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

F

VERSLAG VAN EEN NADER SCHRIFTELIJK OVERLEG

Vastgesteld 21 juni 2023

De leden van de voorgaande vaste commissie voor Justitie en Veiligheid hebben in hun commissievergadering van 9 mei 2023 beraadslaagd over de brief van de Minister van Economische Zaken en Klimaat van 6 februari 2023[1] over het door de Europese Commissie voorgestelde voorstel voor een Verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020.[2] De leden van de fracties van **GroenLinks**, de **PvdA**, de **SP** en de **PvdD** hebben over de beantwoording nog een aantal vervolgvragen. Ook de leden van de fractie van de **PVV** hebben een aantal nadere vragen.

Naar aanleiding hiervan is op 17 mei 2023 een brief gestuurd aan de Minister van Economische Zaken en Klimaat.

De Minister heeft op 19 juni 2023 gereageerd.

De huidige vaste commissie voor Justitie en Veiligheid[3] brengt bijgaand verslag uit van het gevoerde nader schriftelijk overleg.

De griffier van de vaste commissie voor Justitie en Veiligheid,
Van Dooren

---

1 *Kamerstukken I* 2022/23, 36 239, C.

2 COM(2022)454.

3 Samenstelling:
Croll (BBB), Marquart Scholtz (BBB), Heijnen (BBB), Griffioen (BBB), Veldhoen (GL+PvdA), Recourt (GL+PvdA), Kluit (GL+PvdA), Ramsodit (GL+PvdA), Martens (GL+PvdA), Vogels (VVD), Van den Berg (VVD), Meijer (VVD), Doornhof (CDA), Van Toorenburg (CDA), Dittrich (D66), Belhirch (D66), Bezaan (PVV), Nicolaï (PvdD), Van Bijsterveld (Ja21), Janssen (SP), Talsma (CU), Van den Oetelaar (FVD), Van Dijk (SGP), Hartog (Volt), Van Rooijen (50PLUS), Van der Goot (OPNL).

kst-36239-F
ISSN 0921 - 7371
's-Gravenhage 2023

BRIEF VAN DE VOORMALIGE VOORZITTER VAN DE VASTE COMMISSIE VOOR JUSTITIE EN VEILIGHEID

Aan de Minister van Economische Zaken en Klimaat

Den Haag, 17 mei 2023

De leden van vaste commissie voor Justitie en Veiligheid hebben in hun commissievergadering van 9 mei 2023 beraadslaagd over uw brief van 6 februari 2023[4] over het door de Europese Commissie voorgestelde voorstel voor een Verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020.[5] De leden van de fracties van **GroenLinks**, de **PvdA**, de **SP** en de **PvdD** bedanken u voor de beantwoording van hun vragen. Het stemt hen positief dat de regering hun zorgen deelt. Zij hebben over de beantwoording nog enkele vervolgvragen. Ook de leden van de fractie van de **PVV** hebben enkele nadere vragen.

Vragen en opmerkingen van de leden van de fracties van GroenLinks, PvdA, SP en de PvdD

Vrije en open source software

Het stemt de leden tevens positief dat ook de regering meer duidelijkheid wil in de uitzondering voor vrije en open source software in de CRA. Kunt u concreet aangeven hoe u de tekst verduidelijkt wenst te zien worden en in hoeverre zijn er volgens u al verbeteringen in de tekst gekomen met de nieuwste tekstvoorstellen van de CRA?

