22112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 4284 Brief van de minister van Buitenlandse Zaken

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 6 maart 2026

Overeenkomstig de bestaande afspraken ontvangt u hierbij vier fiches die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissie voorstellen (BNC).

Fiche: Verordening versterking *Carbon Border Adjustment Mechanism* en verordening Tijdelijk Fonds voor Koolstofvrijmaking (Kamerstuk 22 112, nr. 4283)
Fiche: Simplificatie NIS2-richtlijn
Fiche: Mededeling EU *Anti-Racism Strategy* 2026-2030 (Kamerstuk 22 112, nr. 4285)
Fiche: Herziening *Cybersecurity Act (Kamerstuk 22 12, nr. 4286)*

De minister van Buitenlandse Zaken,
T.B.W. Berendsen

Fiche: Simplificatie NIS2-richtlijn

1. Algemene gegevens

a) Titel voorstel

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]

b) Datum ontvangst Commissiedocument

20 januari 2026

c) Nr. Commissiedocument

COM (2026) 13

d) EUR-Lex

EUR-Lex - 52026PC0013 - EN - EUR-Lex

e) Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing

SWD(2026) 11

f) Behandelingstraject Raad

Telecom Raad

g) Eerstverantwoordelijk ministerie

Ministerie van Justitie en Veiligheid

h) Rechtsbasis

Artikel 114 VWEU

i) Besluitvormingsprocedure Raad

Gekwalificeerde meerderheid

j) Rol Europees Parlement

Medebeslissing

2. Essentie voorstel

a) Inhoud voorstel

Op 20 januari 2026 heeft de Europese Commissie (hierna: de Commissie) een voorstel gepubliceerd tot simplificatie van de zogeheten NIS2-richtlijn[1] in verband met de simplificatie en aanpassing aan het voorstel voor de nieuwe Cybersecurity Act (2) (hierna: CSA2). Met de NIS2-richtlijn heeft de Europese Unie (hierna: EU) beoogd het gezamenlijke cyberbeveiligingsniveau in de EU te verhogen. De implementatiedeadline voor de NIS2-richtlijn was 17 oktober 2024, deze deadline is door Nederland niet gehaald.[2] De NIS2-richtlijn wordt in Nederland geïmplementeerd met de Cyberbeveiligingswet. Het voorstel voor de Cyberbeveiligingswet ligt ter behandeling in de Tweede Kamer.

Het Commissievoorstel ziet allereerst op een aantal aanpassingen van de beschrijving van entiteiten die onder de NIS2-richtlijn vielen. Dit is volgens de Commissie nodig ter verduidelijking en om lasten bij entiteiten en nationale autoriteiten te verminderen.[3] Zo vallen voortaan bijvoorbeeld elektriciteitsproducenten alleen onder de NIS2-richtlijn indien zij een totale opwekkingscapaciteit van meer dan 1 megawatt hebben. Om het toepassingsbereik van de NIS2-richtlijn met betrekking tot entiteiten binnen de subsector waterstof te verduidelijken, stelt de Commissie daarnaast voor de beschrijving betreffende exploitanten van voorzieningen voor de productie, opslag en transmissie van waterstof op te splitsen en te voorzien van een referentie naar definities uit de Richtlijn (EU) 2024/1788 van het Europees Parlement en de Raad.[4] Bij DNS-dienstverleners[5] wordt ervoor gekozen om

---

[1] Zie https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52026PC0013.
[2] Zie ook de Kamerbrief over gevolgen niet tijdige implementatie NIS2 en CER-richtlijn, Kamerbrief over gevolgen niet tijdige implementatie NIS2 en CER-richtlijn | Kamerstuk | Rijksoverheid.nl.
[3] Zie ook ANNEX to the Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2], EUR-Lex - 52026PC0013 - EN - EUR-Lex.
[4] Zie ook Richtlijn - EU - 2024/1788 - EN - EUR-Lex.
[5] Domaine Name System

dergelijke entiteiten, indien zij micro of klein zijn, buiten het toepassingsbereik van de NIS2-richtlijn te plaatsen.

Daarnaast worden enkele nieuwe soorten entiteiten onder het toepassingsbereik van de NIS2-richtlijn gebracht, ten eerste providers van *European Digital Identity Wallets* (hierna: EUDI-*wallets*) en European Business *Wallets* (binnen de sector digitale infrastructuur). Ook stelt de Commissie voor om (eveneens binnen de sector digitale infrastructuur) operators van onderzeese datatransmissie infrastructuur onder het toepassingsbereik van de NIS2-richtlijn te laten vallen. Dit geldt eveneens voor entiteiten die vallen onder het nieuwe voorstel van de Commissie van november 2025 dat ziet op het vervoer van militair materieel en personeel en van militaire goederen binnen de EU (binnen de subsector wegvervoer).[6]

Om de regeldruk voor zowel entiteiten als toezichthouders te beperken introduceert het voorstel een nieuwe categorie *small mid-cap* bedrijven, in lijn met de aanbeveling van de Europese Commissie 2025/1099.[7] Voor entiteiten die genoemd zijn in bijlage I van de NIS2-richtlijn geldt nu dat zij als essentiële entiteiten worden aangemerkt in geval zij als grote onderneming kwalificeren. Met dit voorstel wordt in plaats daarvan geregeld dat deze soorten entiteiten alleen als zij *groter* zijn dan *small mid-cap* als essentiële entiteiten worden aangemerkt én daardoor dat sommige van deze entiteiten voortaan als belangrijke entiteit worden aangemerkt. Zij zullen daarmee onder een ‘lichter’ toezichtregime vallen.
Ook doet de Commissie voorstellen met betrekking tot certificering in relatie tot de zorgplicht voor essentiële entiteiten en belangrijke entiteiten onder de NIS2-richtlijn. In lijn met het voorgestelde certificeringsraamwerk in de CSA2 wordt de bevoegdheid voor lidstaten gecreëerd om aan entiteiten een zogeheten *cyberposture* certificering op te kunnen leggen, om aan te tonen dat zij voldoen aan de zorgplichtmaatregelen bedoeld in artikel 21 van de NIS2-richtlijn. Toezichthouders mogen bovendien entiteiten niet (meer) onderwerpen aan

---

[6] Zie ook VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD tot vaststelling van een kader van maatregelen om het vervoer van militair materieel en personeel en van militaire goederen in de hele Unie te vergemakkelijken, EUR-Lex - 52025PC0847 - EN - EUR-Lex.
[7] Commission Recommendation (EU) 2025/1099 of 21 May 2025 on the definition of small mid-cap enterprises (OJ L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).

beveiligingsaudits voor zover de betreffende onderdelen door de certificering worden gedekt. Volgens de Commissie zorgt dit, met name voor entiteiten die in meer dan één lidstaat hun diensten verlenen, voor coherentie binnen de interne markt en beperkt het de toezichtlasten.

