- en handhavingsregime van de NIS-richtlijn is ondoeltreffend. De lidstaten zijn bijvoorbeeld zeer terughoudend geweest in het opleggen van sancties aan entiteiten die geen beveiligingseisen stellen of incidenten melden. Dit kan negatieve gevolgen hebben voor de cyberveerkracht van individuele entiteiten.
- De financiële en personele middelen die de lidstaten opzijzetten voor het vervullen van hun taken (zoals de identificatie van of het toezicht op de aanbieders van essentiële diensten), en bijgevolg de verschillende niveaus van rijpheid bij het omgaan met cyberbeveiligingsrisico's, lopen sterk uiteen. Dit vergroot de verschillen in cyberveerkracht tussen de lidstaten nog meer.
- De lidstaten delen niet systematisch informatie met elkaar, wat met name negatieve gevolgen heeft voor de effectiviteit van de cyberbeveiligingsmaatregelen en voor het niveau van gezamenlijk situationeel bewustzijn op EU-niveau. Dit is ook het geval voor de uitwisseling van informatie tussen particuliere entiteiten en voor de betrokkenheid van de samenwerkingsstructuren op EU-niveau en particuliere entiteiten.

- **Raadpleging van belanghebbenden**

De Commissie heeft een breed scala aan belanghebbenden geraadpleegd. De lidstaten en belanghebbenden zijn uitgenodigd om deel te nemen aan de openbare raadpleging en aan de door Wavestone, CEPS en ICF georganiseerde enquêtes en workshops, die door de Commissie zijn gecontracteerd om een studie uit te voeren ter ondersteuning van de herziening van de NIS-richtlijn. De geraadpleegde belanghebbenden waren onder meer bevoegde autoriteiten, organen van de Unie die zich bezighouden met cyberbeveiliging, aanbieders van essentiële diensten, digitaledienstverleners, entiteiten die diensten verlenen die buiten het toepassingsgebied van de huidige NIS-richtlijn vallen, beroepsverenigingen en consumentenorganisaties en burgers.

Bovendien heeft de Commissie voortdurend contact gehad met de bevoegde instanties die belast zijn met de uitvoering van de NIS-richtlijn. De samenwerkingsgroep heeft zich uitgebreid beziggehouden met diverse transversale en sectorale uitvoeringsaspecten. Ten slotte heeft de Commissie tijdens haar NIS-landenbezoeken in 2019 en 2020 154 openbare en particuliere entiteiten en 117 bevoegde autoriteiten geïnterviewd.

- **Bijeenbrengen en benutten van expertise**

De Commissie heeft een consortium van Wavestone, CEPS en ICF gecontracteerd om de Commissie te ondersteunen bij de herziening van de NIS-richtlijn.[6] De contractant heeft niet alleen de belanghebbenden die rechtstreeks te maken hebben met de NIS-richtlijn bereikt door middel van doelgerichte enquêtes en workshops, maar heeft ook overleg gepleegd met een breed scala aan deskundigen op het gebied van cyberbeveiliging, zoals onderzoekers op het gebied van cyberbeveiliging en professionals uit de cyberbeveiligingsindustrie.

[6] Studie ter ondersteuning van de herziening van Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (NIS-richtlijn) - nr. 2020-665. Wavestone, CEPS en ICF.

- **Effectbeoordeling**

Dit voorstel gaat vergezeld van een effectbeoordeling[7], die op 23 oktober 2020 is voorgelegd aan de Raad voor regelgevingstoetsing ("Regulatory Scrutiny Board" — RSB) en op 20 november 2020 een positief advies met opmerkingen van de RSB heeft ontvangen. De RSB heeft met het oog hierop op sommige punten verbeteringen aanbevolen: (1) de rol van grensoverschrijdende overloopeffecten in de probleemanalyse beter weergeven; (2) beter uitleggen hoe het succes van het initiatief eruit zou zien; (3) de lijst van beleidsopties verder motiveren; (4) de kosten van de voorgestelde maatregelen verder uitwerken. De effectbeoordeling werd aangepast om rekening te houden met deze punten en met meer gedetailleerde opmerkingen van de RSB. Zij bevat nu meer gedetailleerde uitleg over de rol van grensoverschrijdende overloopeffecten op het gebied van cyberbeveiliging, een duidelijker overzicht van hoe succes kan worden gemeten, een meer gedetailleerde uitleg over het opzet en de logica van de verschillende beleidsopties en acties die binnen deze opties worden overwogen, een meer gedetailleerde uitleg over de aspecten die zijn geanalyseerd in verband met het sectorale toepassingsgebied van de NIS-richtlijn en verdere verduidelijkingen met betrekking tot de kosten.

De Commissie heeft een aantal beleidsopties overwogen om het rechtskader op het gebied van cyberveerkracht en incidentrespons te verbeteren:

- "Niets doen": De NIS-richtlijn blijft ongewijzigd en er worden geen andere maatregelen van niet-wetgevende aard genomen om de bij de evaluatie van de NIS-richtlijn vastgestelde problemen aan te pakken.
- Optie 1: er zouden geen veranderingen zijn op het niveau van de wetgeving. In plaats daarvan zou de Commissie, na raadpleging van de samenwerkingsgroep, het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) en, indien van toepassing, het netwerk van computer security incident response teams (CSIRT's), aanbevelingen en richtsnoeren uitvaardigen (zoals over de identificatie van aanbieders van essentiële diensten, beveiligingseisen, procedures voor het melden van incidenten en toezicht).
- Optie 2: deze optie houdt gerichte wijzigingen van de NIS-richtlijn in, waaronder een uitbreiding van het toepassingsgebied en diverse andere wijzigingen die erop gericht zijn bepaalde onmiddellijke oplossingen voor de geconstateerde problemen te garanderen en meer duidelijkheid en verdere harmonisatie te bieden (zoals bepalingen om de identificatiedrempels te harmoniseren). In de gewijzigde NIS-richtlijn worden echter de belangrijkste bouwstenen, de aanpak en de motivering gehandhaafd.
- Optie 3: dit scenario houdt systematische en structurele wijzigingen van de NIS-richtlijn in (door middel van een nieuwe richtlijn) die een meer fundamentele verschuiving in de aanpak inhouden naar een breder segment van de economieën in de hele Unie, maar met een meer gericht toezicht op grote en belangrijke spelers. Het zou ook de verplichtingen voor bedrijven stroomlijnen en zorgen voor een hoger niveau van harmonisatie, een effectiever kader voor operationele aspecten creëren en een duidelijke grondslag leggen voor meer gedeelde verantwoordelijkheden en verantwoordingsplicht van verschillende belanghebbenden met betrekking tot cyberbeveiligingsmaatregelen.

[7] **[Links naar het definitieve document en naar het samenvattingsblad toe te voegen]**

De conclusie van de effectbeoordeling is dat de voorkeur uitgaat naar de derde optie (d.w.z. systemische en structurele wijzigingen van het kader voor netwerk- en informatiebeveiliging). Wat de doeltreffendheid betreft, zou de voorkeursoptie duidelijk het toepassingsgebied van de NIS-richtlijn bepalen, dat wordt uitgebreid tot een meer representatief deel van de economieën en samenlevingen in de EU, en de eisen stroomlijnen, samen met een meer gedefinieerd kader voor toezicht en handhaving dat gericht is op het verhogen van het nalevingsniveau. Dit houdt ook maatregelen in die gericht zijn op het verbeteren van de beleidsvorming op het niveau van de lidstaten en het veranderen van het paradigma daarvan, het bevorderen van nieuwe kaders voor risicobeheer van leveranciersrelaties en het coördineren van de bekendmaking van de kwetsbaarheid. Tegelijkertijd legt de voorkeursoptie een duidelijke grondslag voor gedeelde verantwoordelijkheden en verantwoordingsplicht en voorziet zij in mechanismen om meer vertrouwen tussen de lidstaten, zowel de autoriteiten als het bedrijfsleven, te bevorderen, het delen van informatie te stimuleren en te zorgen voor een meer operationele aanpak, zoals de mechanismen voor wederzijdse bijstand en intercollegiale toetsing. Deze optie zou ook voorzien in een EU-kader voor crisisbeheer, voortbouwend op het onlangs gelanceerde operationele netwerk van de EU, en zou ervoor zorgen dat het Enisa, binnen zijn huidige mandaat, meer betrokken is bij het houden van een accuraat overzicht van de cyberbeveiligingstoestand van de Unie.

Wat de efficiëntie betreft, zou de voorkeursoptie weliswaar extra nalevings- en handhavingskosten voor het bedrijfsleven en de lidstaten met zich meebrengen, maar zij zou ook leiden tot efficiënte trade-offs en synergieën, waarbij het beste potentieel van alle geanalyseerde beleidsopties wordt benut om te zorgen voor een groter en consistent niveau van cyberveerkracht van de belangrijkste entiteiten in de hele Unie, wat uiteindelijk zou leiden tot kostenbesparingen voor zowel het bedrijfsleven als de samenleving. Deze beleidsoptie zou bepaalde extra administratieve lasten en nalevingskosten voor de autoriteiten van de lidstaten met zich meebrengen. Per saldo zou het echter op middellange en lange termijn ook aanzienlijke voordelen opleveren door meer samenwerking tussen de lidstaten, ook op operationeel niveau, en door het stimuleren van een algemene toename van de cyberbeveiligingscapaciteiten op nationaal en regionaal niveau via wederzijdse bijstand, mechanismen voor collegiale toetsing en een beter overzicht van en interactie met belangrijke bedrijven. De voorkeursbeleidsoptie zou ook in hoge mate zorgen voor samenhang met andere wetgeving, initiatieven of beleidsmaatregelen, met inbegrip van sectorspecifieke lex specialis.

Het aanpakken van de huidige ontoereikendheid van de paraatheid op het gebied van cyberbeveiliging op het niveau van de lidstaten en op het niveau van de bedrijven en andere organisaties zou kunnen leiden tot efficiëntiewinst en tot vermindering van de extra kosten die voortvloeien uit cyberbeveiligingsincidenten.

- Voor essentiële en belangrijke entiteiten zou het verhogen van de paraatheid op het gebied van cyberbeveiliging kunnen leiden tot een beperking van het potentiële verlies aan inkomsten als gevolg van verstoringen — onder meer door industriële spionage — en zou het de grote uitgaven voor een ad-hocbedreiging kunnen verminderen. Dergelijke winsten zullen waarschijnlijk opwegen tegen de noodzakelijke investeringskosten. De versnippering van de interne markt verminderen zou ook het gelijke speelveld tussen de aanbieders verbeteren.
- Voor de lidstaten zou dit het risico van toenemende begrotingsuitgaven voor het verminderen van ad-hocbedreigingen en extra kosten in geval van noodsituaties in verband met cyberbeveiligingsincidenten verder kunnen verminderen.

- Voor burgers zal het aanpakken van cyberbeveiligingsincidenten naar verwachting leiden tot minder inkomensverlies als gevolg van economische ontwrichting.

De toegenomen cyberbeveiliging in de lidstaten en het vermogen van bedrijven en autoriteiten om snel te reageren op een incident en de gevolgen ervan te beperken, zullen hoogstwaarschijnlijk leiden tot een toename van het algemene vertrouwen van de burgers in de digitale economie, wat een positief effect zou kunnen hebben op de groei en de investeringen.

Het verhogen van het algemene niveau van cyberbeveiliging zal waarschijnlijk leiden tot een verhoogde algemene beveiliging en tot een soepele en ononderbroken werking van essentiële diensten, die kritiek zijn voor de samenleving. Het initiatief kan ook bijdragen tot andere sociale gevolgen, zoals minder cybercriminaliteit en terrorisme en meer civiele bescherming. Het verhogen van het niveau van cyberparaatheid voor bedrijven en andere organisaties kan potentiële financiële verliezen als gevolg van cyberaanvallen voorkomen, waardoor de noodzaak om werknemers te ontslaan, wordt voorkomen.

Een verhoging van het algemene cyberbeveiligingsniveau zou ook kunnen leiden tot het voorkomen van omgevingsrisico's/schade in geval van een aanval op een essentiële dienst. Dit kan met name gelden voor de sectoren energie, watervoorziening en distributie of vervoer. Door de cyberbeveiligingscapaciteiten te versterken, zou het initiatief ertoe kunnen leiden dat er meer gebruik wordt gemaakt van ICT-infrastructuren en -diensten van de nieuwste generatie die ook uit milieu-oogpunt duurzamer zijn, en dat inefficiënte en minder veilige legacy-infrastructuren worden vervangen. Dit zal naar verwachting ook bijdragen aan het verminderen van het aantal dure cyberincidenten, waardoor er middelen vrijkomen voor duurzame investeringen.

- **Regelgevende geschiktheid en vereenvoudiging**

Het voorstel voorziet in een algemene uitsluiting van micro- en kleine entiteiten van het NIB-toepassingsgebied en in een lichtere regeling voor toezicht achteraf, die van toepassing is op een groot aantal van de nieuwe entiteiten die onder het herziene toepassingsgebied vallen (de zogenaamde belangrijke entiteiten). Deze maatregelen hebben tot doel de lasten voor ondernemingen en overheidsdiensten tot een minimum te beperken en in evenwicht te brengen. Bovendien vervangt het voorstel het complexe identificatiesysteem voor aanbieders van essentiële diensten door een algemeen geldende verplichting en voert het een hoger niveau van harmonisatie van de beveiligings- en rapportageverplichtingen in, waardoor de nalevingslast zou afnemen, met name voor entiteiten die grensoverschrijdende diensten verlenen.

Het voorstel beperkt de nalevingskosten voor kleine en middelgrote ondernemingen (kmo's) tot een minimum, aangezien de entiteiten alleen die maatregelen hoeven te nemen die nodig zijn om een niveau van beveiliging van de netwerk- en informatiesystemen te waarborgen dat is afgestemd op het aanwezige risico.

- **Grondrechten**

De EU heeft zich ertoe verbonden hoge normen voor de bescherming van de grondrechten te waarborgen. Alle vrijwillige regelingen voor de uitwisseling van informatie tussen entiteiten die deze richtlijn bevordert, zouden worden uitgevoerd in een betrouwbare omgeving met

volledige inachtneming van de gegevensbeschermingsregels van de Unie, met name Verordening (EU) 2016/679 van het Europees Parlement en de Raad[8].

4. GEVOLGEN VOOR DE BEGROTING

Zie financiële fiche

5. ANDERE ELEMENTEN

- **Uitvoeringsplannen en regelingen voor toezicht, evaluatie en rapportage**

Het voorstel bevat een algemeen plan voor het toezicht op en de evaluatie van de gevolgen op de specifieke doelstellingen, waarbij de Commissie ten minste [54 maanden] na de datum van inwerkingtreding een evaluatie moet uitvoeren en aan het Europees Parlement en de Raad verslag moet uitbrengen over haar belangrijkste bevindingen.

De herziening moet worden uitgevoerd overeenkomstig de richtsnoeren voor betere regelgeving van de Commissie.

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

Het voorstel is opgebouwd rond verschillende belangrijke beleidsgebieden, die onderling verband houden en tot doel hebben het niveau van de cyberbeveiliging in de Unie te verhogen.

Onderwerp en toepassingsgebied (artikel 1 en artikel 2)

De richtlijn bepaalt in het bijzonder: a) dat de lidstaten een nationale strategie voor cyberbeveiliging moeten vaststellen en bevoegde nationale autoriteiten, centrale contactpunten en CSIRT's moeten aanwijzen; b) dat de lidstaten verplichtingen inzake risicobeheer en rapportage op het gebied van cyberbeveiliging moeten vaststellen voor entiteiten die in bijlage I essentiële entiteiten worden genoemd en in bijlage II belangrijke entiteiten; c) dat de lidstaten verplichtingen moeten vaststellen inzake het delen van informatie op het gebied van cyberbeveiliging.

Zij is van toepassing op bepaalde openbare of particuliere essentiële entiteiten die actief zijn in de in bijlage I genoemde sectoren (energie; vervoer; bankwezen; financiëlemarktinfrastructuren; gezondheidszorg, drinkwater; afvalwater; digitale infrastructuur; openbaar bestuur en ruimtevaart) en bepaalde belangrijke entiteiten die actief zijn in de in bijlage II genoemde sectoren (post- en koeriersdiensten; afvalbeheer; vervaardiging, productie en distributie van chemische stoffen; voedingsproductie, -verwerking en -distributie; verwerkende industrie en digitale aanbieders). Micro- en kleine entiteiten in de zin van Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 zijn uitgesloten van het toepassingsgebied van de richtlijn, met uitzondering van aanbieders van elektronische-communicatienetwerken of van openbare elektronische-communicatiediensten, aanbieders van vertrouwensdiensten, registers voor topleveldomeinnamen en overheidsdiensten, en bepaalde andere entiteiten, zoals de enige aanbieder van een dienst in een lidstaat.

[8] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

Nationale kaders voor cyberbeveiliging (artikelen 5 tot en met 11)

De lidstaten moeten een nationale strategie voor cyberbeveiliging vaststellen waarin de strategische doelstellingen en passende beleids- en regelgevingsmaatregelen worden gedefinieerd om een hoog niveau van cyberbeveiliging te bereiken en te handhaven.

De richtlijn stelt ook een kader vast voor de gecoördineerde bekendmaking van de kwetsbaarheid en verplicht de lidstaten de CSIRT's aan te wijzen als betrouwbare tussenpersonen en de interactie tussen de rapporterende entiteiten en de fabrikanten of aanbieders van ICT-producten en ICT-diensten te vergemakkelijken. Het Enisa is verplicht een Europees kwetsbaarheidsregister te ontwikkelen en bij te houden voor de ontdekte kwetsbaarheden.

De lidstaten moeten nationale kaders voor crisisbeheersing op het gebied van cyberbeveiliging opzetten, onder meer door nationale bevoegde autoriteiten aan te wijzen die verantwoordelijk zijn voor het beheer van grootschalige cyberbeveiligingsincidenten en -crises.

De lidstaten moeten ook een of meer nationale bevoegde autoriteiten op het gebied van cyberbeveiliging aanwijzen voor de toezichthoudende taken in het kader van deze richtlijn en een nationaal centraal contactpunt voor cyberbeveiliging (SPOC) aanwijzen dat een verbindingsfunctie heeft om de grensoverschrijdende samenwerking van de autoriteiten van de lidstaten te waarborgen. De lidstaten moeten ook CSIRT's aanwijzen.

Samenwerking (artikelen 12 tot en met 16)

Bij de richtlijn wordt een samenwerkingsgroep opgericht om de strategische samenwerking en de uitwisseling van informatie tussen de lidstaten te ondersteunen en te vergemakkelijken en om vertrouwen te ontwikkelen. Ook wordt er een CSIRT-netwerk opgericht om bij te dragen aan de ontwikkeling van het vertrouwen tussen de lidstaten en om een snelle en doeltreffende operationele samenwerking te bevorderen.

Er wordt een Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe) opgericht om het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en -crises te ondersteunen en om de regelmatige uitwisseling van informatie tussen de lidstaten en de EU-instellingen te garanderen.

Het Enisa moet in samenwerking met de Commissie een tweejaarlijks verslag over de stand van zaken op het gebied van cyberbeveiliging in de Unie opstellen.

De Commissie moet een systeem van collegiale toetsing opzetten dat het mogelijk maakt regelmatig de doeltreffendheid van het cyberbeveiligingsbeleid van de lidstaten te beoordelen.

Verplichtingen inzake risicobeheer en rapportage op het gebied van cyberbeveiliging (artikelen 17 tot en met 23)

De richtlijn vereist dat de lidstaten bepalen dat de beheersorganen van alle entiteiten die onder het toepassingsgebied vallen, de door de respectieve entiteiten genomen maatregelen voor het beheer van cyberbeveiligingsrisico's moeten goedkeuren en een specifieke opleiding op het gebied van cyberbeveiliging moeten volgen.

De lidstaten moeten ervoor zorgen dat de entiteiten die onder het toepassingsgebied vallen, passende en evenredige technische en organisatorische maatregelen nemen om de cyberbeveiligingsrisico's voor de beveiliging van netwerk- en informatiesystemen te beheren. Zij moeten er ook voor zorgen dat de entiteiten de nationale bevoegde autoriteiten of de CSIRT's in kennis stellen van elk cyberbeveiligingsincident dat een significant effect heeft op de verlening van de door hen verleende dienst.

De registers voor topleveldomeinnamen en de entiteiten die registratiediensten voor topleveldomeinnamen verlenen, verzamelen en bewaren nauwkeurige en volledige gegevens over de registratie van domeinnamen. Bovendien zijn dergelijke entiteiten verplicht om legitieme toegangvragende partijen efficiënte toegang te verlenen tot de gegevens van de domeinregistratie.

Jurisdictie en registratie (artikelen 24 en 25)

In de regel worden essentiële en belangrijke entiteiten geacht onder de jurisdictie te vallen van de lidstaat waar zij hun diensten verlenen. Bepaalde soorten entiteiten (DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputerdiensten, aanbieders van datacentra en van netwerken voor de levering van inhoud, alsmede bepaalde digitale aanbieders) worden echter geacht onder de jurisdictie te vallen van de lidstaat waar zij hun hoofdvestiging in de Unie hebben. Dit om ervoor te zorgen dat dergelijke entiteiten niet worden geconfronteerd met een veelheid aan verschillende wettelijke vereisten, aangezien zij in hoge mate grensoverschrijdende diensten verlenen. Het Enisa is verplicht een register van dit laatste type entiteiten aan te maken en bij te houden.

Uitwisseling van informatie (artikelen 26 en 27)

De lidstaten stellen regels vast die entiteiten in staat stellen om informatie over cyberbeveiliging uit te wisselen in het kader van specifieke regelingen voor informatie-uitwisseling op het gebied van cyberbeveiliging, met inachtneming van artikel 101 VWEU. Bovendien staan de lidstaten toe dat entiteiten die buiten het toepassingsgebied van deze richtlijn vallen, op vrijwillige basis melding maken van significante incidenten, cyberbedreigingen of bijna-ongelukken.

Toezicht en handhaving (artikelen 28 tot en met 34)

De bevoegde autoriteiten moeten toezicht houden op de entiteiten die onder het toepassingsgebied van de richtlijn vallen en er met name voor zorgen dat zij voldoen aan de eisen inzake beveiliging en het melden van incidenten. Er wordt een onderscheid gemaakt tussen een regeling voor toezicht vooraf op essentiële entiteiten en een regeling voor toezicht achteraf op belangrijke entiteiten, waarbij de bevoegde autoriteiten later worden verplicht actie te ondernemen wanneer zij bewijzen of aanwijzingen krijgen dat een belangrijke entiteit niet voldoet aan de vereisten inzake beveiliging en het melden van incidenten.

De richtlijn verplicht de lidstaten ook om administratieve boeten op te leggen aan essentiële en belangrijke entiteiten en stelt bepaalde maximumboeten vast.

De lidstaten zijn verplicht samen te werken en elkaar waar nodig bij te staan wanneer entiteiten diensten verlenen in meer dan één lidstaat of wanneer de hoofdvestiging van een entiteit of haar vertegenwoordiger zich in een bepaalde lidstaat bevindt, maar haar netwerk- en informatiesystemen zich in een of meer andere lidstaten bevinden.

2020/0359 (COD)

Voorstel voor een

RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

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

Gezien het advies van het Europees Economisch en Sociaal Comité[9],

Gezien het advies van het Comité van de Regio's[10],

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad[11] heeft tot doel capaciteiten op het gebied van cyberbeveiliging in de hele Unie op te bouwen, de bedreigingen voor netwerk- en informatiesystemen die worden gebruikt om essentiële diensten in belangrijke sectoren aan te bieden, te beperken en de continuïteit van dergelijke diensten te waarborgen wanneer zij worden geconfronteerd met cyberbeveiligingsincidenten, en aldus bij te dragen tot een doeltreffende werking van de economie en de samenleving van de Unie.

(2) Sinds de inwerkingtreding van Richtlijn (EU) 2016/1148 is er aanzienlijke vooruitgang geboekt bij het vergroten van de veerkracht van de Unie op het gebied van cyberbeveiliging. Uit de evaluatie van die richtlijn is gebleken dat zij heeft gediend als katalysator voor de institutionele en regelgevende aanpak van cyberbeveiliging in de Unie, waardoor de weg is vrijgemaakt voor een significante verandering in de manier waarop deze wordt benaderd. Die richtlijn heeft gezorgd voor de voltooiing van nationale kaders door nationale strategieën voor cyberbeveiliging te definiëren, nationale capaciteiten vast te stellen en regelgevende maatregelen uit te voeren die betrekking hebben op essentiële infrastructuren en actoren die door elke lidstaat zijn geïdentificeerd. Zij heeft ook bijgedragen aan de samenwerking op het niveau van de Unie door de oprichting van de

[9] PB C , , blz. .

[10] PB C , , blz. .

[11] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194/1 van 19.7.2016, blz. 1).

samenwerkingsgroep[12] en een netwerk van nationale computer security incident response teams ("netwerk van CSIRT's")[13]. Ondanks deze resultaten heeft de herziening van Richtlijn (EU) 2016/1148 inherente tekortkomingen aan het licht gebracht die verhinderen dat deze richtlijn de hedendaagse en opkomende uitdagingen op het gebied van cyberbeveiliging effectief aanpakt.

(3) Netwerk- en informatiesystemen hebben zich ontwikkeld tot een centraal kenmerk van het dagelijks leven door de snelle digitale transformatie en de onderlinge verbondenheid van de samenleving, ook bij grensoverschrijdende uitwisselingen. Die ontwikkeling heeft geleid tot een uitbreiding van het bedreigingslandschap voor de cyberbeveiliging, wat nieuwe uitdagingen met zich meebrengt, die in alle lidstaten een aangepaste, gecoördineerde en innovatieve respons vereist. Het aantal, de omvang, de complexiteit, de frequentie en de impact van cyberbeveiligingsincidenten nemen toe en vormen een grote bedreiging voor het functioneren van netwerk- en informatiesystemen. Daardoor kunnen cyberincidenten de uitoefening van economische activiteiten in de interne markt belemmeren, financiële verliezen veroorzaken, het vertrouwen van de gebruikers ondermijnen en grote schade toebrengen aan de economie en de samenleving van de Unie. Voor de goede werking van de interne markt zijn paraatheid en doeltreffendheid op het gebied van cyberbeveiliging daarom nu meer dan ooit van essentieel belang.

(4) De rechtsgrondslag voor Richtlijn (EU) 1148/2016 was artikel 114 van het Verdrag betreffende de werking van de Europese Unie, dat tot doel heeft de interne markt tot stand te brengen en te laten functioneren door de maatregelen voor de onderlinge aanpassing van de nationale regels te versterken. De cyberbeveiligingseisen die worden gesteld aan entiteiten die diensten of economisch relevante activiteiten verrichten, verschillen aanzienlijk van lidstaat tot lidstaat wat betreft het soort eis, de mate van gedetailleerdheid en de wijze van toezicht. Deze verschillen brengen extra kosten met zich mee en leveren problemen op voor ondernemingen die goederen of diensten grensoverschrijdend aanbieden. De eisen die door de ene lidstaat worden gesteld en die verschillen van of zelfs in strijd zijn met de eisen die door een andere lidstaat worden gesteld, kunnen een aanzienlijke invloed hebben op deze grensoverschrijdende activiteiten. Bovendien zal de mogelijkheid van een suboptimaal ontwerp of een suboptimale uitvoering van cyberbeveiligingsnormen in een lidstaat waarschijnlijk gevolgen hebben voor het niveau van de cyberbeveiliging in andere lidstaten, met name gezien de intensieve grensoverschrijdende uitwisselingen. Bij de herziening van Richtlijn (EU) 2016/1148 is gebleken dat de lidstaten de richtlijn op zeer uiteenlopende wijze uitvoeren, ook wat het toepassingsgebied betreft, waarvan de afbakening grotendeels aan het oordeel van de lidstaten is overgelaten. Richtlijn (EU) 2016/1148 bood de lidstaten ook een zeer ruime discretionaire bevoegdheid bij de uitvoering van de daarin opgenomen verplichtingen inzake beveiliging en incidentenmelding. Deze verplichtingen zijn daarom op nationaal niveau op aanzienlijk verschillende wijze uitgevoerd. Soortgelijke verschillen in de uitvoering hebben zich voorgedaan met betrekking tot de bepalingen van die richtlijn inzake toezicht en handhaving.

(5) Al deze verschillen leiden tot een versnippering van de interne markt en kunnen een nadelig effect hebben op de werking ervan, wat met name gevolgen heeft voor de grensoverschrijdende dienstverlening, en op de veerkracht van cyberbeveiliging als

[12] Artikel 11 van Richtlijn (EU) 2016/1148.
[13] Artikel 12 van Richtlijn (EU) 2016/1148.

gevolg van de toepassing van verschillende normen. Deze richtlijn heeft tot doel dergelijke grote verschillen tussen de lidstaten weg te werken, met name door minimumvoorschriften vast te stellen voor de werking van een gecoördineerd regelgevingskader, door mechanismen vast te stellen voor een doeltreffende samenwerking tussen de verantwoordelijke autoriteiten in elke lidstaat, door de lijst van sectoren en activiteiten waarvoor cyberbeveiligingverplichtingen gelden bij te werken en door te voorzien in doeltreffende rechtsmiddelen en sancties die bijdragen tot een doeltreffende handhaving van deze verplichtingen. Daarom moet Richtlijn (EU) 2016/1148 worden ingetrokken en door deze richtlijn worden vervangen.

(6) Deze richtlijn laat het vermogen van de lidstaten onverlet om de nodige maatregelen te nemen ter bescherming van de wezenlijke belangen van hun beveiliging, ter vrijwaring van de openbare orde en de openbare veiligheid en om het onderzoek, de opsporing en de vervolging van strafbare feiten mogelijk te maken, met inachtneming van het recht van de Unie. Overeenkomstig artikel 346 VWEU is geen enkele lidstaat verplicht inlichtingen te verstrekken waarvan de openbaarmaking in strijd zou zijn met de wezenlijke belangen van zijn openbare veiligheid. In dit verband zijn de nationale en uniale regels voor de bescherming van gerubriceerde informatie, geheimhoudingsovereenkomsten en informele geheimhoudingsovereenkomsten, zoals het verkeerslichtprotocol[14], van belang.

