Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2022–2023

36 239 Voorstel voor een Verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020

A BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 21 oktober 2022

Overeenkomstig de bestaande afspraken ontvangt u hierbij 2 fiches die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissie voorstellen (BNC).

Fiche 1: Verordening Cyber Resilience Act (CRA)
Fiche 2: Europese Media Vrijheid Verordening en Aanbeveling redactionele onafhankelijkheid en transparantie mediaeigendom

De Minister van Buitenlandse Zaken,
W.B. Hoekstra

kst-36239-A
ISSN 0921 - 7371
's-Gravenhage 2022

Fiche 1: Verordening Cyber Resilience Act (CRA)

1. Algemene gegevens

a) *Titel voorstel*
Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.
b) *Datum ontvangst Commissiedocument*
15 september 2022
c) *Nr. Commissiedocument*
COM(2022) 454
d) *EUR-Lex*
EUR-Lex – 52022PC0454 – EN – EUR-Lex (Europa.eu)
e) *Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing*
SWD(2022) 282
SWD(2022) 283
SEC(2022) 321
f) *Behandelingstraject Raad*
Raad Vervoer, Telecommunicatie en Energie (TTE)
g) *Eerstverantwoordelijk ministerie*
Ministerie van Economische Zaken en Klimaat in nauwe samenwerking met het Ministerie van Justitie en Veiligheid
h) *Rechtsbasis*
Artikel 114 Verdrag betreffende de Werking van de Europese Unie (VWEU)
i) *Besluitvormingsprocedure Raad*
Gekwalificeerde meerderheid
j) *Rol Europees Parlement*
Medebeslissing

2. Essentie voorstel

a) Inhoud voorstel

Hardware- en softwareproducten zijn in toenemende mate onderhevig aan cyberaanvallen, met hoge kosten voor samenlevingen en individuele consumenten als gevolg. Op dit moment is er specifiek voor de Europese Unie (hierna ook: «EU») alleen wetgeving die van toepassing is op bepaalde producten met digitale elementen, maar ontbreekt er een breed wetgevend kader dat de cybersecurity reguleert voor alle hardware- en software producten. Dit heeft als gevolg dat er kwetsbare producten met digitale elementen in omloop zijn op de Europese interne markt die grote schade kunnen berokkenen aan consumenten, bedrijven, en overheden. Omdat deze producten vaak grensoverschrijdend worden gebruikt, kunnen deze incidenten zich snel over de interne markt verspreiden.

De tweeledige hoofddoelstelling van de *Cyber Resilience Act* (hierna ook: «CRA») is (1) het creëren van horizontale robuuste cybersecurity voorwaarden voor alle producten met digitale elementen waar fabrikanten, leveranciers en importeurs van dergelijke producten aan moeten voldoen vóór plaatsing op de interne markt en tijdens de productlevenscyclus, en(2) het zorgen voor transparantie over de mate van cybersecurity van dergelijke producten ten behoeve van de keuze van gebruikers (consumenten en organisaties). Dit moet leiden tot een digitaal veiligere Europese digitale interne markt en samenleving waar onveilige producten van de markt kunnen worden geweerd en gehaald. De EU is wereldwijd de eerste partij die met dergelijke wetgeving komt en kan hiermee mondiaal de standaard zetten voor digitaal veilige producten. Wanneer

derde landen, waar een groot deel van de productie van digitale producten plaatsvindt, volgen, zorgen we als EU voor een wereldwijd veiligere waardenketen.

Onder de reikwijdte van de CRA vallen alle producten met digitale elementen, waarvan het gebruik en redelijk voorstelbaar gebruik een directe of indirecte verbinding tot een eindapparaat of netwerk bevat. Dit omvat alle hardware- of softwareproducten en individuele componenten. Buiten de reikwijdte vallen medische (in-vitro) apparaten, motorvoertuigen, producten gerelateerd aan de burgerluchtvaart, producten die exclusief zijn ontwikkeld voor de nationale veiligheid, militaire doeleinden of om gerubriceerde informatie te verwerken, *Software-as-a-Service* (SaaS, een variant van clouddienstverlening) en *open source* software indien er geen economische activiteit aan is gekoppeld. Onder de aanbieders van producten met digitale elementen wordt verstaan de fabrikanten die de producten ontwikkelen, ontwerpen en beschikbaar stellen onder hun naam of handelsmerk (gratis of tegen betaling), en de leveranciers en de importeurs die de producten beschikbaar stellen in de interne markt. Elk type aanbieder in de productieketen heeft hierbij verschillende verantwoordelijkheden.

Vanwege het horizontale karakter en de brede reikwijdte van de CRA, zijn er raakvlakken met andere (sectorale) EU-wetgeving die de cybersecurity van specifieke producten met digitale elementen of bepaalde diensten reguleren, zoals medische apparatuur of voertuigen. De CRA beoogt de verhouding tot deze sectorale wetgeving te verhelderen om zo juridische duidelijkheid te scheppen voor bedrijven en toezichthouders. Zo zijn er in de CRA bepalingen opgenomen die aangeven welke cybersecurityverplichtingen gelden of juist komen te vervallen indien een product met digitaal element onder de reikwijdte van de CRA én een ander Unie wetgevingsinstrument valt. Ook wordt er bepaald of de conformiteitsbeoordeling van de CRA, van het andere Unie wetgevingsinstrument of een combinatie hiervan gevolgd moet worden.

Het stelsel van verplichtingen dat de CRA introduceert aan de fabrikanten, importeurs en leveranciers kan grofweg in twee categorieën worden onderverdeeld: een set aan *ex-ante* verplichtingen waaraan aanbieders van producten met digitale elementen moeten voldoen vóórdat deze producten op de markt mogen worden geplaatst, en een set aan *ex-post* verplichtingen die gelden nádat de producten op de markt zijn geplaatst.

