Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1148

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 8 april 2024

Hierbij stuur ik uw Kamer het rapport «Onderzoek contractuele afspraken cybersecurity» dat ik heb laten uitvoeren door PricewaterhouseCoopers (hierna: PwC). In deze brief worden de bevindingen en de adviezen besproken die in dit rapport zijn gegeven om afnemers en leveranciers beter in staat te stellen heldere contractuele afspraken over cybersecurity te maken, alsmede de wijze waarop ik hier invulling aan zal geven.

Aanleiding

De Onderzoeksraad voor Veiligheid (hierna: OVV) heeft op 16 december 2021 het rapport «Kwetsbaar door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix» gepubliceerd.[1] Een van de aanbevelingen uit het rapport van de OVV is gericht aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Economische Zaken en Klimaat (hierna: EZK) (ten behoeve van alle organisaties en consumenten in Nederland) en luidt: «bevorder dat Nederlandse organisaties en consumenten gezamenlijk veiligheidseisen formuleren en afdwingen bij softwarefabrikanten. Zorg dat de overheid daarbij een voortrekkersrol speelt. Ga uit van het principe: collectieve samenwerking waar mogelijk; branche-specifiek waar noodzakelijk».

Op 10 oktober 2022 heeft het kabinet de beleidsreactie op het OVV-rapport naar de Kamer gestuurd.[2] In de Kamerbrief is aangegeven dat het kabinet deze aanbeveling omarmt. Daarbij is toegelicht dat voor overeenkomsten tussen overheidspartijen en ICT-leveranciers er al de Inkoopeisen Cybersecurity Overheid (ICO) bestaan, en is ten aanzien van consumentenbescherming verwezen naar de Implementatiewet richtlijnen verkoop goederen en levering digitale inhoud. In de brief is toegezegd dat door het Ministerie van EZK in overleg met brancheorganisaties zal worden

[1] https://onderzoeksraad.nl/onderzoek/kwetsbaar-door-software-lessen-naar-aanleiding-van/.
[2] Bijlage bij Kamerstuk 26 643, nr. 925

kst-26643-1148
ISSN 0921 - 7371
's-Gravenhage 2024

verkend hoe het maken van heldere contractuele afspraken tussen leveranciers en afnemers kan worden gestimuleerd. Hiertoe heb ik een marktonderzoek laten uitvoeren dat zich richt op *business-to-business* (hierna: b2b) relaties.
Het onderzoek heeft zich gericht op de volgende vraag: «Hoe worden cybersecurityvereisten opgenomen in b2b-contracten voor ICT-producten- en diensten in Nederland?» De onderzoekers hebben hiervoor naast het bestuderen van literatuur, wet- en regelgeving en jurisprudentie ook diverse algemene voorwaarden geanalyseerd en interviews afgenomen bij zowel leveranciers als afnemers van zowel grote als kleinere ondernemingen in verschillende sectoren.

Klankbordgroep

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 onvoldoende aan de orde komt, omdat naar hun mening alles primair vanuit het afnemersperspectief benaderd wordt. Zij geven aan dat daardoor een volledige probleemanalyse ontbreekt. Daardoor komt ook de problematiek van security in ketens onvoldoende uit de verf. VNO-NCW, NLdigital en Stichting DINL geven aan uit de voeten te kunnen met de adviezen en de vervolgstappen in het rapport, maar tekenen daarbij aan dat het onderzoek geen nieuwe inzichten biedt. Zij geven aan dat er in Nederland en in de Europese Unie 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. Het ontbreken van deze initiatieven in het rapport wekt volgens deze partijen onnodig de indruk dat er nog weinig wordt gedaan. Zij pleiten voor het versterken van de bestaande trajecten in plaats het starten van nieuwe initiatieven. Hoewel ik deze eenzijdige beeldvorming niet herken in het rapport, kan ik wel onderschrijven dat het niet zo kan zijn dat de volledige verantwoordelijkheid voor cybersecurity bij de leverancier ligt. Beide contractuele partijen hebben verantwoordelijkheden. Europese wet- en regelgeving zal hier een impuls aan geven. Daarnaast richten de aanbevelingen zich op het vergroten van kennis bij beide contacterende partijen. Daarvoor bestaan ook reeds verschillende (publiek-private) initiatieven. Op basis van dit onderzoek en de input van de klankborgroep zie ik dan ook geen noodzaak tot het starten van nieuwe initiatieven. Ik ben van mening dat de bestaande initiatieven toereikend zijn 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. Ik zal hierna verder in gaan op de verschillende Nederlandse en Europese ontwikkelingen.

Adviezen en volgende stappen

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. Om het maken van contrac-

tuele afspraken over cybersecurity in b2b-relaties te bevorderen wordt een aantal adviezen gegeven die zien op drie thema's: 1) het kennisniveau van bedrijven verhogen, 2) standaardisatie en harmonisatie, en 3) het ondersteunen van bedrijven bij incidenten.[3]

1. Het kennisniveau van bedrijven verhogen

Het onderzoek toont aan dat wanneer een van de contracterende partijen een (zwaar) overwicht heeft ten opzichte van de andere partij dit doorwerkt op de contractonderhandelingen. Het overwicht wordt bepaald door de commerciële waarde van de opdracht, het kennisniveau van de partijen en de afhankelijkheid van het type dienstverlening. Afnemers geven aan over het algemeen geen eigen inkoopvoorwaarden af te kunnen spreken, terwijl leveranciers aangeven dat veel afnemers vragen om bepaalde certificeringen zonder deze goed te begrijpen.