(7) Met de intrekking van Richtlijn (EU) 2016/1148 moet het toepassingsgebied per sector worden uitgebreid tot een groter deel van de economie in het licht van de overwegingen (4) tot en met (6). De sectoren die onder Richtlijn (EU) 2016/1148 vallen, moeten daarom worden uitgebreid om de sectoren en diensten die van vitaal belang zijn voor belangrijke maatschappelijke en economische activiteiten binnen de interne markt, volledig te bestrijken. De regels mogen niet verschillen naargelang het gaat om aanbieders van essentiële diensten of digitaledienstverleners. Dat onderscheid is achterhaald gebleken, aangezien het niet het werkelijke belang van de sectoren of diensten voor de maatschappelijke en economische activiteiten in de interne markt weerspiegelt.

(8) Overeenkomstig Richtlijn (EU) 2016/1148 waren de lidstaten verantwoordelijk voor het bepalen welke entiteiten voldoen aan de criteria om als aanbieders van essentiële diensten te worden aangemerkt ("identificatieproces"). Om de grote verschillen tussen de lidstaten in dat opzicht weg te werken en rechtszekerheid te bieden voor de vereisten inzake risicobeheer en de rapportageverplichtingen voor alle relevante entiteiten, moet er een uniform criterium worden vastgesteld dat bepaalt welke entiteiten binnen het toepassingsgebied van deze richtlijn vallen. Dit criterium moet bestaan uit de toepassing van de "size-cap"-regel, waarbij alle middelgrote en grote ondernemingen, zoals gedefinieerd in Aanbeveling 2003/361/EG van de Commissie[15], die actief zijn in de sectoren of het soort diensten verrichten die onder deze richtlijn vallen, binnen de werkingssfeer van de richtlijn vallen. Van de lidstaten mag niet worden verlangd dat zij een lijst opstellen van de entiteiten die aan dit algemeen geldende groottecriterium voldoen.

---

14 Het verkeerslichtprotocol ("Traffic Light Protocol" — TLP) is een middel voor iemand die informatie deelt om zijn publiek te informeren over eventuele beperkingen bij de verdere verspreiding van deze informatie. Het wordt gebruikt in bijna alle CSIRT-gemeenschappen en in sommige centra voor informatie-uitwisseling en -analyse (Information Analysis and Sharing Centres — ISAC's).

15 Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PB L 124 van 20.5.2003, blz. 36).

(9) Kleine of micro-entiteiten die voldoen aan bepaalde criteria die wijzen op een sleutelrol voor de economieën of samenlevingen van de lidstaten of voor bepaalde sectoren of soorten diensten, moeten echter ook onder deze richtlijn vallen. De lidstaten moeten verantwoordelijk zijn voor het opstellen van een lijst van dergelijke entiteiten en deze aan de Commissie voorleggen.

(10) De Commissie kan, in samenwerking met de samenwerkingsgroep, richtsnoeren opstellen voor de toepassing van de criteria die van toepassing zijn op micro- en kleine ondernemingen.

(11) Afhankelijk van de sector waarin zij actief zijn of het soort dienst dat zij verlenen, moeten de entiteiten die onder het toepassingsgebied van deze richtlijn vallen in twee categorieën worden ingedeeld: essentiële en belangrijke. Bij deze indeling in categorieën moet rekening worden gehouden met de mate van kriticiteit van de sector of het soort dienst, alsmede met de mate van afhankelijkheid van andere sectoren of soorten diensten. Voor zowel essentiële als belangrijke entiteiten moeten dezelfde eisen inzake risicobeheer en rapportageverplichtingen gelden. De toezichts- en sanctieregelingen tussen deze twee categorieën entiteiten moeten worden gedifferentieerd om te zorgen voor een billijk evenwicht tussen eisen en verplichtingen enerzijds en de administratieve lasten die voortvloeien uit het toezicht op de naleving anderzijds.

(12) Sectorspecifieke wetgeving en instrumenten kunnen bijdragen tot het waarborgen van een hoog niveau van cyberbeveiliging, waarbij ten volle rekening wordt gehouden met de specifieke kenmerken en de complexiteit van deze sectoren. Wanneer een sectorspecifieke rechtshandeling van de Unie vereist dat essentiële of belangrijke entiteiten risicobeheersmaatregelen op het gebied van cyberbeveiliging nemen of incidenten of significante cyberbedreigingen met ten minste een gelijkwaardig effect als de in deze richtlijn vastgestelde verplichtingen melden, moeten die sectorspecifieke bepalingen, onder meer inzake toezicht en handhaving, van toepassing zijn. De Commissie kan richtsnoeren uitvaardigen met betrekking tot de uitvoering van de lex specialis. Deze richtlijn vormt geen beletsel voor de vaststelling van aanvullende sectorspecifieke handelingen van de Unie met betrekking tot maatregelen voor het beheer van cyberbeveiligingsrisico's en meldingen van incidenten. Deze richtlijn laat de bestaande uitvoeringsbevoegdheden die aan de Commissie zijn verleend in een aantal sectoren, waaronder vervoer en energie, onverlet.

(13) Verordening XXXX/XXXX van het Europees Parlement en de Raad[16] moet worden beschouwd als een sectorspecifieke rechtshandeling van de Unie met betrekking tot deze richtlijn voor wat betreft de entiteiten in de financiële sector. De bepalingen van Verordening XXXX/XXXX betreffende maatregelen voor het risicobeheer op het gebied van informatie- en communicatietechnologie (ICT), het beheer van ICT-gerelateerde incidenten en met name de rapportage van incidenten, alsmede betreffende digitale operationele veerkrachttests, regelingen voor het delen van informatie en risico's van derden op het gebied van ICT, moeten van toepassing zijn in plaats van de bepalingen die in het kader van deze richtlijn zijn vastgesteld. De lidstaten mogen de bepalingen van deze richtlijn betreffende de verplichtingen inzake risicobeheer en rapportage op het gebied van cyberbeveiliging, de uitwisseling van informatie en het toezicht en de handhaving dan ook niet toepassen op financiële entiteiten die onder Verordening XXXX/XXXX vallen. Tegelijkertijd is het van

[16] *[voeg de volledige titel en de publicatiegegevens van het PB in wanneer deze bekend zijn]*

belang een sterke relatie en de uitwisseling van informatie met de financiële sector in het kader van deze richtlijn in stand te houden. Daartoe biedt Verordening XXXX/XXXX alle financiële toezichthouders, de Europese toezichthoudende autoriteiten (ETA's) voor de financiële sector en de nationale bevoegde autoriteiten op grond van Verordening XXXX/XXXX, de mogelijkheid deel te nemen aan strategische beleidsdiscussies en technische werkzaamheden van de samenwerkingsgroep en informatie uit te wisselen en samen te werken met de op grond van deze richtlijn aangewezen centrale contactpunten en met de nationale CSIRT's. De bevoegde autoriteiten uit hoofde van Verordening XXXX/XXXX moeten de details van grote ICT-gerelateerde incidenten ook doorgeven aan de in het kader van deze richtlijn aangewezen centrale contactpunten. Bovendien moeten de lidstaten de financiële sector blijven opnemen in hun cyberbeveiligingsstrategieën en kunnen de nationale CSIRT's de financiële sector bij hun activiteiten betrekken.

(14) Gezien de onderlinge verbanden tussen cyberbeveiliging en de fysieke beveiliging van entiteiten moet een coherente aanpak worden gewaarborgd tussen Richtlijn (EU) XXX/XXX van het Europees Parlement en de Raad[17] en deze richtlijn. Daartoe moeten de lidstaten ervoor zorgen dat kritieke entiteiten en gelijkwaardige entiteiten uit hoofde van Richtlijn (EU) XXX/XXX als essentiële entiteiten uit hoofde van deze richtlijn worden beschouwd. De lidstaten moeten er ook voor zorgen dat hun strategieën op het gebied van cyberbeveiliging voorzien in een beleidskader voor een betere coördinatie tussen de bevoegde autoriteit in het kader van deze richtlijn en die in het kader van Richtlijn (EU) XXX/XXX in de context van de uitwisseling van informatie over incidenten en cyberbedreigingen en de uitoefening van toezichthoudende taken. De autoriteiten in het kader van beide richtlijnen moeten samenwerken en informatie uitwisselen, met name met betrekking tot de identificatie van kritieke entiteiten, cyberbedreigingen, cyberbeveiligingsrisico's, incidenten die kritieke entiteiten treffen en de door kritieke entiteiten genomen cyberbeveiligingsmaatregelen. Op verzoek van de bevoegde autoriteiten uit hoofde van Richtlijn (EU) XXX/XXX moeten de bevoegde autoriteiten uit hoofde van deze richtlijn in staat worden gesteld hun toezichts- en handhavingsbevoegdheden uit te oefenen ten aanzien van een essentiële entiteit die als kritiek is aangemerkt. Beide autoriteiten moeten hiertoe samenwerken en informatie uitwisselen.

(15) Het behoud van een betrouwbaar, veerkrachtig en veilig domeinnaamsysteem (DNS) is een sleutelfactor voor het behoud van de integriteit van het internet en is essentieel voor de continue en stabiele werking ervan, waarvan de digitale economie en de maatschappij afhankelijk zijn. Daarom moet deze richtlijn van toepassing zijn op alle aanbieders van DNS-diensten in de gehele DNS-omzettingsketen, met inbegrip van exploitanten van root-naamservers, topleveldomeinnaamservers, gezaghebbende naamservers voor domeinnamen en recursieve resolvers.

(16) Cloudcomputerdiensten moeten betrekking hebben op diensten die toegang op aanvraag en brede toegang op afstand mogelijk maken tot een schaalbare en elastische pool van gedeelde en gedistribueerde computerbronnen. Deze computerbronnen omvatten middelen zoals netwerken, servers of andere infrastructuur, besturingssystemen, software, opslag, toepassingen en diensten. De invoeringsmodellen van cloudcomputing moeten private, gemeenschaps-, publieke en hybride cloud omvatten. De genoemde dienst- en invoeringsmodellen hebben dezelfde

[17] *[voeg de volledige titel en de publicatiegegevens van het PB in wanneer deze bekend zijn]*

betekenis als de in de ISO/IEC 17788:2014-norm gedefinieerde benamingen van dienst- en invoeringsmodellen. Het vermogen van de cloudcomputergebruiker om eenzijdig zelfvoorzienend te zijn, zoals servertijd of netwerkopslag, zonder enige menselijke interactie door de cloudcomputerdienstverlener, zou kunnen worden omschreven als beheer op verzoek. Met het begrip "brede toegang op afstand" wordt bedoeld: de cloudcapaciteiten worden via het netwerk aangeboden en zijn toegankelijk via mechanismen die het gebruik van heterogene thin- of thick-client-platforms bevorderen (waaronder mobiele telefoons, tablets, laptops, werkstations). Met "schaalbaar" wordt bedoeld: computercapaciteit die, ongeacht de geografische locatie van de capaciteit, op flexibele wijze door aanbieders van cloudcomputerdiensten wordt toegewezen teneinde schommelingen in de vraag te kunnen opvangen Met "elastische groep" wordt bedoeld: de computercapaciteit die, afhankelijk van de vraag, ter beschikking wordt gesteld en wordt vrijgegeven teneinde deze beschikbare capaciteit snel te kunnen verhogen en verlagen naargelang van het werkvolume. Met "gedeeld" wordt bedoeld: de computercapaciteit die ter beschikking wordt gesteld van meerdere gebruikers die een gemeenschappelijke toegang tot de dienst hebben, maar waarbij de verwerking voor elke gebruiker afzonderlijk plaatsvindt, hoewel de dienst door middel van dezelfde elektronische uitrusting wordt verleend. Met "gedistribueerd" wordt bedoeld: de computercapaciteit die zich op verschillende netwerkcomputers of -toestellen bevindt en die onderling communiceert en coördineert door middel van het doorgeven van berichten.

(17) Gezien de opkomst van innovatieve technologieën en nieuwe bedrijfsmodellen wordt verwacht dat er nieuwe invoerings- en servicemodellen voor cloudcomputing op de markt zullen verschijnen als antwoord op de veranderende behoeften van klanten. In die context kunnen cloudcomputerdiensten in een sterk gedistribueerde vorm worden verleend, nog dichter bij de plaats waar de gegevens worden gegenereerd of verzameld, waardoor de overstap van het traditionele model naar een sterk gedistribueerd model ("edge computing") wordt gemaakt.

(18) Diensten die worden aangeboden door aanbieders van datacentradiensten kunnen niet altijd worden verleend in een vorm van een cloudcomputerdienst. Datacentra maken dan ook niet altijd deel uit van de cloudcomputerinfrastructuur. Om alle risico's voor de beveiliging van netwerk- en informatiesystemen te beheren, moet deze richtlijn ook van toepassing zijn op aanbieders van dergelijke datacentrumdiensten die geen cloudcomputerdienstdiensten zijn. Voor de toepassing van deze richtlijn wordt onder "datacentrumdienst" verstaan: de verlening van een dienst die structuren, of groepen van structuren, omvat die bestemd zijn voor de gecentraliseerde accommodatie, de interconnectie en de exploitatie van informatietechnologie en netwerkapparatuur die diensten op het gebied van gegevensopslag, -verwerking en -transport aanbiedt, samen met alle faciliteiten en infrastructuren voor energiedistributie en omgevingscontrole. De term "datacentrumdienst" is niet van toepassing op interne bedrijfsdatacentra die eigendom zijn van en geëxploiteerd worden voor eigen doeleinden van de betreffende entiteit.

(19) Verleners van postdiensten in de zin van Richtlijn 97/67/EG van het Europees Parlement en de Raad[18], alsmede verleners van expres- en koeriersdiensten, moeten onder deze richtlijn vallen indien zij ten minste een van de stappen in de

[18] Richtlijn 97/67/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende gemeenschappelijke regels voor de ontwikkeling van de interne markt voor postdiensten in de Gemeenschap en de verbetering van de kwaliteit van de dienst (PB L 15 van 21.1.1998, blz. 14).

postbestelketen en met name de ophaling, sortering of distributie, met inbegrip van de ophaaldiensten, verzorgen. Vervoersdiensten die niet in samenhang met een van deze stappen worden ondernomen, moeten buiten het toepassingsgebied van de postdiensten vallen.

(20) Deze toenemende onderlinge afhankelijkheid is het resultaat van een steeds meer grensoverschrijdend en onderling afhankelijk dienstverleningsnetwerk dat gebruik maakt van belangrijke infrastructuren in de hele Unie in de sectoren energie, vervoer, digitale infrastructuur, drinkwater en afvalwater, gezondheid, bepaalde aspecten van het openbaar bestuur en de ruimtevaart, voor zover het gaat om de verlening van bepaalde diensten die afhankelijk zijn van grondgebonden infrastructuren die eigendom zijn van, beheerd en geëxploiteerd worden door de lidstaten of door particuliere partijen, en die dus geen betrekking hebben op infrastructuren die eigendom zijn van, beheerd of geëxploiteerd worden door of namens de Unie als onderdeel van haar ruimtevaartprogramma's. Deze onderlinge afhankelijkheid houdt in dat elke verstoring, zelfs als deze aanvankelijk beperkt blijft tot één entiteit of één sector, meer in het algemeen een cascade-effect kan hebben, met mogelijkerwijs verstrekkende en langdurige negatieve gevolgen voor de verlening van diensten op de hele interne markt. De COVID-19-pandemie heeft de kwetsbaarheid van onze steeds meer onderling afhankelijke samenlevingen voor de risico's van lage waarschijnlijkheid aangetoond.

(21) Gezien de verschillen tussen de nationale governancestructuren en om de reeds bestaande sectorale regelingen of toezichts- en regelgevingsorganen van de Unie te vrijwaren, moeten de lidstaten meer dan één nationale bevoegde autoriteit kunnen aanwijzen die verantwoordelijk is voor het vervullen van de taken in verband met de beveiliging van de netwerk- en informatiesystemen van essentiële en belangrijke entiteiten in het kader van deze richtlijn. De lidstaten moeten deze rol kunnen toewijzen aan een bestaande autoriteit.

(22) Om de grensoverschrijdende samenwerking en communicatie tussen de autoriteiten te vergemakkelijken en een doeltreffende uitvoering van deze richtlijn mogelijk te maken, moet elke lidstaat één nationaal centraal contactpunt aanwijzen dat verantwoordelijk is voor de coördinatie van kwesties in verband met de beveiliging van de netwerk- en informatiesystemen en de grensoverschrijdende samenwerking op het niveau van de Unie.

(23) De bevoegde autoriteiten of de CSIRT's moeten de meldingen van incidenten op een effectieve en efficiënte manier van de entiteiten ontvangen. De centrale contactpunten moeten worden belast met het doorsturen van meldingen van incidenten naar de centrale contactpunten van andere betrokken lidstaten. Op het niveau van de autoriteiten van de lidstaten moeten, om te zorgen voor een centraal contactpunt in elke lidstaat, de centrale contactpunten ook de geadresseerden zijn van relevante informatie over incidenten met betrekking tot entiteiten uit de financiële sector van de bevoegde autoriteiten uit hoofde van Verordening XXXX/XXXX, die zij in voorkomend geval moeten kunnen doorsturen naar de relevante nationale bevoegde autoriteiten of CSIRT's uit hoofde van deze richtlijn.

(24) De lidstaten moeten, zowel wat de technische als de organisatorische mogelijkheden betreft, adequaat worden uitgerust om incidenten en risico's van het netwerk- en het informatiesysteem te voorkomen, op te sporen, erop te reageren en te beperken. De lidstaten moeten er daarom voor zorgen dat zij beschikken over goed functionerende CSIRT's, ook bekend als computercrisisresponsteams ("computer emergency response

teams" — "CERT's"), die voldoen aan de essentiële eisen om te garanderen dat zij over doeltreffende en compatibele capaciteiten beschikken om incidenten en risico's aan te pakken en om een efficiënte samenwerking op het niveau van de Unie te waarborgen. Om de vertrouwensrelatie tussen de entiteiten en de CSIRT's te versterken, moeten de lidstaten, in gevallen waarin een CSIRT deel uitmaakt van de bevoegde autoriteit, een functionele scheiding overwegen tussen de operationele taken van de CSIRT's, met name met betrekking tot de uitwisseling van informatie en de ondersteuning van de entiteiten, en de toezichtsactiviteiten van de bevoegde autoriteiten.

(25) Wat de persoonsgegevens betreft, moeten de CSIRT's overeenkomstig Verordening (EU) nr. 2016/679 van het Europees Parlement en de Raad[19] namens en op verzoek van een entiteit in het kader van deze richtlijn een proactieve scan kunnen uitvoeren van de netwerk- en informatiesystemen die voor de verlening van hun diensten worden gebruikt. De lidstaten moeten ernaar streven dat alle sectorale CSIRT's over gelijke technische capaciteiten beschikken. De lidstaten kunnen het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) om bijstand vragen bij de ontwikkeling van nationale CSIRT's.

(26) Gezien het belang van internationale samenwerking op het gebied van cyberbeveiliging moeten de CSIRT's kunnen deelnemen aan internationale samenwerkingsnetwerken, naast het bij deze richtlijn opgerichte CSIRT-netwerk.

(27) Overeenkomstig de bijlage bij Aanbeveling (EU) 2017/1548 van de Commissie inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises ("Blauwdruk")[20], moet onder een grootschalig incident een incident worden verstaan met significante gevolgen voor ten minste twee lidstaten of die verstoringen veroorzaken die te groot zijn om door een getroffen lidstaat alleen te worden verholpen. Afhankelijk van hun oorzaak en gevolgen kunnen grootschalige incidenten escaleren en veranderen in volwaardige crises die de goede werking van de interne markt niet mogelijk maken. Gezien het brede toepassingsgebied en in de meeste gevallen het grensoverschrijdende karakter van dergelijke incidenten, moeten de lidstaten en de betrokken instellingen, organen en agentschappen van de Unie op technisch, operationeel en politiek niveau samenwerken om de respons in de hele Unie naar behoren te coördineren.

(28) Aangezien de exploitatie van kwetsbaarheden in netwerk- en informatiesystemen aanzienlijke verstoringen en schade kan veroorzaken, is het snel identificeren en verhelpen van deze kwetsbaarheden een belangrijke factor in het verminderen van het cyberbeveiligingsrisico. Entiteiten die dergelijke systemen ontwikkelen, moeten daarom passende procedures vaststellen om kwetsbaarheden aan te pakken wanneer deze worden ontdekt. Aangezien kwetsbaarheden vaak door derden (rapporterende entiteiten) worden ontdekt en gemeld (bekendgemaakt), moet de fabrikant of aanbieder van ICT-producten of -diensten ook de nodige procedures invoeren om kwetsbaarheidsinformatie van derden te ontvangen. In dit verband bieden de internationale normen ISO/IEC 30111 en ISO/IEC 29417 richtsnoeren voor

---

19 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

20 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).

respectievelijk de respons op kwetsbaarheden en het bekendmaken van kwetsbaarheden. Wat de bekendmaking van kwetsbaarheden betreft, is met name de coördinatie tussen de rapporterende entiteiten en de fabrikanten of aanbieders van ICT-producten of -diensten van belang. De gecoördineerde bekendmaking van kwetsbaarheden duidt een gestructureerd proces aan waarbij kwetsbaarheden aan organisaties worden gemeld op een manier die de organisatie in staat stelt de kwetsbaarheid te diagnosticeren en te verhelpen voordat gedetailleerde informatie over de kwetsbaarheid aan derden of aan het publiek wordt bekendgemaakt. De gecoördineerde bekendmaking van kwetsbaarheden moet ook de coördinatie tussen de rapporterende entiteit en de organisatie omvatten wat betreft het tijdstip van het herstel en de bekendmaking van de kwetsbaarheden.

(29) De lidstaten moeten daarom maatregelen nemen om een gecoördineerde bekendmaking van kwetsbaarheden te vergemakkelijken door een relevant nationaal beleid vast te stellen. In dit verband moeten de lidstaten een CSIRT aanwijzen die de rol van "coördinator" op zich neemt en die, indien nodig, optreedt als tussenpersoon tussen de rapporterende entiteiten en de fabrikanten of aanbieders van ICT-producten of -diensten. De taken van de CSIRT-coördinator moeten met name bestaan uit het identificeren van en contact opnemen met de betrokken entiteiten, het ondersteunen van de rapporterende entiteiten, het onderhandelen over tijdschema's voor de openbaarmaking en het beheren van kwetsbaarheden die van invloed zijn op meerdere organisaties (openbaarmaking van kwetsbaarheden door meerdere partijen). Wanneer kwetsbaarheden meerdere fabrikanten of aanbieders van ICT-producten of -diensten in meer dan één lidstaat treffen, moeten de aangewezen CSIRT's van elk van de getroffen lidstaten binnen het CSIRT-netwerk samenwerken.

(30) Toegang tot correcte en tijdige informatie over kwetsbaarheden die van invloed zijn op ICT-producten en -diensten draagt bij aan een verbeterd risicobeheer inzake cyberbeveiliging. In dat opzicht zijn bronnen van openbaar beschikbare informatie over kwetsbaarheden een belangrijk instrument voor entiteiten en hun gebruikers, maar ook voor nationale bevoegde autoriteiten en CSIRT's. Daarom moet het Enisa een kwetsbaarheidsregister instellen waarin essentiële en belangrijke entiteiten en hun leveranciers, alsmede entiteiten die niet onder het toepassingsgebied van deze richtlijn vallen, op vrijwillige basis kwetsbaarheden kunnen bekendmaken en de kwetsbaarheidsinformatie kunnen verstrekken die gebruikers in staat stelt passende beperkende maatregelen te nemen.

(31) Hoewel er soortgelijke kwetsbaarheidsregisters of -databases bestaan, worden deze gehost en onderhouden door entiteiten die niet in de Unie zijn gevestigd. Een Europees kwetsbaarheidsregister dat door het Enisa wordt bijgehouden, zou zorgen voor meer transparantie met betrekking tot het bekendmakingsproces voordat de kwetsbaarheid officieel bekend wordt gemaakt, en voor meer veerkracht in geval van verstoringen of onderbrekingen van de verlening van soortgelijke diensten. Om dubbel werk te voorkomen en zoveel mogelijk complementariteit na te streven, moet het Enisa de mogelijkheid onderzoeken om gestructureerde samenwerkingsovereenkomsten te sluiten met soortgelijke registers in jurisdicties van derde landen.

(32) De samenwerkingsgroep moet om de twee jaar een werkprogramma opstellen, met inbegrip van de acties die door de groep moeten worden ondernomen om zijn doelstellingen en taken uit te voeren. Om mogelijke verstoringen van de werkzaamheden van de groep te voorkomen, moet het tijdschema van het eerste programma dat in het kader van deze richtlijn is vastgesteld, worden afgestemd op het

tijdschema van het laatste programma dat in het kader van Richtlijn (EU) 2016/1148 is vastgesteld.

(33) Bij de ontwikkeling van richtsnoeren moet de samenwerkingsgroep consequent nationale oplossingen en ervaringen in kaart brengen, het effect van de resultaten van de samenwerkingsgroep op de nationale aanpak beoordelen, de uitdagingen op het gebied van de uitvoering bespreken en specifieke aanbevelingen formuleren die moeten worden aangepakt door een betere uitvoering van de bestaande regels.

(34) De samenwerkingsgroep moet een flexibel forum blijven en in staat zijn te reageren op veranderende en nieuwe beleidsprioriteiten en -uitdagingen, rekening houdend met de beschikbaarheid van middelen. Hij moet regelmatig gezamenlijke bijeenkomsten organiseren met relevante particuliere belanghebbenden uit de hele Unie om de activiteiten van de groep te bespreken en input te verzamelen over nieuwe beleidsuitdagingen. Om de samenwerking op het niveau van de Unie te versterken, moet de groep overwegen organen en agentschappen van de Unie die betrokken zijn bij het cyberbeveiligingsbeleid, zoals het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3), het Agentschap van de Europese Unie voor de veiligheid van de luchtvaart (EASA) en het Agentschap van de Europese Unie voor het ruimtevaartprogramma (EUSPA), uit te nodigen om deel te nemen aan de werkzaamheden van de groep.

(35) De bevoegde autoriteiten en de CSIRT's moeten de bevoegdheid krijgen om deel te nemen aan uitwisselingsprogramma's voor ambtenaren uit andere lidstaten om de samenwerking te verbeteren. De bevoegde autoriteiten moeten de nodige maatregelen nemen om ambtenaren uit andere lidstaten in staat te stellen een doeltreffende rol te spelen in de activiteiten van de bevoegde autoriteit van ontvangst.

(36) De Unie moet in voorkomend geval overeenkomstig artikel 218 VWEU internationale overeenkomsten met derde landen of internationale organisaties sluiten die hun deelname aan bepaalde activiteiten van de samenwerkingsgroep en het CSIRT-netwerk mogelijk maken en organiseren. Dergelijke overeenkomsten moeten zorgen voor een passende bescherming van de gegevens.

(37) De lidstaten moeten bijdragen aan de totstandbrenging van het in Aanbeveling (EU) 2017/1584 beschreven EU-kader voor crisisrespons op het gebied van cyberbeveiliging via de bestaande samenwerkingsnetwerken, met name het netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe), het CSIRT-netwerk en de samenwerkingsgroep. EU-CyCLONe en het CSIRT-netwerk moeten samenwerken op basis van procedurele regelingen die de modaliteiten van die samenwerking bepalen. In de procedureregels van het EU-CyCLONe moet nader worden gespecificeerd hoe het netwerk moet functioneren, met inbegrip van, maar niet beperkt tot rollen, samenwerkingswijzen, interacties met andere relevante actoren en modellen voor het delen van informatie, alsmede communicatiemiddelen. Voor crisisbeheer op het niveau van de Unie moeten de betrokken partijen zich baseren op de regelingen voor geïntegreerde politieke crisisrespons ("Integrated Political Crisis Response" — IPCR). De Commissie moet hiervoor gebruikmaken van het ARGUS-proces voor sectoroverschrijdende crisiscoördinatie op hoog niveau. Als de crisis een belangrijke externe of gemeenschappelijke veiligheids- en defensiedimensie (GVDB) met zich meebrengt, moet het crisisresponsmechanisme van de Europese Dienst voor extern optreden (EDEO) worden geactiveerd.

(38) Voor de toepassing van deze richtlijn wordt onder "risico" verstaan: de mogelijkheid van verlies of verstoring als gevolg van een cyberbeveiligingsincident; dit wordt

uitgedrukt als een combinatie van de omvang van een dergelijk verlies of verstoring en de waarschijnlijkheid dat een dergelijk incident zich voordoet.

(39) Voor de toepassing van deze richtlijn wordt onder “bijna-ongelukken” verstaan: een gebeurtenis die mogelijkerwijs schade had kunnen veroorzaken, maar die met succes is voorkomen.

(40) Risicobeheersmaatregelen moeten maatregelen omvatten om eventuele risico’s van incidenten te identificeren, om incidenten te voorkomen, op te sporen en te behandelen en om de gevolgen ervan te beperken. De beveiliging van netwerk- en informatiesystemen moet de beveiliging van opgeslagen, verzonden en verwerkte gegevens omvatten.

(41) Om te voorkomen dat aan essentiële en belangrijke entiteiten onevenredige financiële en administratieve lasten worden opgelegd, moeten de eisen inzake het beheer van cyberbeveiligingsrisico’s in verhouding staan tot het risico dat het betrokken netwerk- en informatiesysteem met zich meebrengt, rekening houdend met de stand van de techniek van dergelijke maatregelen.

(42) Essentiële en belangrijke entiteiten moeten de beveiliging van de netwerk- en informatiesystemen die zij bij hun activiteiten gebruiken, waarborgen. Dit zijn voornamelijk particuliere netwerk- en informatiesystemen die door hun interne IT-medewerkers worden beheerd of waarvan de beveiliging is uitbesteed. De vereisten inzake risicobeheer en rapportage voor cyberbeveiliging uit hoofde van deze richtlijn moeten van toepassing zijn op de relevante essentiële en belangrijke entiteiten, ongeacht of zij het onderhoud van hun netwerk- en informatiesystemen intern uitvoeren of uitbesteden.