Zo moeten fabrikanten en importeurs onder het *ex-ante* gedeelte van de verordening ervoor zorgen dat hun producten voldoen aan de essentiële voorwaarden in Annex I, waaronder de verplichting om hun producten zodanig te ontwerpen, ontwikkelen en produceren dat ze een passend niveau van cybersecurity garanderen in overeenstemming met het risico dat voortvloeit uit het gebruik.

Ook mag het product niet onderhevig zijn aan – voor zover bekend – exploiteerbare kwetsbaarheden. Verder moet de fabrikant het product met het digitale element aan een conformiteitsbeoordelingsprocedure onderwerpen om aan te tonen dat het product tegemoet komt aan de bovengenoemde essentiële voorwaarden in Annex I, alvorens het op de interne markt mag worden gebracht. In Annex III zijn twee categorieën kritieke producten met digitale elementen opgenomen die een hoger cybersecurity risico met zich mee brengen en waarvoor zwaardere eisen aan de conformiteitsbeoordelingsprocedure worden gesteld. Voor kritieke producten uit categorie II in Annex III moet de conformiteitsbeoordeling worden uitgevoerd door een onafhankelijke derde partij. De Commissie krijgt de bevoegdheid om via gedelegeerde handelingen producten aan

de lijst van kritieke producten van Annex III te schrappen of toe te voegen, waarbij producenten worden verplicht te voldoen aan een cybersecurity-certificaat volgens het EU-cybersecuritycertificeringsschema. Ten slotte moet de fabrikant informatie en instructies bijvoegen bij het product voor de gebruiker zodat zij/hij het product veilig kan installeren en gebruiken.

Voor de *ex-post* verplichtingen geldt dat de fabrikant voor de verwachte levensduur van het product, of voor een periode van vijf jaar (welke korter is), moet garanderen dat kwetsbaarheden van het product effectief aangepakt worden middels bijvoorbeeld veiligheidsupdates en het product blijft voldoen aan de essentiële voorwaarden in Annex I. Ook moet de fabrikant zonder onnodige vertraging en binnen 24 uur bij de *European Union Agency for Cybersecurity* (hierna ook: «ENISA») melden dat er een kwetsbaarheid in zijn product is geëxploiteerd is en een incident vormt die een impact kan hebben op de veiligheid van het product. ENISA moet deze melding vervolgens zonder vertraging[1] doorzetten naar de aangewezen nationale *Cyber Security Incident Response Team* (hierna ook: «CSIRT») of *Single Point of Contact* en de nationale markttoezichtautoriteit op de hoogte stellen.

Lidstaten moeten toezicht en handhaving van de regels in de CRA binnen hun grondgebied beleggen bij één of meerdere markttoezichthouders. Dit mag een bestaand of nieuw op te richten autoriteit zijn. Waar de markttoezichthouder oordeelt dat een aanbieder van producten met digitale elementen de regels niet naleeft en de gevolgen hiervan niet beperkt zijn tot zijn grondgebied, zal de markttoezichthouder de Commissie en de andere lidstaten informeren over de evaluatie en maatregelen die het *vis-à-vis* de aanbieder heeft genomen. De Commissie kan markttoezicht-houders verzoeken een onderzoek te verrichten als het voldoende redenen heeft om aan te nemen dat een product niet aan de voorwaarden voldoet. In uitzonderlijke omstandigheden waarbij (1) een product een aanzienlijk cybersecurityrisico heeft, (2) het niet aan de voorwaarden voldoet en (3) de relevante markttoezichthouder geen doeltreffende maatregelen heeft genomen, mag de Commissie tot onmiddellijke interventie overgaan en ENISA verzoeken een onderzoek te verrichten. Op basis van dit onderzoek kan de Commissie ervoor kiezen middels een uitvoeringshandeling maatregelen te nemen op EU-niveau, waaronder het terugroepen van het product van de interne markt. Verder kunnen markttoezichthouders zelf, of op verzoek van de Commissie of ENISA, met andere relevante toezicht-houders een gezamenlijk onderzoek te verrichten naar producten die een cybersecurityrisico vormen. Ten slotte kunnen onder de coördinatie van de Commissie gelijktijdige nalevingscontroles worden gehouden door de markttoezichthouders (zogenaamde «*sweeps*»).

b) Impact assessment Commissie

De Commissie heeft in aanloop naar het impact assessment onder andere een publieke consultatie gehouden en verscheidene workshops georganiseerd met stakeholders, waaronder lidstaten, fabrikanten, gebruikers en anderen, over de cybersecurity van producten met digitale elementen. Uit de feedback van deze consultatierondes kwamen twee principiële problemen naar voren: (1) er heerst een laag niveau van cybersecurity van producten met digitale elementen, en (2) er is een gebrek aan kennis en informatie voor gebruikers voor wat betreft de cybersecurity van een product. Ook wordt in het impact assessment geconcludeerd dat de nieuwe verplichtingen nalevings- en handhavingskosten met zich mee zullen brengen, onder andere voor het bedrijfsleven, met name het mkb.

[1] Tenzij om gerechtvaardigde redenen in verband met cybersecurityrisico's.