Essentiële entiteiten en belangrijke entiteiten moeten in het kader van de zorgplicht onder meer maatregelen nemen ten aanzien van de beveiliging van hun toeleveringsketen. Gebleken is dat deze entiteiten ten behoeve daarvan (toekomstige) leveranciers en dienstverleners uitgebreid en op uiteenlopende wijze om informatie verzoeken. De Commissie stelt daarom voor om *guidelines* te ontwikkelen met aanbevelingen met betrekking tot een passend detailniveau en formats inzake het opvragen van dergelijke informatie bij voornoemde leveranciers en dienstverleners. De Commissie beoogt hiermee de lasten voor de leveranciers en dienstverleners te verlichten en om een consistente en efficiënte aanpak voor de beveiliging van de toeleveringsketen te bevorderen.

De Commissie stelt maximumharmonisatie voor in relatie tot de uitvoeringshandelingen met betrekking tot de zorgplichtmaatregelen.[8] Indien de Commissie dergelijke uitvoeringshandelingen vaststelt, wordt lidstaten daarmee op dit onderdeel van de richtlijn de bevoegdheid ontzegd om, zoals nu nog wel krachtens artikel 5 van de NIS2-richtlijn mogelijk is, bepalingen vast te stellen of te handhaven die een hoger cyberbeveiligingsniveau waarborgen. Hiermee beoogt de Commissie de naleving door entiteiten, die in meer dan één lidstaat hun diensten verlenen, en het toezicht te vergemakkelijken.

Vanwege de groeiende ‘quantum-dreiging’ stelt de Commissie voor dat lidstaten post-quantum cryptografie verplicht onderdeel maken van de nationale cyberbeveiligingsstrategie.

Ook stelt de Commissie voor om datacollectie over *ransomware*-aanvallen bij daarbij betrokken essentiële entiteiten of belangrijke entiteiten te harmoniseren en te verbeteren, door te bepalen dat deze entiteiten in het kader van de NIS2-

---

[8] De Commissie beoordeelt regelmatig of er uitvoeringshandelingen voor specifieke sectoren of soorten entiteiten moeten worden vastgesteld. De Europese Commissie heeft op 17 oktober 2024 een uitvoeringsverordening vastgesteld voor de digitale sector die zowel de meldplicht als de zorgplicht voor deze sector specificeert (Implementing regulation - EU - 2024/2690 - EN - EUR-Lex).

meldplicht verplicht worden gesteld aanvullende informatie hierover al dan niet op verzoek aan te leveren bij het CSIRT (Computer Security Incident Response Teams) of bevoegde autoriteit via een communicatiekanaal, inclusief informatie over eventuele betalingen.

Tot slot stelt de Commissie een nieuwe, assisterende rol voor ENISA (het Agentschap van de Europese Unie voor cyberbeveiliging) voor in geval van samenwerking tussen de bevoegde autoriteiten binnen de EU (wederzijdse bijstand). De Commissie beoogt hiermee de naleving van de gestelde verplichtingen onder de NIS2-richtlijn voor entiteiten die in meer dan één lidstaat hun diensten verlenen te vergemakkelijken, de samenhang te waarborgen en efficiënt toezicht te bevorderen.

In relatie hiermee bevat het voorstel ook de verplichting voor lidstaten om voortaan voor alle essentiële entiteiten en belangrijke entiteiten informatie aan te leveren ten behoeve van het register van entiteiten in beheer bij ENISA. Dit register ziet nu slechts op entiteiten in de sectoren digitale infrastructuur en digitale aanbieders. ENISA zal mede aan de hand van deze gegevens analyses uitvoeren over grensoverschrijdende cyberbeveiligingsrisico's en vervolgens een rapport hierover opstellen. Op basis van dit rapport kan ENISA – al dan niet op verzoek van de bevoegde autoriteiten – onder meer aanbevelingen aan de bevoegde autoriteiten doen om gezamenlijke onderzoeksteams op te richten, *guidelines* ontwikkelen voor gezamenlijke toezichtacties en, op verzoek van de bevoegde autoriteiten, bijstand verlenen bij de beoordeling van de mate waarin een essentiële entiteit of belangrijke entiteit voldoet aan de zorgplichtmaatregelen, bedoeld in artikel 21 van de NIS2-richtlijn.

Tot slot stelt de Commissie voor om ENISA aan te merken als volwaardig lid van het netwerk van nationale CSIRT's.

b) Impact assessment Commissie
Hiervoor wordt u verwezen naar het BNC-fiche Herziening CSA.[9]

3. Nederlandse positie ten aanzien van het voorstel

[9] BNC-fiche Herziening CSA

a) Essentie Nederlands beleid op dit terrein

Nederland is één van de meest gedigitaliseerde lidstaten. Vrijwel alle economische en maatschappelijke processen maken gebruik van digitale middelen. Digitale veiligheid is daarom een noodzakelijke voorwaarde om deze processen draaiende te houden. De cybersecurityaanpak van het kabinet is vastgelegd in de Nederlandse Cybersecuritystrategie (hierna: NLCS).[10] De NLCS zet in vier pijlers de kabinetsinzet uiteen voor het realiseren van een digitaal veilige en weerbare samenleving. Naast speerpunten en samenwerking op nationaal niveau, benadrukt de NLCS dat internationale samenwerking, zowel in EU en NAVO-verband als daarbuiten, essentieel is, dit gezien het grensoverschrijdende karakter van cyberdreigingen. Het kabinet zet zich daarom actief in bij de verschillende Europese gremia en samenwerkingsverbanden met als doel de digitale weerbaarheid van de EU te vergroten.

In pijler I van de NLCS wordt het belang van de digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties benadrukt, waarbij het kabinet zich onder andere tot doel stelt dat organisaties zicht hebben op cyberincidenten, - dreigingen en -risico's en dat organisaties hiertegen goed beschermd zijn. Van belang is in dit verband de implementatie van de NIS2-richlijn in de Cyberbeveiligingswet, die zal leiden tot de versterking van de digitale weerbaarheid.

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet onderkent de noodzaak van stevige Europese samenwerking op het gebied van digitale veiligheid en ondersteunt harmonisatie binnen de EU en de daaraan gerelateerde simplificatie van wetgeving op dit gebied. Het kabinet verwelkomt dan ook het voorstel van de Commissie tot simplificatie van de NIS2-richtlijn dat hiertoe strekt.

Het kabinet kijkt ten eerste positief naar de verduidelijkingen van de beschrijving van enkele soorten entiteiten die al onder het toepassingsbereik van de NIS2-richtlijn vielen. De verduidelijkingen leiden tot meer rechtszekerheid en voorkomen mogelijke verschillende interpretaties tussen de lidstaten.

---

[10] Nederlandse Cybersecuritystrategie 2022-2028 | Nationaal Coördinator Terrorismebestrijding en Veiligheid.