(43) Het aanpakken van risico’s op het gebied van cyberbeveiliging die voortvloeien uit de toeleveringsketen van een entiteit en uit haar relatie met haar leveranciers is bijzonder belangrijk gezien de prevalentie van incidenten waarbij entiteiten het slachtoffer zijn geworden van cyberaanvallen en waarbij kwaadwillende actoren de beveiliging van de netwerk- en informatiesystemen van een entiteit in gevaar hebben kunnen brengen door gebruik te maken van kwetsbaarheden die van invloed zijn op producten en diensten van derden. De entiteiten moeten daarom de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners beoordelen en er rekening mee houden, met inbegrip van hun veilige ontwikkelingsprocedures.

(44) Onder de dienstverleners spelen aanbieders van beheerde beveiligingsdiensten (“managed security services providers” — MSSP’s) op het gebied van bijvoorbeeld incidentrespons, penetratietesten, beveiligingsaudits en consultancy een bijzonder belangrijke rol in het bijstaan van entiteiten bij hun inspanningen om incidenten op te sporen en erop te reageren. Deze MSSP’s zijn echter ook zelf het doelwit geweest van cyberaanvallen en vormen door hun nauwe integratie in de activiteiten van de exploitanten een bijzonder cyberbeveiligingsrisico. De entiteiten moeten daarom meer zorgvuldigheid betrachten bij de selectie van een MSSP.

(45) Entiteiten moeten ook aandacht besteden aan de risico’s op het gebied van cyberbeveiliging die voortvloeien uit hun interacties en relaties met andere belanghebbenden binnen een breder ecosysteem. De entiteiten moeten met name passende maatregelen nemen om ervoor te zorgen dat hun samenwerking met academische en onderzoeksinstellingen in overeenstemming is met hun cyberbeveiligingsbeleid en dat zij goede praktijken volgen met betrekking tot veilige

toegang en verspreiding van informatie in het algemeen en de bescherming van de intellectuele eigendom in het bijzonder. Evenzo moeten de entiteiten, gezien het belang en de waarde van gegevens voor de activiteiten van de entiteiten, bij het gebruik van gegevenstransformatie en gegevensanalysediensten van derden, alle passende cyberbeveiligingsmaatregelen nemen.

(46) Om de belangrijkste risico's van de toeleveringsketen verder aan te pakken en entiteiten die actief zijn in sectoren die onder deze richtlijn vallen, te helpen om de risico's van de toeleveringsketen en de leveranciers op het gebied van cyberbeveiliging op passende wijze te beheren, moet de samenwerkingsgroep waarbij de relevante nationale autoriteiten betrokken zijn, in samenwerking met de Commissie en het Enisa, gecoördineerde sectorale risicobeoordelingen van de toeleveringsketen uitvoeren, zoals reeds is gedaan voor 5G-netwerken naar aanleiding van Aanbeveling (EU) 2019/534 inzake cyberbeveiliging van 5G-netwerken[21], met als doel per sector vast te stellen welke de kritieke ICT-diensten, -systemen of -producten, de relevante bedreigingen en kwetsbaarheden zijn.

(47) Bij de beoordeling van de risico's voor de toeleveringsketen moet er, in het licht van de kenmerken van de betrokken sector, rekening worden gehouden met zowel technische als, in voorkomend geval, niet-technische factoren, met inbegrip van die welke zijn gedefinieerd in Aanbeveling (EU) 2019/534, in de gecoördineerde risicobeoordeling van de beveiliging van 5G-netwerken in de hele EU en in het EU-instrumentarium voor 5G-cyberbeveiliging dat door de samenwerkingsgroep is overeengekomen. Om te bepalen welke toeleveringsketens aan een gecoördineerde risicobeoordeling moeten worden onderworpen, moet rekening worden gehouden met de volgende criteria: i) de mate waarin essentiële en belangrijke entiteiten gebruik maken van en vertrouwen op specifieke kritieke ICT-diensten, -systemen of -producten; ii) de relevantie van specifieke kritieke ICT-diensten, -systemen of -producten voor het uitvoeren van kritieke of gevoelige functies, met inbegrip van de verwerking van persoonsgegevens; iii) de beschikbaarheid van alternatieve ICT-diensten, -systemen of -producten; iv) de veerkracht van de gehele toeleveringsketen van ICT-diensten, -systemen of -producten tegen verstorende gebeurtenissen en v) voor opkomende ICT-diensten, -systemen of -producten, hun potentiële toekomstige betekenis voor de activiteiten van de entiteiten.

(48) Om de wettelijke verplichtingen die aan aanbieders van openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten worden opgelegd, te stroomlijnen en aanbieders van vertrouwensdiensten in verband met de beveiliging van hun netwerk- en informatiesystemen in staat te stellen gebruik te maken van het bij deze richtlijn vastgestelde rechtskader (met inbegrip van de aanwijzing van het CSIRT dat verantwoordelijk is voor de behandeling van risico's en incidenten, de deelname van de bevoegde autoriteiten en organen aan de werkzaamheden van de samenwerkingsgroep en het CSIRT-netwerk), moeten zij worden opgenomen in het toepassingsgebied van deze richtlijn. De overeenkomstige bepalingen van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad[22] en Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad[23] met

[21] Aanbeveling (EU) 2019/534 van de Commissie van 26 maart 2019 Cyberbeveiliging van 5G-netwerken (PB L 88 van 29.3.2019, blz. 42).

[22] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PB L 257 van 28.8.2014, blz. 73).

betrekking tot het opleggen van een beveiligings- en meldingsverplichting aan dit soort entiteiten moeten derhalve worden ingetrokken. De regels inzake de rapportageverplichtingen moeten Verordening (EU) nr. 2016/679 en Richtlijn 2002/58/EG van het Europees Parlement en de Raad[24]onverlet laten.

(49) Indien nodig en om onnodige verstoringen te voorkomen, moeten de bestaande nationale richtsnoeren en de nationale wetgeving die zijn vastgesteld voor de omzetting van de in artikel 40, lid 1, van Richtlijn (EU) 2018/1972 vastgestelde regels met betrekking tot beveiligingsmaatregelen, alsmede van de eisen van artikel 40, lid 2, van die richtlijn betreffende de parameters in verband met de ernst van een incident, verder worden gebruikt door de bevoegde autoriteiten die belast zijn met het toezicht en de handhaving voor de toepassing van deze richtlijn.

(50) Gezien het toenemende belang van nummeronafhankelijke interpersoonlijke communicatiediensten moet ervoor worden gezorgd dat ook voor dergelijke diensten passende beveiligingseisen gelden, gelet op hun specifieke aard en economisch belang. Aanbieders van dergelijke diensten moeten dus ook zorgen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op het risico. Aangezien aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten normaal gesproken geen daadwerkelijke controle uitoefenen op de transmissie van signalen over netwerken, kan de mate van risico voor dergelijke diensten in sommige opzichten als lager worden beschouwd dan voor traditionele elektronische-communicatiediensten. Hetzelfde geldt voor interpersoonlijke communicatiediensten die gebruik maken van nummers en die geen daadwerkelijke controle uitoefenen op de signaaloverdracht.

(51) De interne markt is meer dan ooit afhankelijk van het functioneren van het internet. De diensten van vrijwel alle essentiële en belangrijke entiteiten zijn afhankelijk van diensten die via het internet worden verleend. Om te zorgen voor een soepele verlening van diensten die door essentiële en belangrijke entiteiten worden verleend, is het van belang dat openbare elektronische-communicatienetwerken, zoals bijvoorbeeld internetbackbones of onderzeese communicatiekabels, over passende cyberbeveiligingsmaatregelen beschikken en incidenten in verband daarmee melden.

(52) In voorkomend geval moeten de entiteiten de ontvangers van hun diensten op de hoogte brengen van bijzondere en significante bedreigingen en van de maatregelen die zij kunnen nemen om het daaruit voortvloeiende risico voor henzelf te beperken. De verplichting om de ontvangers van dergelijke bedreigingen te informeren mag entiteiten niet ontslaan van de verplichting om op eigen kosten passende en onmiddellijke maatregelen te nemen om eventuele cyberbedreigingen te voorkomen of te verhelpen en het normale beveiligingsniveau van de dienst te herstellen. De verstrekking van dergelijke informatie over beveiligingsrisico's aan de ontvangers moet gratis zijn.

(53) De aanbieders van openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten moeten met name de ontvangers van de dienst op

---

[23] Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie (PB L 321 van 17.12.2018, blz. 36)

[24] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

de hoogte brengen van bijzondere en significante cyberbedreigingen en van de maatregelen die zij kunnen nemen om de beveiliging van hun communicatie te beschermen, bijvoorbeeld door gebruik te maken van specifieke soorten software of encryptietechnologieën.

(54) Om de veiligheid van elektronische-communicatienetwerken en -diensten te waarborgen, moet het gebruik van encryptie, en met name eind-tot-eindcodering, worden bevorderd en, waar nodig, verplicht worden gesteld voor aanbieders van dergelijke diensten en netwerken, overeenkomstig de beginselen van beveiliging en privacy, standaard en door het ontwerp, voor de doeleinden van artikel 18. Het gebruik van eind-tot-eindcodering moet aansluiten op de bevoegdheden van de lidstaten om de bescherming van hun wezenlijke veiligheidsbelangen en de openbare veiligheid te waarborgen en om het onderzoek, de opsporing en de vervolging van strafbare feiten in overeenstemming met het recht van de Unie mogelijk te maken. Oplossingen voor legale toegang tot informatie in eind-tot-eind versleutelde communicatie moeten de effectiviteit van de versleuteling voor de bescherming van de privacy en de beveiliging van de communicatie behouden en tegelijkertijd een effectief antwoord op misdaad bieden.

(55) Deze richtlijn voorziet in een aanpak in twee fasen van de melding van incidenten om het juiste evenwicht te vinden tussen enerzijds een snelle melding die de potentiële verspreiding van incidenten helpt te beperken en entiteiten in staat stelt steun te zoeken, en anderzijds een grondige melding die waardevolle lessen trekt uit individuele incidenten en mettertijd de veerkracht van individuele bedrijven en hele sectoren ten aanzien van cyberbedreigingen verbetert. Wanneer entiteiten zich bewust worden van een incident, moeten zij binnen 24 uur een eerste melding doen, gevolgd door een eindverslag uiterlijk een maand later. De eerste melding hoeft enkel de informatie te bevatten die strikt noodzakelijk is om de bevoegde autoriteiten op de hoogte te brengen van het incident en de entiteit in staat te stellen om, indien nodig, bijstand te vragen. In die melding moet, indien van toepassing, worden aangegeven of het incident vermoedelijk door een onwettige of kwaadwillige handeling is veroorzaakt. De lidstaten moeten ervoor zorgen dat de eis om deze eerste melding in te dienen de middelen van de rapporterende entiteit niet afleidt van activiteiten die verband houden met de incidentenbehandeling en die als prioritair moeten worden aangemerkt. Om verder te voorkomen dat de verplichtingen inzake de melding van incidenten middelen onttrekken aan de incidentrespons of de inspanningen van de entiteiten op dat gebied anderszins in gevaar brengen, moeten de lidstaten ook bepalen dat de betrokken entiteit in naar behoren gemotiveerde gevallen en in overleg met de bevoegde autoriteiten of het CSIRT kan afwijken van de termijnen van 24 uur voor de eerste melding en één maand voor het eindverslag.

(56) Essentiële en belangrijke entiteiten bevinden zich vaak in een situatie waarin een bepaald incident, vanwege de kenmerken ervan, aan verschillende autoriteiten moet worden gemeld als gevolg van meldingsverplichtingen die in verschillende rechtsinstrumenten zijn opgenomen. Dergelijke gevallen creëren extra lasten en kunnen ook leiden tot onzekerheden met betrekking tot het formaat en de procedures van dergelijke meldingen. Met het oog hierop en om de melding van beveiligingsincidenten te vereenvoudigen, moeten de lidstaten *een centraal contactpunt* instellen voor alle meldingen die op grond van deze richtlijn en ook op grond van andere EU-wetgeving, zoals Verordening (EU) nr. 2016/679 en Richtlijn 2002/58/EG, vereist zijn. Het Enisa moet, in samenwerking met de samenwerkingsgroep, gemeenschappelijke meldingsmodellen ontwikkelen door

middel van richtsnoeren die de door het recht van de Unie verlangde rapportage-informatie vereenvoudigen en stroomlijnen en de lasten voor bedrijven verminderen.

(57) Wanneer het vermoeden bestaat dat een incident verband houdt met ernstige criminele activiteiten op grond van het recht van de Unie of het nationale recht, moeten de lidstaten essentiële en belangrijke entiteiten aanmoedigen om, op basis van de toepasselijke regels voor strafrechtelijke procedures in overeenstemming met het recht van de Unie, incidenten met een vermoedelijk ernstig crimineel karakter aan de betrokken rechtshandhavingsinstanties te melden. In voorkomend geval en onverminderd de voor Europol geldende regels inzake de bescherming van persoonsgegevens is het wenselijk dat de coördinatie tussen de bevoegde autoriteiten en de rechtshandhavingsinstanties van de verschillende lidstaten wordt vergemakkelijkt door het EC3 en het Enisa.

(58) Persoonsgegevens worden in veel gevallen in gevaar gebracht als gevolg van incidenten. In dit verband moeten de bevoegde autoriteiten samenwerken en informatie uitwisselen over alle relevante zaken met de gegevensbeschermingsautoriteiten en de toezichthoudende autoriteiten overeenkomstig Richtlijn 2002/58/EG.

(59) Het onderhouden van nauwkeurige en volledige databases van domeinnamen en registratiegegevens (de zogenaamde "WHOIS-gegevens") en het verlenen van rechtmatige toegang tot dergelijke gegevens is essentieel om de beveiliging, stabiliteit en veerkracht van het DNS te waarborgen, wat op zijn beurt bijdraagt tot een hoog gemeenschappelijk niveau van cyberbeveiliging binnen de Unie. Wanneer de verwerking persoonsgegevens omvat, moet die verwerking in overeenstemming zijn met het recht van de Unie inzake gegevensbescherming.

(60) De beschikbaarheid en tijdige toegankelijkheid van deze gegevens voor overheidsinstanties, met inbegrip van de autoriteiten die krachtens het recht van de Unie of het interne recht bevoegd zijn voor het voorkomen, onderzoeken of vervolgen van strafbare feiten, CERT's, CSIRT's, en met betrekking tot de gegevens van hun cliënten voor aanbieders van elektronische-communicatienetwerken en -diensten en aanbieders van cyberbeveiligingstechnologieën en -diensten die namens die cliënten optreden, is van essentieel belang om misbruik van domeinnamensystemen te voorkomen en te bestrijden, met name om cyberbeveiligingsincidenten te voorkomen, op te sporen en erop te reageren. Deze toegang moet in overeenstemming zijn met de EU-wetgeving inzake gegevensbescherming voor zover deze betrekking heeft op persoonsgegevens.

(61) Om de beschikbaarheid van nauwkeurige en volledige domeinnaamregistratiegegevens te waarborgen, moeten registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen (de zogenaamde registratoren) de integriteit en beschikbaarheid van domeinnaamregistratiegegevens verzamelen en waarborgen. Met name registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, moeten beleid en procedures vaststellen om nauwkeurige en volledige registratiegegevens te verzamelen en bij te houden en om onjuiste registratiegegevens te voorkomen en te corrigeren in overeenstemming met de gegevensbeschermingsregels van de Unie.

(62) Registers voor topleveldomeinnamen en de entiteiten die voor hen domeinnaamregistratiediensten verlenen, moeten gegevens voor de registratie van domeinnamen die buiten het toepassingsgebied van de gegevensbeschermingsregels

van de Unie vallen, zoals gegevens die betrekking hebben op rechtspersonen, openbaar maken[25]. Registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, moeten ook legale toegang tot specifieke domeinnaamregistratiegegevens over natuurlijke personen mogelijk maken voor legitieme toegangvragende partijen, in overeenstemming met de wetgeving van de Unie inzake gegevensbescherming. De lidstaten moeten ervoor zorgen dat registers voor topleveldomeinnamen en de entiteiten die voor hen domeinnaamregistratiediensten verlenen, onverwijld reageren op verzoeken van legitieme toegangvragende partijen om openbaarmaking van gegevens over domeinnaamregistratie. Registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor hen verlenen, moeten beleid en procedures vaststellen voor de publicatie en openbaarmaking van registratiegegevens, met inbegrip van overeenkomsten inzake het dienstverleningsniveau voor de behandeling van verzoeken om toegang van legitieme toegangvragende partijen. De toegangsprocedure kan ook het gebruik van een interface, een portaal of een ander technisch hulpmiddel omvatten om een efficiënt systeem te bieden voor het aanvragen en raadplegen van registratiegegevens. Met het oog op de bevordering van geharmoniseerde praktijken in de gehele interne markt kan de Commissie richtsnoeren voor dergelijke procedures vaststellen, zonder afbreuk te doen aan de bevoegdheden van het Europees Comité voor gegevensbescherming.

(63) In de regel worden essentiële en belangrijke entiteiten uit hoofde van deze richtlijn geacht onder de jurisdictie te vallen van de lidstaat waar zij hun diensten verlenen. Indien de entiteit diensten verricht in meer dan één lidstaat, moet zij onder de afzonderlijke en gelijktijdige jurisdictie van elk van deze lidstaten vallen. De bevoegde autoriteiten van deze lidstaten moeten samenwerken, elkaar wederzijds bijstand verlenen en, in voorkomend geval, gezamenlijke toezichtsacties uitvoeren.

(64) Om rekening te houden met het grensoverschrijdende karakter van de diensten en activiteiten van DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van netwerken voor de levering van inhoud, aanbieders van cloudcomputerdiensten, aanbieders van datacentrumdiensten en digitale aanbieders, zou slechts één lidstaat jurisdictie mogen hebben over deze entiteiten. De jurisdictie moet worden toegekend aan de lidstaat waar de respectieve entiteit haar hoofdvestiging in de Unie heeft. Het vestigingscriterium voor de toepassing van deze richtlijn houdt de daadwerkelijke uitoefening van de activiteit in door middel van stabiele regelingen. De rechtsvorm van dergelijke regelingen, hetzij via een filiaal, hetzij via een dochteronderneming met rechtspersoonlijkheid, is in dat opzicht niet bepalend. Of aan dit criterium wordt voldaan, mag niet afhangen van de vraag of het netwerk- en informatiesysteem zich fysiek op een bepaalde plaats bevinden; de aanwezigheid en het gebruik van dergelijke systemen vormen op zich niet een dergelijke hoofdvestiging en zijn dus geen doorslaggevende criteria voor het bepalen van de hoofdvestiging. De belangrijkste vestiging moet de plaats zijn waar de besluiten met betrekking tot de risicobeheersmaatregelen op het gebied van cyberbeveiliging in de Unie worden genomen. Dit zal doorgaans overeenkomen met de plaats van de centrale administratie van de bedrijven in de Unie. Indien dergelijke besluiten niet in de Unie worden

[25] VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD, overweging 14: "Deze verordening heeft geen betrekking op de verwerking van gegevens over rechtspersonen en met name als rechtspersonen gevestigde ondernemingen, zoals de naam en de rechtsvorm van de rechtspersoon en de contactgegevens van de rechtspersoon."

genomen, moet de hoofdvestiging worden geacht zich te bevinden in de lidstaten waar de entiteit een vestiging heeft met het hoogste aantal werknemers in de Unie. Wanneer de diensten door een groep van ondernemingen worden verricht, moet de hoofdvestiging van de zeggenschap uitoefenende onderneming worden beschouwd als de hoofdvestiging van de groep van ondernemingen.

(65) Wanneer een DNS-dienstverlener, register voor topleveldomeinnamen, aanbieder van een netwerk voor de levering van inhoud, aanbieder van cloudcomputerdiensten, aanbieder van datacentrumdiensten en digitale aanbieder die niet in de Unie is gevestigd, diensten binnen de Unie aanbiedt, moet hij een vertegenwoordiger aanwijzen. Om te bepalen of een dergelijke entiteit diensten binnen de Unie aanbiedt, moet worden nagegaan of het duidelijk is dat de entiteit van plan is diensten aan te bieden aan personen in een of meer lidstaten. De loutere toegankelijkheid in de Unie van de website van de entiteit of van een tussenpersoon of van een e-mailadres en van andere contactgegevens, of het gebruik van een taal die algemeen wordt gebruikt in het derde land waar de entiteit is gevestigd, is als zodanig onvoldoende om een dergelijk voornemen vast te stellen. Factoren zoals het gebruik van een taal of een valuta die in een of meer lidstaten algemeen wordt gebruikt en de mogelijkheid om diensten in die andere taal te bestellen, of de vermelding van klanten of gebruikers die zich in de Unie bevinden, kunnen echter duidelijk maken dat de entiteit van plan is om diensten binnen de Unie aan te bieden. De vertegenwoordiger moet namens de entiteit optreden en de bevoegde autoriteiten of de CSIRT's moeten contact met de vertegenwoordiger kunnen opnemen. De vertegenwoordiger moet uitdrukkelijk bij schriftelijke opdracht van de entiteit worden aangewezen om namens de entiteit op te treden met betrekking tot haar verplichtingen uit hoofde van deze richtlijn, met inbegrip van de melding van incidenten.

(66) Wanneer er krachtens de bepalingen van deze richtlijn informatie wordt uitgewisseld, gerapporteerd of anderszins gedeeld die volgens het nationale of het EU-recht als gerubriceerd wordt beschouwd, moeten de overeenkomstige specifieke regels voor de behandeling van gerubriceerde informatie worden toegepast.

(67) Nu cyberbedreigingen complexer en geavanceerder worden, zijn goede opsporings- en preventiemaatregelen voor een groot deel afhankelijk van de regelmatige uitwisseling van informatie over bedreigingen en kwetsbaarheden tussen entiteiten. Het delen van informatie draagt bij aan een grotere bewustwording van cyberbedreigingen, wat op zijn beurt het vermogen van de entiteiten om te voorkomen dat bedreigingen tot echte incidenten leiden, vergroot en de entiteiten in staat stelt om de effecten van incidenten beter te beheersen en efficiënter te herstellen. Bij gebrek aan richtsnoeren op het niveau van de Unie lijken verschillende factoren een dergelijke uitwisseling van inlichtingen te hebben afgeremd, met name de onzekerheid over de verenigbaarheid met de mededingings- en aansprakelijkheidsregels.

(68) Entiteiten moeten worden aangemoedigd om hun individuele kennis en praktische ervaring op strategisch, tactisch en operationeel niveau collectief te benutten om hun capaciteiten te vergroten om cyberbedreigingen adequaat te beoordelen, te monitoren, zich ertegen te verdedigen en ze te bestrijden. Het is dus noodzakelijk om op het niveau van de Unie mechanismen voor vrijwillige informatie-uitwisseling mogelijk te maken. Daarom moeten de lidstaten ook relevante entiteiten die niet onder het toepassingsgebied van deze richtlijn vallen, actief ondersteunen en aanmoedigen om deel te nemen aan dergelijke mechanismen voor informatie-uitwisseling. Deze mechanismen moeten worden uitgevoerd met volledige inachtneming van de

mededingingsregels van de Unie en de regels van het recht van de Unie inzake gegevensbescherming.

(69) De verwerking van persoonsgegevens, voor zover strikt noodzakelijk en evenredig met het oog op de netwerk- en informatiebeveiliging, door entiteiten, overheidsinstanties, CERT's, CSIRT's en aanbieders van beveiligingstechnologieën en -diensten moet een rechtmatig belang van de betrokken verwerkingsverantwoordelijke vormen, zoals bedoeld in Verordening (EU) nr. 2016/679. Dit omvat maatregelen met betrekking tot de preventie, opsporing en analyse van incidenten en de reactie erop, maatregelen om het bewustzijn met betrekking tot specifieke cyberbedreigingen te vergroten, uitwisseling van informatie in het kader van herstel van de kwetsbaarheid en gecoördineerde openbaarmaking, alsmede de vrijwillige uitwisseling van informatie over deze incidenten, alsmede over cyberbedreigingen en kwetsbaarheden, indicatoren voor aantasting, tactieken, technieken en procedures, cyberbeveiligingswaarschuwingen en configuratiehulpmiddelen. Dergelijke maatregelen kunnen de verwerking van de volgende soorten persoonsgegevens vereisen: IP-adressen, uniforme resources locators (URL's), domeinnamen en e-mailadressen.

(70) Ter versterking van de toezichtsbevoegdheden en -maatregelen die bijdragen tot een doeltreffende naleving, moet deze richtlijn voorzien in een minimumlijst van toezichtsmaatregelen en -middelen waarmee de bevoegde autoriteiten toezicht kunnen houden op essentiële en belangrijke entiteiten. Bovendien moet deze richtlijn een onderscheid maken tussen de toezichtsregeling voor essentiële en voor belangrijke entiteiten, teneinde te zorgen voor een billijk evenwicht tussen de verplichtingen voor zowel de entiteiten als de bevoegde autoriteiten. Zo moeten essentiële entiteiten aan een volwaardig toezichtsstelsel (vooraf en achteraf) worden onderworpen, terwijl belangrijke entiteiten aan een licht toezichtsstelsel, uitsluitend achteraf, moeten worden onderworpen. Voor deze laatste categorie betekent dit dat belangrijke entiteiten niet systematisch de naleving van de vereisten inzake risicobeheer voor cyberbeveiliging moeten documenteren, terwijl de bevoegde autoriteiten een reactieve benadering achteraf van het toezicht moeten toepassen en dus geen algemene verplichting hebben om toezicht te houden op die entiteiten.

(71) Om de handhaving doeltreffend te maken, moet er een minimumlijst van administratieve sancties voor inbreuken op de bij deze richtlijn vastgestelde verplichtingen inzake risicobeheer en rapportage op het gebied van cyberbeveiliging worden vastgesteld, waarbij een duidelijk en samenhangend kader voor dergelijke sancties in de hele Unie moet worden opgezet. Er moet terdege rekening worden gehouden met de aard, de ernst en de duur van de inbreuk, de daadwerkelijk veroorzaakte schade of geleden verliezen of de potentiële schade of verliezen die hadden kunnen worden veroorzaakt, het opzettelijke of nalatige karakter van de inbreuk, de maatregelen die zijn genomen om de geleden schade en/of verliezen te voorkomen of te beperken, de mate van verantwoordelijkheid of eventuele relevante eerdere inbreuken, de mate van samenwerking met de bevoegde instantie en elke andere verzwarende of verzachtende omstandigheid. Het opleggen van sancties, met inbegrip van administratieve boeten, moet worden onderworpen aan passende procedurele waarborgen overeenkomstig de algemene beginselen van het recht van de Unie en het Handvest van de grondrechten van de Europese Unie, met inbegrip van een doeltreffende rechtsbescherming en een eerlijke rechtsgang.

(72) Met het oog op een doeltreffende handhaving van de in deze richtlijn vastgestelde verplichtingen moet elke bevoegde autoriteit de bevoegdheid hebben om

administratieve boeten op te leggen of te verzoeken om het opleggen van dergelijke boeten.

(73) Wanneer aan een onderneming administratieve geldboeten worden opgelegd, moet een onderneming voor die doeleinden worden opgevat als een onderneming in de zin van de artikelen 101 en 102 VWEU. Wanneer administratieve boeten worden opgelegd aan personen die geen onderneming zijn, moet de toezichthoudende autoriteit bij het bepalen van het passende bedrag van de boete rekening houden met het algemene inkomensniveau in de lidstaat en met de economische situatie van de persoon. Het is aan de lidstaten om te bepalen of en in welke mate overheidsinstanties aan administratieve boeten moeten worden onderworpen. Het opleggen van een administratieve boete doet geen afbreuk aan de toepassing van andere bevoegdheden van de bevoegde autoriteiten of van andere sancties die zijn vastgesteld in de nationale voorschriften tot omzetting van deze richtlijn.

(74) De lidstaten moeten de mogelijkheid hebben om de regels inzake strafrechtelijke sancties voor inbreuken op de interne voorschriften tot omzetting van deze richtlijn vast te stellen. Het opleggen van strafrechtelijke sancties voor inbreuken op dergelijke interne regels en van daarmee samenhangende administratieve sancties mag echter niet leiden tot een inbreuk op het “ne bis in idem”-beginsel, zoals geïnterpreteerd door het Hof van Justitie.

(75) Wanneer deze richtlijn niet voorziet in de harmonisatie van administratieve sancties of, indien nodig, in andere gevallen, bijvoorbeeld bij ernstige inbreuken op de in deze richtlijn vastgelegde verplichtingen, moeten de lidstaten een systeem toepassen dat voorziet in doeltreffende, evenredige en afschrikkende sancties. De aard van deze strafrechtelijke of bestuursrechtelijke sancties moet door de wetgeving van de lidstaten worden bepaald.

(76) Om de doeltreffendheid en het afschrikkingseffect van de sancties die van toepassing zijn op inbreuken op de uit hoofde van deze richtlijn vastgestelde verplichtingen verder te versterken, moeten de bevoegde instanties de bevoegdheid krijgen om sancties toe te passen die bestaan uit de opschorting van een certificering of vergunning voor een deel of het geheel van de door een essentiële entiteit verleende diensten en het opleggen van een tijdelijk verbod op de uitoefening van bestuursfuncties door een natuurlijke persoon. Gezien de ernst en het effect ervan op de activiteiten van de entiteiten en uiteindelijk op hun consumenten, mogen dergelijke sancties alleen worden toegepast in verhouding tot de ernst van de inbreuk en rekening houdend met de specifieke omstandigheden van elk geval, met inbegrip van het opzettelijke of nalatige karakter van de inbreuk, de maatregelen die zijn genomen om de geleden schade en/of verliezen te voorkomen of te beperken. Dergelijke sancties mogen alleen worden toegepast als ultiem middel, met andere woorden alleen nadat de andere relevante handhavingsacties waarin deze richtlijn voorziet, zijn uitgeput, en alleen totdat de entiteiten waarop zij van toepassing zijn, de nodige maatregelen nemen om de tekortkomingen te verhelpen of te voldoen aan de vereisten van de bevoegde autoriteit waarvoor dergelijke sancties zijn opgelegd. Het opleggen van dergelijke sancties moet worden onderworpen aan passende procedurele waarborgen overeenkomstig de algemene beginselen van het recht van de Unie en het Handvest van de grondrechten van de Europese Unie, met inbegrip van een doeltreffende rechtsbescherming, een eerlijke rechtsgang, het vermoeden van onschuld en de rechten van de verdediging.