In de consultaties gaf het mkb daarom het belang aan van een proportionele aanpak en ondersteunende maatregelen.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Het Cyber Security Beeld Nederland (hierna ook: «CSBN») geeft jaarlijks een overzicht van de digitale dreigingen en weerbaarheid. Opeenvolgende beelden, inclusief het CSBN van 2022[2] trekken vergelijkbare conclusies als het impact assessment van de Europese Commissie, namelijk dat de onveiligheid van ICT-producten en diensten de achilleshiel vormen van de digitale weerbaarheid, en dat de marktdynamiek de beheersing van digitale risico's compliceert. De analyse van het CSBN is de basis voor de kabinetsbrede Nederlandse Cybersecurity Strategie (NLCS)[3]. Het doel van de NLCS is om Nederland digitaal veilig te maken door de digitale weerbaarheid te verhogen en dreigingen tegen te gaan. Het kabinet zet in op het versterken en transformeren van het digitale ecosysteem waarbij één organisatie of één individu niet langer de zwakste schakel kan zijn. Dat vergt een systeemtransformatie die in de vier pijlers van de NLCS wordt uitgelicht. Dit vergt de inzet van een uitgebalanceerd samenspel aan instrumenten: van intensievere publiek-private samenwerking tot nieuwe wetgeving, met als doel een ecosysteem te creëren waarbij burgers, organisaties en (kleine) bedrijven in beginsel veilige producten en diensten kunnen afnemen. In het kader van de Europese digitaal eengemaakte markt, de competitieve wereldeconomie, het streven naar een gelijk speelveld en veilige ICT-producten en diensten zet het kabinet zo veel mogelijk in op het ontwikkelen van Europese wet- en regelgeving. Deze inzet komt tot uiting in pijler II van de NLCS met betrekking tot veilige en innovatieve digitale producten en diensten. De ontwikkeling van de CRA in samenspel met andere Europese wet- en regelgeving en certificering voor ICT-producten en diensten staat centraal in de aanpak naast nationale maatregelen zoals de inkoopeisen cybersecurity van de overheid (ICO). Deze inzet heeft ook een internationaal normatief element, zoals uiteengezet in pijler III van de NLCS. Hierin stelt het kabinet zich ten doel om actief deel te nemen aan internationale discussies over technische standaarden die van invloed zijn op de openheid, vrijheid en veiligheid van het internet door standpunten te coördineren op EU niveau en met gelijkgezinde landen. De CRA biedt een mogelijkheid de internationale discussies over de technische standaarden te beïnvloeden.

b) Beoordeling + inzet ten aanzien van dit voorstel

Het voorstel beoogt de cybersecurity van producten met digitale elementen in de Europese digitale interne markt te vergroten en versterken. Het kabinet steunt deze doelstelling en verwelkomt het voorstel. Over het algemeen is de eerste indruk van het kabinet van het voorstel positief en in lijn met het Nederlandse non-paper[4] en consultatiereactie[5] op dit voorstel die u op 14 december 2021 en op 17 augustus jl. heeft ontvangen. U ontvangt parallel aan dit BNC-fiche het non-paper van Nederland, Denemarken en Duitsland van 12 september jl. Wel is er op een aantal onderdelen nog onduidelijkheid zoals hierna wordt beschreven. Hierover zal het kabinet nadere uitleg vragen.

---

[2] Kamerstuk 2022D28665.
[3] De NLCS is aan uw Kamer aangeboden op 10 oktober 2022.
[4] Kamerstuk 2021D49776.
[5] Kamerstuk 2022D32607.

Het kabinet steunt de keuze om, producten met digitale elementen, inclusief alle hardware- en softwareproducten, en fabrikanten, leveranciers en importeurs van dergelijke producten onder de reikwijdte van het CRA voorstel te brengen. Er bestaat momenteel geen horizontale cybersecuritywetgeving met verplichtingen voor alle marktspelers van digitale producten. Bestaande Uniewetgeving op het gebied van cybersecurity (en wetgeving die op dit moment in onderhandeling is) kent een andere invalshoek, zoals bijvoorbeeld de herziene Richtlijn voor Netwerk- en Informatiebeveiliging (hierna ook: «NIB2») dat een kader biedt voor de beveiliging van essentiële en belangrijke organisaties, de vrijwillige cybersecurity certificering van ICT-producten, diensten en processen onder de *Cybersecurity Act* (hierna ook: «CSA») en de cybersecurityeisen over de Radio Equipment Directive (hierna ook: «RED»). De CRA kan hierin een vangnet vormen met essentiële eisen die voor alle producten met digitale elementen gelden, waarbij sectorale wetgeving als *lex specialis* additionele voorwaarden kan stellen voor specifieke producten en diensten.

Het kabinet is positief over het op termijn intrekken van de gedelegeerde handeling onder de RED voor cybersecurityeisen voor draadloos verbonden apparaten wanneer de horizontale eisen van de CRA in werking treden. Hiermee vloeien de gestelde eisen onder de RED die van kracht worden op 1 augustus 2024 over in de CRA en wordt duplicatie van Europese wet- en regelgeving voorkomen.

De exacte reikwijdte van het begrip producten met digitale elementen is echter nog niet volledig duidelijk. Dit is een aandachtspunt voor het kabinet. Voor het kabinet is het van belang dat voldoende duidelijk is dat bijvoorbeeld alle hard- en softwareproducten, inclusief alle losse software, binnen de definitie valt.

Voor wat betreft de verhouding met reeds bestaande cybersecurity gerelateerde wetgeving (en wetgeving die op dit moment in onderhandeling is) steunt het kabinet een zo ver mogelijke overeenstemming van de personele en materiële reikwijdte van de CRA met de definities die worden gehanteerd in Unie wetgeving waaronder de CSA, NIB2, AI Act, de Machinerichtlijn, de *General Product Safety Regulation* (gerelateerd aan fysieke veiligheid) en andere instrumenten. Dit biedt juridische zekerheid aan zowel bedrijven als lidstaten.