Het kabinet verwelkomt de aanpassing van de definitie voor entiteiten binnen de waterstofsector in lijn met bestaande wet- en regelgeving omdat dit meer duidelijkheid biedt over het toepassingsbereik. Ook staat het kabinet positief tegenover het voorstel om micro- of kleine DNS-dienstverleners niet langer onder het toepassingsbereik van de NIS2-richtlijn te laten vallen. Het kabinet staat ook positief tegenover het beperken van het toepassingsbereik van elektriciteitsproducenten zodat alleen producenten die daadwerkelijk impact kunnen hebben op de stabiliteit van het elektriciteitsnet onder het toepassingsbereik van de NIS2-richtlijn vallen. Het kabinet merkt hierbij op dat de voorgestelde drempelwaarde voor Nederland ontoereikend is. Het kabinet vraagt daarnaast de Commissie om het toepassingsbereik te verduidelijken van exploitanten van laadpunten en marktdeelnemers die energieopslagdiensten verstrekken en dit in lijn te brengen met het toepassingsbereik van elektriciteitsproducenten. Het kabinet zal zich inzetten om te zorgen dat deze definities aansluiten bij het ontwerp van het elektriciteitsnet en de proportionaliteit die het kabinet heeft beoogd met de huidige specificering in de Cyberbeveiligingswet, die op onderdelen afwijkt van het voorstel van de Commissie.

Daarnaast oordeelt het kabinet positief over het voorstel tot uitbreiding van het toepassingsbereik van de NIS2-richtlijn met enkele nieuwe soorten entiteiten, namelijk EUDI-*wallets* en *European Business Wallets* (sector digitale infrastructuur) omdat kan worden onderschreven dat, zoals de Commissie zelf ook aangeeft, deze entiteiten een essentieel deel zijn van de Europese digitale infrastructuur en zij daarom onder meer aan de in de NIS2-richtlijn bedoelde zorgplicht moeten voldoen. Het kabinet staat tevens positief tegenover het onder het toepassingsbereik van de NIS2-richtlijn brengen van operators van onderzeese datatransmissie infrastructuur (binnen de sector digitale infrastructuur) voor zover zij hier nog niet onder vielen, aangezien deze essentieel zijn voor het functioneren van het internet. De exploitanten van de datakabels die momenteel in Nederland aanlanden vallen reeds onder de NIS2-richtlijn omdat zij behoren tot de categorie aanbieders van openbare elektronische communicatienetwerken, maar deze uitbreiding is wenselijk nu ook niet-traditionele partijen zoals *hyperscalers* een groeiend aandeel hebben in deze infrastructuur en het van belang is dat ook zij onder het toepassingsbereik van de NIS2-richtlijn vallen. Ten aanzien van de aanvulling voor de infrastructuur

voor het militair materieel en personeel en van militaire goederen binnen de EU (binnen de subsector wegvervoer) geldt dat het kabinet verwacht dat de beheerders van deze infrastructuur reeds zonder wijziging onder het toepassingsbereik van de NIS2-richtlijn vallen. Het kabinet vraagt de Commissie om verduidelijking of deze soorten entiteiten als essentiële entiteiten dan wel als belangrijke entiteiten zouden worden aangemerkt.

Met het oog op het stroomlijnen van de NIS2-richtlijn en de CER-richtlijn beziet het kabinet nog in hoeverre bovenstaande voorgestelde wijzigingen in de definities en toevoeging van nieuwe sectoren ook gevolgen zou moeten hebben voor de CER-richtlijn.

Het kabinet is positief over het toevoegen van een nieuwe categorie *small mid-cap* bedrijven indien dit bijdraagt aan substantiële lastenvermindering. Naar het kabinet begrijpt, gaat het hier om een categorie die tussen middelgrote en grote bedrijven valt. Dit houdt in dat de criteria om als grote onderneming – en daarmee in de context van NIS2 als essentiële entiteit – te worden aangemerkt, worden verhoogd. Het kabinet kan in het huidige voorstel onvoldoende beoordelen of dit bijdraagt aan lastenvermindering. Het kabinet vraagt mede daarom om nadere toelichting hoe de categorieën van entiteiten zich tot elkaar verhouden en wat dit betekent voor kwalificatie als essentiële of belangrijke entiteit. Onderstaande overwegingen zijn voor het kabinet ook van belang.

Onder de NIS2-richtlijn is er een verschil in toezicht tussen essentiële entiteiten en belangrijke entiteiten: essentiële entiteiten staan onder proactief toezicht en belangrijke entiteiten staan onder reactief toezicht. Daarnaast beschikt de bevoegde autoriteit in de handhaving van de naleving van de verplichtingen door essentiële entiteiten, over meer bevoegdheden dan ten aanzien van de handhaving van de naleving van de verplichtingen door belangrijke entiteiten. De toevoeging van deze nieuwe categorie *small mid-cap* bedrijven zal daarom impact hebben op de lasten voor de toezichthouders, aangezien een deel van de nu als essentieel aangemerkte entiteiten straks als belangrijke entiteiten worden aangemerkt en zij daarmee onder een ‘lichter’ toezichtregime vallen. Het kabinet vraagt zich af wat de langetermijneffecten zijn, specifiek met het oog op de cyberweerbaarheid van Nederland en daarmee Europa, nu de toezichthouders – voor een grotere groep entiteiten – niet meer *vooraf* gaan controleren maar

achteraf, bij signalen van niet-naleving van de verplichtingen onder de NIS2-richtlijn of nadat er al een incident heeft plaatsgevonden.

Het kabinet merkt op dat het voorstel lidstaten de mogelijkheid biedt gebruik te maken van een verplichting voor essentiële of belangrijke entiteiten tot *cyberposture* certificering om daarmee aan te tonen dat zij voldoen aan de zorgplichtmaatregelen. Het kabinet staat positief tegenover het voorstel om lidstaten die mogelijkheid te bieden, omdat het kan bijdragen aan een versterking van de interne markt en het vergroten van de uitvoerbaarheid van de NIS2-richtlijn voor entiteiten die in meer dan één lidstaat hun diensten verlenen. Het kabinet vraagt de Commissie wel om nadere uitleg over hoe de inhoudelijke beoordeling van de *cyberposture* certificering eruit zal zien, hoe de gebruikmaking van deze certificering als vereiste in de praktijk zal werken, met name ook in relatie tot het toezicht, en hoe deze certificering zich verhoudt tot het voorgestelde certificeringsraamwerk in de CSA2.