Andersom, wanneer de contractpartijen een gelijkwaardige kennispositie hebben, noemt het onderzoek voorbeelden van partnerschappen waarin afnemer en leverancier elkaar steunen. Binnen deze partnerschappen worden er meer inhoudelijke discussies gevoerd die beide partijen verder helpen. De afnemer en leverancier ondersteunen elkaar en delen informatie om samen een hoger kennisniveau te bereiken. Bij een partnerschap wordt in het algemeen door de leverancier meer overleg gevoerd met de afnemer en worden concrete plannen gemaakt. Het onderzoek geeft aan deze intensieve samenwerking in een partnerschap niet alleen tussen grote bedrijven te zien, maar ook veel tussen kleinere bedrijven.[4]

Waar het gaat om de ongelijke onderhandelingspositie zie ik met name mogelijkheden om kleinere of ten aanzien van cybersecurity minder volwassen bedrijven te helpen hun kennisniveau te verhogen. Dit geldt zowel voor afnemers als voor leveranciers. Ik zie daarbij een rol voor het Digital Trust Center (hierna: DTC) om contracterende partijen te ondersteunen bij het creëren van een kennisniveau waarop inhoudelijkere discussies gevoerd kunnen worden en het verschil tussen afnemers en leveranciers wordt verkleind, bijvoorbeeld door het geven van passende toelichtingen op regelgeving.[5] Zo kunnen afnemers zich beter bewust worden van welke beveiligingsafspraken zij nodig hebben, en kunnen leveranciers beter in staat worden gesteld om aan afnemers uit te leggen dat beveiligingsmaatregelen de investering waard zijn.

In het rapport adviseren de onderzoekers om op een centrale plek duidelijke en concrete voorbeelden van *best practices* te delen die zien op het nemen van en verbeteren van cybersecuritymaatregelen en het aanbieden van *awareness modules*.[6] Daarnaast geven ze aan dat de informatie die het Nationaal Cyber Security Centrum (hierna: NCSC) en DTC delen wordt gewaardeerd, maar dat nog winst valt te behalen op het bereik. Het is voor organisaties niet altijd duidelijk naar welk loket men toe kan voor welke vraag.[7]

Hieraan wordt al gewerkt door zowel het DTC als private partijen. Op de DTC-website kunnen ondernemers informatie vinden over starten met cybersecurity, veilig digitaal ondernemen en het nemen van concrete

---

[3] Onderzoek contractuele afspraken cybersecurity, pagina 26.
[4] Onderzoek contractuele afspraken cybersecurity, pagina 19.
[5] Onderzoek contractuele afspraken cybersecurity, pagina 28 – stap 5.
[6] Onderzoek contractuele afspraken cybersecurity, pagina 26 en pagina 28 – stap 2.
[7] Onderzoek contractuele afspraken cybersecurity, pagina 24.

maatregelen.[8] Daarnaast biedt het DTC ook een checklist aan voor het opstellen van een *Service Level Agreement* met een IT dienstverlener. Op de website van het DTC is ook een «praatplaat» te vinden, bedoeld om het gesprek tussen een IT-dienstleverancier en een afnemer te vergemakkelijken.[9] Een van de tools die het DTC aanbiedt is de Cyberveilig Check. Het stelt organisaties in staat om hun eigen cybersecurityniveau te meten. De organisatie kan daarna met een actielijst, praktische instructies en tips aan de slag.[10] Ook kan een ondernemer op de website van het DTC zijn of haar beveiligingsbewustzijn testen.[11] Daarnaast wordt tussen ondernemers onderling kennis uitgewisseld in de online DTC-community waarbij momenteel 3820 leden zijn aangesloten. Zoals aangegeven in mijn brief van 8 maart jl. zet het DTC in op het vergroten van het bereik en de impact van producten, diensten en tools die het DTC aanbiedt om zo steeds meer ondernemers te helpen cyberweerbaar te worden.[12] Er wordt steeds opnieuw gekeken naar manieren om deze informatie onder de aandacht van de ondernemer te brengen, bijvoorbeeld door middel van campagnes. Ook zal na de integratie van het DTC, het NCSC en CSIRT voor digitale diensten een centrale plek ontstaan waar alle bedrijven terecht kunnen.[13]

Private partijen zoals brancheorganisaties zetten zich ook in voor het vergroten van het bewustzijn over cybersecurity. Samen Digitaal Veilig (hierna: SDV) is een initiatief van MKB-Nederland en VNO-NCW. SDV is een platform dat bedrijven helpt met het zetten van stappen in het verbeteren van hun cybersecurity. Hierin gaat een gebruiker samen aan de slag met medewerkers en (IT) leveranciers.[14] Naast stimulerende maatregelen zullen de herziene Europese richtlijn voor netwerk- en informatiebeveiliging (de NIS2-richtlijn) en de Europese verordening voor de financiële sector *Digital Operational Resilience Act* (Verordening digitale operationele weerbaarheid, DORA) het maken van contractuele afspraken over cybersecurity af gaan dwingen vanaf middelgrote organisaties in belangrijke sectoren.