Het kabinet is van oordeel dat de relatie tussen de horizontale CRA en de andere genoemde verticale, sectorale wetgeving nog verdere duidelijkheid behoeft om zo bovengenoemde samenhang en aansluiting te garanderen, en duplicatie met deze wetgeving te vermijden.
Zo zal het kabinet verduidelijking vragen hoe de focus op producten met digitale elementen zich verhoudt tot de bredere scope van de CSA die zich richt op ICT-producten, diensten en processen. Ook valt *Software-as-a Service* (SaaS, een vorm van clouddienstverlening) niet onder de CRA omdat deze aanbieders hiervan onder NIB2 reeds worden gereguleerd als essentiële entiteit. Het kabinet zal verhelderingvragen of over deze uitzondering voor de betrokken organisaties voldoende eenduidigheid biedt. Ook de samenhang met andere relevante wetgevingsvoorstellen, zoals de herziening van de eIDAS-verordening en de verschillende meldplichten die onder de CRA en NIB vallen, zijn aandachtspunten voor verdere verheldering. De meldplicht voor fabrikanten over kwetsbaarheden en incidenten dient door ENISA verspreid te worden aan lidstaten of het Europese netwerk van *Cybersecurity Incident Response Teams* (hierna ook: «CSIRTs-netwerk»). Het kabinet beschouwt het van belang dat de reactietermijn van ENISA voor deze meldingen wordt gespecificeerd.

Daarnaast beschouwt het kabinet dat de uitzonderingsgronden voor de meldplicht van fabrikanten afbakening behoeft.

Tot slot zal het kabinet de Commissie om verduidelijking vragen over de totstandkoming en redenering van de lijst van kritieke producten met digitale elementen in Annex III. Het kabinet staat positief tegenover het gebruik van verschillende mogelijkheden tot conformiteitsbeoordeling afhankelijk van de risico's. Daarbij is van belang dat de eisen aan conformiteitsbeoordeling voldoende waarborgen bevatten om ervoor te zorgen dat die beoordeling betrouwbaar wordt uitgevoerd en van voldoende kwaliteit is.

Verder oordeelt het kabinet over het algemeen positief over de inhoudelijke verplichtingen waaraan alle producten met digitale elementen en fabrikanten, leveranciers en importeurs van dergelijke producten aan moeten voldoen. Voor wat betreft de termijn waarop kwetsbaarheden moeten worden verholpen zal het kabinet verheldering vragen wat wordt beoogd met een keuze tussen de kortste van de twee termijnen, de productlevenscyclus of vijf jaar. Voldoende cybersecurity waarborgen gedurende de productlevenscyclus is voor het kabinet van belang. Het voorstel roept op dit punt ook vragen op over de aansluiting met de Europese richtlijnen over de verkoop van goederen en levering van digitale inhoud en diensten. Op basis van deze richtlijnen moet een handelaar een consument van updates voorzien voor een periode die de consument redelijkerwijs kan verwachten. Ten aanzien van de taken die ENISA mede op basis van huidige wetgeving thans heeft[6], zal het kabinet vragen om nadere toelichtingen omtrent de voorgestelde rol en bevoegdheden van ENISA bij bijvoorbeeld de meldplicht voor producenten van geëxploiteerde kwetsbaarheden van producten met een digitaal element bij ENISA en het vervolgens door ENISA doorzetten van deze meldingen naar nationale *Cybersecurity Incident Response Teams* (CSIRTs).

Zoals opgemerkt in het Nederlandse non-paper[7] zal het kabinet aandacht hebben voor de proportionaliteit en juridische zekerheid van deze verplichtingen, met name voor het mkb, met als doel om veilige innovatie te bevorderen en uitvoerbaarheid van de verplichtingen te garanderen.

Op het gebied van markttoezicht steunt het kabinet de keuze om lidstaten vrij te laten bij welke, al dan niet nieuw op te richten autoriteit, het toezicht en de handhaving van de CRA regels op hun grondgebied te beleggen. Wel plaatst het kabinet aandachtspunten bij de precieze rol en bevoegdheden die aan de Commissie en ENISA worden toegekend in het voorstel. Het kabinet zal verduidelijking vragen over de precieze rol van beide laatstgenoemde instanties, onder meer in relatie tot de verantwoordelijkheden van nationale markttoezichthouders en nationale cybersecurity incident response teams zoals bijvoorbeeld ook het Nationaal Cyber Security Centrum (hierna ook: «NCSC») en het *Cyber Security Incident Response Team* voor digitale dienstverleners (hierna ook: «CSIRT-DSP»). Hierbij zal het kabinet benadrukken dat de onafhankelijkheid van de nationale markttoezichthouders in de uitvoering van hun toezichtstaken essentieel is.

Voor een aantal zaken komen de bevoegdheden van de Commissie de wendbaarheid van de CRA ten goede in relatie tot technologische ontwikkelingen of de ontwikkeling van relevante sectorale Europese wet- en regelgeving. Bij één andere bevoegdheid is het kabinet kritischer. De meest verregaande bevoegdheid die aan de Commissie wordt toegekend

[6] Zoals vastgelegd in artikel 7 van de Cybersecurity Act (Verordening (EU) 2019/881) voor ENISA.
[7] Kamerstuk 2021D49776.

is dat zij in uitzonderlijke gevallen digitale producten uit de Europese markt kan laten terugtrekken. Het kabinet zal aandacht houden voor de verdere uitwerking van de bevoegdheden van de Commissie, onder meer of dit op gespannen voet zou kunnen komen te staan met de uitsluitende verantwoordelijkheid van lidstaten op het gebied van bescherming van nationale veiligheid (artikel 4, tweede lid, VEU).

c) Eerste inschatting van krachtenveld

De meeste lidstaten lijken, net als Nederland, het voorstel in de basis te steunen en te verwelkomen. Op het moment van schrijven delen andere lidstaten de vragen van Nederland rondom de reikwijdte, definities, de verhouding met andere Europese wet- en regelgeving zoals NIB2 en CSA, en de voorziene rol van de Commissie en ENISA. Ook zijn er in het afgelopen jaar twee Nederlandse non-papers ontwikkeld over de koers van de CRA. Het eerste non-paper van 14 december 2021 was alleen van NL. Aan een tweede non-paper van 12 september 2022 werd medeondertekend door Duitsland en Denemarken.

