Ministerie van Economische Zaken
en Klimaat

Directoraat-generaal
Economie en Digitalisering
Directie Digitale Economie

Auteur
[redacted]

Aan de Minister van Economische Zaken en Klimaat

TER BESLISSING
Datum
11 juli 2023

Kenmerk
DGED-DE / 33731250

nota

Instemmen compromistekst CRA in Coreper I

Kopie aan

Bijlage(n)
-

Parafenroute

[redacted]

Aanleiding

- Op 19 juli aanstaande ligt de compromistekst voor een algemene oriëntatie van de Raad op de Cyber Resilience Act voor in Coreper I. Hiertoe is besloten nadat het Spaanse voorzitterschap in de raadswerkgroep van 10 juli aangaf voldoende basis te zien voor overeenstemming.
- Een laatste versie van de compromistekst is vandaag in een stilteprocedure aan de lidstaten voorgelegd. Dat houdt in dat die tot donderdagmiddag 13 juli bezwaar kunnen maken tegen de inhoud van het compromis en de agendering in Coreper op 19 juli.
- Om namens Nederland in te kunnen stemmen met de compromistekst is uw voorafgaande akkoord nodig.
- Als het Coreper instemt met de compromistekst verkrijgt het Spaans Voorzitterschap daarmee het mandaat om met deze tekst de onderhandelingen met het Europees Parlement in te gaan.

Geadviseerd besluit

- U wordt geadviseerd akkoord te geven op het voorstel om namens Nederland in te stemmen met de compromistekst.
- U wordt geadviseerd bijgaande brieven aan de Eerste en Tweede Kamer te ondertekenen waarmee de Kamers over dit voornemen worden geïnformeerd voorafgaand aan de bespreking hiervan in Coreper op 19 juli aanstaande. *Deze brieven worden op vrijdag 14 juli uitgestuurd, tenzij er in de stilteprocedure opmerkingen zijn gemaakt die ertoe leiden dat de compromistekst niet op 19 juli in Coreper wordt besproken*.

Directoraat-generaal
Economie en Digitalisering
Directie Digitale Economie

Kenmerk
DGED-DE / 33731250

Kernpunten

Inhoud CRA

- EZK heeft zich, in samenwerking met JenV, actief ingezet voor de totstandkoming en verdere aanscherping van de voorgestelde verordening. Met de Cyber Resilience Act (CRA) wordt een grote bijdrage geleverd aan de doelstelling om digitale producten veiliger te maken (zoals opgenomen in de Nederlandse Cybersecurity Strategie en in de Strategie Digitale Economie). Hiervoor is Europese wetgeving nodig.
- De Cyber Resilience Act 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 Cyber Resilience Act 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.

Proces

- Onder voorbehoud dat geen van de lidstaten bezwaar maakt tegen het compromisvoorstel of agendering daarvan in Coreper I, is de verwachting dat de meerderheid op 19 juli in zal stemmen met de compromistekst als voorlopig akkoord.
- Na aanname van het voorlopig akkoord in Coreper kan het Spaans Voorzitterschap zich deze zomer voorbereiden op de aanvang van de triloogfase over de Cyber Resilience Act.
- Het Europees Parlement moet nog een definitieve positie 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.

Onderhandelingsresultaten

In de brief over de geannoteerde agende voor de formele Telecomraad van 2 juni 2023 heeft u de Tweede Kamer geïnformeerd over de vijf belangrijkste punten voor het kabinet bij de onderhandelingen in de Raad. Op deze vijf punten zijn belangrijke resultaten geboekt, en ook over de bredere linie zijn we heel tevreden over de compromistekst.

De vijf belangrijkste punten 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.

Directoraat-generaal
Economie en Digitalisering
Directie Digitale Economie

Kenmerk
DGED-DE / 33731250

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 EZK 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.