Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 3555

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 30 november 2022

De vaste commissie voor Digitale Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Economische Zaken en Klimaat over de brief van 21 oktober 2022 over het Fiche: Verordening Cyber Resilience Act (CRA) (Kamerstuk 22 112, nr. 3552).

De vragen en opmerkingen zijn op 7 november 2022 aan de Minister van Economische Zaken en Klimaat voorgelegd. Bij brief van 28 november 2022 zijn de vragen beantwoord.

De voorzitter van de commissie,
Kamminga

Adjunct-griffier van de commissie,
Van Tilburg

kst-22112-3555
ISSN 0921 - 7371
's-Gravenhage 2022

Vragen en opmerkingen vanuit de fracties en reactie van de bewindspersoon

Vragen en opmerkingen van de leden van de VVD-fractie en reactie van de bewindspersoon

De leden van de VVD-fractie hebben kennisgenomen van de kabinetspositie inzake de Verordening Cyber Resilience Act (CRA) en hebben hierover nog enkele vragen en opmerkingen.

De leden van de VVD-fractie achten het positief dat vanuit Europa het initiatief wordt genomen om slimme apparaten (IoT apparaten) veiliger te maken zodat het aantal cyberaanvallen verminderd kan worden. Deze leden zijn het eens met de constatering dat helaas te vaak nog cyberaanvallen kunnen worden uitgevoerd via zwakke plekken in de software en hardware van IoT apparaten. Deze leden achten het dan ook van belang om de beveiligingstandaarden van IoT apparaten te verhogen om digitale deuren beter op slot te houden voor cybercriminelen.

VVD 1
De leden van de VVD-fractie lezen dat Standalone software, apps en Software als een service (SaaS) niet onder de reikwijdte van de CRA vallen. Deze leden delen de twijfel van het kabinet omtrent deze uitzondering. Gegeven dat bovenstaande digitale middelen niet onder de CRA vallen, onder welke wettelijke scope wordt hun digitale beveiliging wel voldoende geborgd? Wordt dit bijvoorbeeld geborgd via de NIS2-richtlijn? Welke analyse vormt de basis van deze verdeling? In hoeverre zijn deze verordeningen toereikend als het gaat om Standalone software, apps en Saas?

Antwoord
De CRA legt horizontale verplichtingen op aan de fabrikanten, importeurs en distributeurs van producten met digitale elementen ten behoeve van de cybersecurity van die producten. De reikwijdte is breder dan Internet of Things (IoT) of slimme apparaten. Met betrekking tot stand alone software (met uitzondering van niet-commerciële open source software) en apps begrijpt het kabinet het voorstel zo dat deze onder de definitie van product met digitale elementen vallen, en dus wél onder de CRA vallen. Software-as-a-Service (SaaS) een variant van een cloudcomputingdienst valt buiten de reikwijdte van het voorstel. Daarentegen vallen «remote data processing solutions» wel in scope van de CRA. Dat kunnen ook oplossingen zijn die gebruik maken van SaaS. Het kabinet heeft de Commissie op dit punt om verduidelijking gevraagd. De definities van de CRA moeten helder en werkbaar zijn. De reden dat producten wél en digitale diensten niet onder de voorgestelde scope vallen is op basis van de antwoorden van de Commissie gelegen in het feit dat de CRA is vormgegeven als onderdeel van het New Legislative Framework (NLF). Het NLF is het kader dat een groot deel van de producten op het gebied van veiligheid, gezondheid en milieu op de Europese markt reguleert. De analyse van de Europese Commissie is dat de cybersecurity van SaaS al door de herziene Richtlijn voor Netwerk- en Informatiebeveiliging (NIB2- richtlijn) wordt geregeld. De NIB2-richtlijn regelt de digitale beveiliging voor essentiële en belangrijke entiteiten in verschillende sectoren, waaronder aanbieders van cloudcomputingdiensten waar o.a. SaaS onder valt. De NIB2-richtlijn is met name gericht op de beveiliging van de netwerk- en informatiesystemen die deze entiteiten. Bovendien vallen aanbieders die de drempel voor middelgrote ondernemingen als bedoeld in Aanbeveling 2003/361/EG niet halen niet onder de NIB2-richtlijn tenzij ze vanwege de toepasselijkheid van een of meer specifieke criteria (bv. dienst waarvan verstoring aanzienlijke gevolgen kan hebben voor openbare veiligheid of

volksgezondheid) door de lidstaat toch als essentiële of belangrijke entiteit worden aangemerkt. Fabrikanten, importeurs en distributeurs van producten met digitale elementen vallen ongeacht de omvang van hun onderneming onder de reikwijdte van de CRA. Hierdoor kan er mogelijk een ongewenste lacune overblijven. Als dat inderdaad het geval is, wil het kabinet weten welke andere EU-regelgeving hierin kan voorzien.

VVD 2
Daarnaast lezen de leden van de VVD-fractie dat de verantwoordelijkheid voor het verhogen van de beveiligingseisen van slimme apparaten komt te liggen bij fabrikanten die producten ontwikkelen, ontwerpen en beschikbaar stellen en leveranciers en importeurs die de producten beschikbaar stellen in de interne markt. Hoe verhoudt deze verantwoordelijkheid zich tot producten van buiten de Europese Unie die niet aan de gestelde beveiligingseisen voldoen? In het geval er sprake is van niet veilige producten, wordt dan de betrokken importeur van de producten verantwoordelijk gehouden? Zo ja, betekent dit ook dat deze importeurs verplicht een toets moeten doen op de veiligheidseisen van slimme apparaten vanuit derde landen? Moeten zij op basis van deze toets ook slimme apparaten vanuit derde landen weigeren? Kan het kabinet de hier geldende procedure verduidelijken?