Voor wat betreft het Europees Parlement zijn op het moment van schrijven noch een Commissie, noch een Rapporteur aangewezen als hoofdverantwoordelijke voor behandeling van het voorstel. Er is daarom ook nog geen verdere informatie bekend over de inhoudelijke appreciatie van het voorstel door het Europees Parlement op het moment van schrijven.

4. Beoordeling bevoegdheid, subsidiariteit en proportionaliteit

a) Bevoegdheid

Het oordeel van het kabinet ten aanzien van de bevoegdheid is positief. De voorgestelde rechtsgrondslag is artikel 114 VWEU. Op grond van dit artikel is de EU bevoegd maatregelen vast te stellen inzake de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen van de lidstaten die de instellingen de werking van de interne markt betreffen. Aangezien het voorstel betrekking heeft op het ontwikkelen van robuuste cybersecurity voorwaarden voor alle producten met digitale elementen op de interne markt, kan het kabinet zich vinden in de voorgestelde rechtsgrondslag. Op grond van artikel 4, tweede lid, onder a, van het VWEU hebben de EU en de lidstaten een gedeelde bevoegdheid op het gebied van de interne markt.

b) Subsidiariteit

Het oordeel van het kabinet is positief. De verordening heeft tot doel het creëren van horizontale robuuste cybersecurity voorwaarden voor alle producten met digitale elementen en waar fabrikanten, leveranciers en importeurs van dergelijke producten aan moeten voldoen voor plaatsing op de interne markt. Daarnaast heeft de verordening ook als doel voor transparantie te zorgen over de mate van cybersecurity van dergelijke producten ten behoeve van de keuze van gebruikers (consumenten en organisaties). Dit moet leiden tot een digitaal veiligere Europese digitale interne markt. Gezien het grensoverschrijdende karakter van cybersecurity en het toenemend aantal incidenten met impact in meerdere landen en het feit dat marktspelers over het algemeen actief zijn in meerdere lidstaten of mondiale marktpartijen zijn, kan dit onvoldoende door afzonderlijk optreden van de lidstaten worden bereikt, daarom is een EU-aanpak nodig. Door de verordening wordt het gelijk speelveld op het terrein van cybersecurity gewaarborgd en versterkt, worden belemmeringen op de interne markt voor fabrikanten, leveranciers en importeurs

weggenomen en wordt bijgedragen aan de verhoging van de digitale weerbaarheid van Nederland en de EU. Om die redenen is optreden op het niveau van de EU gerechtvaardigd.

c) Proportionaliteit

Het oordeel van het kabinet is positief. De verordening heeft tot doel horizontale cybersecurityeisen te stellen aan alle producten met digitale elementen voor Europese markttoegang in samenspel met Europese sectorale wet- regelgeving en daarmee bij te dragen aan een digitaal veiligere Europese digitale interne markt. Het voorgestelde optreden is geschikt om deze doelstelling te bereiken, omdat de CRA zal fungeren als vangnet voor producten die vallen buiten sectorale wet- en regelgeving op dit terrein. Dit draagt bij aan de digitaal eengemaakte markt, de rechtszekerheid en de voorspelbaarheid van wetgeving binnen de Unie. De CRA sluit daarnaast aan bij de bestaande Europese systematiek van productregulering voor markttoegang met bijbehorende standaardisatie en toezicht, het zogenaamde *New Legislative Framework* (hierna ook: «NLF»). Bovendien gaat het voorgestelde optreden niet verder dan noodzakelijk, omdat het optreden beperkt blijft tot het verschaffen van dit vangnet.

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

a) Consequenties EU-begroting

De Commissie geeft in het voorstel aan dat ENISA voor de uitvoering 4,5 FTE zal toekennen uit de bestaande budgetten, omdat er synergiën zijn met werkzaamheden en de reeds toegekende budgetten voor NIB2. De Commissie stelt 7 additionele FTE nodig te hebben (€ 5 miljoen euro) per jaar. De benodigde FTE zullen worden gedekt uit reeds bestaande fraudepreventiemaatregelen. Het kabinet is van mening dat de financiële middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van het MFK 2021–2027 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting van de EU.

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

De financiële consequenties van dit voorstel voor de rijksoverheid zien op het inrichten van markttoezicht op nationaal niveau. De financiële gevolgen van het voorstel voor de rijksoverheid en medeoverheden zijn op dit moment nog niet te specificeren, maar zijn naar verwachting substantieel. De Commissie schat in dat voor de hele EU de kosten voor markttoezicht zullen bestaan uit € 7,7 miljard euro. Het inrichten van passend toezicht als sluitstuk is nodig om het beoogde positieve maatschappelijke effect te realiseren dat producten digitaal veiliger zijn. De budgettaire gevolgen voor de Rijksbegroting worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline. Daarbij dient ook rekening gehouden te worden met eventuele budgettaire gevolgen voor medeoverheden.