De leden vragen ook of, en zo ja, op welke manier er in de CRA een prikkel zou moeten worden ingevoegd voor commerciële fabrikanten van digitale producten om ontwikkelaars van niet-commerciële componenten te ondersteunen in het veilig houden ervan?[6]

Duidelijkheid van de eisen

De leden constateren dat onder deskundigen grote zorgen zijn over de werkbaarheid en duidelijkheid van de eisen van de CRA, zowel voor vrije en open source softwareprojecten als voor commerciële producten. Voormalig TIB-lid Hubert uit vele van deze zorgen en waarschuwt dat een aantal onduidelijke eisen van de CRA in de praktijk onhaalbaar zouden kunnen zijn.[7] Ook uit hij zorgen over de omstandigheid dat de praktische uitwerking van de CRA zeer steunt op een nog niet bestaande algemene standaard. Totdat deze standaard er is, verwacht Hubert dat er veel onduidelijkheid zal zijn en hij betwijfelt ook dat het maken van deze standaard voorspoedig zal verlopen omdat er simpelweg geen vergelijkbare standaarden bestaan. Hoe beoordeelt u deze zorgen en deelt u deze? Zo nee, waarom niet en zo ja, op welke manier heeft u deze meegenomen in de onderhandelingen? Zijn er volgens u verbeteringen gekomen met betrekking tot deze zorgen in de nieuwste voorstellen voor de tekst van de CRA?

---

[4] *Kamerstukken I* 2022/23, 36 239, C.
[5] COM(2022)454.
[6] *Kamerstukken I* 2022/23, 36 239, C, p. 11.
[7] https://berthub.eu/articles/posts/eu-cra-secure-coding-solution/ en https://berthub.eu/articles/posts/eu-cra-practicalities/.

Handhaving

Met betrekking tot de handhaving van de CRA vragen de leden welke rechtsingangen burgers en bedrijven straks concreet zullen hebben om de eisen van de CRA af te dwingen? Welke rol hebben collectieve belangenbehartigers hierin? En voorziet u problemen bij het afdwingen door private partijen van de eisen die de CRA stelt aan producten vanwege de potentieel grote technische complexiteit? Of ziet u andere belemmeringen zoals bedrijfsgeheimen en kopieerbeveiliging (digital rights management) die eindgebruikers beperken in hun mogelijkheden om aan te tonen dat de een product niet voldoet aan de eisen van de CRA? Zo ja, wat zal u doen om eindgebruikers te helpen hun rechten onder de CRA te realiseren?

Levensduur

U hebt aangegeven dat u bij de onderhandelingen zal pleiten voor een verplichte ondersteuningstermijn de aansluit op de verwachte productlevensduur. Op welke wijze gaat u dit doen? Zijn er andere landen die dit steunen? En wat zal uw reactie zijn indien die verplichte ondersteuningstermijn uitblijft? Welke financiële gevolgen heeft een verlenging van de ondersteuningstermijn?

Vragen en opmerkingen van de leden van de fractie van de PVV

Kan er misschien al een inschatting worden gegeven van de omvang die de mogelijke financiële steun vanuit de EU en/of het Rijk gaat hebben voor kleine en middelgrote ondernemingen, door wie deze steun wordt betaald, alsmede of deze steun moet worden terugbetaald en of er onderzocht is of eventuele voorwaarden waar kleine en middelgrote ondernemingen aan moeten voldoen inzake mogelijke steun op welke manier dan ook nadelig kunnen uitpakken voor de bedrijfsvoering? Graag ontvangen de leden een gemotiveerd antwoord.

De leden van de vaste commissie voor Justitie en Veiligheid zien uw reactie – bij voorkeur binnen vier weken – met belangstelling tegemoet.

De voorzitter van de vaste commissie voor Justitie en Veiligheid,
M.M. de Boer

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 19 juni 2023

Hierbij zend ik u de beantwoording van de bij brief d.d. 17 mei 2023 gestelde vragen van de leden van de fracties van GroenLinks, de PvdA, de SP en de PvdD gezamenlijk en de leden van de fractie van de PVV over het voorstel voor een Verordening betreffende horizontale cyberbeveiligingsvereisten.

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens

Vragen en opmerkingen van de leden van de fracties van GroenLinks, PvdA, SP en de PvdD

Vrije en open source software

Het stemt de leden tevens positief dat ook de regering meer duidelijkheid wil in de uitzondering voor vrije en open source software in de CRA. Kunt u concreet aangeven hoe u de tekst verduidelijkt wenst te zien worden en in hoeverre zijn er volgens u al verbeteringen in de tekst gekomen met de nieuwste tekstvoorstellen van de CRA?