Antwoord
De CRA is van toepassing op producten met digitale elementen die op de Europese markt beschikbaar worden gesteld, ongeacht of het product binnen of buiten de Europese Unie is ontwikkeld of geproduceerd. 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. Een importeur wordt in het voorstel gedefinieerd als een in de Europese Unie gevestigde natuurlijke of rechtspersoon die een product in de handel brengt (voor het eerst in de EU op de markt aanbiedt) dat de naam of het merk draagt van een natuurlijk of rechtspersoon die is gevestigd buiten de Europese Unie. Feitelijk worden aan geïmporteerde producten dezelfde eisen gesteld. In het voorstel wordt bepaald dat een importeur, voordat hij een dergelijk product in de handel brengt, ervoor moet zorgen dat de voorgeschreven conformiteitsbeoordelingsprocedure is uitgevoerd door de fabrikant, dat de fabrikant de technische documentatie heeft opgesteld en dat het product is voorzien van een CE-markering en vergezeld wordt van de voorgeschreven informatie en gebruiksinstructies. Als de importeur vaststelt (of grond heeft om aan te nemen) dat de het product of de processen van de fabrikant niet aan de in de verordening gestelde beveiligingseisen voldoen, mag de importeur de producten niet in de handel brengen tot dit gebrek is hersteld. Als het product een significant cybersecurityrisico vormt moet de importeur bovendien de fabrikant en de markttoezichthouder hiervan op de hoogte stellen.
Als een importeur pas nadat het product in de handel gebracht is, vaststelt dat het product of de beveiligingsprocessen van de fabrikant niet voldoen aan de beveiligingseisen, moet de importeur volgens het voorstel direct herstelmaatregelen nemen om het product en de processen van de fabrikant alsnog te laten voldoen, of het product terugroepen of uit de handel nemen. Zodra de importeur een kwetsbaarheid identificeert moet hij de fabrikant hierover zonder onnodige vertraging informeren, en wanneer het een significant cybersecurityrisico vormt moet de importeur dit direct melden bij de markttoezichtautoriteiten van de lidstaten waar het product verkrijgbaar is.

Als de markttoezichtautoriteit voldoende grond heeft om te vermoeden dat een geïmporteerd product met digitale elementen een significant cybersecurityrisico vormt wordt een onderzoek ingesteld. Indien de markttoezichtautoriteit vervolgens vaststelt dat een product met digitale elementen niet aan de vereisten voldoet zal het volgens het voorstel aan de relevante marktdeelnemer (in dat geval de importeur) onverwijld de verplichting opleggen om gepaste corrigerende maatregelen te nemen om het product alsnog te laten voldoen, uit de handel te nemen danwel het product terug te roepen. Dit is in lijn met het geldende Europese markttoezichtskader voor productveiligheid.

VVD 3
Naast dat het van belang is dat de cyberbeveiligingseisen voor slimme apparaten verhoogd moeten worden, willen de leden van de VVD-fractie wijzen op de belangrijke complementaire verantwoordelijkheid van consumenten om veilig en bewust om te gaan met (huidige) slimme apparaten. Is het kabinet dit met deze leden eens? Zo ja, is zij bereid om parallel aan de implementatie van de CRA in te zetten op een voorlichting/bewustwordingscampagne rondom het verantwoordelijk gebruiken van slimme apparaten om consumenten tegelijkertijd ook weerbaarder te maken? Zo nee, waarom niet?

Antwoord
In de Nederlandse cybersecuritystrategie (NLCS) die op 10 oktober jl. aan uw Kamer is aangeboden[1], heeft het kabinet uiteengezet dat het beleid ten aanzien van cybersecurity inderdaad rust op meerdere pijlers. Een van de belangrijkste stappen richting digitaal weerbare burgers en organisaties zijn veilige digitale producten, zoals beschreven in pijler II van de NLCS. De CRA is een integraal onderdeel van de acties bij deze doelstelling. Naast het creëren van cybersecurityvoorwaarden voor fabrikanten, leveranciers en importeurs van producten met digitale elementen, is de tweede hoofddoelstelling van de CRA het zorgen voor transparantie over de mate van cybersecurity van dergelijke producten ten behoeve van de keuze van gebruikers (consumenten en organisaties).
De risico's van digitale kwetsbaarheden en dreigingen moeten allereerst worden gedragen door de fabrikanten, importeurs en distributeurs van digitale producten. Maar er zal bijna altijd een restrisico blijven waardoor de burger (of organisatie) ook zelf maatregelen moet nemen. Om deze maatregelen te kunnen nemen moeten burgers en MKB zich allereerst bewust zijn van de risico's en de te nemen cybersecurity basismaatregelen. Het kabinetsbeleid ten aanzien van het vergroten van de bewustwording onder burgers wordt beschreven in pijler IV van de NLCS. Een belangrijk instrument dat het kabinet hiertoe al jaren inzet is de voorlichtingscampagne om de verschillende doelgroepen te informeren over de cybersecurity basismaatregelen die zij kunnen nemen. Een voorbeeld is de publiekscampagne «Doe je updates». Begin december zal de vijfde ronde van deze campagne starten. Daarnaast wordt structurele voorlichting aan burgers gegeven via veiliginternetten.nl.