Het kabinet benadrukt dat certificering toezicht niet mag vervangen en niet mag leiden tot het automatisch voldoen aan de zorgplicht, bedoeld in de NIS2-richtlijn. Het kabinet is daarom kritischer op het voorstel om de auditbevoegdheden van een toezichthouder te beperken. Hoewel er oog is voor de lasten van toezichthandelingen, zowel aan de kant van de toezichthouder als aan de kant van de onder toezicht gestelde entiteit, is de ervaring dat certificering niet voor alle entiteiten als een gelijkwaardige vervanging van een audit door een toezichthouder kan worden gezien. Ook komt het vaker voor dat het certificaat slechts op een beperkt aantal elementen van netwerk- en informatiesystemen ziet. Het kabinet heeft daarom bedenkingen bij het beperken van de auditbevoegdheid van de toezichthouder ingeval van gecertificeerde entiteiten. Bovendien merkt het kabinet op dat voor belangrijke entiteiten de auditbevoegdheid in die gevallen volledig zou komen te vervallen, terwijl de ad-hoc audits voor essentiële entiteiten wel mogelijk blijven.
Ook benadrukt het kabinet dat entiteiten de ruimte moeten blijven houden om andere (nationale en internationale) normenkaders die zij reeds hanteren te behouden om daarmee aantoonbaar aan de zorgplicht te voldoen. Dit ook in het kader van lastenvermindering voor die entiteiten die, zoals bijvoorbeeld binnen de sectoren waarin veel gebruik wordt gemaakt van Operationele Technologie (OT), hun eigen normenkader hanteren.

Tot slot benadrukt het kabinet dat Europese cybersecuritycertificering onder de CSA niet kan worden gelijkgesteld aan, noch in de plaats kan treden van, de specifieke *assurance*-, toezicht- en notificatievereisten die gelden onder eIDAS voor elektronische identificatiemiddelen, vertrouwensdiensten en EUDI-*wallets*.

Het kabinet kijkt positief naar de rol die de Commissie wil pakken voor het ontwikkelen van *guidelines* voor het vergemakkelijken van de uitvoeringspraktijk ten aanzien van het door essentiële entiteiten of belangrijke entiteiten bij leveranciers en dienstverleners opvragen van informatie ten behoeve van het voldoen aan de maatregelen inzake de beveiliging van de toeleveringsketen. Hiermee worden de lasten voor die leveranciers en dienstverleners verlicht en wordt er zorggedragen voor een consistente, proportionele en efficiënte beoordeling van de beveiliging van de toeleveringsketen.

Het kabinet is voorstander van het harmoniseren van de door essentiële entiteiten en belangrijke entiteiten te nemen zorgplichtmaatregelen door middel van uitvoeringshandelingen, met name voor entiteiten die in meer dan één lidstaat hun diensten verlenen en in één sector actief zijn. Het voorstel dient wel in samenhang te worden gezien met wat al nationaal is vastgelegd. Het kabinet plaatst echter wel kanttekeningen bij de nu voorgestelde maximumharmonisatie die daaraan in het voorstel wordt gekoppeld, aangezien het mogelijk is dat er (sector)specifieke dreigingen of risico’s in een lidstaat zijn waarbij het mogelijk dient te blijven om als lidstaat aanvullende zorgplichtmaatregelen te vereisen. Daarnaast vraagt het kabinet zich af of de voorgestelde maximum harmonisatie uitsluitend ziet op de maatregelen, die uitdrukkelijk zijn benoemd in artikel 21, tweede lid, onderdelen a tot en met j, NIS2-richtlijn, of dat het gaat om alle mogelijke maatregelen die in het kader van de zorgplicht getroffen kunnen worden. Het kabinet onderzoekt de werkbaarheid van maximumharmonisatie, onder meer vanwege entiteiten die in meerdere sectoren actief zijn.

Het kabinet verwelkomt het voorstel van het opnemen van post-quantum cryptografie beleid als onderdeel van de nationale cyberbeveiligingsstrategie en omarmt het voorstel omdat dit een ondersteuning is van nationaal beleid.

Het kabinet staat positief tegenover het verbeteren van de datacollectie over *ransomware*-aanvallen. Deze data verzameling kan er namelijk onder meer toe bijdragen dat er betere ondersteuning van deze entiteiten kan plaatsvinden door de CSIRT's en het zicht op *ransomware*-aanvallen binnen de EU wordt vergroot.

Het kabinet heeft wel vragen over de wijze waarop het voorstel is ingericht. Het voorgestelde artikel 23, twaalfde lid, NIS2-richtlijn, waarbij aanvullende informatie wordt gevraagd over de *ransomware*-aanval, wordt gekoppeld aan (toekomstige) uitvoeringshandelingen. Terwijl het voorgestelde artikel 23, dertiende lid, waarbij – op verzoek van het CSIRT – aanvullende informatie wordt gevraagd over eventuele betalingen, *niet* gekoppeld is aan (toekomstige) uitvoeringshandelingen. Het kabinet is van oordeel dat de in het twaalfde lid bedoelde informatie over *ransomware*-aanvallen onlosmakelijk is verbonden met de informatie in het dertiende lid en dat daarom geldt dat het verstrekken van die in het twaalfde lid bedoelde informatie eveneens in de NIS2-richtlijn zelf zou moeten worden opgenomen. Het kabinet vraagt de Commissie hierover graag om nadere uitleg.

Het kabinet merkt ook op dat een duidelijke definitie van het begrip *ransomware* ontbreekt. Een eenduidige definitie is van belang voor de gewenste geharmoniseerde datacollectie. Het kabinet heeft een voorkeur voor een definitie die aansluit bij de definitie die momenteel nationaal wordt gehanteerd, waarbij er niet per definitie sprake hoeft te zijn van versleuteling van de gegevens, maar van alle gevallen waarin losgeld gevraagd wordt. Het kabinet denkt graag mee met opstellen van een passende definitie in lijn met de huidige ontwikkelingen in de ICT. Tot slot is het de inzet van het kabinet om in de wijze waarop de voorstellen die zien op *ransomware* worden vormgegeven, de belangen van de rechtshandhaving te waarborgen.

Het kabinet kijkt positief naar de voorgestelde rol voor ENISA om de samenwerking tussen de bevoegde autoriteiten binnen de EU te bevorderen en te assisteren in wederzijdse bijstand tussen die autoriteiten. In dit verband wil ENISA ook analyses over grensoverschrijdende cyberrisico's opstellen om in het kader daarvan, al dan niet op verzoek van de bevoegde autoriteiten, ondersteunde maatregelen te nemen (waaronder *guidelines* voor gezamenlijke toezichtsacties). Het kabinet ondersteunt het principe dat, omdat verschillende

essentiële entiteiten of belangrijke entiteiten in meer dan één lidstaat diensten verlenen, efficiënte internationale samenwerking tussen toezichthouders noodzakelijk is en ziet in dat verband meerwaarde in het inzichtelijk krijgen van grensoverschrijdende cyberrisico's. Het kabinet ondersteunt het vrijwillige karakter van deze wederzijdse bijstand, zodat lidstaten de ruimte hebben om deze bijstand te verzoeken. Het kabinet volgt de uitwerking van dit voorstel dan ook met interesse, specifiek hoe deze nieuwe rol van ENISA zich gaat verhouden tot het taakgebied van nationale instanties en bevoegde autoriteiten.

