Ministerie van Economische Zaken en Klimaat

Aan de Minister van Economische Zaken en Klimaat

[redacted]

Directoraat-generaal Economie en Digitalisering
Directie Digitale Economie

Auteur
[redacted]

TER BESLISSING
Datum
6 oktober 2022

Kenmerk
DGED-DE / 22511573

Bhm: 22511798

Kopie aan
[redacted]

Bijlage(n)
3

nota

BNC-fiche Cyber Resilience Act

Parafenroute

[redacted]

Aanleiding

Op 15 september jl. 2022 publiceerde de Europese Commissie (EC) het voorstel voor de Cyber Resilience Act (CRA). EZK heeft als eerstverantwoordelijk departement het BNC-fiche geschreven in nauwe samenwerking met JenV en andere departementen dat behandeld zal worden in het interdepartementale BNC-overleg, vervolgens in de CoCo en uiteindelijk na de Ministerraad van 21 oktober a.s. aan de Kamer zal worden gestuurd. Daarnaast worden separaat (1) het Nederlands non-paper over de CRA mede ondertekend door Denemarken en Duitsland en (2) het Nederlandse position paper over de regulatory sandboxes in de Artificial Intelligence Act aan de Kamer gestuurd. Beide stukken zijn door u in een eerder stadium geaccordeerd.

Geadviseerd besluit

- U kunt akkoord gaan met het bijgevoegde BNC-fiche over de Cyber Resilience Act.
- U kunt de aanbiedingsbrief ondertekenen voor het versturen naar de Tweede Kamer van het Nederlandse non-paper over de Cyber Resilience Act en het position paper over regulatory sandboxes in de Artificial Intelligence Act.

[redacted]

Kernpunten

- De tweeledige hoofddoelstelling van de CRA is (1) het creëren van horizontale robuuste cybersecurity voorwaarden voor alle producten met digitale elementen en voorwaarden waar fabrikanten, leveranciers en importeurs van dergelijke producten aan moeten voldoen voor plaatsing op de interne markt en tijdens de productlevenscyclus (2) het zorgen voor transparantie richting gebruikers (consumenten en organisaties) over de mate van cybersecurity van dergelijke producten.
- Dit moet leiden tot een digitaal veiligere Europese digitale interne markt en samenleving waar op termijn 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.
- In het fiche verwelkomt het kabinet het voorstel. Over het algemeen is de eerste indruk van het kabinet over het voorstel positief en in lijn met het Nederlandse non-paper[1] en consultatiereactie[2] op dit voorstel die de Kamer op 14 december 2021 en op 17 augustus jl. heeft ontvangen.
- De CRA volgt de bestaande Europese systematiek van productregulering voor markttoegang met bijbehorende standaarden en markttoezicht.
- In samenspel met (sectorale) Europese wet- en regelgeving kan de CRA een horizontaal vangnet vormen met essentiële cybersecurityeisen die voor alle producten met digitale elementen gelden, waarbij sectorale wetgeving als *lex specialis* additionele voorwaarden kan stellen voor specifieke producten en diensten.
- Tegelijkertijd zijn er nog de nodige zaken die verduidelijking behoeven, zoals het samenspel met andere Europese wet- en regelgeving, definities, reikwijdte en voorgenomen bevoegdheden van de EC en ENISA, het Europees agentschap voor cybersecurity.
- De eerste indruk bij stakeholders is over het algemeen positief. Zij hebben vergelijkbare vragen als het kabinet op de reikwijdte en samenloop met andere Europese wet- en regelgeving. Daarnaast zien mondiale bedrijven graag aansluiting op internationale standaarden.

Toelichting

- Het oordeel op de subsidiariteit is positief. Cybersecurity is een grensoverschrijdend vraagstuk, het toenemend aantal incidenten beperkt zich niet tot landsgrenzen en er zijn veelal internationale marktpartijen actief. Horizontale cybersecurity markttoegangseisen bevorderen het gelijke speelveld en versterken de digitale weerbaarheid van de samenleving en economie voor consumenten en bedrijven.
- Het oordeel op de proportionaliteit is positief. 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.

Reikwijdte: producten met digitale elementen

- 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 is inclusief losse software. De exacte reikwijdte van het begrip producten met digitale elementen en de daarop gemaakte uitzonderingen is echter nog niet volledig duidelijk. Gelet op de verhouding met andere EU wet- en regelgeving is dit een aandachtspunt.

---

[1] Kamerstuk 2021D49776
[2] Kamerstuk 2022D32607

Verplichtingen aan fabrikanten, leveranciers en importeurs

- Fabrikanten en importeurs moeten 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.
- Fabrikanten kunnen op basis van geharmoniseerde standaarden een zelfassessment uitvoeren voor de conformiteitsbeoordeling. Daarnaast zijn in Annex III twee categorieën kritieke producten met digitale elementen opgenomen met een hoger cybersecurity risico. Hiervoor worden zwaardere eisen gesteld aan de conformiteitsbeoordelingsprocedure. In de hoogste categorie moet de conformiteitsbeoordeling worden uitgevoerd door een onafhankelijke derde partij.
- Voor de ex-post verplichtingen geldt dat de fabrikant voor de verwachte levensduur van het product of voor 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 (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 doorzetten naar de nationale cybersecurityorganisaties en de nationale markttoezichtautoriteit op de hoogte stellen.
- In het fiche is opgenomen dat verduidelijkingen nodig zijn op de werking van de meldplicht van fabrikanten in relatie tot de meldplicht in NIB2 en met betrekking tot de rol van ENISA ten opzichte van nationale cybersecurity organisaties, zoals het Nationaal Cyber Security Centrum en het Cybersecurity Incident Response Team voor digitale dienstverleners (CSIRT-DSP).
- Daarnaast is verduidelijking nodig over de termijn van verplichte ondersteuning van kwetsbaarheden. Voldoende cybersecurity waarborgen gedurende de productlevenscyclus is voor het kabinet van belang.

Samenspel met andere Europese wet- en regelgeving

- De precieze relatie met betrekking tot andere Europese wet- en regelgeving (of voorstellen in onderhandeling) met het oog op samenhang en toepassing in de praktijk zijn zaken waarop Nederland verduidelijking zal vragen. Hierbij gaat het onder meer om relatie met de herziene richtlijn voor Netwerk- en Informatiebeveiliging (NIB2), de Cyber Security Act (certificering van ICT-producten, diensten en processen), de eIDAS-verordening, AI act en de richtlijnen verkoop goederen en digitale inhoud.

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.

Nederlands position paper over de regulatory sandboxes in de Artificial Intelligence Act

- Een belangrijk punt van Nederland voor de AI Act is sterkere harmonisatie van AI regulatory sandboxes. Regulatory sandboxes zijn testomgevingen waar ontwikkelaars in samenwerking met toezichthouders kunnen onderzoeken hoe hun innovatieve producten het beste aan de AI Act kunnen voldoen. Het position paper beargumenteert dat opgedane kennis tijdens de sandbox duidelijk wordt vastgelegd via een deelnameplan en een eindrapport achteraf. Deze kennis moet vervolgens door de Europese Commissie, AI Board en Europese standaardisatieorganisaties worden gebruikt voor: (i) verbetering van toezicht, (ii) aanpassing van de AI Act waar nodig en (iii) handvatten voor de Al-markt zoals guidance. In het paper noemen we dit regulatory learning. Zo zorgen we ervoor dat de gehele Al-markt profiteert van ervaringen in de sandboxes.