VVD 4
Is het kabinet het met de leden van de VVD-fractie eens dat het net zo belangrijk is om de beveiligingseisen van huidige slimme apparaten die al op de markt zijn gebracht, te verhogen? Zo ja, welke mogelijkheden ziet zij, al dan niet via de CRA, om de beveiligingseisen niet alleen voor toekomstige maar ook voor huidige slimme apparaten te verhogen? Is zij ook voornemens om deze voorstellen kenbaar te maken in de onderhandelingen? Zo nee, waarom niet?

[1] Kamerstuk 26 643, nr. 925

Antwoord
Het kabinet is voorstander van een breed toepassingsbereik voor de CRA, maar met het oog op algemene rechtsbeginselen is het logisch dat deze generieke beveiligingseisen alleen worden gesteld aan producten die na een redelijke inwerkingtredingstermijn na vaststelling van de CRA in de handel worden gebracht of nadien substantieel zijn gemodificeerd in hun ontwerp of beoogd gebruik. Voor de digitale weerbaarheid zou het uiteraard goed zijn als ook digitale producten die reeds in de handel zijn gebracht beter beveiligd worden door de fabrikanten, maar dat is in veel gevallen niet goed uitvoerbaar. Zoals aangegeven in het voorgaande antwoord hecht het kabinet daarom ook veel belang aan bewustzijn van cyberrisico's en goede voorlichting aan gebruikers van digitale producten en diensten. Het kabinet wijst er daarnaast nog op dat de meldplicht voor fabrikanten in artikel 11 van het voorstel wel zal gelden ten aanzien van producten die vóór de datum van inwerkingtreding van de CRA in de handel zijn gebracht (zie artikel 55, derde lid, van het voorstel). Het kabinet wijst er tot slot op dat de eisen uit de gedelegeerde verordening onder de radioapparatuurrichtlijn (ook wel: Radio Equipment Directive, verordening EU 2014/53/EU) al op 1 augustus 2024 van toepassing zullen zijn op draadloos verbonden (en daarmee ook slimme) apparaten die vanaf dan in de handel worden gebracht. Deze eisen zullen op termijn opgaan in de CRA.

VVD 5
Tevens lezen de leden van de VVD-fractie dat fabrikanten conform de CRA zonder onnodige vertraging en binnen 24 uur ontdekte kwetsbaarheden in producten moeten melden bij de European Union Agency for Cybersecurity (ENISA). Wat wordt bedoeld met «onnodige vertraging» en hoe haalbaar acht het kabinet deze tijdspanne, in het bijzonder voor middelkleine en kleine fabrikanten die deze meldingen moeten maken gegeven de nalevings- en handhavingskosten die dit met zich meebrengt? Kunt het kabinet dit toelichten?

Antwoord
Het kabinet ziet het belang van het zo snel mogelijk melden van kwetsbaarheden en steunt daarom in beginsel een 24 uurs-termijn voor het melden van kwetsbaarheden die reeds actief misbruikt zijn. Het kabinet erkent de spanning tussen haalbaarheid van het melden van kwetsbaarheden, bijvoorbeeld door het MKB, en de mogelijkheid die de melding biedt om tijdig te handelen om de negatieve gevolgen van de exploitatie zo veel mogelijk te beperken en slachtoffers te voorkomen. Het kabinet ziet daarom graag verduidelijkt door de Commissie wat wordt bedoeld met «onnodige vertraging». Ook heeft het kabinet de Commissie om verduidelijking gevraagd over hoe de verschillende meldplichten (uit de NIS2-richtlijn, AI Act, Cybersecurity Act en het CRA-voorstel) zich tot elkaar verhouden, het kabinet acht samenhang hiertussen van belang. We gaan over de CRA-meldplicht in gesprek met marktpartijen, de Commissie en andere lidstaten.

VVD 6
In het kader van de uitvoerbaarheid en proportionaliteit voor ondernemers hebben de leden van de VVD-fractie de nodige zorgen en stellen daarom graag de volgende vragen. De CRA in de huidige vorm stelt fabrikanten verplicht om elke actief misbruikte kwetsbaarheid in een product te melden bij ENISA. In hoeverre acht het kabinet dit uitvoerbaar voor ondernemers? Niet elke misbruikte kwetsbaarheid brengt significante veiligheidsrisico's met zich mee en daarmee zou het melden van elke misbruikte kwetsbaarheid ongeacht zwaarte en risiconiveau een enorme druk leggen op de werkzaamheden van ondernemers en dat achten deze leden onwenselijk zeker gezien de andere verplichtingen die

gaan gelden voor ondernemers als gevolg van andere Europese wetgeving zoals de NIS2-richtlijn, de Cybersecurity Act en de AI Act, deelt het kabinet deze zorgen? Zo ja, ziet zij mogelijkheden om de meldplicht te beperken tot significante incidenten waarbij aan een bepaald risiconiveau moet worden voldaan? Zo nee, waarom niet? Zo ja, is het kabinet bereid dit onder de aandacht te brengen in de onderhandelingen?