Ook is het voor het kabinet (nog) onduidelijk of de uitbreiding van het register van entiteiten in beheer bij ENISA, waarbij de verplichting voor lidstaten is opgenomen om voortaan voor alle essentiële entiteiten en belangrijke entiteiten informatie aan te leveren, bedoeld is voor de assisterende rol van ENISA. Het kabinet vraagt zich in dit verband af of het noodzakelijk is om in het kader van de bovenbedoelde analyses deze verplichting voor lidstaten op te nemen. Het kabinet ziet hierover graag een nadere onderbouwing. Het kabinet vraagt zich daarnaast af of en zo ja, waarvoor de ten behoeve van het register bij ENISA aan te leveren informatie nog meer gebruikt zou (kunnen) worden, waarom het voorstel voor een uitbreiding van dat register van entiteiten bij ENISA ongeclausuleerd is en waarom gebruikmaking van het register noodzakelijk zou zijn voor het verrichten van eventuele andere doeleinden. Daarbij verwijst het kabinet naar de zorgen die zij reeds in het fiche aangaande de Digitale Omnibus en het fiche aangaande de CSA-herziening heeft geuit bij de rol van ENISA ten aanzien van een Europees centraal platform voor rapportageverplichtingen, voor zover deze nog niet zijn weggenomen.

Tot slot vraagt het kabinet zich af of het noodzakelijk is om ENISA als volwaardig lid aan te merken van het netwerk van nationale CSIRT's en ziet hiervoor graag een nadere onderbouwing gekoppeld aan de taken van ENISA.

c) Eerste inschatting van krachtenveld

De meerderheid van lidstaten verwelkomt naar verwachting dat de Commissie met dit voorstel de NIS2-richtlijn wil versimpelen en regeldruk wil verlagen. Ook het verduidelijken van enkele beschrijvingen en de uitbreiding van het toepassingsbereik van de NIS2-richtlijn kan naar verwachting op hun steun rekenen. Lidstaten zullen goed de samenhang bestuderen met het voorstel voor

de CSA2 als het gaat om certificering en de rol van ENISA, evenals de Digitale Omnibus, ten aanzien waarvan geldt dat een grote groep lidstaten zorgen heeft geuit over de oprichting van één Europees meldpunt van incidenten. De positie van het Europees Parlement is onbekend.

4. Beoordeling bevoegdheid, subsidiariteit en proportionaliteit

a) Bevoegdheid

Als onderdeel van de toets of de EU mag optreden conform de EU-verdragen toetst het kabinet of de EU handelt binnen de grenzen van de bevoegdheden die haar door de lidstaten in de EU-verdragen zijn toegedeeld om de daarin bepaalde doelstellingen te verwezenlijken. Het oordeel van het kabinet over de bevoegdheid voor dit voorstel tot wijziging van de NIS2-richtlijn positief.
Het voorstel is gebaseerd op artikel 114 VWEU. Artikel 114 VWEU geeft de EU de bevoegdheid tot het vaststellen van maatregelen betreffende de interne markt. Het kabinet kan zich vinden in deze voorgestelde rechtsgrondslag, nu de in dit voorstel vervatte bepalingen in hoofdzaak betrekking hebben op de werking van de interne markt. Op het terrein van de interne markt is sprake van een gedeelde bevoegdheid tussen de EU en de lidstaten (artikel 4, tweede lid, sub a, VWEU). Het kabinet zal er steeds op toe blijven zien dat de inhoud van het voorstel, bijvoorbeeld als het gaat om de voorgestelde maximum harmonisatie in relatie tot de uitvoeringshandelingen betreffende de zorgplicht, niet op gespannen voet komt te staan met in het bijzonder de uitsluitende verantwoordelijkheid van de lidstaten op het gebied van de nationale veiligheid (artikel 4, tweede lid, VEU).

b) Subsidiariteit

Als onderdeel van de toets of de EU mag optreden conform de EU-verdragen toetst het kabinet de subsidiariteit van het optreden van de Commissie. Dit houdt in dat het kabinet op de gebieden die niet onder de exclusieve bevoegdheid van de Unie vallen of wanneer sprake is van een voorstel dat gezien zijn aard enkel door de EU kan worden uitgeoefend, toetst of het overwogen optreden niet voldoende door de lidstaten op centraal, regionaal of lokaal niveau kan worden verwezenlijkt, maar vanwege de omvang of de gevolgen van het overwogen optreden beter door de Unie kan worden bereikt (het subsidiariteitsbeginsel).

Het oordeel van het kabinet over de subsidiariteit is voor dit voorstel positief. Vanwege de hoge mate van verwevenheid van digitale processen binnen de EU en de grensoverschrijdende gevolgen van incidenten is een gemeenschappelijke benadering voor een hoog gezamenlijk niveau van cyberbeveiliging noodzakelijk. Het voorstel heeft tot doel om het gezamenlijke cyberbeveiligingsniveau in de EU te verhogen. Om dat te bereiken wordt de NIS2-richtlijn verder gesimplificeerd en geharmoniseerd.. Deze doelstelling kan onvoldoende door afzonderlijk optreden van de lidstaten op centraal, regionaal of lokaal niveau worden verwezenlijkt. Daarom is optreden op EU-niveau nodig. Daar komt bij dat een wijziging van bestaande EU-regelgeving slechts op EU-niveau kan plaatsvinden.

c) Proportionaliteit

Als onderdeel van de toets of de EU mag optreden conform de EU-verdragen toetst het kabinet of de inhoud en vorm van het optreden van de Unie niet verder gaan dan wat nodig is om de doelstellingen van de EU-verdragen te verwezenlijken (het proportionaliteitsbeginsel). Het oordeel van het kabinet ten aanzien van de proportionaliteit is positief met enkele kanttekeningen. Het voorstel heeft zoals boven toegelicht tot doel om het gezamenlijke cyberbeveiligingsniveau in de EU te verhogen. Om dat te bereiken wordt de NIS2-richtlijn verder gesimplificeerd en geharmoniseerd. Het kabinet acht dit voorstel op de meeste onderdelen, waaronder het verduidelijken en uitbreiden van soorten entiteiten die onder het toepassingsbereik van de NIS2-richtlijn vallen én het in geval van *ransomware*-aanvallen door essentiële entiteiten en belangrijke entiteiten in het kader van de meldplicht daarover verschaffen van informatie, geschikt om dat doel te bereiken en niet verdergaand dan met het oog op dat doel noodzakelijk is.

Wel heeft het kabinet bij drie onderdelen van het voorstel kanttekeningen. Ten eerste plaatst het kabinet, zolang een nadere toelichting hierop niet is gegeven, een kanttekening bij de voorgestelde uitbreiding van het register bij ENISA, bedoeld in artikel 27 van de NIS2-richtlijn, met gegevens over voortaan alle essentiële entiteiten en belangrijke entiteiten, mede ook omdat daarbij in het desbetreffende artikel niet expliciet wordt gemaakt voor welke taken van ENISA die uitbreiding van de registratie nodig is. Deze voorgestelde uitbreiding van het register lijkt verder te gaan dan noodzakelijk is voor het bereiken van het doel van het voorstel, met name ook omdat dit voorstel niet duidelijk is gekoppeld aan een of meer specifieke taken van ENISA, de uitbreiding daarmee

ongeclausuleerd is, en het gelet hierop niet helder is waarom het noodzakelijk is dat ENISA gegevens bij zou gaan houden over alle essentiële entiteiten en belangrijke entiteiten. Het kabinet ziet daarom graag eerst een nadere onderbouwing van dit voorstel, en in het bijzonder op de hiervoor genoemde punten, om te kunnen beoordelen of de voorgestelde uitbreiding van het register al dan niet noodzakelijk is.