(77) In deze richtlijn moeten overeenkomstig Verordening (EU) nr. 2016/679 regels worden vastgesteld voor de samenwerking tussen de bevoegde autoriteiten en de toezichthoudende autoriteiten bij de behandeling van inbreuken in verband met persoonsgegevens.

(78) Deze richtlijn moet gericht zijn op het waarborgen van een hoge mate van verantwoordelijkheid voor de risicobeheersmaatregelen en rapportageverplichtingen op het gebied van cyberbeveiliging op het niveau van de organisaties. Om deze redenen moeten de beheersorganen van de entiteiten die onder het toepassingsgebied van deze richtlijn vallen, de maatregelen inzake cyberbeveiligingsrisico's goedkeuren en toezicht houden op de uitvoering ervan.

(79) Er moet een mechanisme van collegiale toetsing worden ingevoerd, dat het mogelijk maakt de uitvoering van het cyberbeveiligingsbeleid te laten beoordelen door deskundigen die door de lidstaten zijn aangewezen, met inbegrip van het niveau van de capaciteiten en de beschikbare middelen van de lidstaten.

(80) Om rekening te houden met nieuwe cyberbedreigingen, technologische ontwikkelingen of specifieke kenmerken van de sector, moet de bevoegdheid om handelingen vast te stellen overeenkomstig artikel 290 VWEU aan de Commissie worden gedelegeerd ten aanzien van de elementen met betrekking tot de bij deze richtlijn vereiste risicobeheersmaatregelen. De Commissie moet ook de bevoegdheid krijgen om gedelegeerde handelingen vast te stellen waarin wordt bepaald welke categorieën van essentiële entiteiten verplicht zijn om een certificaat te verkrijgen en onder welke specifieke Europese certificeringsregelingen inzake cyberbeveiliging. Het is van bijzonder belang dat de Commissie tijdens haar voorbereidende werkzaamheden passende raadplegingen houdt, onder meer op deskundigenniveau, en dat deze raadplegingen plaatsvinden overeenkomstig de beginselen die zijn vastgelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven[26]. Met name om te zorgen voor een gelijke deelname aan de voorbereiding van gedelegeerde handelingen, ontvangen het Europees Parlement en de Raad alle documenten op hetzelfde moment als de deskundigen van de lidstaten en hebben hun deskundigen systematisch toegang tot de vergaderingen van de deskundigengroepen van de Commissie die zich bezighouden met de voorbereiding van de gedelegeerde handelingen.

(81) Om te zorgen voor uniforme voorwaarden voor de uitvoering van de relevante bepalingen van deze richtlijn betreffende de procedurele regelingen die nodig zijn voor het functioneren van de samenwerkingsgroep, de technische elementen met betrekking tot de risicobeheersmaatregelen of het soort informatie, het formaat en de procedure voor de melding van incidenten, moeten aan de Commissie uitvoeringsbevoegdheden worden toegekend. Deze bevoegdheden moeten worden uitgeoefend overeenkomstig Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad[27]

(82) De Commissie moet deze richtlijn op gezette tijden herzien, in overleg met de betrokken partijen, met name om vast te stellen of er wijzigingen nodig zijn in het licht van veranderingen in de maatschappelijke, politieke, technologische of marktomstandigheden.

---

[26] PB L 123 van 12.5.2016, blz. 1.

[27] Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren (PB L 55 van 28.2.2011, blz. 13).

(83) Aangezien de doelstelling van deze richtlijn, namelijk het bereiken van een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie, niet voldoende door de lidstaten kan worden verwezenlijkt, maar vanwege de gevolgen van het optreden beter op het niveau van de Unie kan worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie vastgestelde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel vastgestelde evenredigheidsbeginsel gaat deze richtlijn niet verder dan nodig is om deze doelstelling te verwezenlijken.

(84) Deze richtlijn eerbiedigt de grondrechten en neemt de beginselen in acht die zijn erkend in het Handvest van de grondrechten van de Europese Unie, met name het recht op eerbiediging van het privéleven en van de communicatie, de bescherming van persoonsgegevens, de vrijheid van ondernemerschap, het recht op eigendom, het recht op een doeltreffende voorziening in rechte en het recht om te worden gehoord. Deze richtlijn moet worden uitgevoerd overeenkomstig deze rechten en beginselen,

HEBBEN DEZE RICHTLIJN VASTGESTELD:

HOOFDSTUK I

Algemene bepalingen

Artikel 1

Onderwerp

1. In deze richtlijn worden maatregelen vastgesteld om een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie te waarborgen.

2. Met het oog hierop worden in deze richtlijn:

(a) verplichtingen voor de lidstaten vastgesteld om nationale strategieën voor cyberbeveiliging vast te stellen en om bevoegde nationale autoriteiten, centrale contactpunten en computer security incident response teams (CSIRT's) aan te wijzen;

b) verplichtingen vastgesteld inzake risicobeheer en rapportage op het gebied van cyberbeveiliging voor entiteiten van een type dat in bijlage I wordt aangeduid als essentiële entiteiten en in bijlage II als belangrijke entiteiten;

(c) verplichtingen vastgesteld met betrekking tot het delen van informatie op het gebied van cyberbeveiliging.

Artikel 2

Toepassingsgebied

1. Deze richtlijn is van toepassing op openbare en particuliere entiteiten van een type dat in bijlage I als essentiële entiteiten en in bijlage II als belangrijke entiteiten wordt aangeduid. Deze richtlijn is niet van toepassing op entiteiten die kunnen worden

gekwalificeerd als micro- en kleine ondernemingen in de zin van Aanbeveling 2003/361/EG van de Commissie.[28]

2. Deze richtlijn is echter, ongeacht hun omvang, ook van toepassing op de in de bijlagen I en II bedoelde entiteiten, wanneer:

(a) de diensten worden verleend door een van de volgende entiteiten:

i) de in punt 8 van bijlage I bedoelde openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten;

ii) de in punt 8 van bijlage I bedoelde aanbieders van vertrouwensdiensten;

iii) de in punt 8 van bijlage I bedoelde registers voor topleveldomeinnamen en DNS-dienstverleners;

b) de entiteit een overheidsinstantie is zoals gedefinieerd in artikel 4, punt 23;

c) de entiteit de enige aanbieder van een dienst in een lidstaat is;

d) een mogelijke verstoring van de dienstverlening door de entiteit gevolgen kan hebben voor de openbare veiligheid, de openbare beveiliging of de volksgezondheid;

e) een mogelijke verstoring van de dienstverlening door de entiteit systeemrisico's met zich mee kan brengen, met name voor de sectoren waar een dergelijke verstoring een grensoverschrijdende impact kan hebben;

f) de entiteit kritiek is vanwege het specifieke belang ervan op regionaal of nationaal niveau voor de specifieke sector of het specifieke type dienst, of voor andere onderling afhankelijke sectoren in de lidstaat;

g) de entiteit wordt geïdentificeerd als een kritieke entiteit overeenkomstig Richtlijn (EU) XXXX/XXXX van het Europees Parlement en de Raad[29] [Richtlijn inzake de veerkracht van kritieke entiteiten], of als een entiteit die gelijkwaardig is aan een kritieke entiteit overeenkomstig artikel 7 van die richtlijn.

De lidstaten stellen een lijst van overeenkomstig de punten b) tot en met f) geïdentificeerde entiteiten op en dienen deze uiterlijk [zes maanden na de uiterste datum voor omzetting] bij de Commissie in. De lidstaten herzien de lijst regelmatig, en vervolgens ten minste om de twee jaar, en werken deze zo nodig bij.

3. Deze richtlijn laat de bevoegdheden van de lidstaten inzake de handhaving van de openbare veiligheid, defensie en nationale veiligheid met inachtneming van het recht van de Unie onverlet.

4. Deze richtlijn is van toepassing onverminderd Richtlijn 2008/114/EG van de Raad[30], Richtlijn 2011/93/EU[31] en Richtlijn 2013/40/EU[32] van het Europees Parlement en de Raad.

---

28 Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PB L 124 van 20.5.2003, blz. 36).

29 *[voeg de volledige titel en de publicatiegegevens van het PB in wanneer deze bekend zijn]*

30 Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de

5. Onverminderd artikel 346 VWEU worden gegevens die krachtens de voorschriften van de Unie en de lidstaten vertrouwelijk zijn, zoals de voorschriften inzake het zakengeheim, alleen met de Commissie en andere betrokken autoriteiten uitgewisseld wanneer deze uitwisseling noodzakelijk is voor de toepassing van deze richtlijn. De uitgewisselde informatie blijft beperkt tot de informatie die relevant is en in verhouding staat tot het doel van die uitwisseling. Bij de uitwisseling van informatie wordt de vertrouwelijkheid van die informatie gewaarborgd en worden de veiligheids- en commerciële belangen van essentiële of belangrijke entiteiten beschermd.

6. Indien bepalingen van sectorspecifieke handelingen van het Unierecht voorschrijven dat essentiële of belangrijke entiteiten ofwel maatregelen voor risicobeheersing op het gebied van cyberbeveiliging moeten nemen, ofwel incidenten of significante cyberbedreigingen moeten melden, en indien deze eisen ten minste gelijkwaardig zijn aan de in deze richtlijn vastgestelde verplichtingen, zijn de relevante bepalingen van deze richtlijn, met inbegrip van de bepaling inzake toezicht en handhaving als bedoeld in hoofdstuk VI, niet van toepassing.

Artikel 3

Minimumharmonisatie

Onverminderd hun andere verplichtingen uit hoofde van het recht van de Unie kunnen de lidstaten in overeenstemming met deze richtlijn bepalingen vaststellen of handhaven die een hoger niveau van cyberbeveiliging waarborgen.

Artikel 4

Definities

Voor de toepassing van deze richtlijn gelden de volgende definities:

1) “netwerk- en informatiesysteem”:

   a) een elektronisch communicatienetwerk in de zin van artikel 2, lid 1, van Richtlijn (EU) 2018/1972;

   b) elk apparaat of elke groep van onderling verbonden of verwante apparaten, waarvan er een of meer, overeenkomstig een programma, een automatische verwerking van digitale gegevens uitvoeren;

---

beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren (PB L 345 van 23.12.2008, blz. 75).

31 Richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad (PB L 335 van 17.12.2011, blz. 1).

32 Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (PB L 218, van 14.8.2013, blz. 8).

c) digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in punten a) en b) bedoelde elementen met het oog op de werking, het gebruik, de bescherming en het onderhoud ervan;

2) "beveiliging van netwerk- en informatiesystemen": het vermogen van netwerk- en informatiesystemen om op een bepaald niveau van vertrouwen weerstand te bieden aan elke handeling die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen of verzonden of verwerkte gegevens of de daarmee verband houdende diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar brengt;

3) "cyberbeveiliging": cyberbeveiliging in de zin van artikel 2, lid 1, van Verordening (EU) 2019/881 van het Europees Parlement en de Raad[33];

4) "nationale strategie inzake cyberbeveiliging": een samenhangend kader van een lidstaat met strategische doelstellingen en prioriteiten inzake de beveiliging van netwerk- en informatiesystemen in die lidstaat;

5) "incident": elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de daarmee verband houdende diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt;

6) "incidentenbehandeling": alle acties en procedures die gericht zijn op het opsporen, analyseren en indammen van en de respons op een incident;

7) "cyberbedreiging": een cyberbedreiging in de zin van artikel 2, lid 8, van Verordening (EU) 2019/881;

8) "kwetsbaarheid": een zwakheid, vatbaarheid of gebrek van een activum, systeem, proces of controle die door een cyberbedreiging kan worden uitgebuit;

9) "vertegenwoordiger": elke in de Unie gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om op te treden namens i) een DNS-dienstverlener, een register voor topleveldomeinnamen, een aanbieder van cloudcomputerdiensten, een aanbieder van datacentrumdiensten, een aanbieder van een netwerk voor de voor de levering van inhoud als bedoeld in punt 8 van bijlage I of ii) entiteiten als bedoeld in punt 6 van bijlage II die niet in de Unie zijn gevestigd en die door een nationale bevoegde autoriteit of een CSIRT kunnen worden aangesproken in plaats van de entiteit met betrekking tot de verplichtingen van die entiteit uit hoofde van deze richtlijn;

10) "norm": een norm in de zin van artikel 2, lid 1, van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad[34];

---

[33] 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).

[34] Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad (PB L 316 van 14.11.2012, blz. 12).

11) “technische specificatie”: een technische specificatie in de zin van artikel 2, lid 4, van Verordening (EU) nr. 1025/2012;

12) “internetuitwisselingspunt (IXP)”: een netwerkfaciliteit die de interconnectie van meer dan twee onafhankelijke netwerken (autonome systemen) mogelijk maakt, in de eerste plaats om de uitwisseling van internetverkeer te vergemakkelijken; een IXP biedt alleen interconnectie voor autonome systemen; een IXP vereist niet dat het internetverkeer dat tussen een paar deelnemende autonome systemen verloopt, via een derde autonoom systeem verloopt, noch dat het dat verkeer wijzigt of anderszins verstoort;

13) “domeinnaamsysteem (DNS)”: een hiërarchisch gedistribueerd naamgevingssysteem dat de eindgebruikers in staat stelt diensten en bronnen op het internet te bereiken;

14) “DNS-dienstverlener”: een entiteit die recursieve of gezaghebbende diensten op het gebied van domeinnaamomzetting verleent aan interneteindgebruikers en andere DNS-dienstverleners;

15) “register voor topleveldomeinnamen”: een entiteit waaraan een specifieke topleveldomeinnaam is gedelegeerd en die verantwoordelijk is voor het beheer van de topleveldomeinnaam, met inbegrip van de registratie van domeinnamen onder de topleveldomeinnaam en de technische exploitatie van de topleveldomeinnaam, met inbegrip van de exploitatie van de naamservers, het onderhoud van de databases en de verdeling van de zonebestanden van de topleveldomeinnaam over de naamservers;

16) “digitale dienst”: een dienst in de zin van artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad[35];

17) “elektronische marktplaats”: een digitale dienst in de zin van artikel 2, punt n), van Richtlijn 2005/29/EG van het Europees Parlement en de Raad[36];

18) “onlinezoekmachine”: een digitale dienst in de zin van artikel 2, lid 5, van Verordening (EU) 2019/1150 van het Europees Parlement en de Raad[37];

19) “cloudcomputerdienst”: een digitale dienst die administratie op aanvraag en brede toegang op afstand tot een schaalbare en elastische pool van gedeelde en gedistribueerde computerbronnen mogelijk maakt.

20) “datacentrumdienst”: een dienst die structuren, of groepen van structuren, omvat die bestemd zijn voor de gecentraliseerde accommodatie, de interconnectie en de exploitatie van informatietechnologie en netwerkapparatuur die diensten op het gebied van gegevensopslag, -verwerking en -transport aanbiedt, samen met alle faciliteiten en infrastructuren voor energiedistributie en omgevingscontrole.

---

35 Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij. (PB L 241 van 17.9.2015, blz. 1).

36 Richtlijn 2005/29/EG van het Europees Parlement en de Raad van 11 mei 2005 betreffende oneerlijke handelspraktijken van ondernemingen jegens consumenten op de interne markt en tot wijziging van Richtlijn 84/450/EEG van de Raad, Richtlijnen 97/7/EG, 98/27/EG en 2002/65/EG van het Europees Parlement en de Raad en van Verordening (EG) nr. 2006/2004 van het Europees Parlement en de Raad (“Richtlijn oneerlijke handelspraktijken”) (PB L 149 van 11.6.2005, blz. 22).

37 Verordening (EU) nr. 2019/1150 van het Europees Parlement en de Raad van 20 juni 2019 ter bevordering van billijkheid en transparantie voor zakelijke gebruikers van onlinetussenhandelsdiensten (PB L 186 van 11.7.2019, blz. 57).

21) “netwerk voor de levering van inhoud”: een netwerk van geografisch verspreide servers met het oog op een hoge beschikbaarheid, toegankelijkheid of snelle levering van digitale inhoud en diensten aan internetgebruikers ten behoeve van aanbieders van inhoud en diensten;

22) “platform voor socialenetwerkdiensten: een platform dat eindgebruikers in staat stelt zich met elkaar te verbinden, te delen, te ontdekken en met elkaar te communiceren via meerdere apparaten, en met name via chats, posts, video’s en aanbevelingen);

23) “overheidsinstantie”: een entiteit in een lidstaat die aan de volgende criteria voldoet:

(a) zij is opgericht om te voorzien in behoeften van algemeen belang en heeft geen industrieel of commercieel karakter;

(b) zij heeft rechtspersoonlijkheid;

(c) zij wordt grotendeels gefinancierd door de staat, de regionale overheid of andere publiekrechtelijke organen; of zij is onderworpen aan beheerstoezicht door deze overheden of organen; of zij heeft een bestuurs-, leidinggevend of toezichthoudend orgaan waarvan de leden voor meer dan de helft door de staat, de regionale overheden of andere publiekrechtelijke organen worden benoemd;

(d) zij heeft de bevoegdheid om administratieve of regelgevende besluiten tot natuurlijke of rechtspersonen te richten die van invloed zijn op hun rechten op het grensoverschrijdende verkeer van personen, goederen, diensten of kapitaal.

Overheidsinstanties die activiteiten uitvoeren op het gebied van openbare veiligheid, rechtshandhaving, defensie of nationale veiligheid zijn uitgesloten.

24) “entiteit”: elke natuurlijke of rechtspersoon die als zodanig is opgericht en erkend volgens het nationale recht van zijn vestigingsplaats, en die in eigen naam rechten kan uitoefenen en aan verplichtingen kan worden onderworpen;

25) “essentiële entiteit”: elke entiteit van een type dat in bijlage I wordt aangeduid als een essentiële entiteit;

26) “belangrijke entiteit”: elke entiteit van een type dat in bijlage II wordt aangeduid als een belangrijke entiteit.

HOOFDSTUK II

Gecoördineerde regelgevende kaders op het gebied van cyberbeveiliging

Artikel 5

Nationale cyberbeveiligingsstrategie

1. Elke lidstaat moet een nationale cyberbeveiligingsstrategie vaststellen waarin de strategische doelstellingen en passende beleids- en regelgevingsmaatregelen worden gedefinieerd om een hoog niveau van cyberbeveiliging te bereiken en te handhaven. De nationale cyberbeveiligingsstrategie omvat met name de volgende zaken:

(a) een definitie van de doelstellingen en prioriteiten van de strategie van de lidstaten inzake cyberbeveiliging;

(b) een governancekader om deze doelstellingen en prioriteiten te verwezenlijken, met inbegrip van het in lid 2 bedoelde beleid en de taken en verantwoordelijkheden van overheidsorganen en -entiteiten en andere relevante actoren;

(c) een beoordeling om relevante activa en cyberbeveiligingsrisico's in die lidstaat vast te stellen;

(d) een inventarisatie van de maatregelen om te zorgen voor paraatheid, respons en herstel bij incidenten, met inbegrip van samenwerking tussen de openbare en de particuliere sector;

(e) een lijst van de verschillende autoriteiten en actoren die betrokken zijn bij de uitvoering van de nationale cyberbeveiligingsstrategie;

(f) een beleidskader voor een betere coördinatie tussen de bevoegde autoriteiten in het kader van deze richtlijn en Richtlijn (EU) XXXX/XXXX van het Europees Parlement en de Raad[38] [richtlijn betreffende de veerkracht van kritieke entiteiten] met het oog op de uitwisseling van informatie over incidenten en cyberbedreigingen en de uitoefening van toezichthoudende taken.

2. In het kader van de nationale strategie inzake cyberbeveiliging stellen de lidstaten met name het volgende beleid vast:

a) een beleid dat gericht is op cyberbeveiliging in de toeleveringsketen voor ICT-producten en -diensten die door essentiële en belangrijke entiteiten worden gebruikt voor het verlenen van hun diensten;

b) richtsnoeren voor het opnemen en specificeren van aan cyberbeveiliging gerelateerde eisen voor ICT-producten en -diensten in overheidsopdrachten;

c) een beleid ter bevordering en vergemakkelijking van een gecoördineerde bekendmaking van de kwetsbaarheid in de zin van artikel 6;

d) een beleid met betrekking tot het in stand houden van de algemene beschikbaarheid en integriteit van de openbare kern van het open internet;

e) een beleid ter bevordering en ontwikkeling van vaardigheden op het gebied van cyberbeveiliging, bewustmaking en initiatieven op het gebied van onderzoek en ontwikkeling;

f) een beleid ter ondersteuning van academische en onderzoeksinstellingen bij de ontwikkeling van instrumenten voor cyberbeveiliging en een veilige netwerkinfrastructuur;

g) een beleid, relevante procedures en passende instrumenten voor het delen van informatie ter ondersteuning van de vrijwillige uitwisseling van informatie op het gebied van cyberbeveiliging tussen bedrijven in overeenstemming met het recht van de Unie;

h) een beleid dat gericht is op de specifieke behoeften van kmo's, met name die welke zijn uitgesloten van het toepassingsgebied van deze richtlijn, met betrekking tot begeleiding en ondersteuning bij het verbeteren van hun weerbaarheid tegen bedreigingen van de cyberbeveiliging.

[38] *[voeg de volledige titel en de publicatiegegevens van het PB in wanneer deze bekend zijn]*

3. De lidstaten stellen de Commissie binnen drie maanden na de goedkeuring ervan in kennis van hun nationale cyberbeveiligingsstrategieën. De lidstaten kunnen specifieke informatie van de melding uitsluiten indien en voor zover dit strikt noodzakelijk is om de nationale veiligheid te waarborgen.

4. De lidstaten beoordelen hun nationale cyberbeveiligingsstrategieën ten minste om de vier jaar op basis van kernprestatie-indicatoren en wijzigen deze waar nodig. Het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) helpt de lidstaten op verzoek bij de ontwikkeling van een nationale strategie en van kernprestatie-indicatoren voor de beoordeling van de strategie.

Artikel 6

Gecoördineerde bekendmaking van de kwetsbaarheid en een Europees kwetsbaarheidsregister

1. Elke lidstaat wijst een van zijn CSIRT's als bedoeld in artikel 9 aan als coördinator met het oog op een gecoördineerde bekendmaking van de kwetsbaarheid. Het aangewezen CSIRT treedt op als een betrouwbare tussenpersoon en vergemakkelijkt, waar nodig, de interactie tussen de verslagleggende entiteit en de fabrikant of aanbieder van ICT-producten of -diensten. Wanneer de gemelde kwetsbaarheid betrekking heeft op meerdere fabrikanten of aanbieders van ICT-producten of -diensten in de Unie, werkt het aangewezen CSIRT van elke betrokken lidstaat samen met het CSIRT-netwerk.

2. Het Enisa ontwikkelt en onderhoudt een Europees kwetsbaarheidsregister. Daartoe stelt het Enisa de passende informatiesystemen, beleidsmaatregelen en procedures vast en onderhoudt deze, met name om belangrijke en essentiële entiteiten en hun leveranciers van netwerk- en informatiesystemen in staat te stellen de in ICT-producten of ICT-diensten aanwezige kwetsbaarheden bekend te maken en te registreren, en om alle belanghebbende partijen toegang te verlenen tot de informatie over de in het register opgenomen kwetsbaarheden. Het register bevat met name informatie over de kwetsbaarheid, het betrokken ICT-product of de betrokken ICT-diensten en de ernst van de kwetsbaarheid wat betreft de omstandigheden waaronder deze kan worden uitgebuit, de beschikbaarheid van gerelateerde patches en, bij gebrek aan beschikbare patches, richtsnoeren voor gebruikers van kwetsbare producten en diensten over de wijze waarop de risico's die voortvloeien uit bekendgemaakte kwetsbaarheden, kunnen worden beperkt.

Artikel 7

Nationale kaders voor crisisbeheer op het gebied van cyberbeveiliging

1. Elke lidstaat wijst een of meer bevoegde autoriteiten aan die verantwoordelijk zijn voor het beheer van grootschalige incidenten en crises. De lidstaten zorgen ervoor dat de bevoegde autoriteiten over voldoende middelen beschikken om de hun toegewezen taken doeltreffend en efficiënt uit te voeren.

2. Elke lidstaat stelt vast welke capaciteiten, middelen en procedures in geval van een crisis voor de toepassing van deze richtlijn kunnen worden ingezet.

3. Elke lidstaat stelt een nationaal plan voor incidenten en crisisrespons op het gebied van cyberbeveiliging vast waarin doelstellingen en modaliteiten voor het beheer van grootschalige incidenten en crises op het gebied van cyberbeveiliging zijn vastgelegd. In het plan wordt met name het volgende bepaald:

   a) doelstellingen van nationale paraatheidsmaatregelen en -activiteiten;

   b) de taken en verantwoordelijkheden van de nationale bevoegde autoriteiten;

   c) procedures voor crisisbeheer en kanalen voor de uitwisseling van informatie;

   d) paraatheidsmaatregelen, met inbegrip van oefeningen en opleidingsactiviteiten;

   e) de betrokken openbare en particuliere belanghebbenden en de betrokken infrastructuur;

   f) nationale procedures en regelingen tussen de betrokken nationale autoriteiten en instanties om de effectieve deelname van de lidstaat aan het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en -crises op het niveau van de Unie en de ondersteuning daarvan te waarborgen.

4. De lidstaten stellen de Commissie in kennis van de aanwijzing van hun bevoegde autoriteiten als bedoeld in lid 1 en dienen hun nationale responsplannen op het gebied van cyberbeveiligingsincidenten en -crises als bedoeld in lid 3 in binnen drie maanden na die aanwijzing en de goedkeuring van die plannen. De lidstaten kunnen specifieke informatie van het plan uitsluiten indien en voor zover dit strikt noodzakelijk is om hun nationale veiligheid te waarborgen.

Artikel 8

Nationale bevoegde autoriteiten en centrale contactpunten

1. Elke lidstaat wijst een of meer bevoegde autoriteiten aan die verantwoordelijk zijn voor cyberbeveiliging en voor de in hoofdstuk VI van deze richtlijn bedoelde toezichthoudende taken. De lidstaten kunnen daartoe een of meer bestaande instanties aanwijzen.

2. De in lid 1 bedoelde bevoegde autoriteiten houden toezicht op de toepassing van deze richtlijn op nationaal niveau.

3. Elke lidstaat wijst een nationaal centraal contactpunt voor cyberbeveiliging aan (“centraal contactpunt”). Wanneer een lidstaat slechts één bevoegde autoriteit aanwijst, is die bevoegde autoriteit ook het centrale contactpunt voor die lidstaat.

4. Elk centraal contactpunt oefent een verbindingsfunctie uit om de grensoverschrijdende samenwerking van de autoriteiten van zijn lidstaat met de relevante autoriteiten in andere lidstaten te waarborgen, alsmede om te zorgen voor sectoroverschrijdende samenwerking met andere bevoegde nationale autoriteiten binnen zijn lidstaat.

5. De lidstaten zien erop toe dat de in lid 1 bedoelde bevoegde autoriteiten en de centrale contactpunten over voldoende middelen beschikken om de hun toegewezen taken doeltreffend en efficiënt uit te voeren en aldus de doelstellingen van deze richtlijn te verwezenlijken. De lidstaten zorgen voor een doeltreffende, efficiënte en veilige samenwerking tussen de aangewezen vertegenwoordigers in de in artikel 12 bedoelde samenwerkingsgroep.

6. Elke lidstaat stelt de Commissie onverwijld in kennis van de aanwijzing van de in lid 1 bedoelde bevoegde autoriteit en het in lid 3 bedoelde centrale contactpunt, van hun taken en van elke latere wijziging daarvan. Elke lidstaat maakt de aanwijzing ervan bekend. De Commissie publiceert de lijst van de aangewezen centrale contactpunten.

Artikel 9

Computer security incident response teams (CSIRT's)

1. Elke lidstaat wijst een of meer CSIRT's aan die voldoen aan de vereisten van artikel 10, lid 1, en die ten minste de in de bijlagen I en II bedoelde sectoren, subsectoren of entiteiten bestrijken en verantwoordelijk zijn voor de incidentenbehandeling volgens een welbepaald proces. Een CSIRT kan worden ingesteld bij een bevoegde autoriteit als bedoeld in artikel 8.
2. De lidstaten zorgen ervoor dat elk CSIRT over voldoende middelen beschikt om zijn in artikel 10, lid 2, omschreven taken doeltreffend uit te voeren.
3. De lidstaten zorgen ervoor dat elk CSIRT over een passende, veilige en veerkrachtige communicatie- en informatie-infrastructuur beschikt om informatie uit te wisselen met essentiële en belangrijke entiteiten en andere relevante belanghebbende partijen. Daartoe zorgen de lidstaten ervoor dat de CSIRT's bijdragen aan de invoering van veilige instrumenten voor informatie-uitwisseling.
4. De CSIRT's werken samen en wisselen in voorkomend geval relevante informatie uit overeenkomstig artikel 26 met betrouwbare sectorale of sectoroverschrijdende gemeenschappen van essentiële en belangrijke entiteiten.
5. De CSIRT's nemen deel aan de overeenkomstig artikel 16 georganiseerde intercollegiale toetsingen.
6. De lidstaten zorgen voor een doeltreffende, efficiënte en veilige samenwerking van hun CSIRT's in het in artikel 13 bedoelde netwerk van CSIRT's.
7. De lidstaten stellen de Commissie onverwijld in kennis van de overeenkomstig lid 1 aangewezen CSIRT's, de overeenkomstig artikel 6, lid 1, aangewezen CSIRT-coördinator en hun respectieve taken met betrekking tot de in de bijlagen I en II bedoelde entiteiten.
8. De lidstaten kunnen bij de ontwikkeling van nationale CSIRT's de hulp van het Enisa inroepen.