Antwoord
In de NIB2-richtlijn is bepaald dat een essentiële of belangrijke entiteit een incident aan het CSIRT en/of de toezichthouder moet melden als dit «aanzienlijke gevolgen» heeft voor de dienstverlening (artikel 23). In de Cybersecurity Act wordt voorgeschreven dat de houder van een Europees cyberbeveiligingscertificaat «kwetsbaarheden of onregelmatigheden in verband met de beveiliging van gecertificeerde ICT-producten, -diensten of -processen die achteraf zijn vastgesteld en die gevolgen kunnen hebben voor de naleving van de met de certificering verband houdende voorschriften» moet melden (artikel 56). In de AI Act is bepaald dat aanbieders van AI-systemen met een hoog risico «ernstige incidenten met of storingen van» die systemen die een niet-nakoming van verplichtingen krachtens Unierecht ter bescherming van grondrechten inhouden, moeten melden (artikel 62).
In het voorstel voor de CRA worden fabrikanten verplicht om «geëxploiteerde kwetsbaarheden» te melden. Dit zijn kwetsbaarheden die actief misbruikt worden door kwaadwillenden om bijvoorbeeld cyberaanvallen uit te voeren richting gebruikers van het product. Het is wenselijk dat actief misbruikte kwetsbaarheden gemeld worden zodat eindgebruikers (burgers en organisaties) passende beschermingsmaatregelen kunnen nemen. De Commissie heeft omwille van de proportionaliteit ervoor gekozen om niet alle kwetsbaarheden te laten melden. Uit de definitie van geëxploiteerde kwetsbaarheid vloeit voort dat dit inhoudt dat er al een aanvaller bezig is met het exploiteren van de kwetsbaarheid. Dat houdt een bepaalde mate van ernst/risico in. Zoals ook in antwoord op vraag VVD 7 toegelicht, onderschrijft het kabinet het doel van de meldplicht van actief geëxploiteerde kwetsbaarheden, om de negatieve gevolgen van het misbruik zoveel mogelijk te kunnen beperken en ter voorkoming van slachtoffers van cybercriminelen. Voor wat betreft de belastbaarheid van de meldplicht onder de CRA hecht het kabinet aan een goede belangenafweging, ook hierover gaat het kabinet nog graag in gesprek met partijen, andere lidstaten en de Europese Commissie.

VVD 7
In het verlengde van het melding doen bij de ENISA, zouden de leden van de VVD-fractie nog willen in gaan op de keuze voor de ENISA als toezichthouder ook in relatie tot de nog aan te wijzen nationale markttoezichthouder. Hoe beoordeelt het kabinet het feit dat aanbieders van slimme apparaten een melding moeten doen bij het Europese ENISA en niet bij de nationale markttoezichthouder, gezien het feit dat de ENISA daarna verplicht is om de melding door te zetten naar de nationale Cyber Security Incident Response Team? Hoe beoordeelt het kabinet deze procedure en rolverdeling? Is zij het met deze leden eens dat het inefficiënt en daarmee onverstandig is om de meldingen bij de ENISA onder te brengen om ze vervolgens weer naar de nationale autoriteiten door te sturen zoals bij het Nationaal Cyber Security Centrum (NCSC) of de CSIRT-DSP? Zo ja, is het kabinet het met deze leden eens dat het verstandiger is om de procedure te vereenvoudigen en efficiënter te maken door de meldingen eerst aan de nog aan te wijzen nationale markttoezichthouder te doen en vervolgens de Nederlandse nationale cybersecurity incident response teams op de hoogte moeten worden gebracht? Zo ja, is het kabinet bereid om dit voorstel kenbaar te maken in de onderhandelingen? Zo nee, waarom niet?

Antwoord
Het kabinet onderschrijft het doel om een efficiënte en effectieve meldplicht in te richten. Zoals het kabinet in pijler 1 van de NLCS beschrijft, is het tijdig ontvangen van informatie over dreigingen en kwetsbaarheden een van de belangrijkste elementen voor een digitaal weerbaar Nederland. Het kabinet onderschrijft de meerwaarde voor een centraal meldloket van meldingen met betrekking tot cybersecuritykwetsbaarheden en -incidenten. Voor wat betreft een Europees centraal meldpunt beraadt het kabinet zich nog op een positie voor de precieze inrichting van een dergelijk loket, lettende op procedure en rolverdeling tussen belanghebbenden (zoals de markttoezichthouder en het NCSC). Conform het BNC-fiche, heeft het kabinet de Commissie gevraagd, ten aanzien van de taken die ENISA mede op basis van huidige wetgeving thans heeft, om nadere toelichting omtrent de voorgestelde rol en bevoegdheden van ENISA bij bijvoorbeeld de meldplicht voor producenten van geëxploiteerde kwetsbaarheden bij ENISA en het vervolgens door ENISA doorzetten van deze meldingen naar nationale Cybersecurity Incident Response Teams (CSIRTs). Ook beschouwt het kabinet het van belang dat de reactietermijn van ENISA voor deze meldingen wordt gespecificeerd en dat de uitzonderingsgronden voor (het doorsturen van) de meldplicht afbakening behoeft. Ook heeft het kabinet de Commissie, mede gelet op de inrichting van andere meldplichten op het terrein van cybersecurity, om verduidelijking gevraagd over de keuze om in het CRA-voorstel de meldingen bij ENISA te laten plaatsvinden. Onder meer in afwachting van verdere verduidelijking rondom de voorgestelde rol van ENISA en in afwachting van een toekomstige discussie en uitwisseling van standpunten in de ambtelijke werkgroepen van de Raad van EU, beraadt het kabinet zich nog op een verdere positie op de rol van ENISA omtrent de meldplicht.
Ook zal het kabinet verduidelijking vragen over de precieze rol van zowel de Commissie als ENISA, 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»).