Daarnaast plaatst het kabinet een kanttekening bij de voorgestelde wijziging van artikel 21, vijfde lid, in samenhang met die van artikel 5, van de NIS2-richtlijn, die lidstaten de mogelijkheid ontzegt om in geval van een uitvoeringshandeling als bedoeld in artikel 21, vijfde lid, aanvullende eisen te stellen aan de maatregelen in het kader van de zorgplicht. Niet duidelijk is hoe verstrekkend het ontzeggen van die mogelijkheid moet worden geacht te zijn én in samenhang daarmee of daarvoor geldt dat dat noodzakelijk is. Zo is bijvoorbeeld onduidelijk of lidstaten al dan niet nog eisen kunnen stellen met betrekking tot andere dan de in artikel 21, tweede lid, onder a tot en met j, uitdrukkelijk benoemde maatregelen in het kader van de zorgplicht. Ook vraagt het kabinet zich af of en waarom het voor lidstaten eventueel niet meer mogelijk zou moeten zijn om, in geval van specifieke dreigingen in een lidstaat, eisen te stellen aan zorgplichtmaatregelen. Daarbij geldt overigens ook dat het risico aanwezig is dat de voorgestelde wijziging zou kunnen inhouden dat lidstaten hiermee wordt belet dergelijke eisen te stellen in situaties waarin de bescherming van de nationale veiligheid naar het oordeel van een lidstaat hiertoe noodzaakt. Indien de voorgestelde wijziging lidstaten, zonder enig onderscheid, belet om in genoemde situaties nadere eisen met betrekking tot de maatregelen in het kader van de zorgplicht te stellen, gaat dit verder dan noodzakelijk is om het doel van het voorstel te bereiken.

Het kabinet plaatst tot slot een kanttekening bij de beperking van de auditbevoegdheden. Het kabinet is van mening dat de beperking op de auditbevoegdheden van toezichthouders in geval van certificering, verder gaat dan strikt noodzakelijk om het doel van het voorstel te bereiken. In tegenstelling tot certificering, kan een audit betrekking hebben op specifieke kwetsbaarheden en actuele risico’s. Ook biedt een audit de mogelijkheid om in dialoog te treden over de genomen of te nemen maatregelen. Het beperken van de bevoegdheid audits te doen leidt naar verwachting tot een lagere cyberweerbaarheid,

waarmee afbreuk wordt gedaan aan het uiteindelijke doel om cyberveiligheid te vergroten. Het kabinet onderkent de wens om de toezichtlasten laag te houden en onderschrijft in principe het vertrouwen dat partijen in deze certificering mogen hebben.
Het kabinet ziet echter graag dat lagere toezichtlasten op een andere wijze worden bereikt dan een beperking van de juridische bevoegdheid audits te doen en treedt daarover graag in overleg met de Commissie.

5. Financiële consequenties, gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

a) Consequenties EU-begroting

Voor de consequenties voor de EU-begroting wordt u verwezen naar het BNC-fiche Herziening CSA.[11] Het kabinet is van mening dat de benodigde EU-middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2021-2027 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting. Het kabinet wil niet vooruitlopen op de integrale afweging van middelen na 2027. Daarnaast moet de ontwikkeling van de administratieve uitgaven in lijn zijn met de ER-conclusies van juli 2020 over het MFK-akkoord. Het kabinet is kritisch over de stijging van het aantal werknemers.

b) Financiële consequenties (incl. personele) voor rijksoverheid en/ of medeoverheden

Voor de financiële consequenties wordt u verwezen naar het BNC-fiche Herziening CSA. [12] De budgettaire gevolgen worden ingepast op de begroting van het/het beleidsverantwoordelijk departement, conform de regels van de budgetdiscipline. Voor zover we nu kunnen inschatten zullen eventuele gevolgen voor de rijksoverheid beperkt zijn.

c) Financiële consequenties en gevolgen voor regeldruk voor bedrijfsleven en burger

Nederland zet zich in voor het verminderen van regeldruk en het bevorderen van betere regelgeving, zoals vastgelegd in het Actieprogramma Minder Druk Met

[11] BNC-fiche Herziening CSA
[12] BNC-fiche Herziening CSA

Regels (MDMR).[13] In lijn met deze inzet is een van de uitgangspunten van het kabinet in de non-paper over regeldruk en digitale wetgeving in november 2025 met uw Kamer gedeeld.[14] De simplificatievoorstellen uit het voorstel passen binnen de bredere doelstelling van het kabinet om de regeldruk terug te dringen. Daarbij zal het voorstel volgens het kabinet in brede zin bijdragen aan het vergroten van de cyberveiligheid en weerbaarheid in de gehele Unie.

In lijn met bovenstaande heeft Nederland de NIS2-richtlijn beleidsarm geïmplementeerd en zijn er geen nationale koppen toegevoegd. Nog voordat de NIS2-richtlijn in Nederland is geïmplementeerd, heeft de Commissie een simplificatie van de NIS2-richtlijn aangekondigd. Het doel van dit voorstel is het verlagen van de regeldruk. Zowel de NIS2-richtlijn als de simplificatie van de NIS2-richtlijn, hebben geen gevolgen voor de regeldruk voor burgers, evenmin voor entiteiten die niet binnen het toepassingsbereik van de NIS2-richlijn vallen. Hieronder zal per onderdeel nader worden ingegaan op de regeldrukimplicaties voor bedrijven die wel binnen het bereik van de NIS2-richtlijn vallen.
Het voorstel ziet allereerst op een uitbreiding van het toepassingsbereik. Hierdoor moeten ‘nieuwe groepen van entiteiten’ onder andere voldoen aan de zorgplicht, meldplicht en registratieplicht. De verwachting is dat deze entiteiten, in het kader van de zorgplicht, veelal beveiligingsmaatregelen hebben getroffen, zijnde een combinatie van technische, operationele en organisatorische maatregelen. Voor de continuïteit van hun eigen bedrijfsvoering is het immers cruciaal dat maatregelen worden getroffen op het gebied van netwerk- en informatiebeveiliging. Op dit moment is het voor het kabinet nog onduidelijk hoeveel nieuwe entiteiten onder de NIS2-richtlijn komen te vallen, het kabinet streeft ernaar hier zo snel mogelijk inzicht in te krijgen.