Artikel 10

Eisen en taken van de CSIRT's

1. De CSIRT's voldoen aan de volgende eisen:
   a) de CSIRT's garanderen een hoge mate van beschikbaarheid van hun communicatiediensten door zwakke punten (single points of failure) te voorkomen en beschikken over diverse kanalen waarlangs te allen tijde contact met hen kan worden opgenomen en contact met anderen kan worden opgenomen. De communicatiekanalen worden voorts duidelijk gespecificeerd en meegedeeld aan de gebruikersgroep en de samenwerkingspartners;

b) de lokalen van CSIRT's en de ondersteunende informatiesystemen bevinden zich op beveiligde locaties;

c) de CSIRT's worden, met het oog op vlotte overdrachten, uitgerust met een adequaat systeem voor het beheren en routeren van verzoeken;

d) de CSIRT's krijgen voldoende personeel om een volcontinue beschikbaarheid te garanderen;

e) de CSIRT's zijn uitgerust met redundante systemen en reservewerkruimten om de continuïteit van hun diensten te waarborgen;

f) de CSIRT's hebben de mogelijkheid om deel te nemen aan internationale samenwerkingsnetwerken.

2. De CSIRT's hebben tot taak:

a) het monitoren van cyberbedreigingen, kwetsbaarheden en incidenten op nationaal niveau;

b) het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie onder essentiële en belangrijke entiteiten en aan andere belanghebbende partijen over cyberbedreigingen, kwetsbaarheden en incidenten;

c) de respons op incidenten;

d) het verstrekken van dynamische risico- en incidentenanalyses en situationeel bewustzijn met betrekking tot cyberbeveiliging;

e) het op verzoek van een entiteit proactief scannen van de netwerk- en informatiesystemen die voor de verlening van hun diensten worden gebruikt;

f) het deelnemen aan het CSIRT-netwerk en het verlenen van wederzijdse bijstand aan andere leden van het netwerk op hun verzoek.

3. De CSIRT's brengen samenwerkingsrelaties tot stand met relevante actoren in de particuliere sector, teneinde de doelstellingen van de richtlijn beter te verwezenlijken.

4. Om de samenwerking te vergemakkelijken, bevorderen de CSIRT's de invoering en het gebruik van gemeenschappelijke of gestandaardiseerde praktijken, classificatieschema's en taxonomieën met betrekking tot de volgende zaken:

a) procedures voor de incidentenbehandeling;

b) crisisbeheer op het gebied van cyberbeveiliging;

c) gecoördineerde bekendmaking van kwetsbaarheden.

Artikel 11

Samenwerking op nationaal niveau

1. Wanneer zij gescheiden zijn, werken de in artikel 8 bedoelde bevoegde autoriteiten, het centrale contactpunt en het (de) CSIRT(’s) van dezelfde lidstaat met elkaar samen om de in deze richtlijn vastgestelde verplichtingen na te komen.

2. De lidstaten zorgen ervoor dat ofwel hun bevoegde autoriteiten, ofwel hun CSIRT's meldingen ontvangen over incidenten en significante cyberbedreigingen en bijna-

ongelukken die uit hoofde van deze richtlijn worden ingediend. Wanneer een lidstaat besluit dat zijn CSIRT's die meldingen niet ontvangen, krijgen de CSIRT's, voor zover dat nodig is voor de uitvoering van hun taken, toegang tot gegevens over de door de essentiële of belangrijke entiteiten gemelde incidenten, overeenkomstig artikel 20.

3. Elke lidstaat zorgt ervoor dat zijn bevoegde autoriteiten of CSIRT's zijn centrale contactpunt in kennis stellen van meldingen van incidenten, significante cyberbedreigingen en bijna-ongelukken die op grond van deze richtlijn worden ingediend.

4. Voor zover dat nodig is om de in deze richtlijn vastgestelde taken en verplichtingen doeltreffend uit te voeren, zorgen de lidstaten voor passende samenwerking tussen de bevoegde autoriteiten en de centrale contactpunten en de rechtshandhavingsautoriteiten, de gegevensbeschermingsautoriteiten en de autoriteiten die krachtens Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten] verantwoordelijk zijn voor kritieke infrastructuur en de nationale financiële autoriteiten die overeenkomstig Verordening (EU) XXXX/XXXX van het Europees Parlement en de Raad[39] [de DORA-verordening] in die lidstaat zijn aangewezen.

5. De lidstaten zorgen ervoor dat hun bevoegde autoriteiten regelmatig informatie verstrekken aan de overeenkomstig Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten] aangewezen bevoegde autoriteiten over cyberbeveiligingsrisico's, cyberbedreigingen en incidenten die van invloed zijn op essentiële entiteiten die overeenkomstig Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten] als kritiek zijn aangemerkt, of als entiteiten die gelijkwaardig zijn aan kritieke entiteiten, alsmede over de maatregelen die door de bevoegde autoriteiten zijn genomen naar aanleiding van deze risico's en incidenten.

HOOFDSTUK III

Samenwerking

Artikel 12

Samenwerkingsgroep

1. Om de strategische samenwerking en de uitwisseling van informatie tussen de lidstaten op het gebied van de toepassing van de richtlijn te ondersteunen en te vergemakkelijken, wordt er een samenwerkingsgroep opgericht.

2. De samenwerkingsgroep voert zijn taken uit op basis van de in lid 6 bedoelde tweejaarlijkse werkprogramma's.

3. De samenwerkingsgroep bestaat uit vertegenwoordigers van de lidstaten, de Commissie en het Enisa. De Europese Dienst voor extern optreden neemt als waarnemer deel aan de activiteiten van de samenwerkingsgroep. De Europese

[39] *[voeg de volledige titel en de publicatiegegevens van het PB in wanneer deze bekend zijn]*

toezichthoudende autoriteiten (ETA's) kunnen overeenkomstig artikel 17, lid 5, punt c), van Verordening (EU) XXXX/XXXX [de DORA-verordening] deelnemen aan de activiteiten van de samenwerkingsgroep.

Waar nodig kan de samenwerkingsgroep vertegenwoordigers van belanghebbenden uitnodigen om deel te nemen aan zijn werkzaamheden.

De Commissie verzorgt het secretariaat.

4. De samenwerkingsgroep heeft tot taak:

   a) richtsnoeren aan de bevoegde autoriteiten verstrekken met betrekking tot de omzetting en uitvoering van deze richtlijn;

   b) beste praktijken en informatie uitwisselen met betrekking tot de uitvoering van deze richtlijn, onder meer met betrekking tot cyberbedreigingen, incidenten, kwetsbaarheden, bijna-ongelukken, bewustmakingsinitiatieven, opleidingen, oefeningen en vaardigheden, capaciteitsopbouw en normen en technische specificaties;

   c) advies uitwisselen en samenwerken met de Commissie rond nieuwe beleidsinitiatieven op het gebied van cyberbeveiliging;

   d) advies uitwisselen en samenwerken met de Commissie rond ontwerpen van uitvoeringshandelingen of gedelegeerde handelingen van de Commissie die overeenkomstig deze richtlijn worden vastgesteld;

   e) beste praktijken en informatie uitwisselen met de betrokken instellingen, organen en instanties van de Unie;

   f) de verslagen van de in artikel 16, lid 7, bedoelde intercollegiale toetsing bespreken;

   g) de resultaten van de in artikel 34 bedoelde werkzaamheden van het gemeenschappelijk toezicht in grensoverschrijdende gevallen bespreken;

   h) strategische richtsnoeren aan het CSIRT-netwerk verstrekken over specifieke nieuwe kwesties;

   i) bijdragen tot de cyberbeveiligingscapaciteiten in de hele Unie door de uitwisseling van nationale ambtenaren te vergemakkelijken via een programma voor capaciteitsopbouw waarbij personeel van de bevoegde autoriteiten van de lidstaten of van de CSIRT's betrokken is;

   j) regelmatige gezamenlijke bijeenkomsten organiseren met particuliere belanghebbenden uit de hele Unie om de activiteiten van de groep te bespreken en input te verzamelen over nieuwe beleidsuitdagingen;

   k) de werkzaamheden in verband met cyberbeveiligingsoefeningen, met inbegrip van het werk van het Enisa, bespreken.

5. De samenwerkingsgroep kan het CSIRT-netwerk verzoeken om een technisch verslag over geselecteerde onderwerpen.

6. Uiterlijk ... [24 maanden na de datum van inwerkingtreding van deze richtlijn] en vervolgens om de twee jaar stelt de samenwerkingsgroep een werkprogramma op met betrekking tot de acties die moeten worden ondernomen om de doelstellingen en taken van de groep uit te voeren. Het tijdschema van het eerste programma dat in het kader van deze richtlijn wordt vastgesteld, wordt afgestemd op het tijdschema van het laatste in het kader van Richtlijn (EU) 2016/1148 vastgestelde programma.

7. De Commissie kan uitvoeringshandelingen vaststellen tot vaststelling van de voor de werking van de samenwerkingsgroep noodzakelijke procedurele regelingen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 37, lid 2, bedoelde onderzoeksprocedure.

8. De samenwerkingsgroep komt regelmatig en ten minste eenmaal per jaar bijeen met de krachtens Richtlijn (EU) XXXX/XXXX [richtlijn inzake de veerkracht van kritieke entiteiten] opgerichte groep voor de veerkracht van kritieke entiteiten om de strategische samenwerking en de uitwisseling van informatie te bevorderen.

Artikel 13

CSIRT-netwerk

1. Om bij te dragen aan de ontwikkeling van het vertrouwen en een snelle en doeltreffende operationele samenwerking tussen de lidstaten te bevorderen, wordt een netwerk van de nationale CSIRT's opgericht.

2. Het CSIRT-netwerk bestaat uit vertegenwoordigers van de lidstaten en van CERT-EU. De Commissie neemt als waarnemer deel aan het CSIRT-netwerk. Het Enisa verzorgt het secretariaat en ondersteunt de samenwerking tussen de CSIRT's actief.

3. Het CSIRT-netwerk heeft tot taak:

   (a) informatie over de capaciteiten van CSIRT's uitwisselen;

   (b) relevante informatie uitwisselen over incidenten, bijna-ongelukken, cyberbedreigingen, risico's en kwetsbaarheden;

   (c) op verzoek van een vertegenwoordiger van het CSIRT-netwerk die mogelijkerwijs door een incident wordt getroffen, informatie uitwisselen en bespreken met betrekking tot dat incident en de daarmee samenhangende cyberbedreigingen, risico's en kwetsbaarheden;

   (d) op verzoek van een vertegenwoordiger van het CSIRT-netwerk, een gecoördineerde respons op een incident dat binnen het rechtsgebied van die lidstaat is vastgesteld, bespreken en waar mogelijk uitvoeren;

   (e) steun verlenen aan de lidstaten bij de aanpak van grensoverschrijdende incidenten in het kader van deze richtlijn;

   (f) samenwerken met en bijstand verlenen aan de in artikel 6 bedoelde aangewezen CSIRT's met betrekking tot het beheer van de met meerdere partijen gecoördineerde openbaarmaking van kwetsbaarheden die van invloed zijn op meerdere fabrikanten of aanbieders van ICT-producten, ICT-diensten en ICT-processen die in verschillende lidstaten zijn gevestigd;

   (g) verdere vormen van operationele samenwerking bespreken en identificeren, ook met betrekking tot:

      i) categorieën van cyberbedreigingen en -incidenten;

      ii) vroegtijdige waarschuwingen;

      iii) wederzijdse bijstand;

      iv) beginselen en modaliteiten voor de coördinatie in verband met grensoverschrijdende risico's en incidenten;

v) bijdrage aan het nationale incident- en crisisresponsplan op het gebied van cyberbeveiliging als bedoeld in artikel 7, lid 3;

(h) de samenwerkingsgroep informeren over zijn activiteiten en over de verdere vormen van operationele samenwerking die op grond van punt g) worden besproken, waarbij zo nodig om richtsnoeren in dat verband wordt verzocht;

(i) de balans opmaken van cyberbeveiligingsoefeningen, ook van de door het Enisa georganiseerde oefeningen;

(j) op verzoek van een individuele CSIRT, de capaciteiten en de paraatheid van die CSIRT bespreken;

(k) samenwerken en informatie uitwisselen met regionale en uniale centra voor beveiligingsoperaties ("Security Operations Centres" — SOC's) om het gemeenschappelijk situationeel bewustzijn inzake incidenten en bedreigingen in de hele Unie te verbeteren;

(l) de verslagen bespreken van de in artikel 16, lid 7, bedoelde intercollegiale toetsing;

(m) richtsnoeren uitvaardigen om de convergentie van de operationele praktijken met betrekking tot de toepassing van de bepalingen van dit artikel inzake operationele samenwerking te vergemakkelijken.

4. Met het oog op de in artikel 35 bedoelde evaluatie en uiterlijk [24 maanden na de datum van inwerkingtreding van deze richtlijn], en vervolgens om de twee jaar, beoordeelt het CSIRT-netwerk de voortgang van de operationele samenwerking en stelt het een verslag op. In het verslag worden met name conclusies getrokken over de resultaten van de in artikel 16 bedoelde intercollegiale toetsingen met betrekking tot de nationale CSIRT's, met inbegrip van conclusies en aanbevelingen, die op grond van dit artikel worden uitgevoerd. Dit verslag wordt ook aan de samenwerkingsgroep voorgelegd.

5. Het CSIRT-netwerk stelt zijn eigen reglement van orde vast.

Artikel 14

Het Europese netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe)

1. Om het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en -crises op operationeel niveau te ondersteunen en te zorgen voor een regelmatige uitwisseling van informatie tussen de lidstaten en de instellingen, organen en agentschappen van de Unie, wordt hierbij het Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe) opgericht.

2. Het EU-CyCLONe bestaat uit de vertegenwoordigers van de overeenkomstig artikel 7 aangewezen autoriteiten voor crisisbeheer van de lidstaten, de Commissie en het Enisa. Het Enisa verzorgt het secretariaat van het netwerk en ondersteunt de veilige uitwisseling van informatie.

3. Het EU-CyCLONe heeft tot taak:

a) het niveau van de paraatheid verhogen bij het beheer van grootschalige incidenten en crises;

b) een gedeeld situationeel bewustzijn van relevante cyberbeveiligingsgebeurtenissen ontwikkelen;

c) grootschalige incidenten en crisisbeheer coördineren en de besluitvorming op politiek niveau met betrekking tot dergelijke incidenten en crises ondersteunen;

d) de in artikel 7, lid 2, bedoelde nationale cyberbeveiligingsincidenten en responsplannen bespreken.

4. Het EU-CyCLONe stelt zijn reglement van orde vast.

5. Het EU-CyCLONe brengt regelmatig verslag uit aan de samenwerkingsgroep over cyberbedreigingen, incidenten en trends, waarbij met name aandacht wordt besteed aan de gevolgen ervan voor essentiële en belangrijke entiteiten.

6. Het EU-CyCLONe werkt samen met het CSIRT-netwerk op basis van overeengekomen procedurele regelingen.

Artikel 15

Verslag over de stand van zaken op het gebied van de cyberbeveiliging in de Unie

1. Het Enisa stelt in samenwerking met de Commissie een tweejaarlijks verslag over de stand van zaken op het gebied van cyberbeveiliging in de Unie op. Het verslag bevat met name een beoordeling van het volgende:

(a) de ontwikkeling van cyberbeveiligingscapaciteiten in de hele Unie;

(b) de technische, financiële en personele middelen waarover de bevoegde autoriteiten en het cyberbeveiligingsbeleid beschikken, en de uitvoering van toezichtsmaatregelen en handhavingsacties in het licht van de resultaten van de in artikel 16 bedoelde intercollegiale toetsingen;

(c) een cyberbeveiligingsindex die voorziet in een geaggregeerde beoordeling van het rijpheidsniveau van de cyberbeveiligingscapaciteiten.

2. Het verslag bevat specifieke beleidsaanbevelingen voor het verhogen van het cyberbeveiligingsniveau in de Unie en een samenvatting van de bevindingen voor de specifieke periode uit de technische situatieverslagen inzake de EU-cyberbeveiliging van het Agentschap, die overeenkomstig artikel 7, lid 6, van Verordening (EU) nr. 2019/881 door het Enisa zijn opgesteld.

Artikel 16

Collegiale toetsingen

1. De Commissie stelt, na raadpleging van de samenwerkingsgroep en het Enisa, uiterlijk 18 maanden na de inwerkingtreding van deze richtlijn, de methodologie en de inhoud vast van een systeem van collegiale toetsing ter beoordeling van de doeltreffendheid van het cyberbeveiligingsbeleid van de lidstaten. De beoordelingen worden uitgevoerd door technisch deskundigen op het gebied van cyberbeveiliging, afkomstig uit andere lidstaten dan de geëvalueerde lidstaat, en hebben ten minste betrekking op de volgende zaken:

i) de doeltreffendheid van de uitvoering van de in de artikelen 18 en 20 bedoelde vereisten inzake het risicobeheer en de rapportageverplichtingen op het gebied van cyberbeveiliging;

ii) het niveau van de capaciteiten, met inbegrip van de beschikbare financiële, technische en personele middelen, en de doeltreffendheid van de uitoefening van de taken van de nationale bevoegde autoriteiten;

iii) de operationele capaciteit en de doeltreffendheid van de CSIRT's;

iv) de doeltreffendheid van de in artikel 34 bedoelde wederzijdse bijstand;

v) de doeltreffendheid van het in artikel 26 van deze richtlijn bedoelde kader voor de uitwisseling van informatie.

2. De methodologie omvat objectieve, niet-discriminerende, eerlijke en transparante criteria op basis waarvan de lidstaten deskundigen aanwijzen die in aanmerking komen om de collegiale toetsingen uit te voeren. Het Enisa en de Commissie wijzen deskundigen aan om als waarnemers deel te nemen aan de collegiale toetsingen. De Commissie stelt met de steun van het Enisa binnen de in lid 1 bedoelde methodologie een objectief, niet-discriminerend, eerlijk en transparant systeem vast voor de selectie en de willekeurige toewijzing van deskundigen voor elke collegiale toetsing.

3. De organisatorische aspecten van de intercollegiale toetsingen worden, met steun van het Enisa, vastgesteld door de Commissie en worden, na raadpleging van de samenwerkingsgroep, gebaseerd op criteria die zijn gedefinieerd in de in lid 1 bedoelde methodologie. De intercollegiale toetsingen beoordelen de in lid 1 bedoelde aspecten voor alle lidstaten en sectoren, met inbegrip van gerichte kwesties die specifiek zijn voor een of meer lidstaten of een of meer sectoren.

4. De intercollegiale toetsingen omvatten daadwerkelijke of virtuele bezoeken ter plaatse en uitwisselingen elders. Met het oog op het beginsel van goede samenwerking verstrekken de lidstaten die worden geëvalueerd, de aangewezen deskundigen de gevraagde informatie die nodig is voor de beoordeling van de geëvalueerde aspecten. Alle informatie die via de collegiale toetsing wordt verkregen, wordt uitsluitend voor dat doel gebruikt. De deskundigen die aan de collegiale toetsing deelnemen, maken geen gevoelige of vertrouwelijke informatie die zij in het kader van die toetsing hebben verkregen, bekend aan derden.

5. Na de evaluatie in een lidstaat worden dezelfde aspecten in die lidstaat niet meer aan een intercollegiale toetsing onderworpen gedurende de twee jaar die volgen op de afsluiting van een intercollegiale toetsing, tenzij de Commissie na overleg met het Enisa en de samenwerkingsgroep anders beslist.

6. De lidstaten zorgen ervoor dat elk risico van belangenconflicten met betrekking tot de aangewezen deskundigen onverwijld aan de andere lidstaten, de Commissie en het Enisa wordt gemeld.

7. Deskundigen die deelnemen aan collegiale toetsingen stellen verslagen op over de bevindingen en conclusies van de toetsingen. De verslagen worden ingediend bij de Commissie, de samenwerkingsgroep, het CSIRT-netwerk en het Enisa. De verslagen worden besproken in de samenwerkingsgroep en het CSIRT-netwerk. De verslagen kunnen worden gepubliceerd op de speciale website van de samenwerkingsgroep.

HOOFDSTUK IV

Verplichtingen inzake risicobeheer en rapportage op het gebied van cyberbeveiliging

AFDELING I

Risicobeheer en rapportage op het gebied van cyberbeveiliging

Artikel 17

Governance

1. De lidstaten zorgen ervoor dat de beheersorganen van essentiële en belangrijke entiteiten de door deze entiteiten genomen maatregelen voor het risicobeheer op het gebied van cyberbeveiliging goedkeuren om te voldoen aan artikel 18, toezicht houden op de uitvoering ervan en verantwoordelijk zijn voor de niet-naleving door de entiteiten van de verplichtingen uit hoofde van dit artikel.
2. De lidstaten zorgen ervoor dat de leden van het beheersorgaan regelmatig specifieke opleidingen volgen om voldoende kennis en vaardigheden te verwerven om risico's en beheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de activiteiten van de entiteit te kunnen opsporen en beoordelen.

Artikel 18

Maatregelen voor het beheer van cyberbeveiligingsrisico's

1. De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten passende en evenredige technische en organisatorische maatregelen nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten bij het verlenen van hun diensten gebruiken, te beheren. Rekening houdend met de stand van de techniek zorgen deze maatregelen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op het aanwezige risico.
2. De in lid 1 bedoelde maatregelen omvatten ten minste het volgende:
   (a) risicoanalyse en beleid inzake de beveiliging van informatiesystemen;
   (b) incidentenbehandeling (preventie en opsporing van en respons op incidenten);
   (c) bedrijfscontinuïteit en crisisbeheer;
   (d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar leveranciers of dienstverleners, zoals leveranciers van diensten op het gebied van gegevensopslag en -verwerking of beheerde beveiligingsdiensten;
   (e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
   (f) beleid en procedures (testen en audits) om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;

(g) het gebruik van cryptografie en encryptie.

3. De lidstaten zorgen ervoor dat de entiteiten, wanneer zij de in lid 2, punt d), bedoelde passende maatregelen overwegen, rekening houden met de specifieke kwetsbaarheden van elke leverancier en dienstverlener en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures.

4. De lidstaten zien erop toe dat wanneer een entiteit vaststelt dat haar diensten of taken niet in overeenstemming zijn met de in lid 2 vastgestelde eisen, zij onverwijld alle nodige corrigerende maatregelen neemt om de betrokken dienst in overeenstemming te brengen.

5. De Commissie kan uitvoeringshandelingen vaststellen om de technische en methodologische specificaties van de in lid 2 bedoelde elementen vast te stellen. Bij de voorbereiding van deze handelingen gaat de Commissie te werk volgens de in artikel 37, lid 2, bedoelde onderzoeksprocedure en volgt zij zoveel mogelijk de internationale en Europese normen en de relevante technische specificaties.

6. De Commissie is bevoegd overeenkomstig artikel 36 gedelegeerde handelingen vast te stellen ter aanvulling van de in lid 2 vastgestelde elementen om rekening te houden met nieuwe cyberbedreigingen, technologische ontwikkelingen of specifieke kenmerken van de sector.

Artikel 19

Gecoördineerde risicobeoordelingen van kritieke toeleveringsketens in de EU

1. De samenwerkingsgroep kan, in samenwerking met de Commissie en het Enisa, gecoördineerde beveiligingsrisicobeoordelingen van specifieke kritieke ICT-diensten, -systemen of producttoeleveringsketens uitvoeren, waarbij rekening wordt gehouden met technische en, indien van toepassing, niet-technische risicofactoren.

2. Na overleg met de samenwerkingsgroep en het Enisa stelt de Commissie vast welke specifieke kritieke ICT-diensten, -systemen of -producten aan de in lid 1 bedoelde gecoördineerde risicobeoordeling kunnen worden onderworpen.

Artikel 20

Rapportageverplichtingen

1. De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten de bevoegde autoriteiten of het CSIRT overeenkomstig de leden 3 en 4 onverwijld in kennis stellen van elk incident dat aanzienlijke gevolgen heeft voor de verlening van hun diensten. In voorkomend geval stellen deze entiteiten de ontvangers van hun diensten onverwijld in kennis van incidenten die een nadelige invloed kunnen hebben op de verlening van die dienst. De lidstaten zorgen ervoor dat deze entiteiten onder meer alle informatie rapporteren die de bevoegde autoriteiten of het CSIRT in staat stelt om eventuele grensoverschrijdende gevolgen van het incident te bepalen.

2. De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten de bevoegde autoriteiten of het CSIRT onverwijld in kennis stellen van elke significante

cyberbedreiging die deze entiteiten vaststellen en die tot een significant incident had kunnen leiden.

Indien van toepassing stellen deze entiteiten de ontvangers van hun diensten die mogelijkerwijs door een significante cyberbedreiging worden getroffen, zonder onnodige vertraging in kennis van de maatregelen of middelen die deze ontvangers kunnen nemen als antwoord op die bedreiging. In voorkomend geval stellen de entiteiten deze ontvangers ook zelf in kennis van de bedreiging. De melding mag de meldende entiteit niet aan een verhoogde aansprakelijkheid onderwerpen.

3. Een incident wordt als significant beschouwd als:

(a) het incident een aanzienlijke operationele verstoring of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken;

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

4. De lidstaten zorgen ervoor dat de betrokken entiteiten, voor de in lid 1 bedoelde melding bij de bevoegde autoriteiten of het CSIRT:

(a) zonder onnodige vertraging en in ieder geval binnen 24 uur nadat het incident bekend is geworden, een eerste melding indienen, waarin, indien van toepassing, wordt aangegeven of het incident vermoedelijk door een onwettige of kwaadwillige handeling is veroorzaakt;

(b) op verzoek van een bevoegde autoriteit of een CSIRT, een tussentijds verslag indienen over relevante updates van de situatie;

(c) uiterlijk één maand na de indiening van het in punt a) bedoelde verslag, een eindverslag indienen waarin ten minste het volgende is opgenomen:

i) een gedetailleerde beschrijving van het incident, 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.

De lidstaten bepalen dat de betrokken entiteit in naar behoren gemotiveerde gevallen en in overleg met de bevoegde autoriteiten of het CSIRT kan afwijken van de in de punten a) en c) vastgestelde termijnen.

5. De bevoegde nationale autoriteiten of het CSIRT verstrekken binnen 24 uur na ontvangst van de eerste melding als bedoeld in lid 4, punt a), een antwoord aan de meldende entiteit, met inbegrip van een eerste feedback over het incident en, op verzoek van de entiteit, richtsnoeren voor de uitvoering van mogelijke risicobeperkende maatregelen. Wanneer het CSIRT de in de lid 1 bedoelde melding niet heeft ontvangen, worden de richtsnoeren door de bevoegde autoriteit in samenwerking met het CSIRT verstrekt. Het CSIRT verleent aanvullende technische ondersteuning indien de betrokken entiteit daarom verzoekt. Wanneer wordt vermoed dat het incident van criminele aard is, geven de bevoegde nationale autoriteiten of het CSIRT ook richtsnoeren voor het melden van het incident aan de rechtshandhavingsinstanties.

6. In voorkomend geval, en met name wanneer het in lid 1 bedoelde incident betrekking heeft op twee of meer lidstaten, stelt de bevoegde autoriteit of het CSIRT de andere

getroffen lidstaten en het Enisa in kennis van het incident. Daarbij beschermen de bevoegde autoriteiten, de CSIRT's en de centrale contactpunten, in overeenstemming met het recht van de Unie of de nationale wetgeving die in overeenstemming is met het recht van de Unie, de beveiligings- en commerciële belangen van de entiteit, alsmede de vertrouwelijkheid van de verstrekte informatie.

7. Wanneer publieke bewustmaking nodig is om een incident te voorkomen of een lopend incident aan te pakken, of wanneer de bekendmaking van het incident anderszins in het algemeen belang is, kunnen de bevoegde autoriteit of het CSIRT, en in voorkomend geval de autoriteiten of de CSIRT's van andere betrokken lidstaten, na raadpleging van de betrokken entiteit, het publiek over het incident informeren of van de entiteit verlangen dat zij dit doet.

8. Op verzoek van de bevoegde autoriteit of het CSIRT stuurt het centrale contactpunt de overeenkomstig de leden 1 en 2 ontvangen meldingen door naar de centrale contactpunten van de andere betrokken lidstaten.

9. Het centrale contactpunt dient maandelijks bij het Enisa een samenvattend verslag in met geanonimiseerde en geaggregeerde gegevens over incidenten, significante cyberbedreigingen en bijna-ongelukken die overeenkomstig de leden 1 en 2 en overeenkomstig artikel 27 zijn gemeld. Om bij te dragen tot het verstrekken van vergelijkbare informatie kan het Enisa technische richtsnoeren geven over de parameters van de informatie in het samenvattend verslag.

10. De bevoegde autoriteiten verstrekken de overeenkomstig Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten] aangewezen bevoegde autoriteiten informatie over incidenten en cyberbedreigingen die overeenkomstig de leden 1 en 2 zijn gemeld door essentiële entiteiten die overeenkomstig Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten] zijn geïdentificeerd als kritieke entiteiten, of als entiteiten die gelijkwaardig zijn aan kritieke entiteiten.

11. De Commissie kan uitvoeringshandelingen vaststellen waarin het soort informatie, het formaat en de procedure van een overeenkomstig de leden 1 en 2 ingediende melding nader worden gespecificeerd. De Commissie kan ook uitvoeringshandelingen vaststellen om de gevallen waarin een incident als significant wordt beschouwd als bedoeld in lid 3, nader te specificeren. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 37, lid 2, bedoelde onderzoeksprocedure.

Artikel 21

Gebruik van Europese cyberbeveiligingscertificeringsregelingen

1. Om aan te tonen dat aan bepaalde eisen van artikel 18 wordt voldaan, kunnen de lidstaten eisen dat essentiële en belangrijke entiteiten bepaalde ICT-producten, ICT-diensten en ICT-processen certificeren in het kader van specifieke Europese cyberbeveiligingscertificeringsregelingen die op grond van artikel 49 van Verordening (EU) nr. 2019/881 zijn vastgesteld. De producten, diensten en processen die aan certificering onderworpen zijn, kunnen door een essentiële of belangrijke entiteit worden ontwikkeld of bij derden worden ingekocht.

2. De Commissie krijgt de bevoegdheid om gedelegeerde handelingen vast te stellen waarin wordt bepaald welke categorieën van essentiële entiteiten verplicht zijn om een certificaat te verkrijgen en in hoofde van welke specifieke Europese cyberbeveiligingscertificeringsregelingen overeenkomstig lid 1. De gedelegeerde handelingen worden vastgesteld overeenkomstig artikel 36.