Antwoord
Het voorstel wordt momenteel besproken in de Raadswerkgroep *Horizontal Working Party on Cyber Issues* onder Zweeds voorzitterschap. Het voorzitterschap heeft de afgelopen maanden diverse compromisvoorstellen gedaan die in de Raadswerkgroep zijn besproken. Op basis van de onderhandelingen en compromistekstvoorstellen die het voorzitterschap heeft gedaan, kan ik met u delen dat in een van de overwegingen nu een duidelijkere uitleg wordt geven van de omstandigheden die maken dat open source software al dan niet onder de CRA valt. De CRA bevat uitsluitend voorschriften voor producten met digitale elementen, waaronder software, die «op de markt wordt aangeboden» in de Europese Unie. De definitie van «op de markt aanbieden» bepaalt dat hiervan alleen sprake is als het product wordt verstrekt in het kader van een handelsactiviteit (in het Engels: *supplied in the course of a commercial activity*). De overweging geeft nu duidelijker weer dat hieruit voortvloeit dat degene die open source software op niet-commerciële wijze aanbiedt, om die reden niet onder de verplichtingen van de CRA valt. Ook is verduidelijkt wat maakt of een product commercieel wordt aangeboden. Daarvoor is uitsluitend van belang onder welke voorwaarden het product wordt aangeboden: als er voor moet worden betaald (in geld of door verstrekken van persoonsgegevens) of een technisch ondersteuningscontract voor wordt afgesloten waar meer voor in rekening wordt gebracht dan het dekken van de daadwerkelijke kosten of met een winstoogmerk is het op «in het kader van een handelsactiviteit verstrekt» en dus «op de markt is aangeboden». Wat nu ook duidelijk wordt gemaakt, is dat de omstandigheden waaronder het product ontwikkeld is, of hoe de ontwikkeling is gefinancierd, niet van belang zijn bij het bepalen of een product «op de markt is aangeboden» en dus aan de regels van de CRA moet voldoen. Ook gaat de overweging inmiddels in op de rol van online platforms waarop open source software wordt ontwikkeld, onderhouden en gedistribueerd. Deze platforms worden alleen als «distributeur» met bijbehorende verplichtingen onder de CRA gezien als zij de software «in het kader van een handelsactiviteit verstrekken» en aldus «op de markt aanbieden». Hiermee worden de ons bekende zorgen over onduidelijkheid met betrekking tot open source software, die uit gesprekken met stakeholders uit deze gemeenschap naar voren kwamen, uitgebreid geadresseerd. Mijn beeld is dat op dit punt voldoende verbetering worden doorgevoerd in het compromisvoorstel.

De leden vragen ook of, en zo ja, op welke manier er in de CRA een prikkel zou moeten worden ingevoegd voor commerciële fabrikanten van digitale producten om ontwikkelaars van niet-commerciële componenten te ondersteunen in het veilig houden ervan?[8]

Antwoord
Fabrikanten die een product op de markt aanbieden waarin zij componenten van derden gebruiken, zijn verantwoordelijk voor de conformiteit

[8] *Kamerstuk* 36 239, C, p. 11.