Om de regeldruk voor onder andere entiteiten te beperken, introduceert het voorstel een nieuwe categorie *small mid-cap* bedrijven. Het gaat daarbij om een categorie die tussen middelgrote en grote ondernemingen in komt. Deze bedrijven worden nu als essentiële entiteiten aangemerkt, maar met het voorstel als belangrijke entiteit aangemerkt. Onder de NIS2-richtlijn is er verschil in toezicht tussen essentiële entiteiten en belangrijke entiteiten: essentiële

---

[13] Kamerbrief over actieprogramma Minder Druk Met Regels | Kamerstuk | Rijksoverheid.nl.
[14] https://www.tweedekamer.nl/kamerstukken/detail?id=2025D46264&did=2025D46264.

entiteiten staan onder proactief toezicht en belangrijke entiteiten staan onder reactief toezicht. Daarnaast beschikt de bevoegde autoriteit in de handhaving van de naleving van de verplichtingen door essentiële entiteiten, over meer bevoegdheden dan ten aanzien van de handhaving van de naleving van de verplichtingen door belangrijke entiteiten. Doordat deze nieuwe categorie *small mid-cap* onder een lichter toezichtregime zullen vallen, zal dit leiden tot minder regeldruk voor deze entiteiten ten aanzien van toezicht. Op dit moment is het voor het kabinet nog onduidelijk hoeveel entiteiten onder deze nieuwe categorie komen te vallen, het kabinet streeft ernaar hier zo snel mogelijk inzicht in te krijgen.

Ook doet de Commissie voorstellen zodat certificering expliciet ingezet kan worden ter ondersteuning van EU-wetgeving. Op deze wijze kan *cyberposture* certificering worden ingezet om daarmee aantoonbaar te voldoen aan de zorgplichtmaatregelen, bedoeld in de NIS2-richtlijn. Hoewel in het voorstel geen verplichting is opgenomen voor entiteiten om zich te certificeren heeft de Commissie hiervoor de mogelijke kosten in kaart gebracht: in haar impact assessment gaat de Europese Commissie uit van een bedrag van €30.000 voor het behalen van certificering. De structurele kosten om gecertificeerd te blijven worden over heel Europa geschat op 501 miljoen euro over vijf jaar. Dit is eenzelfde bedrag als de eenmalige kosten voor certificering. Daarmee zullen de structurele kosten voor het behoud van certificering op €6000 per jaar worden geschat. Het kabinet zal verduidelijking vragen over de kosten van het periodiek vernieuwen van de certificering.

Ook stelt de Commissie maximum harmonisatie van de uitvoeringshandelingen voor met betrekking tot de zorgplichtmaatregelen. De Commissie beoordeelt regelmatig of er uitvoeringshandelingen voor specifieke sectoren of soorten entiteiten moeten worden vastgesteld. De Commissie heeft momenteel nog geen nieuwe uitvoeringshandelingen aangekondigd, waardoor het voor het kabinet nog niet duidelijk is voor welke specifieke sectoren of soorten entiteiten eventuele uitvoeringshandelingen worden verwacht.
Het kabinet merkt daarnaast op dat de onzekerheid die voortkomt uit mogelijke uitvoeringshandelingen een risico op (onvoorziene) regeldruk met zich meebrengt.

Het voorstel richt zich ook op harmonisatie en verbeterde datacollectie van *ransomware*. Deze modaliteit zal een aanvulling zijn op de al bestaande verplichting tot het melden van significante
Incidenten. In geval het hier gaat om een *ransomware*-aanval, dient er meer informatie te worden ingevuld en volgen er meer vervolghandelingen. De kostenimpact wordt door de Commissie als nihil ingeschat, omdat de verplichting reeds bestaat voor het melden van incidenten en het aanleveren van de extra informatie geen tot nauwelijks extra tijd kost. Door de extra informatie hoopt de Commissie op termijn meer inzicht te krijgen in *ransom* en daarmee hopen ze een kostenbesparing door te voeren. Hoewel Nederland een bredere definitie aanhangt van *ransomware* dan de Commissie, levert dit extra regeldruk op voor de entiteiten die een meldingen moeten maken, omdat de kostenimpact als nihil wordt ingeschat.

Het kabinet merkt tot slot op dat de wijziging op bestaande processen en procedures bij bedrijven naar aanleiding van het voorstel ook kosten met zich mee kunnen brengen.

ATR advies
Het eerste concept van het BNC-fiche is voor advies voorgelegd aan het Adviescollege toetsing regeldruk (ATR). Het ATR adviseert over de regeldrukeffecten van het voorstel van de Europese Commissie. Het ATR adviseert als volgt:
“1. ATR adviseert om de regeldrukgevolgen vanwege het uitgebreidere toepassingsbereik in kaart te brengen, conform de Rijksbrede methodiek.
2. ATR adviseert om in beeld te brengen bij hoeveel bedrijven certificering leidt tot effecten voor de regeldruk.
3. ATR adviseert om te inventariseren wat cyberbeveiliging aan bedrijfseigen kosten oplevert en hoe zich dat verhoudt tot de (versimpeling van) NIS2-verplichtingen.
4. ATR adviseert om toe te lichten wat de verschillende toezichtregimes inhouden en welke regeldrukgevolgen een lichter en/of reactief toezichtregime heeft.
5. ATR adviseert om tijdig in kaart te brengen wat de regeldrukgevolgen zijn van de door de Europese Commissie vast te stellen uitvoeringshandelingen en van de door ENISA op te stellen *guidelines*.

- ATR adviseert dit keer uitsluitend op basis van de regeldrukparagraaf. ATR heeft op basis van de verstrekte informatie niet kunnen adviseren over de volle breedte van de taakopdracht met betrekking tot de BNC-fiches.

Hieronder volgt een reactie van het kabinet op de adviespunten:

Reactie kabinet
Het kabinet licht ten aanzien van de specifieke punten het volgende toe:

1. Voor nieuwe entiteiten die onder het toepassingsbereik van de NIS2-richtlijn worden gebracht, zal de regeldruk worden berekend conform de methodiek die de Rijksoverheid heeft gehanteerd bij de Cyberbeveiligingswet (Cbw) en de onderliggende regelgeving.
2. Het voorstel geeft lidstaten de bevoegdheid om entiteiten te verplichten zich te certificeren, oftewel er is hier geen sprake van een verplichting met gevolgen voor de regeldruk. In de situatie dat NL een dergelijke bevoegdheid zou willen inzetten, zal de regeldruk voor bedrijven integraal bij een dergelijk besluit moeten worden betrokken en worden berekend en zal hierover – zoals gebruikelijk - ook advies aan ATR worden gevraagd.
3. Het voorstel bevat geen inhoudelijke voorstellen ten aanzien van de beveiligingsmaatregelen die entiteiten moeten treffen en daarmee heeft dit voorstel op dit punt geen gevolgen voor de regeldruk. Het kabinet heeft toegelicht wat de verschillende toezichtregimes inhouden. Voor het kwantificeren van de regeldruk zal eerst het aantal entiteiten in kaart gebracht moeten worden.
4. Het kabinet zal wanneer hier voldoende informatie over is de regeldrukgevolgen van de uitvoeringshandelingen en *guidelines* bezien.

