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
28 maart 2024

Kenmerk
DGED-DE / 52351205

Kopie aan

Bijlage(n)
2

nota

Beslisnota bij Kamerbrief beleidsreactie
onderzoek contractuele afspraken cybersecurity

Parafenroute

[redacted]

Aanleiding

Naar aanleiding van de kabinetsreactie op het rapport van de Onderzoeksraad voor Veiligheid (OVV) "Kwetsbaar door software - Lessen naar aanleiding van beveiligingslekken door software van Citrix" heeft PwC in opdracht van EZK een onderzoek uitgevoerd naar contractuele afspraken cybersecurity in business-to-bussinessrelaties (b2b). Dit rapport zal met bijgevoegde beleidsreactie aan de Kamer worden gezonden.

Geadviseerd besluit

U kunt de brief ondertekenen, waarin wordt gesteld dat er geen aanvullende initiatieven vanuit het kabinet nodig zijn om de adviezen van het PwC-onderzoek over de cybersecurityeisen in b2b-contracten te adresseren. Er valt nog wel winst te behalen in het verder onder de aandacht brengen van deze initiatieven bij bedrijven.

Kernpunten

- Een van de aanbevelingen uit het OVV-rapport is om te bevorderen dat Nederlandse organisaties en consumenten gezamenlijk veiligheidseisen formuleren en afdwingen bij softwarefabrikanten.
- Op 10 oktober 2022 heeft het kabinet de beleidsreactie op het OVV-rapport naar de Kamer gestuurd. In die brief is toegezegd dat door het ministerie van EZK in overleg met brancheorganisaties zal worden verkend hoe het maken van heldere contractuele afspraken tussen leveranciers en afnemers kan worden gestimuleerd. Dit onderzoek is gestart om beter zicht te krijgen op de huidige praktijk.
- Het onderzoek heeft zich gericht op de volgende vraag: "Hoe worden cybersecurityvereisten opgenomen in b2b-contracten voor ICT-producten- en diensten in Nederland?"
- Het onderzoek toont aan dat contractuele afspraken over cybersecurity in de praktijk vaak niet doorslaggevend zijn om voor een leverancier van een ICT-

product of dienst te kiezen. Ook geeft het onderzoek aan dat bij een cybersecurityincident weinig teruggegrepen wordt op de gemaakte contractuele afspraken. Het gaat in grotere mate om het vertrouwen dat de afnemer heeft in de capaciteiten van de leverancier en de meerwaarde van de service die geboden wordt. Toch zijn contractuele voorwaarden over cybersecurity wel nuttig: met het vaststellen van een passende minimale norm, wordt wel degelijk bijgedragen aan het verhogen van de digitale weerbaarheid van een organisatie.

- De adviezen zien op drie thema's:
    1. het kennisniveau van bedrijven verhogen,
    2. standaardisatie en harmonisatie, en
    3. het ondersteunen van bedrijven bij incidenten.
- Op basis van dit onderzoek en de input uit het veld is er geen noodzaak tot het starten van nieuwe initiatieven om de adviezen te adresseren. De bestaande initiatieven en recente Europese ontwikkelingen ten aanzien van wet- en regelgeving en certificering geven invulling aan de inzet om bedrijven te ondersteunen in het maken van contractuele afspraken over cybersecurity. Er valt nog winst te behalen in het verder onder de aandacht brengen van deze initiatieven bij bedrijven.
- Enkele voorbeelden hiervan zijn:
    - De recent uitonderhandelde Europese Cyber Resilience Act (cybersecurityeisen voor alle hard- en software), de Cyber Security Act (certificering van ICT-producten, diensten en processen) en de herziene richtlijn voor Netwerk- en Informatiebeveilliging (NIS2, verplichtingen voor essentiële en belangrijke sectoren om cybersecuritymaatregelen te nemen).
    - Verschillende hulpmiddelen van het Digital Trust Center zoals de Cyberveilig Check.
    - Publiek-private projecten zoals Samen Digitaal Veilig met branches van VNO-NCW en de Online Trust Coalitie.
    - Het in ontwikkeling zijnde keurmerk voor IT-leveranciers voor het mkb (o.b.v. Kamermotie Rajkowski).

Toelichting

- In de klankbordgroep voor dit onderzoek namen afgevaardigden van CIO Platform Nederland, VNO-NCW, NLdigital en Stichting DINL deel. De drie laatstgenoemden hebben daarbij aangegeven dat het rapport in hun ogen een te eenzijdig beeld schetst van de rol van de leverancier. Zij zijn van mening dat het leveranciersperspectief in het rapport nauwelijks aan de orde komt, omdat naar hun mening alles primair vanuit het afnemersperspectief benaderd wordt. Zij geven aan dat daardoor een volledige probleemanalyse ontbreekt. Daarnaast geven zij aan dat er in Nederland en in de EU reeds veel bestaande initiatieven zijn en dat Europese wet- en regelgeving het maken van cybersecurityafspraken tussen afnemers en leveranciers af zal gaan dwingen voor groepen bedrijven. Zij pleiten voor het versterken van de bestaande trajecten in plaats het starten van nieuwe initiatieven. Deze toelichting is opgenomen in de Kamerbrief. Daarbij wordt aangegeven dat hoewel u de eenzijdige beeldvorming in het rapport niet herkent, u wel kunt onderschrijven dat het niet zo kan zijn dat de volledige verantwoordelijkheid voor cybersecurity bij de leverancier ligt. Beide contractuele partijen hebben verantwoordelijkheden.
- Over de verdere voortgang van de diverse in de brief genoemde acties zal de Kamer verder worden geïnformeerd bij de jaarlijkse voortgangsbrief van de Nederlandse Cybersecuritystrategie (NLCS) in het najaar van 2024.