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

Het voorstel heeft financiële consequenties en verhoogt de regeldruk voor het bedrijfsleven. Dit moet worden afgezet tegen de baten voor de verschillende stakeholders en de samenleving als geheel. Het *impact assessment* van de Commissie maakt de diverse elementen inzichtelijk.

De Commissie stelt dat voor hard- en softwarefabrikanten de nalevingskosten bestaan uit het opnemen van de veiligheidseisen in hun producten met digitale elementen in de productlevenscyclus, het uitvoeren van de conformiteitsbeoordeling, verplichtingen voor documentatie en een meldplicht bij kwetsbaarheden. Bovendien wordt een risicogebaseerde benadering gekozen met oog voor administratieve lasten en nalevingskosten. Enerzijds worden de administratieve lasten beperkt doordat organisaties door middel van een zelfassessment de conformiteitsbeoordeling uit kunnen voeren. Anderzijds zijn kritieke producten met digitale elementen gedefinieerd waarvan de cybersecurityrisico's en potentiële negatieve impact van kwetsbaarheden hoger zijn. Voor deze kritieke producten gelden zwaardere eisen ten aanzien van de conformiteitsbeoordelingsprocedure waarbij in de hoogste risicoklasse de conformiteitsbeoordeling plaats moet vinden door een onafhankelijke derde partij. De Commissie schat in dat het aandeel kritieke producten met digitale elementen 10% van het totaal aantal gereguleerde producten is. De totale nalevingskosten in de hele EU schat de Commissie in op ongeveer 29 miljard euro op een totale marktomzet van 1485 miljard euro per jaar. De nalevingskosten voor een bedrijf zullen variëren en zijn afhankelijk van de complexiteit en omvang van het product, de bestaande cybersecurity praktijk van een bedrijf, de omgeving (*business-to-consumer* of *business-to-business*) en de omvang van het bedrijf. Dit geldt voor het mkb tot grote bedrijven en is afhankelijk van hun rol in de digitale economie. De gemiddeld geschatte kosten van een zelfassessment zijn 18.400 euro en een conformiteitsbeoordeling door een derde partij zijn 25.000 euro. Voor bedrijven worden met Europese horizontale verplichtingen nalevingskosten gereduceerd ten opzichte van nalevingskosten in verschillende lidstaten. Daarnaast verwacht de Commissie dat het aantal cybersecurity incidenten met producten met digitale elementen met bijkomende incidentresponskosten en reputatieschade met 33% vermindert. Voor de hele EU verwacht de Commissie een kostenbesparing als gevolg van incidenten van rond de 180 miljard per jaar tot 290 miljard euro per jaar. Het is aannemelijk dat bedrijven de verhoogde kosten zullen doorberekenen in hun prijs naar gebruikers (organisaties en consumenten). Dit moet worden afgewogen tegen de baten van gebruikers van verhoogde transparantie, dat producten met digitale elementen die zij afnemen standaard veiliger zijn en hun fundamentele rechten zoals privacy en bescherming van hun data ook beter zijn geborgd. Wel wordt er in het *impact assessment* aandacht gevraagd door het mkb voor een proportionele benadering en ondersteunende maatregelen, gezien het mkb dat naar verwachting relatief hogere regeldruk zal ervaren.

d) Gevolgen voor concurrentiekracht en geopolitieke aspecten

Met het verhogen van de cybersecurity van producten met digitale elementen beoogt de EU de weerbaarheid van de digitale samenleving en economie te vergroten. Europese wet- en regelgeving met bijbehorende standaarden en toezicht zoals in de CRA dragen bij aan de veiligheid en weerbaarheid van de wereldwijde waardeketen en stimuleren digitaal veilige innovaties. Dit stelt de EU in staat wereldwijd een sterkere positie in het digitale domein in te nemen. Het is daarnaast goed dat de EU inzet op een horizontale verordening. Gefragmenteerde standaarden en regulering over cybersecurity verzwakken niet alleen het concurrentievermogen van Europese bedrijven en de cybersecurity van consumenten, ze ondermijnen ook de open strategische autonomie van de EU. Met het verhogen van de digitale weerbaarheid behoudt de EU ook een open economie en een platform voor samenwerking met internationale partners. De EU is wereldwijd de eerste partij die dergelijke wettelijke veiligheidseisen introduceert voor producten met digitale elementen. Wanneer de EU, verantwoordelijk voor meer dan een derde van de

wereldimport en -export, cybersecuritystandaarden stelt, dan kunnen producenten ervoor kiezen om deze standaarden, omwille van kosteneffi-ciëntie, voor alle geproduceerde producten toe te passen, niet alleen die voor de EU. Hiermee draagt de CRA bij aan een wereldwijd veiligere waardenketen van digitale producten en veiligere digitale samenlevingen. Door samenwerking met gelijkgezinde derde landen kan de EU leidend zijn in het stimuleren van gelijksoortige wettelijke eisen en standaarden wereldwijd. Wereldwijde aanname van vergelijkbare cybersecurityeisen aan producten met digitale elementen bevordert zowel de digitale weerbaarheid van het hele ecosysteem als de concurrentiekracht van Europese bedrijven in de mondiale economie.

