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

G

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 14 juli 2023

Op 19 juli 2023 ligt er in het Comité van Permanente Vertegenwoordigers (Coreper) van de lidstaten van de Europese Unie een compromistekst op de Cyber Resilience Act[1] (CRA) voor. Hierbij informeer ik uw Kamer[2] over het voornemen om namens Nederland in te stemmen met deze compromistekst, en daarmee het Raadsvoorzitterschap mandaat te geven om met deze tekst te onderhandelen met het Europees Parlement. Het Europees Parlement heeft nog geen formele positie ingenomen.

De Nederlandse Cybersecuritystrategie (NLCS) beschrijft het Nederlandse beleid ten aanzien van cybersecurity. In pijler 2 van de NLCS is het beleid ten aanzien van digitaal veilige producten en diensten omschreven. Om digitale producten veiliger te maken is Europese wetgeving nodig waarin eisen worden gesteld ten aanzien van de cybersecurity van digitale producten waarin de verantwoordelijkheid voor de cybersecurity wordt neergelegd bij de fabrikant.
Nederland is dan ook een groot voorstander van horizontale wetgeving die de cybersecurity van producten regelt. In aanloop naar de publicatie van het Commissievoorstel voor de CRA heeft Nederland haar ideeën hierover kenbaar gemaakt en ook met de Commissie gedeeld in twee non-papers (waarvan één met Duitsland en Denemarken).[3] In september 2022 heeft de Europese Commissie het voorstel voor de CRA gepubliceerd. Het BNC-fiche hierover is in oktober 2022 naar de Kamer gestuurd.[4]

[1] Voorstel van de Europese Commissie voor een Verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020.
[2] Een gelijkluidende brief heb ik verstuurd aan de Eerste Kamer.
[3] Kamerstuk 22 112, nr. 3523.
[4] Kamerstuk 22 112, nr. 3552.

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

Ik heb uw Kamer in de brief d.d. 26 mei 2023, over de geannoteerde agenda voor de formele Telecomraad van 2 juni 2023, geïnformeerd over de vijf belangrijkste punten voor Nederland bij de onderhandelingen in de Raad. Op deze vijf punten zijn op werkgroepniveau belangrijke resultaten geboekt en goede compromissen gesloten. Ook de bredere linie van de compromistekst die in Coreper voorligt, sluit goed aan bij de wensen van Nederland. Voor Nederland is deze tekst een verdere verbetering ten opzichte van het oorspronkelijke voorstel van de Commissie en biedt een goede basis voor de onderhandelingen met het Europees Parlement. Ik zal de compromistekst zodra deze openbaar is naar uw Kamer verzenden. In de tussentijd verwijs ik u naar Delegates Portal, waar deze tekst ter inzage beschikbaar is.

De CRA vereist dat digitale producten (alle hardware, software en losse componenten) aan essentiële cybersecurityeisen voldoen voordat zij in de EU in de handel mogen worden gebracht, dit geldt ook voor producten die van buiten de EU worden geïmporteerd. Ook moeten fabrikanten zorgen voor gratis veiligheidsupdates wanneer er nadien kwetsbaarheden worden geconstateerd, en geëxploiteerde kwetsbaarheden en incidenten melden. Met de CRA zullen Europese gebruikers, zowel consumenten als zakelijke gebruikers, er in de toekomst op kunnen rekenen dat de hard- en software die zij gebruiken veilig is.

De vijf belangrijkste punten voor Nederland betreffen:

1. Een **ondersteuningstermijn** waarin de fabrikant verantwoordelijk blijft voor het effectief reageren op kwetsbaarheden (door het aanbieden van gratis veiligheidsupdates) die geldt voor de redelijk te verwachten levensduur van het product, in plaats van de door de Europese Commissie voorgestelde maximumtermijn van vijf jaar.
2. Een duidelijke regeling voor de toepassing op **Open Source-software**: niet-commercieel aangeboden software valt buiten de Cyber Resilience Act zolang deze niet in de handel wordt gebracht; de fabrikant die deze software in een commercieel product gebruikt is degene die met dat product aan de CRA moet voldoen.
3. Een voor zowel Computer Security Incident Response Teams (CSIRT's) als fabrikanten goed uitvoerbare **meldplicht** bij (geëxploiteerde) kwetsbaarheden en incidenten, met een effectieve en veilige meldstructuur.
4. Het **uitgangspunt is dat fabrikanten zelf de conformiteit beoordelen** van hun product aan de eisen van de CRA, waarbij voor meer gevoelige producten (opgesomd in een bijlage van de CRA) wordt voorgeschreven dat de **conformiteitsbeoordeling door een onafhankelijke derde partij** moet worden uitgevoerd.
5. Een **redelijke implementatietermijn**, waarbij voldoende tijd is voor de ontwikkeling en implementatie van de technische normen aan de hand waarvan fabrikanten de conformiteit met de essentiële cybersecurityvereisten van de CRA kunnen beoordelen.

Daarnaast heeft Nederland zich ingezet voor ondersteuning van met name kleine en microbedrijven bij het voldoen aan de eisen van de CRA. Dit heeft geleid tot diverse ondersteunende maatregelen in de overwegingen en artikelen voor deze doelgroep.

Concluderend ligt er een ambitieuze en werkbare tekst voor in Coreper, waar Nederland op 19 juli mee kan instemmen. Na aanname van het voorlopig akkoord in Coreper kan het Spaans Voorzitterschap zich deze zomer voorbereiden op de aanvang van de triloogfase over de CRA. Het Europees Parlement zal nog een definitieve positie moeten innemen, de

plenaire stemming zal naar verwachting in september plaatsvinden. In comitéverband is er in het Europees Parlement al over gesproken en zijn er compromisamendementen overeengekomen.

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