van het hele product met de cybersecurityeisen van de CRA op het moment dat het product in de handel wordt gebracht, maar ook voor het veilig houden ervan gedurende de verwachte productlevensduur. In het compromisvoorstel wordt duidelijker bepaald dat de fabrikant verantwoordelijk is voor het oplossen van kwetsbaarheden (vertrekken van veiligheidsupdates) in het product, inclusief de componenten. Indien dit een component is die commercieel in de handel is gebracht, valt de fabrikant van die component zelf onder de CRA en heeft de componentfabrikant dus ook een zelfstandige verplichting om de kwetsbaarheid aan te pakken en een veiligheidsupdate te verstrekken. Indien dit een niet-commerciële component is, is dat niet het geval en is het dus aan de fabrikant van het commerciële product om dit op te lossen. Dit kan een prikkel geven om de ontwikkelaar of beheerder van de niet-commerciële component te ondersteunen bij het ontwikkelen van een update die de kwetsbaarheid verhelpt. De fabrikant is daarnaast verplicht degene die de component onderhoudt op de hoogte te stellen zodra hij een kwetsbaarheid in de component identificeert. Als de fabrikant een veiligheidsupdate heeft ontwikkeld voor de component is deze volgens het compromisvoorstel bovendien verplicht de relevante code te delen met degene die de component beheert. Het kabinet zet zich in voor behoud van deze voorlopige onderhandelingsresultaten in de uiteindelijke tekst van de CRA.

Duidelijkheid van de eisen

De leden constateren dat onder deskundigen grote zorgen zijn over de werkbaarheid en duidelijkheid van de eisen van de CRA, zowel voor vrije en open source softwareprojecten als voor commerciële producten. Voormalig TIB-lid Hubert uit vele van deze zorgen en waarschuwt dat een aantal onduidelijke eisen van de CRA in de praktijk onhaalbaar zouden kunnen zijn.[9] Ook uit hij zorgen over de omstandigheid dat de praktische uitwerking van de CRA zeer steunt op een nog niet bestaande algemene standaard. Totdat deze standaard er is, verwacht Hubert dat er veel onduidelijkheid zal zijn en hij betwijfelt ook dat het maken van deze standaard voorspoedig zal verlopen omdat er simpelweg geen vergelijkbare standaarden bestaan. Hoe beoordeelt u deze zorgen en deelt u deze? Zo nee, waarom niet en zo ja, op welke manier heeft u deze meegenomen in de onderhandelingen? Zijn er volgens u verbeteringen gekomen met betrekking tot deze zorgen in de nieuwste voorstellen voor de tekst van de CRA?

Antwoord
Deze zorgen zijn mij bekend en ik neem deze signalen serieus. De CRA, als horizontale verordening, schrijft voor een zeer brede reikwijdte aan producten met digitale elementen voor dat deze digitaal veilig moet zijn. Hier vallen zowel consumentenproducten als industriële systemen onder, zowel hardware als standalone software, en producten met uiteenlopende niveaus van cybersecurityrisico's. Ik ben van mening dat het voor deze brede toepasbaarheid en voor de toekomstbestendigheid van de cybersecurityeisen in de CRA goed is dat deze open en techniekneutraal zijn geformuleerd in bijlage I van het voorstel, om ze vervolgens door Europese standaardiseringsorganisaties te laten uitwerken in praktisch toepasbare technische normen. Deze kunnen worden toegespitst op diverse productcategorieën. Na goedkeuring van een technische norm door de Europese Commissie, zal deze als geharmoniseerde standaard worden vastgesteld. De beoordeling of een product aan de eisen van de CRA voldoet zal dus in de praktijk kunnen worden gedaan aan de hand

[9] https://berthub.eu/articles/posts/eu-cra-secure-coding-solution/ en https://berthub.eu/articles/posts/eu-cra-practicalities/.