3. De Commissie kan het Enisa verzoeken een potentiële regeling op te stellen overeenkomstig artikel 48, lid 2, van Verordening (EU) nr. 2019/881 in gevallen waarin geen passende Europese cyberbeveiligingscertificeringsregeling voor de toepassing van lid 2 beschikbaar is.

Artikel 22

Normalisatie

1. Om de convergente uitvoering van artikel 18, leden 1 en 2, te bevorderen, moedigen de lidstaten, zonder het gebruik van een bepaald type technologie op te leggen of te bevoordelen, het gebruik aan van Europese of internationaal aanvaarde normen en specificaties die relevant zijn voor de beveiliging van netwerk- en informatiesystemen.

2. Het Enisa stelt in samenwerking met de lidstaten adviezen en richtsnoeren op over de technische gebieden die in verband met lid 1 in aanmerking moeten worden genomen, alsmede over de reeds bestaande normen, met inbegrip van de nationale normen van de lidstaten, die het mogelijk maken deze gebieden te bestrijken.

Artikel 23

Databases van domeinnamen en registratiegegevens

1. Om bij te dragen aan de beveiliging, stabiliteit en veerkracht van het DNS zorgen de lidstaten ervoor dat de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, nauwkeurige en volledige domeinnaamregistratiegegevens verzamelen en bijhouden in een speciale databasefaciliteit met inachtneming van de EU-wetgeving inzake gegevensbescherming voor wat betreft gegevens die persoonsgegevens zijn.

2. De lidstaten zorgen ervoor dat de in lid 1 bedoelde databases met gegevens over de registratie van domeinnamen relevante informatie bevatten om de houders van de domeinnamen en de contactpunten die de domeinnamen onder de topleveldomeinnamen beheren, te identificeren en te contacteren.

3. De lidstaten zorgen ervoor dat de registers voor topleveldomeinnamen en de instanties die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, over beleidslijnen en procedures beschikken om ervoor te zorgen dat de databases juiste en volledige informatie bevatten. De lidstaten zorgen ervoor dat deze beleidslijnen en procedures openbaar worden gemaakt.

4. De lidstaten zorgen ervoor dat de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, zonder onnodige vertraging na de registratie van een domeinnaam, domeinregistratiegegevens die geen persoonsgegevens zijn, publiceren.

5. De lidstaten zorgen ervoor dat de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, op rechtmatige en naar behoren gemotiveerde verzoeken van legitieme toegangvragende partijen toegang verlenen tot specifieke domeinnaamregistratiegegevens, met inachtneming van de gegevensbeschermingswetgeving van de Unie. De lidstaten zorgen ervoor dat de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, alle verzoeken om toegang zonder onnodige vertraging beantwoorden. De lidstaten zorgen ervoor dat het beleid en de procedures voor de bekendmaking van dergelijke gegevens openbaar worden gemaakt.

AFDELING II

Jurisdictie en registratie

Artikel 24

Jurisdictie en territorialiteit

1. DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputerdiensten, aanbieders van datacentra en van netwerken voor de levering van inhoud als bedoeld in punt 8 van bijlage I, alsmede digitale aanbieders als bedoeld in punt 6 van bijlage II, worden geacht onder de jurisdictie te vallen van de lidstaat waar zij hun hoofdvestiging in de Unie hebben.

2. Voor de toepassing van deze richtlijn worden de in lid 1 bedoelde entiteiten geacht hun hoofdvestiging in de Unie te hebben in de lidstaat waar de besluiten met betrekking tot de risicobeheersmaatregelen op het gebied van cyberbeveiliging worden genomen. Indien dergelijke besluiten in geen enkele vestiging in de Unie worden genomen, wordt de hoofdvestiging geacht zich te bevinden in de lidstaat waar de entiteiten de vestiging met het grootste aantal werknemers in de Unie hebben.

3. Indien een in lid 1 bedoelde entiteit niet in de Unie is gevestigd, maar diensten in de Unie aanbiedt, wijst zij een vertegenwoordiger in de Unie aan. De vertegenwoordiger is gevestigd in een van de lidstaten waar de diensten worden aangeboden. Deze entiteit wordt geacht onder de jurisdictie te vallen van de lidstaat waar de vertegenwoordiger is gevestigd. Bij ontstentenis van een aangewezen vertegenwoordiger binnen de Unie uit hoofde van dit artikel kan elke lidstaat waar de entiteit diensten verricht, gerechtelijke stappen ondernemen tegen de entiteit wegens niet-nakoming van de verplichtingen uit hoofde van deze richtlijn.

4. De aanwijzing van een vertegenwoordiger door een entiteit als bedoeld in lid 1 laat rechtsvorderingen die tegen de entiteit zelf kunnen worden ingesteld, onverlet.

Artikel 25

Register voor essentiële en belangrijke entiteiten

1. Het Enisa creëert en onderhoudt een register voor de in artikel 24, lid 1, bedoelde essentiële en belangrijke entiteiten. De entiteiten dienen uiterlijk [twaalf maanden na de inwerkingtreding van de richtlijn] de volgende informatie bij het Enisa in:

   (a) de naam van de entiteit;

   (b) het adres van haar hoofdvestiging en haar andere wettelijke vestigingen in de Unie of, indien deze niet in de Unie zijn gevestigd, van haar overeenkomstig artikel 24, lid 3, aangewezen vertegenwoordiger;

   (c) actuele contactgegevens, inclusief e-mailadressen en telefoonnummers van de entiteiten.

2. De in lid 1 bedoelde entiteiten stellen het Enisa onverwijld, en in ieder geval binnen drie maanden na de datum waarop de wijziging van kracht is geworden, in kennis van eventuele wijzigingen in de gegevens die zij op grond van lid 1 hebben ingediend.

3. Na ontvangst van de in lid 1 bedoelde informatie stuurt het Enisa deze door naar de centrale contactpunten, afhankelijk van de aangegeven locatie van de hoofdvestiging van elke entiteit of, indien deze niet in de Unie is gevestigd, van de aangewezen vertegenwoordiger van de entiteit. Wanneer een entiteit als bedoeld in lid 1 naast haar hoofdvestiging in de Unie nog andere vestigingen in andere lidstaten heeft, stelt het Enisa ook de centrale contactpunten van die lidstaten daarvan in kennis.

4. Wanneer een entiteit haar activiteiten niet binnen de in lid 1 gestelde termijn registreert of de relevante informatie niet verstrekt, is elke lidstaat waar de entiteit diensten verricht, bevoegd om ervoor te zorgen dat die entiteit de in deze richtlijn vastgestelde verplichtingen nakomt.

HOOFDSTUK V

Het delen van informatie

Artikel 26

Regelingen voor informatie-uitwisseling op het gebied van cyberbeveiliging

1. Onverminderd Verordening (EU) nr. 2016/679 zorgen de lidstaten ervoor dat essentiële en belangrijke entiteiten onderling relevante informatie over cyberbeveiliging kunnen uitwisselen, met inbegrip van informatie over cyberbedreigingen, kwetsbaarheden, indicatoren voor aantasting, tactieken, technieken en procedures, cyberbeveiligingswaarschuwingen en configuratiehulpmiddelen. Het delen van deze informatie:

   (a) heeft tot doel incidenten te voorkomen, op te sporen, te bestrijden of te beperken;

   (b) verhoogt het niveau van de cyberbeveiliging, met name door de bewustwording met betrekking tot cyberbedreigingen te vergroten, het vermogen dergelijke bedreigingen om zich te verspreiden, te beperken of te belemmeren, een reeks verdedigingscapaciteiten te ondersteunen, het herstel en

openbaarmaking van kwetsbaarheden, technieken voor het opsporen van bedreigingen, beperkingsstrategieën of respons- en herstelfasen.

2. De lidstaten zorgen ervoor dat de informatie-uitwisseling plaatsvindt binnen vertrouwde gemeenschappen van essentiële en belangrijke entiteiten. Deze uitwisseling wordt uitgevoerd door middel van regelingen voor de informatie-uitwisseling met betrekking tot de potentieel gevoelige aard van de gedeelde informatie en met inachtneming van de in lid 1 bedoelde regels van het recht van de Unie.

3. De lidstaten stellen regels vast waarin de procedure, de operationele elementen (met inbegrip van het gebruik van specifieke ICT-platforms), de inhoud en de voorwaarden van de in lid 2 bedoelde regelingen voor informatie-uitwisseling worden gespecificeerd. In deze regels worden ook de details van de betrokkenheid van de overheid bij dergelijke regelingen vastgelegd, alsmede de operationele elementen, met inbegrip van het gebruik van specifieke IT-platforms. De lidstaten bieden steun aan voor de toepassing van dergelijke regelingen overeenkomstig hun in artikel 5, lid 2, punt g), bedoelde beleid.

4. Essentiële en belangrijke entiteiten stellen de bevoegde autoriteiten in kennis van hun deelname aan de in lid 2 bedoelde regelingen voor informatie-uitwisseling wanneer zij dergelijke regelingen aangaan, of, indien van toepassing, van hun terugtrekking uit dergelijke regelingen, zodra de terugtrekking van kracht wordt.

5. In overeenstemming met het recht van de Unie ondersteunt het Enisa de invoering van de in lid 2 bedoelde regelingen voor informatie-uitwisseling op het gebied van cyberbeveiliging door het verstrekken van beste praktijken en richtsnoeren.

Artikel 27

Vrijwillige melding van relevante informatie

De lidstaten zorgen ervoor dat, onverminderd artikel 3, entiteiten die buiten het toepassingsgebied van deze richtlijn vallen, op vrijwillige basis meldingen kunnen doen van significante incidenten, cyberbedreigingen of bijna-ongelukken. Bij de verwerking van de meldingen handelen de lidstaten volgens de procedure van artikel 20. De lidstaten kunnen voorrang geven aan de verwerking van verplichte meldingen boven vrijwillige meldingen. Vrijwillige rapportage mag niet leiden tot het opleggen van bijkomende verplichtingen aan de rapporterende entiteit waaraan zij niet onderworpen zou zijn geweest indien zij de melding niet had ingediend.

HOOFDSTUK VI

Toezicht en handhaving

Artikel 28

Algemene aspecten van het toezicht en de handhaving

1. De lidstaten zorgen ervoor dat de bevoegde autoriteiten effectief toezicht houden op de naleving van deze richtlijn, en met name de verplichtingen van de artikelen 18 en 20, en nemen daartoe de nodige maatregelen.

2. De bevoegde autoriteiten werken nauw samen met de gegevensbeschermingsautoriteiten bij de aanpak van incidenten die leiden tot inbreuken in verband met persoonsgegevens.

Artikel 29

Toezicht en handhaving voor essentiële entiteiten

1. De lidstaten zorgen ervoor dat de toezichts- of handhavingsmaatregelen die met betrekking tot de in deze richtlijn vastgestelde verplichtingen aan essentiële entiteiten worden opgelegd, doeltreffend, evenredig en afschrikkend zijn, rekening houdend met de omstandigheden van elk afzonderlijk geval.

2. De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun toezichthoudende taken met betrekking tot essentiële entiteiten de bevoegdheid hebben om deze entiteiten te onderwerpen aan:

   a) inspecties ter plaatse en toezicht elders, met inbegrip van steekproefsgewijze controles;

   b) regelmatige audits;

   c) gerichte beveiligingsaudits op basis van risicobeoordelingen of beschikbare risicogerelateerde informatie;

   d) beveiligingsscans op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria;

   e) verzoeken om informatie die nodig is om de door de entiteit genomen cyberbeveiligingsmaatregelen te beoordelen, met inbegrip van gedocumenteerd cyberbeveiligingsbeleid, alsmede de naleving van de verplichting om het Enisa op grond van artikel 25, lid 1 en lid 2, in kennis te stellen;

   f) verzoeken om toegang tot gegevens, documenten of informatie die nodig zijn voor de uitoefening van hun toezichthoudende taken;

   g) verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen.

3. Bij de uitoefening van hun bevoegdheden uit hoofde van lid 2, punt e) tot en met g), vermelden de bevoegde autoriteiten het doel van het verzoek en de gevraagde informatie.

4. De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun handhavingsbevoegdheden ten aanzien van essentiële entiteiten, de bevoegdheid hebben om:

   (a) waarschuwingen te geven over de niet-naleving van de in deze richtlijn vastgestelde verplichtingen door de entiteiten;

   (b) bindende instructies te geven of een bevel uit te vaardigen waarin deze entiteiten worden verplicht de vastgestelde tekortkomingen of de inbreuken op de in deze richtlijn vastgestelde verplichtingen te verhelpen;

(c) deze entiteiten te gelasten een einde te maken aan gedragingen die niet in overeenstemming zijn met de in deze richtlijn vastgestelde verplichtingen en af te zien van herhaling van die gedragingen;

(d) deze entiteiten te gelasten hun risicobeheersmaatregelen en/of rapportageverplichtingen op een gespecificeerde wijze en binnen een gespecificeerde termijn in overeenstemming te brengen met de in de artikelen 18 en 20 vastgestelde verplichtingen;

(e) deze entiteiten te gelasten de natuurlijke of rechtspersonen aan wie zij diensten verlenen of voor wie zij activiteiten uitvoeren die mogelijkerwijs door een significante cyberbedreiging worden beïnvloed, in kennis te stellen van alle mogelijke beschermings- of herstelmaatregelen die door deze natuurlijke of rechtsperso(o)n(en) kunnen worden genomen als antwoord op die bedreiging;

(f) deze entiteiten te gelasten de naar aanleiding van een beveiligingsaudit gedane aanbevelingen binnen een redelijke termijn uit te voeren;

(g) een controlefunctionaris aan te wijzen die gedurende een bepaalde periode duidelijk omschreven taken heeft om toe te zien op de naleving van de in de artikelen 18 en 20 bedoelde verplichtingen;

(h) deze entiteiten te gelasten aspecten van niet-naleving van de in deze richtlijn vastgestelde verplichtingen op een bepaalde manier openbaar te maken;

(i) een openbare verklaring af te leggen waarin wordt aangegeven welke natuurlijke of rechtsperso(o)n(en) verantwoordelijk is/zijn voor de inbreuk van een in deze richtlijn vastgestelde verplichting en wat de aard van die inbreuk is;

(j) een administratieve geldboete op te leggen of de oplegging ervan door de bevoegde organen of rechtbanken overeenkomstig de nationale wetgeving te verzoeken overeenkomstig artikel 31 bovenop of in plaats van de in punten a) tot en met i) van dit lid bedoelde maatregelen, afhankelijk van de omstandigheden van elk afzonderlijk geval.

5. Indien de op grond van lid 4, punt a) tot en met d) en punt f), genomen handhavingsmaatregelen ondoeltreffend blijken te zijn, zorgen de lidstaten ervoor dat de bevoegde autoriteiten de bevoegdheid hebben om een termijn vast te stellen waarbinnen de essentiële entiteit wordt verzocht de nodige maatregelen te nemen om de tekortkomingen te verhelpen of aan de eisen van die autoriteiten te voldoen. Indien de gevraagde actie niet binnen de gestelde termijn wordt ondernomen, zorgen de lidstaten ervoor dat de bevoegde autoriteiten de bevoegdheid hebben om:

(a) een certificering of vergunning op te schorten of een certificerings- of vergunningsinstantie te verzoeken deze op te schorten met betrekking tot een deel of alle diensten of activiteiten die door een essentiële entiteit worden verleend;

(b) een tijdelijk verbod op te leggen of de oplegging ervan door de bevoegde organen of rechtbanken overeenkomstig de nationale wetgeving te verzoeken, aan personen met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur of de wettelijke vertegenwoordiger in die essentiële entiteit en aan andere natuurlijke personen die voor de inbreuk verantwoordelijk worden gehouden, om leidinggevende functies in die entiteit uit te oefenen.

Deze sancties worden alleen toegepast totdat de entiteit de nodige maatregelen neemt om de tekortkomingen te verhelpen of voldoet aan de vereisten van de bevoegde autoriteit waarvoor dergelijke sancties zijn opgelegd.

6. De lidstaten zorgen ervoor dat elke natuurlijke persoon die verantwoordelijk is voor of optreedt als vertegenwoordiger van een essentiële entiteit op basis van de bevoegdheid om deze te vertegenwoordigen, de bevoegdheid om namens deze entiteit beslissingen te nemen of de bevoegdheid om toezicht uit te oefenen op deze entiteit, de bevoegdheid heeft om ervoor te zorgen dat deze entiteit de in deze richtlijn vastgestelde verplichtingen nakomt. De lidstaten zorgen ervoor dat deze natuurlijke personen aansprakelijk kunnen worden gesteld voor het niet nakomen van hun verplichtingen om de in deze richtlijn vastgestelde verplichtingen na te komen.

7. Bij het nemen van handhavingsmaatregelen of het opleggen van sancties overeenkomstig de leden 4 en 5 eerbiedigen de bevoegde autoriteiten de rechten van de verdediging en houden zij rekening met de omstandigheden van elk afzonderlijk geval, en houden zij ten minste naar behoren rekening met:

   (a) de ernst van de inbreuk en het belang van de geschonden bepalingen. Tot de inbreuken die als ernstig moeten worden beschouwd, behoren: herhaalde inbreuken, het niet melden of verhelpen van incidenten met een significant verstorend effect, het niet verhelpen van tekortkomingen naar aanleiding van bindende instructies van de bevoegde autoriteiten, het belemmeren van audits of toezichtsactiviteiten waartoe de bevoegde autoriteit opdracht heeft gegeven naar aanleiding van de vaststelling van een inbreuk, het verstrekken van valse of zeer onnauwkeurige informatie met betrekking tot de in de artikelen 18 en 20 vastgestelde eisen inzake risicobeheer of rapportageverplichtingen.

   (b) de duur van de inbreuk, met inbegrip van het element van herhaalde inbreuken;

   (c) de daadwerkelijk veroorzaakte schade of geleden verliezen of de potentiële schade of verliezen die hadden kunnen worden veroorzaakt, voor zover deze kunnen worden vastgesteld. Bij de beoordeling van dit aspect wordt onder meer rekening gehouden met feitelijke of potentiële financiële of economische verliezen, effecten op andere diensten, aantal getroffen of mogelijk getroffen gebruikers;

   (d) het opzettelijke of nalatige karakter van de inbreuk;

   (e) maatregelen die door de entiteit worden genomen om de schade en/of verliezen te voorkomen of te beperken;

   (f) de naleving van goedgekeurde gedragscodes of goedgekeurde certificeringsmechanismen;

   (g) het niveau van samenwerking van de verantwoordelijke natuurlijke of rechtspersonen met de bevoegde autoriteiten.

8. De bevoegde autoriteiten geven een gedetailleerde motivering van hun handhavingsbesluiten. Alvorens dergelijke besluiten te nemen, stellen de bevoegde autoriteiten de betrokken entiteiten in kennis van hun voorlopige bevindingen en geven zij deze entiteiten een redelijke termijn om opmerkingen te maken.

9. De lidstaten zorgen ervoor dat hun bevoegde autoriteiten de relevante bevoegde autoriteiten van de betrokken lidstaat die zijn aangewezen overeenkomstig Richtlijn (EU) XXXX/XXXX [richtlijn inzake de veerkracht van kritieke entiteiten] in kennis stellen wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om

ervoor te zorgen dat een essentiële entiteit die op grond van Richtlijn (EU) XXXX/XXXX [richtlijn inzake de veerkracht van kritieke entiteiten] als kritieke entiteit of als met een kritieke entiteit gelijkgestelde entiteit wordt aangemerkt, voldoet aan de verplichtingen uit hoofde van deze richtlijn. Op verzoek van de bevoegde autoriteiten uit hoofde van Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten] kunnen de bevoegde autoriteiten hun toezichts- en handhavingsbevoegdheden uitoefenen ten aanzien van een essentiële entiteit die als kritiek of gelijkwaardig is aangemerkt.

Artikel 30

Toezicht en handhaving voor belangrijke entiteiten

1. Wanneer het bewijs of de aanwijzing wordt geleverd dat een belangrijke entiteit de in deze richtlijn, en met name in de artikelen 18 en 20, vastgestelde verplichtingen niet nakomt, zorgen de lidstaten ervoor dat de bevoegde autoriteiten zo nodig maatregelen nemen door middel van toezichtsmaatregelen achteraf.

2. De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun toezichthoudende taken met betrekking tot belangrijke entiteiten de bevoegdheid hebben om deze entiteiten te onderwerpen aan:

   (a) inspecties ter plaatse en toezicht elders achteraf;

   (b) gerichte beveiligingsaudits op basis van risicobeoordelingen of beschikbare risicogerelateerde informatie;

   (c) beveiligingsscans op basis van objectieve, eerlijke en transparante risicobeoordelingscriteria;

   (d) verzoeken om alle informatie die nodig is om achteraf de cyberbeveiligingsmaatregelen te beoordelen, met inbegrip van gedocumenteerd cyberbeveiligingsbeleid, alsmede de naleving van de verplichting om het Enisa op grond van artikel 25, leden 1 en 2, in kennis te stellen;

   (e) verzoeken om toegang tot gegevens, documenten of/of informatie die nodig zijn voor de uitoefening van hun toezichthoudende taken;

3. Bij de uitoefening van hun bevoegdheden uit hoofde van lid 2, punten e) tot en met g), vermelden de bevoegde autoriteiten het doel van het verzoek en de gevraagde informatie.

4. De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun handhavingsbevoegdheden ten aanzien van belangrijke entiteiten, de bevoegdheid hebben om:

   (a) waarschuwingen te geven over de niet-naleving van de in deze richtlijn vastgestelde verplichtingen door de entiteiten;

   (b) bindende instructies te geven of een bevel uit te vaardigen waarin deze entiteiten worden verplicht de vastgestelde tekortkomingen of de inbreuk op de in deze richtlijn vastgestelde verplichtingen te verhelpen;

   (c) deze entiteiten te gelasten een einde te maken aan gedragingen die niet in overeenstemming zijn met de in deze richtlijn vastgestelde verplichtingen en af te zien van herhaling van die gedragingen;

(d) deze entiteiten te gelasten hun risicobeheersmaatregelen en/of rapportageverplichtingen op een gespecificeerde wijze en binnen een gespecificeerde termijn in overeenstemming te brengen met de in de artikelen 18 en 20 vastgestelde verplichtingen;

(e) deze entiteiten te gelasten de natuurlijke of rechtspersonen aan wie zij diensten verlenen of voor wie zij activiteiten uitvoeren die mogelijkerwijs door een significante cyberbedreiging worden beïnvloed, in kennis te stellen van alle mogelijke beschermings- of herstelmaatregelen die door deze natuurlijke of rechtsperso(o)n(en) kunnen worden genomen als antwoord op die bedreiging;

(f) deze entiteiten te gelasten de naar aanleiding van een beveiligingsaudit gedane aanbevelingen binnen een redelijke termijn uit te voeren;

(g) deze entiteiten te gelasten aspecten van niet-naleving van de in deze richtlijn vastgestelde verplichtingen op een bepaalde manier openbaar te maken;

(h) een openbare verklaring af te leggen waarin wordt aangegeven welke natuurlijke of rechtsperso(o)n(en) verantwoordelijk is of zijn voor de inbreuk van een in deze richtlijn vastgestelde verplichting en wat de aard van die inbreuk is;

(i) een administratieve geldboete op te leggen of de oplegging ervan door de bevoegde organen of rechtbanken overeenkomstig de nationale wetgeving te verzoeken overeenkomstig artikel 31 bovenop of in plaats van de in punten a) tot en met h) van dit lid bedoelde maatregelen, afhankelijk van de omstandigheden van elk afzonderlijk geval.

5. Artikel 29, leden 6 tot en met 8, is ook van toepassing op de toezichts- en handhavingsmaatregelen waarin dit artikel voorziet voor de in bijlage II genoemde belangrijke entiteiten.

Artikel 31

Algemene voorwaarden voor het opleggen van administratieve boeten aan essentiële en belangrijke entiteiten

1. De lidstaten zorgen ervoor dat het opleggen van administratieve boeten aan essentiële en belangrijke entiteiten uit hoofde van dit artikel in verband met inbreuken op de verplichtingen uit hoofde van deze richtlijn in elk afzonderlijk geval doeltreffend, evenredig en afschrikkend is.

2. Administratieve boeten worden, afhankelijk van de omstandigheden van elk afzonderlijk geval, opgelegd naast of in plaats van de in artikel 29, lid 4, punten a) tot en met i), artikel 29, lid 5, en artikel 30, lid 4, punten a) tot en met h), bedoelde maatregelen.

3. Bij het besluit om een administratieve geldboete op te leggen en bij de vaststelling van het bedrag ervan in elk afzonderlijk geval wordt er ten minste rekening gehouden met de in artikel 29, lid 7, genoemde elementen.

4. De lidstaten zorgen ervoor dat overtredingen van de verplichtingen van artikel 18 of artikel 20 overeenkomstig de leden 2 en 3 van dit artikel worden bestraft met administratieve boeten van ten minste 10 000 000 EUR of ten hoogste 2 % van de totale wereldwijde jaaromzet van de onderneming waartoe de essentiële of

belangrijke entiteit in het voorgaande boekjaar behoorde, afhankelijk van welk bedrag hoger is.

5. De lidstaten kunnen voorzien in de bevoegdheid om dwangsommen op te leggen om een essentiële of belangrijke entiteit te dwingen een inbreuk te staken in overeenstemming met een voorafgaand besluit van de bevoegde autoriteit.

6. Onverminderd de bevoegdheden van de bevoegde autoriteiten uit hoofde van de artikelen 29 en 30 kan elke lidstaat bepalen of en in welke mate administratieve boeten kunnen worden opgelegd aan de in artikel 4, lid 23, bedoelde overheidsdiensten met inachtneming van de verplichtingen uit hoofde van deze richtlijn.

Artikel 32

Inbreuken die een inbreuk op de persoonsgegevens inhouden

1. Wanneer de bevoegde autoriteiten aanwijzingen hebben dat de inbreuk door een essentiële of belangrijke entiteit op de in de artikelen 18 en 20 vastgestelde verplichtingen een inbreuk in verband met persoonsgegevens, zoals gedefinieerd in artikel 4, lid 12, van Verordening (EU) nr. 2016/679, met zich meebrengt, die overeenkomstig artikel 33 van die verordening moet worden gemeld, stellen zij de overeenkomstig de artikelen 55 en 56 van die verordening bevoegde toezichthoudende autoriteiten daarvan binnen een redelijke termijn in kennis.

2. Indien de overeenkomstig de artikelen 55 en 56 van Verordening (EU) nr. 2016/679 bevoegde toezichthoudende autoriteiten besluiten hun bevoegdheden overeenkomstig artikel 58, punt i), van die verordening uit te oefenen en een administratieve boete op te leggen, leggen de bevoegde autoriteiten voor dezelfde inbreuk geen administratieve boete op grond van artikel 31 van deze richtlijn op. De bevoegde autoriteiten kunnen echter de handhavingsacties toepassen of de sanctiebevoegdheden uitoefenen waarin artikel 29, lid 4, punten a) tot en met i), artikel 29, lid 5, en artikel 30, lid 4, punten a) tot en met h), van deze richtlijn voorzien.

3. Wanneer de op grond van Verordening (EU) nr. 2016/679 bevoegde toezichthoudende autoriteit in een andere lidstaat dan de bevoegde autoriteit is gevestigd, kan de bevoegde autoriteit de in dezelfde lidstaat gevestigde toezichthoudende autoriteit daarvan in kennis stellen.

Artikel 33

Sancties

1. De lidstaten stellen regels vast voor de sancties die van toepassing zijn op inbreuken op de krachtens deze richtlijn vastgestelde nationale bepalingen en nemen alle nodige maatregelen om ervoor te zorgen dat deze worden uitgevoerd. De vastgestelde sancties moeten doeltreffend, evenredig en afschrikkend zijn.

2. De lidstaten stellen de Commissie uiterlijk [twee] jaar na de inwerkingtreding van deze richtlijn in kennis van deze regels en maatregelen en stellen haar onverwijld in kennis van eventuele latere wijzigingen daarvan.

Artikel 34

Wederzijdse bijstand

1. Wanneer een essentiële of belangrijke entiteit diensten verricht in meer dan één lidstaat, of haar hoofdvestiging of een vertegenwoordiger in een lidstaat heeft, maar haar netwerk- en informatiesystemen zich in een of meer andere lidstaten bevinden, werken de bevoegde autoriteit van de lidstaat van de hoofdvestiging of andere vestiging of van de vertegenwoordiger, en de bevoegde autoriteiten van die andere lidstaten met elkaar samen en verlenen ze elkaar indien nodig bijstand. Die samenwerking houdt ten minste in dat:

   (a) de bevoegde autoriteiten die in een lidstaat toezichts- of handhavingsmaatregelen toepassen, via het centrale contactpunt de bevoegde autoriteiten in de andere betrokken lidstaten informeren en raadplegen over de genomen toezichts- en handhavingsmaatregelen en de opvolging daarvan, overeenkomstig de artikelen 29 en 30;

   (b) een bevoegde autoriteit een andere bevoegde autoriteit kan verzoeken de in de artikelen 29 en 30 bedoelde toezichts- of handhavingsmaatregelen te nemen;

   (c) een bevoegde autoriteit, na ontvangst van een met redenen omkleed verzoek van een andere bevoegde autoriteit, de andere bevoegde autoriteit bijstand verleent, zodat de in de artikelen 29 en 30 bedoelde toezichts- of handhavingsacties op een effectieve, efficiënte en consistente wijze kunnen worden uitgevoerd. Deze wederzijdse bijstand kan betrekking hebben op verzoeken om informatie en toezichtsmaatregelen, met inbegrip van verzoeken om inspecties ter plaatse of toezicht elders of gerichte beveiligingsaudits uit te voeren. Een bevoegde autoriteit tot wie een verzoek om bijstand is gericht, mag dat verzoek niet weigeren, tenzij na een uitwisseling met de andere betrokken autoriteiten, het Enisa en de Commissie wordt vastgesteld dat de autoriteit niet bevoegd is om de gevraagde bijstand te verlenen of dat de gevraagde bijstand niet in verhouding staat tot de toezichthoudende taken van de bevoegde autoriteit die overeenkomstig artikel 29 of artikel 30 worden uitgevoerd.