6. Implicaties juridisch

a) Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)

Het is noodzakelijk te voorzien in de benodigde nationale uitvoeringsbepalingen om uitwerking te kunnen geven aan deze verordening. Zo moet een bevoegde autoriteit worden aangewezen. Ook moeten regels worden vastgesteld wat betreft de sancties die van toepassing zijn op inbreuken op de verordening, moeten er maatregelen worden getroffen die ervoor zorgen dat deze sancties worden toegepast en moeten er regels worden vastgesteld over de vraag of en in hoeverre administratieve boetes mogen worden opgelegd aan overheidsinstanties en overheidsorganen. In het voorstel van de Commissie staat dat indien de overtreder een onder-neming is, een omzet-gerelateerde boete moet worden opgelegd indien dat bedrag hoger is dan het maximale bedrag dat volgt uit de verord-ening. De hoogte van deze boete wijkt mogelijk af van de hoogte die geldt volgens het systeem zoals dat momenteel in het Warenwetbesluit bestuurlijke boetes is opgenomen. Hier dient de wetgeving eventueel op aangepast te worden.

b) Gedelegeerde en/of uitvoeringshandelingen, incl. NL-beoordeling daarvan

Op basis van artikel 290 VWEU bevat het voorstel de volgende bevoegd-heden voor de Commissie voor gedelegeerde handelingen:

1. Het actualiseren van de lijst van categorieën van kritieke producten met digitale elementen in Annex III en het specificeren van definities van deze producten
2. Het identificeren van producten met digitale elementen waarvoor andere Unie wetgeving hetzelfde beschermingsniveau als de CRA garandeert, het vervolgens specificeren of een beperking of uitzonde-ring van de reikwijdte van de verordening nodig is en, indien nodig, de reikwijdte van de beperking te bepalen
3. De mogelijkheid om certificering te verplichten van bepaalde hoog kritieke producten met digitale elementen op basis van beoordelings-criteria die in de verordening staan
4. Het specificeren van de minimale hoeveelheid informatie in de EU verklaring van conformiteit
5. Het aanvullen van elementen die onderdeel moeten zijn van de technische documentatie

Voor wat betreft de hierboven genoemde gedelegeerde handelingen kan het kabinet zich vinden in de toekenning van de bevoegdheden die worden toegekend aan de Commissie. Omdat er geen sprake lijkt te zijn van essentiële onderdelen, is toekenning van deze bevoegdheden mogelijk. Ook acht het kabinet de toegekende handelingen wenselijk omdat elke individuele gedelegeerde handeling ervoor zorgt dat de

verordening toekomstbestendig blijft tegen het licht van relevante technologische- en marktontwikkelingen. Zo geeft gedelegeerde handeling «1» (artikel 6 lid 2 en 3) de Commissie de bevoegdheid om de lijst van kritieke producten met digitale elementen in Annex III te actualiseren middels het toevoegen of verwijderen van categorieën van kritieke producten. Het is immers voorstelbaar dat de evolutie van huidige technologieën of de opkomst van een compleet nieuwe technologie kan leiden tot een categorie van kritieke producten met digitale elementen die nu nog niet kan worden voorzien. Deze logica geldt in dezelfde mate voor handelingen «2» (artikel 6 lid 5), «3» (artikel 20 lid 5), «4» (artikel 20 lid 5) en «5» (artikel 23 lid 5). Ook geldt voor alle gedelegeerde handelingen dat delegatie in plaats van uitvoering voor de hand ligt omdat het een aanvulling of wijziging van de wetgevingshandeling betreft. Ten slotte acht het kabinet de vijf bevoegdheden voldoende afgebakend qua doel, inhoud en strekking. De duur van de bevoegdheidstoekenning lijkt niet te zijn opgenomen in het voorstel. Het kabinet heeft een voorkeur voor toekenning van deze bevoegdheden voor bepaalde tijd, met mogelijkheid tot stilzwijgende verlenging.

Het voorstel bevat de volgende bevoegdheden voor de Commissie voor uitvoeringshandelingen ten behoeve van uniforme uitvoering van de verordening, op basis van de verordening (EU)182/2011:

1. Het specificeren van het format en de elementen van de software bill of materials
2. Het specificeren van het soort informatie, format en procedure van de meldingen van actief misbruikte kwetsbaarheden en incidenten die door fabrikanten moeten worden gemeld bij ENISA
3. Het specificeren van welke Europese cybersecurity certificeringsche-ma's onder de Cyber Security Act kunnen worden gebruikt om conformiteit aan te tonen met de essentiële eisen in Annex I van het voorstel
4. Het adopteren van gemeenschappelijke specificaties in relatie tot de essentiële eisen in Annex I van het voorstel
5. Technische specificaties opstellen voor pictogrammen of andere beeldmerken in relatie tot de cybersecurity van producten met digitale elementen en mechanismen om hun gebruik te stimuleren
6. Besluiten over corrigerende of restrictieve maatregelen op Unie niveau in buitengewone omstandigheden die directe interventie rechtvaardigen om het goed functioneren van de interne markt te behouden.

Ook voor de uitvoeringshandelingen geldt dat, met uitzondering van handeling «6», het kabinet zich kan vinden in de toekenning van de bevoegdheden. Omdat er geen sprake lijkt te zijn van essentiële onder-delen, is toekenning van deze bevoegdheden mogelijk. Toekenning van deze bevoegdheden voor handelingen «1» tot en met «5» acht het kabinet wenselijk omdat voor alle uitvoeringshandelingen geldt dat het de toekomstbestendigheid van de verordening ten goede komt. Zo is uitvoeringshandeling «1» (artikel 10 lid 15) nuttig omdat het de Commissie de bevoegdheid geeft het format en de elementen van de *software bill of materials* te wijzigen, die, tegen het licht van relevante markt- en technologische ontwikkelingen, geactualiseerd dienen te worden. Handelingen «2» (artikel 11 lid 5), «3» (artikel 18 lid 4), «4» (artikel 19) en «5» (artikel 22 lid 6) dienen eenzelfde doel waarbij de toekomstbestendigheid centraal staat. Ook de keuze voor uitvoering in plaats van delegatie ligt voor handelingen «1» tot en met «6» voor de hand omdat hiermee wordt gewaarborgd dat de verordening volgens eenvormige voorwaarden wordt uitgevoerd, hetgeen ten goede komt van de werking van de interne markt. De uitvoeringshandelingen worden vastgesteld volgens de onderzoeksprocedure als bedoeld in artikel 5 van

verordening 182/2011. Toepassing van de deze procedure is hier volgens het kabinet op zijn plaats omdat het gaat om handelingen die de veiligheid van mensen betreffen (artikel 2, lid 2, onder iii, verordening 182/2011).