VVD 8
Ook willen de leden van de VVD-fractie nader ingaan op de bevoegdheid die de CRA aan de Europese Commissie toekent, namelijk dat zij uitzonderlijke gevallen digitale producten uit de Europese markt kan laten terugtrekken. Deze leden maken zich zorgen over deze bevoegdheid gezien de onzekerheid die zich met zich meebrengt voor ondernemers. In hoeverre worden de risico's die ondernemers lopen door deze bevoegdheid adequaat ondervangen door de CRA? Ziet het kabinet aanvullende mogelijkheden om deze risico's te ondervangen? Zo ja, welke?

Antwoord
Zoals opgenomen in het BNC-fiche, zal het kabinet 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). In de eerste plaats ligt het toezicht bij de markttoezichthouders in de lidstaten. In artikel 45 van het voorstel worden de situaties omschreven waarin de Commissie in het uiterste geval corrigerende of restrictieve maatregelen kan opleggen voor de gehele Unie, waaronder het laten terugroepen of uit de handel nemen van een product met digitale elementen dat niet aan de vereisten voldoet en dat een significant cybersecurityrisico vormt. Deze procedure is met waarborgen omkleed, waardoor de drempel voor de

inzet van deze bevoegdheid hoog ligt. Zo moet het gaan om uitzonderlijke omstandigheden die een onmiddellijke interventie om het goed functioneren van de interne markt te waarborgen rechtvaardigen, en moet de Commissie voldoende redenen hebben om aan te nemen dat het product met digitale elementen blijvend niet aan de vereisten voldoet en dat geen effectieve maatregelen zijn genomen door de relevante markttoezichtautoriteiten. Vervolgens dient de Commissie voordat zij tot een dergelijke maatregel overgaat eerst ENISA een conformiteitstoets laten doen (evaluation of conformity) waar de relevante marktdeelnemers aan mee moeten werken. Op basis van de conformiteitstoets door ENISA kan de Commissie besluiten dat corrigerende of restrictieve maatregelen nodig zijn, door digitale producten terug te laten roepen of uit de handel te laten nemen. Hierover moeten eerst de betrokken lidstaten en de betrokken marktdeelnemers worden geconsulteerd. Bij deze consultatie zullen ook de belangen van ondernemers, zowel de aanbieder van het betreffende product met digitale elementen, als de eindgebruikers ervan, aan de orde komen. Het opleggen van een maatregel door de Commissie gebeurt in de vorm van een uitvoeringshandeling, waarop de onderzoeksprocedure bedoeld in artikel 5 van de Comitologieverordening[2] van toepassing is. De maatregel geldt uitsluitend voor de duur van de uitzonderlijke situatie die de interventie door de Commissie rechtvaardigt en zo lang het product nog niet voldoet aan de gestelde voorschriften.
Artikel 46 voorziet daarnaast ook in de bevoegdheid van de Commissie om dergelijke maatregelen op te leggen als uit de conformiteitstoets van ENISA blijkt dat het product voldoet aan de gestelde voorschriften, maar alsnog een significant cybersecurityrisico vormt. Dit is echter alleen mogelijk indien sprake is van in het eerste lid van artikel 46 genoemde aanvullende (verzwarende) omstandigheden. Het kabinet heeft op dit punt verduidelijking gaat hierover het gesprek aan met de marktpartijen, de Commissie en andere lidstaten om te bezien of deze bevoegdheden passend zijn.

Vragen en opmerkingen van de leden van de Volt-fractie en reactie van de bewindspersoon

De leden van de Volt-fractie hebben met interesse kennisgenomen van het BNC-Fiche met betrekking tot de Verordening Cyber Resilience Act. Daarover zijn deze leden in principe positief gestemd. Zij kunnen zich vinden in een aanzienlijk deel van de posities die het kabinet inneemt. Over de kabinetspositie hebben zij nog wel enkele vragen.

Volt 1
De leden van de Volt-fractie merken op dat een van de voornaamste standpunten die het kabinet inneemt is dat de CRA niet alleen over digitale producten zou moeten gaan maar ook over alle ICT-producten, processen en diensten, ongeacht of zij aan consumenten of bedrijven worden aangeboden. Ziet het kabinet bij de andere lidstaten dezelfde wens? Wat is hier het krachtenveld? Welke inspanningen levert het kabinet om dit doel te bereiken? Kan het kabinet toelichten welke producten onder de reikwijdte van de CRA zouden moeten vallen en welke producten specifiek niet?