van deze geharmoniseerde standaarden, die veel concreter en duidelijker zullen zijn in wat er precies van de fabrikant wordt verlangd. Met dit stelsel en het bijbehorende proces van het opstellen van standaarden is al jarenlange ervaring ten aanzien van de Europese productveiligheidseisen (ten aanzien van de fysieke veiligheid) waaraan producten moeten voldoen om in de Europese Unie op de markt te worden gebracht. Cybersecurityeisen zijn daarin een relatief nieuw terrein waarmee momenteel ervaring wordt opgedaan in de uitwerking van de cybersecurityeisen in de gedelegeerde handeling onder de *Radio Equipment Directive* (Richtlijn 2014/53/EU). Voor een goede werking van de CRA is het belangrijk dat op het moment van inwerkingtreding veruit de meeste fabrikanten zelf, zonder inschakeling van een derde partij, kunnen beoordelen of hun product aan de CRA voldoet en dat daarvoor tijdig een geharmoniseerde standaard beschikbaar moet zijn. Het kabinet heeft daarom gepleit voor een realistische implementatietermijn die voldoende tijd biedt voor het ontwikkelen van geharmoniseerde standaarden en het implementeren daarvan door fabrikanten. Op basis van gesprekken met experts die betrokken zijn bij de ontwikkeling van deze normen door Europese standaardiseringsorganisaties is mijn inschatting dat de implementatieperiode van 24 maanden die de Europese Commissie in haar voorstel had voorzien erg kort is. Daarom pleit ik in de Raad voor een langere termijn van 36 maanden. De implementatieperiode is op dit moment nog onderwerp van de Europese onderhandelingen in de Raadswerkgroep om te komen tot een gemeenschappelijk standpunt, maar er lijkt voldoende steun voor deze langere termijn.

Handhaving

Met betrekking tot de handhaving van de CRA vragen de leden welke rechtsingangen burgers en bedrijven straks concreet zullen hebben om de eisen van de CRA af te dwingen? Welke rol hebben collectieve belangenbehartigers hierin? En voorziet u problemen bij het afdwingen door private partijen van de eisen die de CRA stelt aan producten vanwege de potentieel grote technische complexiteit? Of ziet u andere belemmeringen zoals bedrijfsgeheimen en kopieerbeveiliging (digital rights management) die eindgebruikers beperken in hun mogelijkheden om aan te tonen dat de een product niet voldoet aan de eisen van de CRA? Zo ja, wat zal u doen om eindgebruikers te helpen hun rechten onder de CRA te realiseren?

Antwoord
Burgers en bedrijven zullen als consument of zakelijke gebruiker van producten met digitale elementen kunnen rekenen op een stelsel van Europese cybersecurityeisen waar elke digitaal product aan moet voldoen om in de EU in de handel te mogen worden gebracht. De fabrikant (of de importeur bij producten van buiten de EU) zal met een CE-markering op het product moeten weergeven dat het product aan de CRA-eisen voldoet. Daarnaast zal verplichte informatie moeten worden meegeleverd aan de gebruiker over de naam en contactgegevens van de fabrikant, het contactpunt voor melden en ontvangen van informatie over cybersecuritykwetsbaarheden van het product, voor welk gebruik het product bedoeld is en informatie over de beveiligingseigenschappen, welke technische beveiligingsondersteuning de fabrikant biedt, wat de verwachte productlevensduur is (inclusief een duidelijke einddatum) waarin kwetsbaarheden zullen worden verholpen met veiligheidsupdates en – als de fabrikant daarvoor kiest – de *software bill of materials*. Markttoezichthouders zien toe op de naleving van al deze regels, in Nederland zal dit de Rijksinspectie voor Digitale Infrastructuur (RDI) zijn.

Ik verwacht daarmee ook een veel sterkere positie voor gebruikers om bij de fabrikant of distributeur af te dwingen dat het product voldoet, of dat veiligheidsupdates worden verstrekt in geval van kwetsbaarheden. Waar dit niet het geval is kan een melding bij RDI worden gedaan en in het geval van schade kan de gebruiker de fabrikant aansprakelijk stellen. De regels van de CRA bieden dan, veel meer dan in de huidige situatie, een duidelijk toetsingskader voor de rechter om te beoordelen of de fabrikant voldoende cybersecuritymaatregelen heeft genomen, dan wel aansprakelijk is voor de geleden schade. De CRA zal volgens het compromisvoorstel bovendien representatieve vorderingen ter bescherming van de collectieve belangen van consumenten mogelijk maken waar schending van de CRA de collectieve belangen van consumenten (kunnen) schaden.