Wanneer duidelijk is of en in welke vorm de voorstellen van de Europese Commissie daadwerkelijk tot wet worden verheven en er daarmee meer informatie is over de regeldrukeffecten, zal het kabinet weer bezien op welke manier gevolg kan worden gegeven aan de adviespunten van het ATR.
Wat betreft het punt van het ATR over de advisering op basis van de regeldrukparagraaf hecht het kabinet te benoemen dat het ATR vroegtijdig is betrokken en een conceptversie van het fiche heeft ontvangen. Het kabinet hecht waarde aan deze adviestaak van het ATR en gaat met ATR in gesprek over

de informatievoorziening aan het ATR bij toekomstige Commissievoorstellen voor deze nieuwe adviestaak.

d) Gevolgen voor concurrentiekracht en geopolitieke aspecten
De Commissie heeft dit voorstel gepubliceerd om wetgeving te simplificeren en daarmee de interne markt binnen Europa te bevorderen. Dit kan op langere termijn positief uitwerken op de concurrentiekracht van de Europese digitale economie.

6. Implicaties juridisch

a) Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)
Het voorstel vergt verschillende aanpassingen van nationale wetgeving (in het bijzonder de aanstaande Cyberbeveiligingswet).

b) Gedelegeerde en/of uitvoeringshandelingen, incl. NL-beoordeling daarvan
Het kabinet oordeelt op zich positief over het voorstel van de Commissie tot aanvulling van de in artikel 21, vijfde lid, tweede alinea, reeds opgenomen bevoegdheid voor de Commissie om uitvoeringshandelingen vast te stellen met technologische en methodologische vereisten voor de maatregelen, bedoeld in artikel 21, tweede lid, van de NIS-richtlijn met betrekking tot andere essentiële en belangrijke entiteiten dan die genoemd in de eerste alinea van artikel 21, vijfde lid. Die aanvulling behelst dat de Commissie regelmatig zal monitoren of die uitvoeringshandelingen voor specifieke sectoren of soorten entiteiten moeten worden vastgesteld én dat de Commissie daarbij in het bijzonder de nadruk zal leggen op het grensoverschrijdende karakter van sectoren of soorten entiteiten. Ook met inachtneming hiervan geldt naar het oordeel van het kabinet dat toekenning van deze bevoegdheid nog steeds mogelijk is, omdat het hierbij niet gaat om essentiële onderdelen van de regelgeving. De keuze voor een uitvoeringshandeling in plaats van delegatie ligt hierbij nog steeds voor de hand, omdat deze handelingen waarborgen dat de richtlijn in alle lidstaten volgens eenvormige voorwaarden wordt uitgevoerd. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de onderzoeksprocedure als bedoeld in artikel 5 van Verordening (EU) nr. 182/2011. Toepassing van die procedure is hier volgens het kabinet op zijn plaats, omdat het uitvoeringshandelingen van algemene strekking betreft.

Daarnaast bevat het voorstel een aanvulling op de reeds in artikel 23, elfde lid, van de NIS2-richtlijn opgenomen bevoegdheid van de Commissie om uitvoeringshandelingen vast te stellen over het soort informatie, het format en de procedure betreffende verplichte meldingen van significante incidenten. Daarbij gaat het om een nieuw twaalfde lid van datzelfde artikel, inhoudende dat de Commissie in geval van een dergelijke uitvoeringshandeling als vereist zal opnemen dat informatie door de betrokken entiteit wordt verstrekt over het al dan niet gedetecteerd hebben van een *ransomware*-aanval, de aanvalsvector van die aanval en het al dan niet getroffen zijn van mitigerende maatregelen in verband met die aanval. Toekenning van deze aanvulling op de bevoegdheid van de Commissie is niet mogelijk, omdat deze aanvulling naar het oordeel van het kabinet een essentieel onderdeel van de regelgeving betreft. Dat blijkt naar het oordeel van het kabinet in het bijzonder ook uit de omstandigheid dat met dit voorstel tevens een nieuw dertiende lid aan artikel 23 wordt toegevoegd, dat net als het twaalfde lid betrekking heeft op *ransomware*-aanvallen én inhoudt dat de betrokken entiteit in het kader van de meldplicht bij dergelijke aanvallen het CSIRT of de bevoegde autoriteit erover informeert of een *ransom*-verzoek is gedaan, of daaraan is voldaan, en welk bedrag daarbij is betaald. Naar het oordeel van het kabinet geldt voor de in het twaalfde lid bedoelde informatie over *ransomware*-aanvallen dat die onlosmakelijk is verbonden met die in het dertiende lid, dat het verstrekken van ook die in het twaalfde lid bedoelde informatie niet van een eventuele uitvoeringshandeling afhankelijk zou moeten zijn, en dat het verstrekken van laatstbedoelde informatie dan ook eveneens, in relatie tot de meldplicht, in de richtlijn zelf zou moeten worden opgenomen.

c) Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en besluiten) met commentaar t.a.v. haalbaarheid

De door de Commissie voorgestelde termijn van twaalf maanden is voor Nederland, gelet op de benodigde wijzigingen van wetgeving, niet haalbaar. In plaats hiervan wordt daarom aangedrongen op een termijn van ten minste achttien maanden.

d) Wenselijkheid evaluatie-/horizonbepaling

Het voorstel bevat geen evaluatiebepaling. Voor de NIS2-richtlijn geldt echter dat in artikel 40 is geregeld dat de Commissie de werking van die richtlijn periodiek evalueert en daarover verslag uitbrengt aan het Europees Parlement en de Raad. Het kabinet gaat ervan uit dat de wijzigingen van de NIS2-richtlijn in dit voorstel, zodra dat voorstel richtlijn is geworden en in werking is getreden, deel gaan uitmaken van de evaluaties van de NIS2-richtlijn als bedoeld in artikel 40. Met het oog hierop is het kabinet van oordeel dat een afzonderlijke evaluatiebepaling in dit voorstel inderdaad achterwege kan blijven.

e) Constitutionele toets

N.v.t.

7. Implicaties voor uitvoering en/of handhaving

Uitvoeringsorganisaties hechten aan vereenvoudiging van wet- en regelgeving. Zodra de details van de simplificatie van de NIS2-richtlijn meer duidelijk zijn, moeten de implicaties in kaart worden gebracht met de uitvoeringstoets. Daarnaast is het wenselijk dat er meer duidelijkheid komt over de samenhang tussen de recente wetsvoorstellen van de Commissie onderling en bestaande wet- en regelgeving. Tevens is het wenselijk om de uitvoeringsconsequenties van het totaal van nieuwe wet- en regelgeving te onderzoeken.

8. Implicaties voor ontwikkelingslanden

Geen implicaties voor ontwikkelingslanden.