Antwoord
Voorafgaand aan het uitkomen van het voorstel heeft het kabinet in een non-paper d.d. 14 december 2021 en een tweede non-paper samen met Duitsland en Denemarken d.d. 12 september 2022, onder andere gepleit

[2] Verordening EU 182/2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren

voor een brede scope, waarbij wij het liefst zouden zien dat de CRA cybersecurityvereisten stelt aan alle ICT-producten, processen en diensten, ongeacht of zij aan consumenten of bedrijven worden aangeboden. Het voorstel zoals het er nu ligt heeft een wat beperktere, maar alsnog ruime scope waarbij de vereisten gelden voor alle producten met digitale elementen, ongeacht of zij aan consumenten of bedrijven worden aangeboden.
Het kabinet dringt er bij de Commissie op aan dat de definities en reikwijdte in de eerste plaats helder zijn. Voor het kabinet is het van belang dat voldoende duidelijk is dat bijvoorbeeld alle hard- en softwareproducten, inclusief alle losse software (met uitzondering van niet-commerciële open source software), binnen de definitie vallen. Ook zal het kabinet verduidelijking vragen hoe de focus op producten met digitale elementen zich verhoudt tot de bredere scope van de Cybersecurity Act die zich richt op ICT-producten, diensten en processen. Ook valt zoals besproken in het antwoord op de vraag VVD 1 Software-as-a Service (SaaS, een vorm van clouddienstverlening) niet onder de voorgestelde CRA, omdat, zo geeft de Commissie aan, aanbieders hiervan onder de NIB2-richtlijn reeds worden gereguleerd als essentiële entiteit. Het kabinet zal verheldering vragen wat het niet meenemen van digitale dienstverlening onder de verordening betekent voor de cybersecurity van deze diensten, of het geen onnodige cyberrisico's oplevert en of er geen lacunes ontstaan. Ook zal het kabinet vragen of de uitzondering voor de betrokken organisaties werkbaar is en voldoende eenduidigheid biedt. Veel lidstaten beraden zich nog op hun positie, mogelijk ontstaat hier iets meer zicht op na de Telecomraad.

Volt 2
De leden van de Volt-fractie merken op dat het kabinet in haar position paper, in samenwerking met Denemarken en Duitsland, schrijft dat zij verheldering wenst te krijgen ten aanzien van de verhouding tussen de CRA en andere (concept)wetgeving op het gebied van cybersecurity. Van welke specifieke vragen en/of onduidelijkheden wenst het kabinet verheldering te krijgen?

Antwoord
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 kabinet acht het van belang dat enerzijds overlap in wetgeving op het gebied van cybersecurity wordt voorkomen en anderzijds goed inzichtelijk wordt gemaakt welke wetgevingslacunes er overblijven, en met welke Europese wetgeving deze gaten kunnen worden gedicht. Een voorbeeld is de eerdergenoemde digitale dienstverlening, die niet onder de voorgestelde CRA valt. Daarentegen vallen digitale diensten wel onder de reikwijdte van vrijwillige Europese cybersecurity certificeringsschema's die worden ontwikkeld onder de Cyber Security Act. In het voorstel worden diverse koppelingen gelegd. Zoals ook beschreven in het antwoord op vraag VVD1, is het voor het kabinet belangrijk dat er geen ongewenste lacunes in Europese wetgeving ontstaan en wil het verduidelijking op de vraag of het buiten het toepassingsbereik van de CRA laten van bijvoorbeeld SaaS geen onnodige cyberrisico's oplevert. Ook valt op dat de meldplicht in de voorgestelde CRA anders wordt ingericht dan de meldplicht in de NIB2-richtlijn, de AI Act en de Cybersecurity Act. Mede gelet daarop heeft het kabinet om nadere verduidelijking van de meldplicht in dit voorstel gevraagd.

Volt 3

De leden van de Volt-fractie hebben ten aanzien van het beoogde toezicht op de CRA en de meldplicht die de concepttekst voorschrijft ook nog enkele vragen. Allereerst merken de leden op dat er een meldplicht komt voor hackincidenten. Daarbij is het niet ondenkbaar dat samenloop ontstaat met de meldplicht voor datalekken in de AVG en de meldplicht voor cyberincidenten in kritieke sectoren onder de NIB2-richtlijn. Het toezicht op de verschillende wet- en regelgeving ligt in Nederland niet bij dezelfde toezichthouder. Dat leidt – zo merkt het kabinet terecht op – tot meer administratieve lasten. Het kabinet gaat de Europese Commissie hierop bevragen. Welke specifieke vragen gaat het kabinet stellen? Voor bedrijven zou het contact met de (Nederlandse) overheid zo simpel mogelijk moeten zijn. Om de meldingsbereidheid te vergroten – en daarmee de risico's van cyberincidenten voor de samenleving te verkleinen – kan het van waarde zijn om het mogelijk te maken om de melding via één loket te doen. Is het kabinet voornemens om het voor bedrijven mogelijk te maken om de verschillende meldingen via één loket te doen? Zo niet, welke andere maatregelen zal zij treffen om de melding zo simpel mogelijk te maken? In aanvulling op het bovenstaande: doordat het toezicht is verdeeld over meerdere toezichthouders, wordt het toezichtslandschap niet overzichtelijker. Deelt het kabinet dit standpunt? Welke inspanningen levert zij om de onoverzichtelijkheid te beperken? Zijn er andere lidstaten in de EU die soortgelijke toezichtsconstructies hebben of lidstaten die het juist anders doen? Wat kan Nederland daarvan leren?