2. In voorkomend geval kunnen de bevoegde autoriteiten van verschillende lidstaten in onderlinge overeenstemming de in de artikelen 29 en 30 bedoelde gezamenlijke toezichtsacties uitvoeren.

HOOFDSTUK VII

Overgangs- en slotbepalingen

Artikel 35

Evaluatie

De Commissie evalueert op gezette tijden de werking van deze richtlijn en brengt verslag uit aan het Europees Parlement en de Raad. In het verslag wordt met name de relevantie van de in de bijlagen I en II bedoelde sectoren, subsectoren, omvang en type van entiteiten voor het functioneren van de economie en de samenleving met betrekking tot cyberbeveiliging

beoordeeld. Met het oog hierop en om de strategische en operationele samenwerking verder te bevorderen, houdt de Commissie rekening met de verslagen van de samenwerkingsgroep en het CSIRT-netwerk over de opgedane ervaring op strategisch en operationeel niveau. Het eerste verslag wordt uiterlijk ... [54 maanden na de datum van inwerkingtreding van deze richtlijn ingediend[.

Artikel 36

Uitoefening van de bevoegdheidsdelegatie

1. De bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend onder de in dit artikel vastgestelde voorwaarden.
2. De bevoegdheid om de in artikel 18, lid 6, en artikel 21, lid 2, bedoelde gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend voor een periode van vijf jaar vanaf [...].
3. Het Europees Parlement of de Raad kan de in artikel 18, lid 6, en artikel 21, lid 2, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het wordt van kracht op de dag na die van de bekendmaking ervan in het Publicatieblad van de Europese Unie of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.
4. Alvorens een gedelegeerde handeling vast te stellen, raadpleegt de Commissie de door elke lidstaat aangewezen deskundigen overeenkomstig de beginselen die zijn vastgelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven.
5. Zodra de Commissie een gedelegeerde handeling heeft vastgesteld, doet zij daarvan gelijktijdig kennisgeving aan het Europees Parlement en de Raad.
6. Een overeenkomstig artikel 18, lid 6, en artikel 21, lid 2, vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement noch de Raad daartegen binnen een termijn van twee maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie hebben medegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of van de Raad met twee maanden verlengd.

Artikel 37

Comitéprocedure

1. De Commissie wordt bijgestaan door een comité. Dat comité is een comité in de zin van Verordening (EU) nr. 182/2011.
2. Wanneer naar dit lid wordt verwezen, is artikel 5 van Verordening (EU) nr. 182/2011 van toepassing.
3. Wanneer het advies van het comité via een schriftelijke procedure moet worden verkregen, wordt deze procedure zonder gevolg beëindigd wanneer de voorzitter van

het comité binnen de termijn voor het uitbrengen van het advies daartoe besluit of wanneer een lid van het comité daarom verzoekt.

Artikel 38

Omzetting

1. De lidstaten dienen uiterlijk op ... [18 maanden na de datum van inwerkingtreding van deze richtlijn] de nodige wettelijke en bestuursrechtelijke bepalingen vast te stellen en bekend te maken om aan deze richtlijn te voldoen. Zij delen de Commissie de tekst van die bepalingen onverwijld mede. Zij passen die bepalingen toe vanaf … [één dag na in het eerste sublid genoemde datum].
2. Wanneer de lidstaten die bepalingen aannemen, wordt in die bepalingen zelf of bij de officiële bekendmaking ervan naar deze richtlijn verwezen. De regels voor die verwijzing worden vastgesteld door de lidstaten.

Artikel 39

Wijziging van Verordening (EU) nr. 910/2014

Artikel 19 van Verordening (EU) nr. 910/2014 wordt geschrapt.

Artikel 40

Wijziging van Richtlijn (EU) 2018/1972

Artikel 40 en artikel 41 van Richtlijn (EU) 2018/1972 worden geschrapt.

Artikel 41

Intrekking

Richtlijn (EU) 2016/1148 wordt ingetrokken met ingang van... [uiterste datum voor omzetting van de Richtlijn].

Verwijzingen naar Richtlijn (EU) 2016/1148 gelden als verwijzingen naar deze richtlijn, volgens de concordantietabel in de bijlage III.

Artikel 42

Inwerkingtreding

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

Artikel 43

Geadresseerden

Deze richtlijn is gericht tot de lidstaten.

Gedaan te Brussel,

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

FINANCIEEL MEMORANDUM

Inhoudsopgave

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

Voorstel voor een richtlijn houdende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148

1.2. Betrokken beleidsterrein(en) *(programmacluster)*

Communicatienetwerken, inhoud en technologie

1.3. Het voorstel/initiatief betreft:

☐ **een nieuwe actie**

☐ **een nieuwe actie na een proefproject / voorbereidende actie**[40]

☒ **de verlenging van een bestaande actie**

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

1.4. Motivering van het voorstel/initiatief

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

De herziening is bedoeld om de cyberveerkracht van een allesomvattende reeks ondernemingen die in de Europese Unie actief zijn in alle relevante sectoren te vergroten, om verschillen in de veerkracht op de interne markt in de sectoren die reeds onder de richtlijn vallen te beperken en om de gemeenschappelijke situationele kennis en de collectieve paraatheid en responscapaciteit te vergroten.

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

De cyberveerkracht in de Unie kan niet doeltreffend zijn als zij op verschillende manieren wordt aangepakt via nationale of regionale silo's. De NIS-richtlijn moest dat probleem oplossen door een kader tot stand te brengen voor de beveiliging van netwerk en -informatiesystemen op nationaal en Unieniveau. Bij de eerste periodieke evaluatie van de NIS-richtlijn kwamen echter een aantal inherente gebreken aan het licht, die uiteindelijk hebben geleid tot aanzienlijke verschillen tussen de lidstaten met betrekking tot de capaciteiten, de planning en het beschermingsniveau, die tegelijkertijd de eerlijke mededingingsvoorwaarden voor vergelijkbare ondernemingen op de interne markt aantasten.

EU-optreden dat verder gaat dan de huidige maatregelen van de NIS-richtlijn is hoofdzakelijk gerechtvaardigd vanwege: (i) de grensoverschrijdende aard van het probleem; (ii) het potentieel van EU-optreden om doeltreffende nationale beleidsmaatregelen te verbeteren en te vergemakkelijken; (iii) de bijdrage van op

[40] In de zin van artikel 58, lid 2, punt a) of b), van de Financiële Verordening.

overleg en samenwerking gebaseerde NIS-beleidsmaatregelen aan de daadwerkelijke bescherming van gegevens en van de persoonlijke levenssfeer.

De vooropgestelde doelstellingen kunnen beter op EU- niveau worden bereikt dan door de afzonderlijke lidstaten.

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

De NIS-richtlijn is het eerste horizontale internemarktinstrument dat erop gericht is de veerkracht van netwerken en systemen in de Unie tegen cyberbeveiligingsrisico's te vergroten. Zij heeft reeds een aanzienlijke bijdrage geleverd aan het verhogen van het gemeenschappelijke cyberbeveiligingsniveau in de lidstaten. Uit de evaluatie van de werking en de uitvoering van de richtlijn zijn echter een aantal tekortkomingen naar voren gekomen, die, samen met de toenemende digitalisering en de behoefte aan een meer actuele respons, moeten worden behandeld in een herziene wetshandeling.

1.4.4. Samenhang en eventuele synergie met andere relevante instrumenten

Het nieuwe voorstel is volledig in overeenstemming en samenhangend met andere relevante initiatieven zoals het voorstel voor een verordening betreffende digitale operationele veerkracht voor de financiële sector ("DORA") en het voorstel voor een richtlijn betreffende de veerkracht van kritieke exploitanten van essentiële diensten. Het strookt ook met het Europees Wetboek voor elektronische communicatie, de algemene verordening gegevensbescherming en de eIDAS-verordening.

Het voorstel vormt een wezenlijk onderdeel van de EU-strategie voor de veiligheidsunie.

1.5. Duur en financiële gevolgen

☐ **beperkte geldigheidsduur**

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

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

☒ **onbeperkte geldigheidsduur**

– uitvoering met een opstartperiode vanaf 2022 tot en met 2025,

– gevolgd door een volledige uitvoering.

1.6. Geplande beheersvorm(en)[41]

Direct beheer door de Commissie

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

– ☐door de uitvoerende agentschappen

☐ **Gedeeld beheer** met de lidstaten

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

– ☐ derde landen of de door hen aangewezen organen;

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

– ☐de EIB en het Europees Investeringsfonds;

– X☐ de in de artikelen 70 en 71 van de Financiële Verordening bedoelde organen;

– ☐ publiekrechtelijke organen;

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

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

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

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

Opmerkingen

Het Agentschap van de Europese Unie voor cyberbeveiliging, Enisa, waaraan een nieuw permanent mandaat is verleend bij de cyberbeveiligingsverordening, zou de lidstaten en de Commissie bijstaan in de uitvoering van de herziene NIS-richtlijn.

Ten gevolge van de herziene NIS-richtlijn zal Enisa met ingang van 2022/23 aanvullende actiegebieden hebben. Hoewel die actiegebieden volgens het mandaat van Enisa onder haar algemene taken zouden vallen, zullen zij een aanvullende werklast met zich meebrengen voor het Agentschap. Volgens het Commissievoorstel voor een herziene NIS-richtlijn zal ENISA,

[41] Nadere gegevens over de beheersvormen en verwijzingen naar de Financiële Verordening zijn beschikbaar op BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

bovenop haar huidige actiegebieden, meer bepaald verplicht zijn om onder meer de volgende acties specifiek in haar werkprogramma op te nemen: (i) een Europees kwetsbaarheidsregister ontwikkelen en handhaven (artikel 6, lid 2, van het voorstel), (ii) het secretariaat van het Europees Netwerk van verbindingsorganisaties voor cybercrises (CyCLONe) verzekeren (artikel 14 van het voorstel) en een jaarverslag over de staat van cyberbeveiliging in de EU opstellen (artikel 15 van het voorstel), (iii) de organisatie van collegiale toetsingen tussen de lidstaten ondersteunen (artikel 16 van het voorstel), (iv) geaggregeerde gegevens over incidenten verzamelen bij de lidstaten en technische richtsnoeren opstellen (artikel 20, lid 9, van het voorstel), (v) een register van entiteiten die grensoverschrijdende diensten verlenen opzetten en bijhouden (artikel 25 van het voorstel).

Vanaf 2022 zal er derhalve een verzoek om 5 aanvullende VTE's worden ingediend, met een overeenkomstige begroting van ongeveer 0,61 miljoen EUR per jaar om die nieuwe functies in te vullen (zie afzonderlijk financieel memorandum voor agentschappen).

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

Vermeld frequentie en voorwaarden.

Op gezette tijden evalueert de Commissie de werking van deze richtlijn en brengt zij daarover verslag uit aan het Europees Parlement en de Raad. Dat gebeurt voor het eerst drie jaar na de inwerkingtreding.

De Commissie zal tevens nagaan of de lidstaten de richtlijn correct omzetten.

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

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

De eenheid binnen DG CNECT die belast is met het beleidsterrein zal de uitvoering van de richtlijn beheren.

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

Bijzonder laag risico, aangezien het ecosysteem voor de NIS-richtlijn al bestaat.

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

Niet van belang. Louter gebruik van de administratieve begroting (“algemene toewijzing”).

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

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

Niet van belang. Louter gebruik van de administratieve begroting (“algemene toewijzing”).

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

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

Rubriek van het meerjarige financiële kader	Begrotingsonderdeel	Soort uitgaven	Bijdrage			
	Nummer [Rubriek…7……...……]	GK/NGK[42]	van EVA-landen[43]	van kandidaat-lidstaten[44]	van derde landen	in de zin van artikel [21, lid 2, punt b),] van de Financiële Verordening
	20 02 06 uitgaven voor beheer 20 02 06	NGK	NEE	NEE	NEE	NEE

[42] GK = gesplitste kredieten/NGK = niet-gesplitste kredieten.
[43] EVA: Europese Vrijhandelsassociatie.
[44] Kandidaat-lidstaten en, in voorkomend geval, aspirant-kandidaten van de Westelijke Balkan.

3.2. Geraamde gevolgen voor de uitgaven

3.2.1. Samenvatting van de geraamde gevolgen voor de uitgaven

In miljoen EUR (tot op drie decimalen)

Rubriek van het meerjarige financiële kader	**<…>**	[Rubriek……...……]

			2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Na 2027***	**TOTAAL**
Beleidskredieten (uitgesplitst naar de onder 3.1 vermelde begrotingsonderdelen)	Vastleggingen	(1)									
	Betalingen	(2)									
Administratieve kredieten gefinancierd uit het budget van het programma[45]	Vastleggingen = Betalingen	(3)									
TOTALE kredieten voor het budget van het programma	Vastleggingen	=1+3									
	Betalingen	=2+3									

Rubriek van het meerjarige financiële kader	7	"Administratieve uitgaven" Vergaderingen: de voltallige vergaderingen van de NIS-samenwerkingsgroep vinden gewoonlijk vier keer per jaar plaats. De Commissie dekt kosten met betrekking tot de catering- en reisonkosten van vertegenwoordigers van 27 lidstaten (een vertegenwoordiger per lidstaat). De kosten voor een vergadering kunnen maximaal 15 000 EUR bedragen. Dienstreizen: dienstreizen houden verband met het toezicht op de uitvoering van de NIS-richtlijn. Voorbeeld: In een jaar (mei 2019 - juli 2020) was het de bedoeling dat

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

		wij zogeheten “NIS-landenbezoeken” zouden organiseren en alle 27 lidstaten zouden bezoeken om de uitvoering van de NIS-richtlijn in de EU te bespreken.

Dit deel moet worden ingevuld aan de hand van de “administratieve begrotingsgegevens”, die eerst moeten worden opgenomen in de bijlage bij het financieel memorandum, die is geüpload in DECIDE met het oog op overleg tussen de diensten.

In miljoen EUR (tot op drie decimalen)

		2021	2022	2023	2024	2025	2026	2027	*Na 2027*	TOTAAL
Personele middelen		1,14	1,14	1,14	1,14	1,14	1,14	**1,14**		**7,98**
Andere administratieve uitgaven		**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**		**0,63**
TOTALE kredieten in RUBRIEK 7 van het meerjarige financiële kader	(totaal vastleggingen = totaal betalingen)	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**		**8,61**

In miljoen EUR (tot op drie decimalen)

		2021	2022	2023	2024	2025	2026	2027	*Na 2027*	TOTAAL
TOTAAL kredieten in alle RUBRIEKEN van het meerjarige financiële kader	Vastleggingen									
	Betalingen									

3.2.2. Samenvatting van de geraamde gevolgen voor de administratieve kredieten

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

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

In miljoen EUR (tot op drie decimalen)

Jaar	2021	2022	2023	2024	2025	2026	2027	TOTAAL
RUBRIEK 7 van het meerjarige financiële kader								
Personele middelen	1,14	1,14	1,14	1,14	1,14	1,14	**1,14**	**7,98**
Andere administratieve uitgaven	0,09	0,09	0,09	0,09	0,09	0,09	**0,09**	**0,63**
Subtotaal RUBRIEK 7 van het meerjarige financiële kader	1,23	1,23	1,23	1,23	1,23	1,23	**1,23**	**8,61**
Buiten RUBRIEK 7[46] of the multiannual financial framework								
Personele middelen								
Andere administratieve uitgaven								
Subtotaal buiten RUBRIEK 7 van het meerjarige financiële kader								
TOTAAL	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**8,61**

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

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

3.2.2.1. Geraamde personeelsbehoeften

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

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

Raming in voltijdequivalenten

Jaar		2021	2022	2023	2024	2025	2026	2027
• Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)								
Zetel en vertegenwoordigingen van de Commissie		6	6	6	6	6	6	6
Delegaties								
Onderzoek								
• Extern personeel (in voltijdequivalenten: VTE) - AC, AL, END, INT en JED[47] Rubriek 7								
Gefinancierd uit RUBRIEK 7 van het meerjarige financiële kader	- zetel	3	3	3	3	3	3	3
	- delegaties							
Gefinancierd uit het budget van het programma [48]	- zetel							
	- delegaties							
Onderzoek								
Andere (gelieve toe te lichten)								
TOTAAL		**9**	**9**	**9**	**9**	**9**	**9**	**9**

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

Beschrijving van de uit te voeren taken:

Ambtenaren en tijdelijk personeel	• voorbereiding van gedelegeerde handelingen overeenkomstig artikel 18, lid 6, artikel 21, lid 2, artikel 36; • voorbereiding van uitvoeringshandelingen overeenkomstig artikel 12, lid 8, artikel 18, lid 5, artikel 20, lid 11; • inrichting van een secretariaat voor de NIS-samenwerkingsgroep; • organisatie van de voltallige vergaderingen en workstreamvergaderingen van de NIS-samenwerkingsgroep; • coördinatie van de werkzaamheden van de lidstaten inzake diverse documenten (richtsnoeren, instrumentaria enz.); • overleg met andere diensten van de Commissie, Enisa en nationale autoriteiten met het oog op de uitvoering van de NIS-richtlijn; • analyse van de nationale methoden en beste praktijken met betrekking tot de uitvoering van de NIS-richtlijn.
Extern personeel	Ondersteuning voor alle bovenstaande taken, waar nodig

[47] AC= Agent Contractuel (arbeidscontractant); AL= Agent Local (plaatselijk functionaris); END = Expert National Détaché (gedetacheerd nationaal deskundige); INT= Intérimaire (uitzendkracht); JPD = Junior Professionals in Delegations (jonge deskundige in delegaties).

[48] Submaximum voor extern personeel uit beleidskredieten (vroegere "BA"-onderdelen).

3.2.3. Bijdragen van derden

Het voorstel/initiatief:

– X☐ voorziet niet in medefinanciering door derden

– ☐ voorziet in medefinanciering, zoals hieronder wordt geraamd:

Kredieten in miljoen EUR (tot op drie decimalen)

Jaar	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTAAL**
Medefinancieringsbron								
TOTAAL medegefinancierde kredieten								

3.3. Geraamde gevolgen voor de ontvangsten

– ☐X Het voorstel/initiatief heeft geen financiële gevolgen voor de ontvangsten

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

☐ voor de eigen middelen

☐ voor overige ontvangsten

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

In miljoen EUR (tot op drie decimalen)

Begrotingsonderdeel voor ontvangsten:	Gevolgen van het voorstel/initiatief[49]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Artikel …….							

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

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

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

BIJLAGE
bij het FINANCIEEL MEMORANDUM

Naam van het voorstel/initiatief:

Voorstel voor een richtlijn tot herziening van Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie

……
……

1. NODIG GEACHTE PERSONELE MIDDELEN en KOSTEN DAARVAN

2. ANDERE ADMINISTRATIEVE UITGAVEN

3. VOOR KOSTENRAMINGEN GEBRUIKTE BEREKENINGSMETHODEN

3,1 Personele middelen

3,2 Andere administratieve uitgaven

*Deze bijlage, **die moet worden ingevuld door elk van de DG's/diensten die aan het voorstel/initiatief deelnemen,** moet het financieel memorandum vergezellen wanneer met de dienstenoverkoepelende raadpleging wordt begonnen.*

De gegevens in tabelvorm worden gebruikt als bron voor de in het financieel memorandum opgenomen tabellen. Zij zijn voor strikt intern gebruik binnen de Commissie.

1. Kosten van nodig geachte aantal personele middelen

☐ Voor het voorstel/initiatief zijn geen personele middelen nodig

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

In miljoen EUR (tot op drie decimalen)

RUBRIEK 7 van het meerjarige financiële kader		**2021**		**2022**		**2023**		**2024**		**2025**		**2026**		**2027**		**TOTAAL**	
		VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten
• Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)																	
Zetel en vertegenwoordigingen van de Commissie	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42	6,3
	AST																
EU-delegaties	AD																
	AST																
• Extern personeel[50] 0,24																	
totale financiële middelen	AC	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	END																
	INT																
EU-delegaties	AC																
	AL																

[50] AC= Agent Contractuel (arbeidscontractant); AL= Agent Local (plaatselijk functionaris); END = Expert National Détaché (gedetacheerd nationaal deskundige); INT= Intérimaire (uitzendkracht); JPD = Junior Professionals in Delegations (jonge deskundige in delegaties).

	END																
	INT																
	JPD																
Ander begrotingsonderdeel (geef aan welk)																	
Subtotaal – RUBRIEK 7 van het meerjarige financiële kader		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

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

Buiten RUBRIEK 7 van het meerjarige financiële kader		2021		2022		2023		2024		2025		2025		2025		TOTAAL	
		VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten
• Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)																	
Onderzoek	AD																
	AST																
• Extern personeel [51]																	
Onder het maximum voor extern personeel uit beleidskredieten (vroegere "-"BA"-onderdelen).	- zetel AC																
	- zetel END																
	- zetel INT																
	- EU-delegaties AC																
	- EU-delegaties AL																
	- EU-delegaties END																
	- EU-delegaties INT																
	- EU-delegaties JPD																
Onderzoek)	AC																
	END																
	INT																

[51] AC= Agent Contractuel (arbeidscontractant); AL= Agent Local (plaatselijk functionaris); END = Expert National Détaché (gedetacheerd nationaal deskundige); INT= Intérimaire (uitzendkracht); JPD = Junior Professionals in Delegations (jonge deskundige in delegaties).

Ander begrotingsonderdeel (geef aan welk)																	
Subtotaal – buiten RUBRIEK 7 van het meerjarige financiële kader																	

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

Geraamde gevolgen voor personele middelen van Enisa

Het Agentschap van de Europese Unie voor cyberbeveiliging, Enisa, waaraan een nieuw permanent mandaat is verleend bij de cyberbeveiligingsverordening, zou de lidstaten en de Commissie bijstaan in de uitvoering van de herziene NIS-richtlijn.

Ten gevolge van de herziene NIS-richtlijn zal Enisa met ingang van 2022/23 aanvullende actiegebieden hebben. Hoewel die actiegebieden volgens het mandaat van Enisa onder haar algemene taken zouden vallen, zullen zij een aanvullende werklast met zich meebrengen voor het Agentschap. Volgens het Commissievoorstel voor een herziene NIS-richtlijn zal ENISA, bovenop haar huidige actiegebieden, meer bepaald verplicht zijn om onder meer de volgende acties specifiek in haar werkprogramma op te nemen: (i) een Europees kwetsbaarheidsregister ontwikkelen en handhaven (artikel 6, lid 2, van het voorstel), (ii) het secretariaat van het Europees Netwerk van verbindingsorganisaties voor cybercrises (CyCLONe) verzekeren (artikel 14 van het voorstel) en een jaarverslag over de staat van cyberbeveiliging in de EU opstellen (artikel 15 van het voorstel), (iii) de organisatie van collegiale toetsingen tussen de lidstaten ondersteunen (artikel 16 van het voorstel), (iv) geaggregeerde gegevens over incidenten verzamelen bij de lidstaten en technische richtsnoeren opstellen (artikel 20, lid 9, van het voorstel), (v) een register van entiteiten die grensoverschrijdende diensten verlenen opzetten en bijhouden (artikel 25 van het voorstel).

Vanaf 2022 zal er derhalve een verzoek om 5 aanvullende VTE's worden ingediend, met een overeenkomstige begroting van ongeveer 0,61 miljoen EUR per jaar om die nieuwe functies in te vullen (zie afzonderlijk financieel memorandum voor agentschappen).

Vanaf 2022 zal er derhalve een verzoek om 5 aanvullende VTE's worden ingediend, met een overeenkomstige begroting om die nieuwe functies in te vullen.

☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

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

In miljoen EUR (tot op drie decimalen)

	Jaar **N** [52] **2022**	Jaar **N+1** **2023**	Jaar **N+2** **2024**	Jaar **N+3** **2025**	zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)	**TOTAAL**

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

Tijdelijke functionarissen (AD-rangen)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Tijdelijke functionarissen (AST-rangen)								
Arbeidscontractanten	0,160	0,160	0,160	0,160	0,160	0,160		
Gedetacheerde nationale deskundigen								**0,96**

TOTAAL	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Personeelsbehoeften (VTE):

	Jaar **N** [53] **2022**	Jaar **N+1** **2023**	Jaar **N+2** **2024**	Jaar **N+3** **2025**	zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)	**TOTAAL**

Tijdelijke functionarissen (AD-rangen)	3	3	3	3	3	3		**18**
Tijdelijke functionarissen (AST-rangen)								

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

Arbeidscontractanten	2	2	2	2	2	2		**12**
Gedetacheerde nationale deskundigen								

TOTAAL	**5**	**5**	**5**	**5**	**5**	**5**		**30**

2. Andere administratieve uitgaven

☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

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

In miljoen EUR (tot op drie decimalen)

RUBRIEK 7 van het meerjarige financiële kader	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Totaal**
Zetel:								
Dienstreizen en representatie	0,03	0,03	0,03	0,03	0,03	0,03	0,03	**0,21**
Conferenties en vergaderingen	0,06	0,06	0,06	0,06	0,06	0,06	0,06	**0,42**
Comités[54]								
Studies en adviezen								

[54] Specificeer het soort comité en de groep waartoe het behoort.

Informatie- en beheerssystemen								
ICT-apparatuur en -diensten[55]								
Andere begrotingsonderdelen (te vermelden waar nodig)								
EU-delegaties								
Dienstreizen, conferenties en representatie								
Bijscholing van personeel								
Aankoop, huur en daarmee samenhangende uitgaven								
Materieel, meubilair, leveringen en diensten								
Subtotaal RUBRIEK 7 van het meerjarige financiële kader	0,09	0,09	0,09	0,09	0,09	0,09	0,09	**0,63**

[55] ICT: ICT Informatie- en communicatietechnologieën: DIGIT moet worden geraadpleegd.

In miljoen EUR (tot op drie decimalen)

Buiten RUBRIEK 7 van het meerjarige financiële kader	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Totaal**
Uitgaven voor technische en administratieve bijstand (exclusief extern personeel) uit beleidskredieten (vroegere "BA"-onderdelen)								
- zetel								
- EU-delegaties								
Overige beheersuitgaven voor onderzoek								
Andere begrotingsonderdelen (te vermelden waar nodig)								
Subtotaal – Buiten RUBRIEK 7 van het meerjarige financiële kader								

TOTAAL **RUBRIEK 7 en buiten RUBRIEK 7** van het meerjarige financiële kader	1,23	1,23	1,23	1,23	1,23	1,23	1,23	**8,61**

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

3. Voor kostenramingen gebruikte berekeningsmethoden

3,1 Personele middelen

In dit deel wordt de berekeningsmethode toegelicht die is gebruikt om de benodigde personele middelen te ramen (veronderstelde werklast, bijzondere taken (Sysper 2-taakprofielen, personeelscategorieën en overeenkomstige gemiddelde kosten))

RUBRIEK 7 van het meerjarige financiële kader
NB: De gemiddelde kosten van elke personeelscategorie op het hoofdkantoor zijn te vinden op BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
• Ambtenaren en tijdelijk personeel 6 VTE-ambtenaren (gemiddelde kosten 0,150) = 0,9 per jaar - voorbereiding van gedelegeerde handelingen overeenkomstig artikel 18, lid 6, artikel 21, lid 2, artikel 36; - voorbereiding van uitvoeringshandelingen overeenkomstig artikel 12, lid 8, artikel 18, lid 5, artikel 20, lid 11; - inrichting van een secretariaat voor de NIS-samenwerkingsgroep; - organisatie van de voltallige vergaderingen en workstreamvergaderingen van de NIS-samenwerkingsgroep; - coördinatie van de werkzaamheden van de lidstaten inzake diverse documenten (richtsnoeren, instrumentaria enz.); - overleg met andere diensten van de Commissie, Enisa en nationale autoriteiten met het oog op de uitvoering van de NIS-richtlijn; - analyse van de nationale methoden en beste praktijken met betrekking tot de uitvoering van de NIS-richtlijn.
• Extern personeel 3 AC (gemiddelde kosten 0,08) = 0,24 per jaar - Ondersteuning voor alle bovenstaande taken, waar nodig

Buiten RUBRIEK 7 van het meerjarige financiële kader
• Alleen uit de begroting voor onderzoek gefinancierde posten
• Extern personeel

3,2 Andere administratieve uitgaven

Verstrek gegevens over de voor elk begrotingsonderdeel gebruikte berekeningsmethode

en meer in het bijzonder over de achterliggende aannamen (bv. aantal vergaderingen per jaar, gemiddelde kosten, enz.)

RUBRIEK 7 van het meerjarige financiële kader

Vergaderingen: de voltallige vergaderingen van de NIS-samenwerkingsgroep vinden gewoonlijk vier keer per jaar plaats. De Commissie dekt kosten met betrekking tot de catering- en reisonkosten van vertegenwoordigers van 27 lidstaten (een vertegenwoordiger per lidstaat). De kosten voor een vergadering kunnen maximaal 15 000 EUR bedragen, wat neerkomt op 60 000 EUR per jaar.

Dienstreizen: dienstreizen houden verband met het toezicht op de uitvoering van de NIS-richtlijn. Voorbeeld: In een jaar (mei 2019 - juli 2020) was het de bedoeling dat wij zogeheten "NIS-landenbezoeken" zouden organiseren en alle 27 lidstaten zouden bezoeken om

de uitvoering van de NIS-richtlijn in de EU te bespreken.

Buiten RUBRIEK 7 van het meerjarige financiële kader

BIJLAGE 7

bij het
BESLUIT VAN DE COMMISSIE

inzake de interne regels betreffende de uitvoering van de algemene begroting van de Europese Unie (afdeling Europese Commissie) ter attentie van de diensten van de Commissie

FINANCIEEL MEMORANDUM "AGENTSCHAPPEN"

Dit financieel memorandum heeft betrekking op het verzoek om het personeel van Enisa met ingang van 2022 te verhogen met 5 VTE's om aanvullende werkzaamheden te verrichten in verband met de uitvoering van de NIS-richtlijn. Deze werkzaamheden vallen reeds onder het mandaat van Enisa.