Over handeling «6» (artikel 45 lid 4) twijfelt het kabinet of toekenning van deze bevoegdheid wenselijk is. Hieraan wordt de bevoegdheid toegekend aan de Commissie om in uitzonderlijke gevallen digitale producten uit de Europese markt te laten terugtrekken. Mogelijk is het wenselijk om dit in de verordening zelf op te nemen of om deze bevoegdheid op een andere wijze vorm te geven in de verordening.

c) Voorgestelde datum inwerkingtreding (bij verordeningen en besluiten) met commentaar t.a.v. haalbaarheid

De verordening zal twintig dagen na publicatie in werking treden en na 24 maanden van kracht zijn. De meldplicht voor fabrikanten in artikel 11 wordt 12 maanden na inwerkingtreding van kracht. Het kabinet acht deze termijn haalbaar en wenselijk aangezien dagelijks kwetsbaarheden in producten met digitale elementen worden ontdekt en het aantal cybersecurity incidenten met aanzienlijke gevolgen voor gebruikers blijven toenemen.

d) Wenselijkheid evaluatie-/horizonbepaling

In het voorstel is opgenomen dat de verordening 36 maanden na inwerkingtreding en daarna elke 4 jaar zal worden geëvalueerd door de Commissie. De Commissie zal het evaluatierapport sturen naar de Europese Raad en het Europees Parlement en het rapport openbaar maken.

Gezien de doorlopende technologische en maatschappelijke ontwikkelingen die raken aan de cybersecurity producten met digitale elementen acht het kabinet deze periodieke evaluatie passend en wenselijk.

e) Constitutionele toets

Het voorstel moet bijdragen aan het creëren van horizontale robuuste cybersecurityvoorwaarden voor alle producten met digitale elementen, waar fabrikanten, leveranciers en importeurs van dergelijke producten aan moeten voldoen voor plaatsing op de interne markt. Dit kan gevolgen hebben voor de vrijheid van ondernemerschap. In het geval dat een product een significant cybersecurity risico vormt en er binnen de daarvoor door de toezichthouder aangewezen periode geen passende maatregelen zijn getroffen, dient de toezichthouder maatregelen te treffen waardoor het betreffende product niet meer op de nationale markt aangeboden kan worden. In een uiterst geval is bovendien de Commissie bevoegd corrigerende of beperkende maatregelen op te leggen op Unieniveau. Tegelijkertijd helpt het creëren van een hoger niveau van cybersecurity van producten met digitale elementen en het bevorderen van kennis en informatie voor gebruikers ook bij de bescherming van de bescherming van fundamentele rechten en vrijheden zoals de persoonlijke levenssfeer, de bescherming van persoonsgegevens, en de bescherming van eigendom of persoonlijke waardigheid en integriteit. Het is van belang dat het voorstel de juiste balans weet te vinden tussen de diverse grondrechten die erdoor worden geraakt. Het kabinet ziet in het voorstel duidelijk aandacht voor deze balans, maar zal hier blijvend aandacht voor hebben.

7. Implicaties voor uitvoering en/of handhaving

Lidstaten moeten toezicht en handhaving van de regels in de CRA binnen hun grondgebied beleggen bij één of meerdere markttoezichthouders. Dit mag een bestaand of nieuw op te richten autoriteit zijn. Gezien de aan Agentschap Telecom (hierna ook: «AT») toegekende taken op het gebied van cybersecurity onder RED (toezicht op (cybersecurity) markttoegangseisen voor draadloos verbonden apparaten) en CSA (nationale cyberbeveiligingscertificeringsautoriteit voor ICT-producten, dienst en processen), en de regels ter implementatie van Europese NIB-richtlijn in de Wet beveiliging netwerk- en informatiesystemen en de Telecomwet (toezicht op de continuïteit van de sectoren telecom, digitale infrastructuur en energie) ligt het voor de hand om AT aan te wijzen als nationale markttoezichthouder. Het toezicht op de CRA ligt in het verlengde van deze taken. Toezicht op de CRA betekent een taakverzwaring voor AT, ondanks dat er naar verwachting synergiën mogelijk zullen zijn met de huidige taken van AT. AT kan voortbouwen op de opgebouwde capaciteit en expertise voor toezicht onder de RED. De Commissie stelt dat de cybersecurity markttoegangseisen onder de RED over zullen gaan in de CRA. Tegelijkertijd is de reikwijdte van de CRA aanzienlijk breder en worden meer partijen onder toezicht gesteld. Dit betekent dat investeringen nodig zullen zijn in de capaciteit en expertise bij AT om passend toezicht in te kunnen richten. Ten aanzien van de handhaafbaarheid oordeelt het kabinet dat de CRA handhaafbaar is omdat wordt aangesloten op de bestaande NLF-systematiek van Europese productregulering. Net als marktpartijen is AT bekend met deze werkwijze aangezien onder andere de RED ook werkt op basis van deze systematiek.

8. Implicaties voor ontwikkelingslanden

De verordening stelt eisen aan producten die in de Unie op de markt gebracht worden. Producenten, zo ook die in ontwikkelingslanden, dienen aan deze standaarden te voldoen.