Antwoord
Het kabinet onderschrijft het belang van een efficiënte en effectieve meldplicht, waarbij de verschillende belangen van snelheid, proportionaliteit, uitvoerbaarheid, en het voorkomen van onnodige administratieve lasten moeten worden afgewogen. Daarbij is het van belang om op te merken dat de meldplicht voor de AVG en de CRA anders van aard zijn. De meldplicht van de AVG ziet op het melden van datalekken (inbreuken in verband met persoonsgegevens). De meldplicht zoals voorgesteld in de CRA ziet op kwetsbaarheden in producten met digitale elementen. Het kan voorkomen dat één situatie een melding onder beide wettelijke kaders vereist, maar dat hoeft geenszins het geval te zijn. Het is ook belangrijk dat een goede opvolging wordt gegeven aan de melding: ten aanzien van een datalek is dat het best te beoordelen door de Autoriteit Persoonsgegevens, terwijl bij een melding van geëxploiteerde kwetsbaarheden weer andere expertise (op het terrein van cybersecurity) van belang is. Ten aanzien van de relatie tussen de meldplicht in de CRA en de meldplicht in de NIB2-richtlijn beraadt het kabinet zich nog op haar positie, in afwachting van de antwoorden op verhelderende vragen die hierover aan de Commissie worden gesteld. Met betrekking tot de toekenning van toezichtstaken heeft elke lidstaat de vrijheid om keuzes te maken die het best passen bij de eigen inrichting. Het kabinet hecht eraan dat de toezichthouder geëquipeerd is met de nodige gespecialiseerde kennis om haar taken te kunnen uitoefenen, in dit geval van cybersecurity. Bij Agentschap Telecom (AT) is deze kennis aanwezig, gelet op haar taken in het kader van de Cybersecurity Act, de radioapparatuurrichtlijn, de huidige NIB-richtlijn voor de sectoren energie en digitale infrastructuur, eIDAS en de Telecommunicatiewet. Het toekomstig toezicht op de CRA sluit goed aan bij deze andere taken en marktpartijen zijn reeds bekend met het AT op dit terrein. Daarnaast werkt het AT in haar taakuitoefening werkt nauw samen met andere toezichthouders.

Vragen en opmerkingen van het lid van de BBB-fractie en reactie van de bewindspersoon

BBB 1

Het lid van de BBB-fractie heeft met interesse kennisgenomen van de Cyber Resilience Act. Graag hoort het lid wat de stand van zaken in Nederland is van aan de CRA gerelateerde wetgeving op het gebied van cybersecurity? En op welke wijze is of worden deze Europese wetgeving (-svoorstellen) al dan niet omgezet in Nederlandse wetgeving?

Antwoord
Het voorstel voor de NIB2-richtlijn dat voorziet in maatregelen ter verhoging van de cybersecurity van essentiële en belangrijke entiteiten, is op 10 november j.l. goedgekeurd door het Europees parlement. De NIB2-richtlijn zal gelet op de implementatietermijn van 21 maanden naar verwachting uiterlijk in het najaar van 2024 moeten worden omgezet in Nederlandse wetgeving door middel van aanpassing van de Wet beveiliging netwerk- en informatiesystemen. Daarnaast regelt de Cybersecurity Act de vrijwillige cybersecurity certificering van ICT-producten, diensten en processen. Deze verordening heeft rechtstreekse werking, de uitvoering is in Nederland geregeld in de Uitvoeringswet cyberbeveiligingsverordening. Tot slot is er nog de gedelegeerde verordening 2022/30/EU onder de radioapparatuurrichtlijn waarin vanaf 1 augustus 2024 cybersecurityvereisten worden gesteld aan draadloos verbonden apparaten. Na een overgangsperiode wordt naleving verplicht vanaf 1 augustus 2024. De radioapparatuurrichtlijn is al omgezet in de Telecommunicatiewet en het Besluit radioapparaten 2016, er is geen wijziging nodig voor de gedelegeerde verordening.

BBB 2
Het doel van de CRA is om de toename van cyberaanvallen in de afgelopen jaren een halt toe te roepen. De CRA moet hiermee de digitale samenleving en de grondrechten, zoals privacy en gegevensbescherming, beter beschermen. Het lid van de BBB-fractie hoort graag in hoeverre de CRA regelt dat ook de bestaande slimme apparaten die al bij consumenten thuis of bij bedrijven staan veilig zijn? Overweegt het kabinet een bewustwordingscampagne voor consumenten en bedrijven gericht op onveilige slimme apparaten, inclusief de apparaten die nu al bij consumenten thuis of bij bedrijven staan?

Antwoord
Verwezen wordt naar het antwoord op vraag VVD 4 met betrekking tot het stellen van veiligheidseisen aan bestaande apparaten en het antwoord op vraag VVD 3 met betrekking tot pijler IV van de NLCS en de publiekscampagnes zoals «Doe je updates» en de website veiliginternetten.nl, Daarmee worden consumenten bewust gemaakt en voorgelicht over wat zij zelf kunnen doen om hun digitale weerbaarheid te vergroten. Daarnaast biedt het Digital Trust Center informatie en advies aan bedrijven om hun digitale weerbaarheid te vergroten.