Levensduur

U hebt aangegeven dat u bij de onderhandelingen zal pleiten voor een verplichte ondersteuningstermijn die aansluit op de verwachte productlevensduur. Op welke wijze gaat u dit doen? Zijn er andere landen die dit steunen? En wat zal uw reactie zijn indien die verplichte ondersteuningstermijn uitblijft? Welke financiële gevolgen heeft een verlenging van de ondersteuningstermijn?

Antwoord
Nederland heeft een non-paper opgesteld, dat is medeondertekend door Denemarken, België, Oostenrijk, Italië, Finland en Spanje,[10] waarin wij pleiten voor een verplichte ondersteuningstermijn die aansluit op de redelijkerwijs verwachte productlevensduur. Dit heeft geleid tot de gewenste aanpassingen in het compromisvoorstel, die een meerderheid in de Raad lijkt te steunen. Ook heeft het non-paper de rapporteur van het Europees Parlement geïnspireerd om in het conceptrapport dezelfde aanpassingen van de ondersteuningstermijn voor te stellen. Ik vertrouw er daarmee op dat deze verplichte ondersteuningstermijn in de uiteindelijke wettekst terecht zal komen.

De financiële gevolgen van een langere ondersteuningstermijn zijn enerzijds gelegen in de hogere kosten voor de fabrikant om voor veiligheidsupdates te zorgen wanneer er een kwetsbaarheid in het product wordt geconstateerd. Daar staat tegenover dat consumenten én zakelijke gebruikers van deze producten minder schade als gevolg van veiligheidsissues zullen ondervinden dan als hun product na vijf jaar niet langer ondersteund is met veiligheidsupdates en nog wel wordt gebruikt, dan wel dat zij hun product na vijf jaar moeten vervangen door een nieuw product dat veilig kan worden gebruikt. Deze noodzaak producten eerder dan de werkelijke levensduur te moeten vervangen om op een goede cybersecurity te kunnen rekenen zou bovendien ongewenste gevolgen veroorzaken met het oog op duurzaamheid.

Vragen en opmerkingen van de leden van de fractie van de PVV

Kan er misschien al een inschatting worden gegeven van de omvang die de mogelijke financiële steun vanuit de EU en/of het Rijk gaat hebben voor kleine en middelgrote ondernemingen, door wie deze steun wordt betaald, alsmede of deze steun moet worden terugbetaald en of er onderzocht is of eventuele voorwaarden waar kleine en middelgrote ondernemingen aan moeten voldoen inzake mogelijke steun op welke manier dan ook nadelig kunnen uitpakken voor de bedrijfsvoering? Graag ontvangen de leden een gemotiveerd antwoord.

[10] *Nonpaper on a support period covering the entire expected product lifetime in the Cyber Resilience Act*, 30 maart 2023, Kenmerk 2023D13133.

Antwoord
Ik deel uw gevoel over de noodzaak om te kijken hoe we mkb-fabrikanten, en met name micro- en kleinbedrijven, kunnen ondersteunen bij de implementatie van de CRA. Onder het subsidieprogramma *Digital Europe* zal hiervoor geld beschikbaar worden gemaakt. Met dit geld kunnen bijvoorbeeld mkb-fabrikanten worden begeleid in het doorlopen van de conformiteitsbeoordelingsprocedure (veelal zelfverklaring). In het geval mkb-fabrikanten een derde partij de beoordeling laten doen, schrijft de CRA voor dat conformiteitsbeoordelende instanties bij hun tariefstelling rekening houden met het feit dat zij mkb zijn. Ook wordt besproken of de vereiste documentatie in geval van mkb-fabrikanten in vereenvoudigde vorm kan worden opgeleverd.

Hoeveel geld er vanuit Digital Europe beschikbaar gesteld kan worden voor ondersteuning van het mkb en onder welke voorwaarden, moet nog nader worden vastgesteld. Hierover gaat het kabinet nog nader in gesprek met de Europese Commissie.