Inhoudsopgave

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

Voorstel voor een richtlijn houdende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148

1.2. Betrokken beleidsterrein(en)

Communicatienetwerken, inhoud en technologie

1.3. Het voorstel/initiatief betreft

☐ **een nieuwe actie**

☐ **een nieuwe actie na een proefproject / voorbereidende actie**[56]

☒ **de verlenging van een bestaande actie**

☐ **de samenvoeging van een of meer acties naar een andere/een nieuwe actie**

1.4. Doelstelling(en)

1.4.1. Algemene doelstelling(en)

De herziening is bedoeld om de cyberveerkracht van een allesomvattende reeks ondernemingen die in de Europese Unie actief zijn in alle relevante sectoren te vergroten, om verschillen in de veerkracht op de interne markt in de sectoren die reeds onder de richtlijn vallen te beperken en om de gemeenschappelijke situationele kennis en de collectieve paraatheid en responscapaciteit te vergroten.

1.4.2. Specifieke doelstelling(en)

Om het probleem van de beperkte cyberveerkracht van ondernemingen die in de Europese Unie actief zijn aan te pakken, bestaat de specifieke doelstelling erin dat entiteiten in alle sectoren die afhankelijk zijn van netwerk- en informatiesystemen en die essentiële diensten verlenen aan de economie en de samenleving in haar geheel verplicht worden om cyberbeveiligingsmaatregelen te nemen en incidenten te melden teneinde de algemene cyberveerkracht op de gehele interne markt te verhogen.

Om het probleem van uiteenlopende veerkracht in de verschillende lidstaten en sectoren aan te pakken, is het de specifieke doelstelling om ervoor te zorgen dat alle entiteiten die actief zijn in sectoren die onder het NIS-rechtskader vallen en die een vergelijkbare omvang en rol hebben, aan hetzelfde regelgevingsstelsel worden onderworpen (en dus ofwel binnen, ofwel buiten het toepassingsgebied vallen), ongeacht onder welke jurisdictie zij vallen binnen de EU.

Om ervoor te zorgen dat alle entiteiten die actief zijn in sectoren die onder het NIS-rechtskader vallen dezelfde, op risicobeheer gebaseerde verplichtingen met betrekking tot beveiligingsmaatregelen moeten nakomen en alle incidenten moeten melden op basis van een gelijkvormige reeks criteria, bestaan de specifieke doelstellingen erin te verzekeren dat de bevoegde autoriteiten de in het rechtsinstrument vastgestelde voorschriften doeltreffender handhaven, via onderling afgestemde toezichts- en handhavingsmaatregelen en dat de

[56] In de zin van artikel 58, lid 2, punt a) of b), van de Financiële Verordening.

bevoegde autoriteiten in de verschillende lidstaten vergelijkbare middelen toegewezen krijgen opdat zij de kerntaken van het NIS-kader kunnen vervullen.

Om het gebrek aan gemeenschappelijke situationele kennis en het gebrek aan een gemeenschappelijke crisisrespons te verhelpen, bestaat de specifieke doelstelling erin te verzekeren dat essentiële informatie wordt uitgewisseld tussen de lidstaten, door te voorzien in duidelijke verplichtingen voor bevoegde autoriteiten om informatie te delen en samen te werken op het gebied van cyberbedreigingen en -incidenten en door een gemeenschappelijke operationele capaciteit voor crisisrespons van de EU te ontwikkelen.

1.4.3. Verwacht(e) resulta(a)t(en) en gevolg(en)

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

Het voorstel zal naar verwachting de volgende significante voordelen opleveren: uit de ramingen blijkt dat het tot een daling van de kosten van cyberbeveiligingsincidenten met 11,3 miljard EUR kan leiden. Het sectorale toepassingsgebied zou aanzienlijk worden uitgebreid binnen het NIS-kader, maar naast bovenstaande voordelen zouden de lasten die de NIS-voorschriften met zich zouden brengen, met name uit toezichtsoogpunt, ook evenwichtig zijn voor zowel de nieuwe entiteiten die onder het kader zouden vallen als de bevoegde autoriteiten. De reden daarvoor is dat het nieuwe NIS-kader een tweeledige aanpak tot stand zou brengen, waarin de nadruk ligt op grote en essentiële entiteiten en een onderscheid wordt gemaakt in de toezichtregelingen waardoor voor een groot aantal van die entiteiten uitsluitend ex-posttoezicht wordt toegelaten, met name voor ondernemingen die "belangrijk" maar nog niet "essentieel" worden geacht.

Over het algemeen zou het voorstel tot efficiënte trade-offs en synergieën leiden, met het grootste potentieel van alle geanalyseerde beleidsopties om een hoger, consistent niveau van cyberveerkracht van essentiële entiteiten te verzekeren in de gehele Unie, dat uiteindelijk tot kostenbesparingen zou leiden voor zowel ondernemingen als de samenleving.

Het voorstel zou ook tot bepaalde nalevings- en handhavingskosten leiden voor de betrokken autoriteiten van de lidstaten (er werd een totale verhoging van de middelen met ongeveer 20-30 % geraamd). Het nieuwe kader zou echter ook aanzienlijke voordelen opleveren dankzij een beter overzicht van en een betere interactie met essentiële bedrijven, een betere grensoverschrijdende operationele samenwerking en mechanismen voor wederzijdse bijstand en collegiale toetsing. Dat zou tot een algemene toename van de cyberbeveiligingscapaciteiten in de lidstaten leiden.

Voor de ondernemingen die onder het toepassingsgebied van het NIS-kader zouden vallen, wordt geraamd dat zij hun uitgaven voor ICT-beveiliging in de jaren na de invoering van het nieuwe NIS-kader met maximaal 22 % zouden moeten verhogen (dit zou 12 % zijn voor ondernemingen die al onder het toepassingsgebied van de huidige NIS-richtlijn vallen). De gemiddelde stijging van de uitgaven voor ICT-beveiliging zou echter een evenredig voordeel opleveren van dergelijke investeringen, met name vanwege een aanzienlijke daling van de kosten van cyberbeveiligingsincidenten (die op 118 miljoen EUR gedurende tien jaar worden geraamd).

Kleine en micro-ondernemingen zouden worden vrijgesteld van de NIS-richtlijn. Voor middelgrote ondernemingen is een toename van de uitgaven voor ICT-beveiliging te verwachten in de eerste jaren na de invoering van het nieuwe NIS-kader. Tegelijk zou het verhogen van de beveiligingseisen voor die entiteiten ook hun cyberbeveiligingscapaciteiten stimuleren en hun beheer van ICT-risico's helpen verbeteren.

Er zouden gevolgen zijn voor de nationale begrotingen en administraties: op korte en middellange termijn zou een geraamde verhoging van de middelen met ongeveer 20-30 % te verwachten vallen.

Er vallen geen andere significante nadelige gevolgen te verwachten. Het voorstel zal naar verwachting tot meer robuuste cyberbeveiligingscapaciteiten leiden en zou derhalve een belangrijker beperkend effect hebben op het aantal incidenten, met inbegrip van gegevenslekken, en de ernst ervan. Ze zal waarschijnlijk ook een positief effect hebben op het verzekeren van eerlijke mededingingsvoorwaarden in de lidstaten voor alle entiteiten die

onder het toepassingsgebied van de NIS-richtlijn vallen en de ongelijke spreiding van informatie over cyberbeveiliging beperken.

1.4.4. Prestatie-indicatoren

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

De indicatoren zullen worden beoordeeld door de Commissie, met ondersteuning van Enisa en de samenwerkingsgroep, te beginnen drie jaar na de inwerkingtreding van de nieuwe NIS-wetshandeling. Hieronder volgt een overzicht van monitoringindicatoren op basis waarvan het succes van de NIS-herziening zou worden beoordeeld:

- Een betere afhandeling van incidenten: Door cyberbeveiligingsmaatregelen te treffen, verbeteren ondernemingen niet alleen hun vermogen om bepaalde incidenten geheel te vermijden, maar ook hun capaciteit om op incidenten te reageren. De maatstaven voor succes zijn daarom i) de verkorting van de gemiddelde tijd die nodig is om een incident te detecteren, ii) de tijd die organisaties gemiddeld nodig hebben om te herstellen van een incident en iii) de gemiddelde kosten van de door een incident veroorzaakte schade.

- Een beter bewustzijn van cyberbeveiligingsrisico's bij het hoger management van ondernemingen: door ondernemingen te verplichten om maatregelen te treffen, zou een herziene NIS-richtlijn bijdragen aan de bewustmaking over risico's in verband met cyberbeveiliging bij het hoger management. Dit kan worden gemeten door te bestuderen in hoeverre ondernemingen die onder de NIS-richtlijn vallen van cyberbeveiliging een prioriteit maken in hun intern bedrijfsbeleid en -processen, zoals blijkt uit interne documentatie, relevante opleidingsprogramma's en bewustmakingsactiviteiten voor de werknemers en de prioriteit die wordt gegeven aan beveiligingsgerelateerde ICT-investeringen. Het management van alle essentiële en belangrijke entiteiten moet zich ook bewust zijn van de voorschriften die in de NIS-richtlijn zijn vastgesteld.

- Nivellering van sectorspecifieke uitgaven: de uitgaven voor ICT-beveiliging verschillen sterk van sector tot sector in de EU. Door ondernemingen in meer sectoren te verplichten maatregelen te treffen, zouden de afwijkingen van de gemiddelde sectorspecifieke uitgaven voor ICT-beveiliging, uitgedrukt als percentage van de totale ICT-uitgaven, moeten afnemen tussen sectoren en lidstaten.

- Sterkere bevoegde autoriteiten en meer samenwerking: in een herziene NIS-richtlijn zouden mogelijk aanvullende taken worden toevertrouwd aan de bevoegde autoriteiten. Dat zou een meetbaar effect hebben op de financiële en personele middelen voor cyberbeveiligingsagentschappen op nationaal niveau en zou ook een positief effect moeten hebben op de capaciteit van bevoegde autoriteiten om proactief samen te werken en zo het aantal gevallen te verhogen waarin bevoegde autoriteiten met elkaar overleggen om grensoverschrijdende incidenten aan te pakken of gemeenschappelijke toezichtsactiviteiten te verrichten.

- Meer informatie-uitwisseling: De herziene NIS-richtlijn zou ook de informatie-uitwisseling tussen ondernemingen en met de bevoegde autoriteiten ten goede komen. Een van de streefdoelen van de herziening zou erin kunnen bestaan het aantal entiteiten dat deelneemt aan de verschillende vormen van informatie-uitwisseling te verhogen.

1.5. Motivering van het voorstel/initiatief

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

Het voorstel is bedoeld om de cyberveerkracht van een omvattende reeks ondernemingen die in de Europese Unie actief zijn in alle relevante sectoren te vergroten, om verschillen in de veerkracht op de interne markt in de sectoren die reeds onder de richtlijn vallen te beperken en om de gemeenschappelijke situationele kennis en de collectieve paraatheid en responscapaciteit te vergroten. Het zal voortbouwen op wat er de afgelopen vier jaar is verwezenlijkt met de uitvoering van Richtlijn (EU) 2016/1148.

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

De cyberveerkracht in de Unie kan niet doeltreffend zijn als zij op verschillende manieren wordt aangepakt via nationale of regionale silo's. De NIS-richtlijn moest dat probleem oplossen door een kader tot stand te brengen voor de beveiliging van netwerk en -informatiesystemen op nationaal en Unieniveau. Bij de eerste periodieke evaluatie van de NIS-richtlijn kwamen echter een aantal inherente gebreken aan het licht, die uiteindelijk hebben geleid tot aanzienlijke verschillen tussen de lidstaten met betrekking tot de capaciteiten, de planning en het beschermingsniveau, die tegelijkertijd de eerlijke mededingingsvoorwaarden voor vergelijkbare ondernemingen op de interne markt aantasten.

EU-optreden dat verder gaat dan de huidige maatregelen van de NIS-richtlijn is hoofdzakelijk gerechtvaardigd vanwege: (i) de grensoverschrijdende aard van het probleem; (ii) het potentieel van EU-optreden om doeltreffende nationale beleidsmaatregelen te verbeteren en te vergemakkelijken; (iii) de bijdrage van op overleg en samenwerking gebaseerde NIS-beleidsmaatregelen aan de daadwerkelijke bescherming van gegevens en van de persoonlijke levenssfeer.

De vooropgestelde doelstellingen kunnen beter op EU- niveau worden bereikt dan door de afzonderlijke lidstaten.

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

De NIS-richtlijn is het eerste horizontale internemarktinstrument dat erop gericht is de veerkracht van netwerken en systemen in de Unie tegen cyberbeveiligingsrisico's te vergroten. De richtlijn heeft sinds de inwerkingtreding in 2016 reeds een aanzienlijke bijdrage geleverd aan het verhogen van het gemeenschappelijke cyberbeveiligingsniveau in de lidstaten. Uit de evaluatie van de werking en de uitvoering van de richtlijn zijn echter een aantal tekortkomingen naar voren gekomen, die, samen met de toenemende digitalisering en de behoefte aan een meer actuele respons, moeten worden behandeld in een herziene wetshandeling.

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

Het nieuwe voorstel is volledig in overeenstemming en samenhangend met andere relevante initiatieven zoals het voorstel voor een verordening betreffende digitale operationele veerkracht voor de financiële sector ("DORA") en het voorstel voor een richtlijn betreffende de veerkracht van kritieke exploitanten van essentiële diensten. Het strookt ook met het Europees Wetboek voor elektronische communicatie, de algemene verordening gegevensbescherming en de eIDAS-verordening.

Het voorstel vormt een wezenlijk onderdeel van de EU-strategie voor de veiligheidsunie.

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

Het beheer van deze taken door Enisa vereist specifieke profielen en een aanvullende werklast die niet kunnen worden opgevangen zonder een verhoging van de personele middelen.

1.6. Duur en financiële gevolgen van het voorstel/initiatief

☐ **beperkte geldigheidsduur**

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

– ☐ financiële gevolgen vanaf JJJJ tot en met JJJJ

☒ **onbeperkte geldigheidsduur**

– uitvoering met een opstartperiode vanaf 2022 tot en met 2025,

– gevolgd door een volledige uitvoering.

1.7. Geplande beheersvorm(en)[57]

☒ **Direct beheer** door de Commissie

door

– ☐ de uitvoerende agentschappen

☐ **Gedeeld beheer** met de lidstaten

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

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

☐de EIB en het Europees Investeringsfonds;

☒ de in de artikelen 70 en 71 bedoelde organen;

☐ publiekrechtelijke organen;

☐ privaatrechtelijke organen met een openbare dienstverleningstaak, voor zover zij voldoende financiële garanties bieden;

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

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

Opmerkingen

Het Agentschap van de Europese Unie voor cyberbeveiliging, Enisa, waaraan een nieuw permanent mandaat is verleend bij de cyberbeveiligingsverordening, zou de lidstaten en de Commissie bijstaan in de uitvoering van de herziene NIS-richtlijn.

Ten gevolge van de herziene NIS-richtlijn zal Enisa met ingang van 2022/23 aanvullende actiegebieden hebben. Hoewel die actiegebieden volgens het mandaat van Enisa onder haar algemene taken zouden vallen, zullen zij een aanvullende werklast met zich meebrengen voor het Agentschap. Volgens het Commissievoorstel voor een herziene NIS-richtlijn zal ENISA, bovenop haar huidige actiegebieden, meer bepaald verplicht zijn om onder meer de volgende acties specifiek in haar werkprogramma op te nemen: (i) een Europees kwetsbaarheidsregister ontwikkelen en handhaven (artikel 6, lid 2, van het voorstel), (ii) het secretariaat van het Europees Netwerk van verbindingsorganisaties voor cybercrises

[57] Nadere gegevens over de beheersvormen en verwijzingen naar de Financiële Verordening zijn beschikbaar op BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

(CyCLONe) verzekeren (artikel 14 van het voorstel) en een jaarverslag over de staat van cyberbeveiliging in de EU opstellen (artikel 15 van het voorstel), (iii) de organisatie van collegiale toetsingen tussen de lidstaten ondersteunen (artikel 16 van het voorstel), (iv) geaggregeerde gegevens over incidenten verzamelen bij de lidstaten en technische richtsnoeren opstellen (artikel 20, lid 9, van het voorstel), (v) een register van entiteiten die grensoverschrijdende diensten verlenen opzetten en bijhouden (artikel 25 van het voorstel).

Er zal met ingang van 2022 derhalve een verzoek om 5 aanvullende VTE's worden ingediend, met een overeenkomstige begroting van ongeveer 0,61 miljoen EUR per jaar voor de nieuwe functies.

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

Vermeld frequentie en voorwaarden.

Op gezette tijden evalueert de Commissie de werking van deze richtlijn en brengt zij daarover verslag uit aan het Europees Parlement en de Raad. Dat gebeurt voor het eerst drie jaar na de inwerkingtreding.

De Commissie zal tevens nagaan of de lidstaten de richtlijn correct omzetten.

Het toezicht op en de verslaglegging over het voorstel zullen de in het permanente mandaat van Enisa uit hoofde van Verordening (EU) 2019/881 (cyberbeveiligingsverordening) beschreven beginselen volgen.

De gegevensbronnen die worden gebruikt voor het geplande toezicht zouden hoofdzakelijk afkomstig zijn van Enisa, de samenwerkingsgroep, het netwerk van CSIRT's en de autoriteiten van de lidstaten. Naast de gegevens uit de verslagen (waaronder de jaarlijkse activiteitenverslagen) van Enisa, de samenwerkingsgroep en het netwerk van CSIRT's, zouden specifieke gegevensvergaringsinstrumenten kunnen worden gebruikt waar nodig (bijvoorbeeld enquêtes bij de nationale autoriteiten, de Eurobarometer en verslagen van de campagne rond de maand van de cyberbeveiliging en de pan-Europese oefeningen).

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

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

De eenheid binnen DG CNECT die belast is met het beleidsterrein zal de uitvoering van de richtlijn beheren.

Wat het beheer van Enisa betreft, is in artikel 15 van de cyberbeveiligingsverordening een gedetailleerde lijst opgenomen van de controletaken van de raad van bestuur van Enisa.

Volgens artikel 31 van de cyberbeveiligingsverordening is de uitvoerend directeur van Enisa verantwoordelijk voor de uitvoering van de begroting van Enisa en heeft de interne controleur van de Commissie ten aanzien van Enisa dezelfde bevoegdheden als ten aanzien van de diensten van de Commissie. De raad van bestuur van Enisa brengt advies uit over de definitieve rekeningen van Enisa.

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

Bijzonder laag risico, aangezien het ecosysteem voor de NIS-richtlijn al bestaat en reeds betrekking heeft op Enisa, dat sinds de inwerkingtreding van de cyberbeveiligingsverordening in 2019 over een permanent mandaat beschikt.

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

De gevraagde verhoging van de begrotingsmiddelen past titel 1 toe en is bedoeld om salarissen te financieren. Dit houdt een bijzonder laag risico op fouten op betalingsniveau in.

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

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

De preventie- en beschermingsmaatregelen van Enisa zouden van toepassing zijn, en meer specifiek:

- Betalingen voor aangevraagde diensten of studies worden door het personeel van het Agentschap gecontroleerd alvorens de betaling wordt gedaan, rekening houdend met eventuele contractuele verplichtingen, economische beginselen en goede financiële of beheerspraktijken. Alle overeenkomsten en contracten tussen het Agentschap en de ontvangers van eventuele betalingen zullen antifraudebepalingen (toezicht, verslagleggingsvereisten enz.) bevatten.

- Om fraude, corruptie en andere onrechtmatige activiteiten te bestrijden, zijn de bepalingen van Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad van 25 mei 1999 betreffende onderzoeken door het Europees Bureau voor fraudebestrijding (OLAF) onverminderd van toepassing.

- Volgens artikel 33 van de Schengenuitvoeringsovereenkomst is Enisa uiterlijk op 28 december 2019 toegetreden tot het interinstitutioneel akkoord van 25 mei 1999 tussen het Europees Parlement, de Raad van de Europese Unie en de Commissie van de Europese Gemeenschappen betreffende de interne onderzoeken verricht door het Europees Bureau voor Fraudebestrijding (OLAF). Enisa stelt onverwijld de passende, voor alle werknemers van het Agentschap geldende bepalingen vast.

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

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

- Bestaande begrotingsonderdelen

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

Rubriek van het meerjarige financiële kader	Begrotingsonderdeel	Soort uitgaven	Bijdrage			
	Nummer	GK/NGK[58]	van EVA-landen[59]	van kandidaat-lidstaten[60]	van derde landen	in de zin van artikel 21, lid 2, punt b), van de Financiële Verordening
2	02 10 04	./NGK	JA	NEE	NEE	NEE

- Te creëren nieuwe begrotingsonderdelen

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

[58] GK = gesplitste kredieten/NGK = niet-gesplitste kredieten.
[59] EVA: Europese Vrijhandelsassociatie.
[60] Kandidaat-lidstaten en, in voorkomend geval, aspirant-kandidaten van de Westelijke Balkan.

Rubriek van het meerjarige financiële kader	Begrotingsonderdeel	Soort uitgaven	Bijdrage			
	Nummer	GK/NGK	van EVA-landen	van kandidaat-lidstaten	van derde landen	in de zin van artikel 21, lid 2, punt b), van de Financiële Verordening
	[XX.YY.YY.YY]		JA/NEEN	JA/NEEN	JA/NEEN	JA/NEEN

3.2. Geraamde gevolgen voor de uitgaven

3.2.1. Samenvatting van de geraamde gevolgen voor de uitgaven

In miljoen EUR (tot op drie decimalen)

Rubriek van het meerjarige financiële kader	Nummer	[Rubriek…2 Eengemaakte markt, innovatie en digitaal beleid……..……]

[Orgaan]: <…Enisa….>			Jaar **N**[61] **2022**	Jaar **N+1** **2023**	Jaar **N+2** **2024**	Jaar **N+3** **2025**	zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6) **2026**	**2027**		**TOTAAL**
Titel 1:	Vastleggingen	(1)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Betalingen	(2)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
Titel 2:	Vastleggingen	(1a)								
	Betalingen	(2a)								
Titel 3:	Vastleggingen	(3a)								
	Betalingen	(3b)								
TOTAAL kredieten voor [orgaan] <Enisa…….>	Vastleggingen	=1+1a +3a	0,61	0,61	O.61	0,61	0,61	0,61		**3,66**
	Betalingen	=2+2a +3b	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

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

Rubriek van het meerjarige financiële kader	**5**	"Administratieve uitgaven"

In miljoen EUR (tot op drie decimalen)

		Jaar **N**	Jaar **N+1**	Jaar **N+2**	Jaar **N+3**	zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)			**TOTAAL**
DG: <…….>									
• Personele middelen									
• Andere administratieve uitgaven									
TOTAAL DG <…….>	Kredieten								

TOTAAL kredieten in RUBRIEK 5 van het meerjarige financiële kader	(totaal vastleggingen = totaal betalingen)								

In miljoen EUR (tot op drie decimalen)

		Jaar **N**[62] **2022**	Jaar **N+1** **2023**	Jaar **N+2** **2024**	Jaar **N+3** **2025**	zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6) **2026**	**2027**		**TOTAAL**
TOTAAL kredieten in de RUBRIEKEN 1 t/m 5 van het meerjarige financiële kader	Vastleggingen	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Betalingen	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

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

3.2.2. Geraamde gevolgen voor de kredieten van [orgaan]

– ☐x Voor het voorstel/initiatief zijn geen beleidskredieten nodig

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

Vastleggingskredieten, in miljoen EUR (tot op drie decimalen)

Vermeld doelstellingen en outputs ⇩			Jaar **N**		Jaar **N+1**		Jaar **N+2**		Jaar **N+3**		zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)						**TOTAAL**	
	OUTPUTS																	
	Soort [63]	Gem. kosten	Nee	Kos-ten	Nee	Kos-ten	Nee	Kos-ten	Nee	Kos-ten	Nee	Kos-ten	Nee	Kos-ten	Nee	Kos-ten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 1[64]…																		
- Output																		
- Output																		
- Output																		
Subtotaal voor specifieke doelstelling nr. 1																		
SPECIFIEKE DOELSTELLING NR. 2…																		
- Output																		
Subtotaal voor specifieke doelstelling nr. 2																		

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

[64] Zoals beschreven in punt 1.4.2. “Specifieke doelstelling(en)…”.

TOTALE KOSTEN															

3.2.3. Geraamde gevolgen voor personele middelen van Enisa

3.2.3.1. Samenvatting

Ten gevolge van de herziene NIS-richtlijn zal Enisa met ingang van 2022/23 aanvullende taken hebben. Hoewel die taken onder het mandaat van Enisa zouden vallen, zullen zij een aanvullende werklast met zich brengen voor het Agentschap. Volgens het Commissievoorstel voor een herziene NIS-richtlijn zal ENISA, bovenop haar huidige taken, meer bepaald belast worden met (i) de ontwikkeling en het bijhouden van een Europees kwetsbaarheidsregister (artikel 6, lid 2), (ii) het verzekeren van het secretariaat van het Europees Netwerk van verbindingsorganisaties voor cybercrises (CyCLONe) (artikel 14) en het opstellen van een jaarverslag over de staat van cyberbeveiliging in de EU (artikel 15), (iii) het ondersteunen van de organisatie van collegiale toetsingen tussen de lidstaten (artikel 16), (iv) het verzamelen van geaggregeerde gegevens over incidenten bij de lidstaten en het opstellen van technische richtsnoeren (artikel 20, lid 9), (v) het opzetten en bijhouden van een register van entiteiten die grensoverschrijdende diensten verlenen (artikel 25).

Er zal met ingang van 2022 derhalve een verzoek om 5 aanvullende VTE's worden ingediend, met een overeenkomstige begroting voor de nieuwe functies.

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

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

In miljoen EUR (tot op drie decimalen)

	Jaar **N** [65] **2022**	Jaar **N+1** **2023**	Jaar **N+2** **2024**	Jaar **N+3** **2025**	zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6) **2026** **2027**			**TOTAAL**
Tijdelijke functionarissen (AD-rangen)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Tijdelijke functionarissen (AST-rangen)								
Arbeidscontractanten	0,160	0,160	0,160	0,160	0,160	0,160		**0,96**
Gedetacheerde nationale deskundigen								

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

TOTAAL	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Personeelsbehoeften (VTE):

	Jaar **N** [66] **2022**	Jaar **N+1** **2023**	Jaar **N+2** **2024**	Jaar **N+3** **2025**	zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6) **2026** **2027**			**TOTAAL**
Tijdelijke functionarissen (AD-rangen)	3	3	3	3	3	3		**18**
Tijdelijke functionarissen (AST-rangen)								
Arbeidscontractanten	2	2	2	2	2	2		**12**
Gedetacheerde nationale deskundigen								
TOTAAL	**5**	**5**	**5**	**5**	**5**	**5**		**30**

3.2.3.2. Geraamde personeelsbehoeften voor het bevoegde DG

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

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

Raming in een geheel getal (of met hoogstens één decimaal)

	Jaar **N**	Jaar **N+1**	Jaar **N+2**	Jaar **N+3**	zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)		
• **Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)**							
XX 01 01 01 (zetel en vertegenwoordigingen van de Commissie)							
XX 01 01 02 (delegaties)							

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

XX 01 05 01 (onderzoek door derden)								
10 01 05 01 (eigen onderzoek)								
• Extern personeel (in voltijdequivalenten: VTE)[67]								
XX 01 02 01 (AC, END, SNE van de "algemene toewijzing")								
XX 01 02 02 (AC, AL, END, INT en JPD in de delegaties)								
XX 01 04 ***jj***[68]	- zetel[69]							
	- delegaties							
XX 01 05 02 (AC, END, INT – onderzoek door derden)								
10 01 05 02 (AC, END, SNE – eigen onderzoek)								
Ander begrotingsonderdeel (te vermelden)								
TOTAAL								

XX is het beleidsterrein of de begrotingstitel.

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

Beschrijving van de uit te voeren taken:

Ambtenaren en tijdelijk personeel	
Extern personeel	

De omschrijving van de berekening van de kosten voor VTE-eenheden dient te worden opgenomen in bijlage V, punt 3.

67 AC= Agent Contractuel (arbeidscontractant); AL= Agent Local (plaatselijk functionaris); END = Expert National Détaché (gedetacheerd nationaal deskundige); INT= Intérimaire (uitzendkracht); JPD = Junior Professionals in Delegations (jonge deskundige in delegaties).

68 Subplafond voor extern personeel uit beleidskredieten (vroegere "BA"-onderdelen).

69 Voornamelijk voor de structuurfondsen, het Europees Landbouwfonds voor plattelandsontwikkeling (Elfpo) en het Europees Visserijfonds (EVF).

3.2.4. Verenigbaarheid met het huidige meerjarige financiële kader

– ☒ Het voorstel/initiatief is verenigbaar met het huidige meerjarige financiële kader

– ☐ Het voorstel/initiatief vergt herprogrammering van de betrokken rubriek van het meerjarige financiële kader

Zet uiteen welke herprogrammering nodig is, onder vermelding van de betrokken begrotingsonderdelen en de desbetreffende bedragen. Het voorstel is verenigbaar met het MFK 21/27. De aangevraagde begroting voor de verhoging van de personele middelen in Enisa zal worden gecompenseerd door de begroting van het programma Digitaal Europa in dezelfde rubriek met hetzelfde bedrag te verlagen.

– ☐ Het voorstel/initiatief vergt toepassing van het flexibiliteitsinstrument of herziening van het meerjarige financiële kader[70].

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

3.2.5. Bijdragen van derden

– Het voorstel/initiatief voorziet niet in medefinanciering door derden.

– Het voorstel/initiatief voorziet in medefinanciering, zoals hieronder geraamd:

In miljoen EUR (tot op drie decimalen)

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

[70] Zie de artikelen 11 en 17 van Verordening (EU, Euratom) nr. 1311/2013 tot bepaling van het meerjarige financiële kader voor de jaren 2014- 2020.

3.3. Geraamde gevolgen voor de ontvangsten

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

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

☐ voor de eigen middelen

☐ voor overige ontvangsten

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

In miljoen EUR (tot op drie decimalen)

Begrotingsonderdeel voor ontvangsten:	Voor het lopende begrotingsjaar beschikbare kredieten	Gevolgen van het voorstel/initiatief[71]						
		Jaar **N**	Jaar **N+1**	Jaar **N+2**	Jaar **N+3**	zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)		
Artikel ……								

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

Vermeld de wijze van berekening van de gevolgen voor de ontvangsten.

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