BBB 3
Het lid wil graag weten in hoeverre aanbieders van Europese portemonnees voor digitale identiteit onder de CRA vallen en aan welke eisen moeten zij voldoen.

Antwoord
In overweging 18 van het voorstel wordt ingegaan op de eisen voor aanbieders van Europese portemonnees voor digitale identiteit. Voor zover hun producten vallen onder de CRA moeten deze aanbieders zowel voldoen aan de horizontale essentiële vereisten van de CRA als de specifieke beveiligingsvereisten die de voorgestelde herziening van de eIDAS-verordening (Verordening EU 910/2014) stellen. Aanbieders van dergelijke portemonnees moeten met het certificeren van hun producten

op grond van de Cybersecurity Act (Verordening EU 2019/881) gefaciliteerd worden in het kunnen aantonen dat zij voldoen aan deze vereisten.

BBB 4
Het lid van de BBB-fractie vraagt of met de CRA volgens het kabinet voldoende wordt gestimuleerd dat bedrijven meer zullen investeren in veilig ontwerp en ontwikkeling en het leveren van beveiligingsupdates?

Antwoord
De CRA schrijft veilig ontwerp en het verstrekken van beveiligingsupdates (gedurende 5 jaar of de levensduur van het product) voor als onderdeel van de essentiële beveiligingseisen. Hiermee wordt een enorme stimulans gegeven aan bedrijven om hier in te investeren. Producten met digitale elementen moeten voldoen aan deze eisen om toegang te krijgen tot de Europese interne markt.

BBB 5.
En hoe vindt het kabinet dat de meldplicht verder kan worden afgebakend?

Antwoord
Zoals reeds besproken in het antwoord op vragen VVD 6 en VVD 8 onderschrijft het kabinet het doel om een efficiënte en effectieve meldplicht in te richten. Ook heeft het kabinet hierover verduidelijking gevraagd bij de Commissie en beraadt het kabinet zich nog op een uitgewerktstandpunt hierover.

BBB 6
Het lid van de BBB-fractie wil graag weten wie in Nederland toezicht gaat houden op de CRA? En welke middelen deze toezichthouder heeft voor adequaat toezicht en of dat voldoende is?

Antwoord
Zoals aangegeven in het BNC-fiche is het kabinet voornemens om Agentschap Telecom (AT) als toezichthouder aan te wijzen. AT beschikt over de nodige specialistische kennis op het terrein van cybersecurity gelet op de taken die zij al vervult of zal vervullen met betrekking tot de Cybersecurity Act en de radioapparatuurrichtlijn, de huidige NIB-richtlijn voor de sectoren energie en digitale infrastructuur, eIDAS en de Telecommunicatiewet. Het toekomstig toezicht op de CRA sluit goed aan bij deze andere taken en marktpartijen zijn reeds bekend met AT op dit terrein. Het inrichten van passend toezicht als sluitstuk is nodig om het beoogde positieve maatschappelijke effect te realiseren dat producten digitaal veiliger zijn. De financiële gevolgen van het voorstel voor de rijksoverheid zijn op dit moment nog niet te specificeren, maar ze zijn gelet op de brede reikwijdte van de CRA naar verwachting substantieel. De budgettaire gevolgen voor de Rijksbegroting worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.

BBB 7
Welke lidstaten vinden net als Nederland dat de versterkte rol van de Europese Commissie op het toezicht verduidelijking behoeft?

Antwoord
De veranderende rol van de Europese Commissie wordt nog besproken in de ambtelijke werkgroepen van de Raad van de EU. In deze fase gaat het nog voornamelijk om verkenning en zijn de standpunten veelal nog niet duidelijk. Mogelijk kan na de Telecomraad wat meer zicht worden geboden op de standpunten van andere lidstaten.

BBB 8
Het lid van de BBB-fractie wil graag van het kabinet weten wanneer meer inzicht gegeven kan worden in de financiële gevolgen van de CRA voor de Rijksbegroting en de budgettaire gevolgen voor medeoverheden? En natuurlijk wil het lid ook weten wat de financiële gevolgen voor producenten, importeurs en distributeurs/detailhandel zijn en welke invloed dit gaat hebben op de verkoopprijzen van de producten.

Antwoord
In onderdeel 5 van het BNC-fiche wordt uitgebreid ingegaan op de financiële consequenties voor de rijksoverheid, mede-overheden en marktdeelnemers. Voor mede-overheden verwacht het kabinet geen financiële consequenties. De financiële consequenties van dit voorstel voor de rijksoverheid zien op het inrichten van markttoezicht op nationaal niveau. Deze zijn op dit moment nog niet te specificeren, maar ze zijn gelet op de brede reikwijdte van de CRA naar verwachting substantieel. Het inrichten van passend toezicht als sluitstuk is echter nodig om het beoogde positieve maatschappelijke effect te realiseren dat producten digitaal veiliger zijn.
Het voorstel heeft financiële consequenties en verhoogt de regeldruk voor producenten, importeurs en distributeurs. Dit moet worden afgezet tegen de naar verwachting significante baten voor de verschillende stakeholders en de samenleving als geheel. Het impact assessment van de Commissie maakt de diverse elementen inzichtelijk.
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.
Daar staat tegenover dat de Commissie verwacht 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.