Het rapport adviseert daarnaast het gebruik van modelovereenkomsten.[15]

Een modelovereenkomst is een document met standaardbepalingen en -clausules die vaak voorkomen in overeenkomsten. Contracterende partijen kunnen aan de hand van deze modelovereenkomsten overwegen welke contractvoorwaarden in hun situatie wenselijk kunnen zijn. Er bestaan private initiatieven zoals brancheorganisaties die modelovereenkomsten beschikbaar stellen en ik moedig deze initiatieven aan. Daarbij is vooral behoefte aan passende modelovereenkomsten voor bepaalde typen producten of diensten. Zo zijn er bijvoorbeeld andere contractvoorwaarden relevant bij het afnemen of leveren van clouddiensten, dan bij een contract voor mobiele apparatuur. Daarnaast wordt vanuit de overheid voor veilig aanbesteden en inkopen gewerkt met de Inkoopeisen Cybersecurity Overheid (ICO). De overheid wil hiermee de vraag naar digitaal veilige ICT-producten en diensten stimuleren, haar eigen veiligheid verhogen en een goed voorbeeld geven. Hiertoe is een inkooptool, de ICO-Wizard, ontwikkeld om veilig inkopen te vergemakke-

[8] https://www.digitaltrustcenter.nl/.
[9] https://www.digitaltrustcenter.nl/sites/default/files/2021–12/Praatplaat_digitale_veiligheid.pdf.
[10] Onderzoek contractuele afspraken cybersecurity, pagina 28 – stap 3; https://tools.digitaltrustcenter.nl/cyberveilig-check/.
[11] Bijvoorbeeld: https://www.digitaltrustcenter.nl/test-je-kennis-phishing en https://www.digitaltrustcenter.nl/test-je-kennis/fraude.
[12] Kamerstuk 26 643, nr. 1143.
[13] Kamerstuk 26 643, nr. 1143.
[14] https://www.samendigitaalveilig.nl/.
[15] Onderzoek contractuele afspraken cybersecurity, pagina 28 – stap 4.

lijken. Deze tool is online te raadplegen en biedt ondersteuning bij het kiezen van informatiebeveiligingseisen toegespitst op de soort dienst die wordt ingekocht.[16] Deze eisen kunnen ook gebruikt worden door bedrijven om inkoopeisen te stellen.

2. Standaardisatie en harmonisatie

De onderzoekers wijzen erop dat het reguleren van organisaties of sectoren zorgt voor een stimulans in het bewustzijn van de organisatie, zoals het geval is in de financiële sector, verzekeringsbranche of vitale sectoren. Deze regulering kan komen vanuit de overheid, maar hetzelfde effect kan uitgaan van zelfregulering vanuit overkoepelende organisaties en/of samenwerkingsverbanden. Wanneer een organisatie gereguleerd wordt, is een duidelijk kennisverschil op te merken, organisaties zijn *compliance-driven*.[17]

Deze uitkomst is herkenbaar en onderschrijft ook de ontwikkelingen die zijn ingezet in de Nederlandse Cybersecurity Strategie (hierna: NLCS)[18] en in Europa. De komende jaren worden fabrikanten verplicht om de cybersecurity van hard- en software die in de Europese Unie op de markt komt te waarborgen dankzij de *Cyber Resilience Act* (CRA). Daarop vooruitlopend worden in augustus 2025 de cybersecurityvereisten voor draadloos verbonden (slimme) apparaten onder de *Radio Equipment Directive* (RED) van kracht. Met deze regels en de verdere uitwerking daarvan in technische normen, wordt het voor bedrijven duidelijker wat je van elkaar kan verwachten. Daarbij krijgt iedere fabrikant in de keten een eigen verantwoordelijkheid voor de cybersecurity van de componenten die hij levert. Ik verwacht dat deze regels een impuls gaan geven aan wat bedrijven contractueel vastleggen over cybersecurity, naast het positieve effect dat de eisen zullen hebben op het algehele niveau van de digitale veiligheid van de digitale producten die consumenten én bedrijven in Europa gebruiken.

Daarnaast komt in het onderzoek naar voren dat het aantal certificeringen op de digitale markt snel groeit, maar dat er weinig standaardisatie is.[19] Dit kan leiden tot wildgroei en versnippering.

Keurmerken en certificeringen zijn belangrijke instrumenten, waarvan ik de ontwikkelingen in het cybersecuritydomein wil stimuleren. Het mkb-keurmerk is daar een voorbeeld van. Om ondernemers bij de keuze voor een ICT-leverancier te ondersteunen wordt ter invulling van de motie van het lid Rajkowski c.s.[20] een mkb-keurmerk opgesteld dat zich richt op het certificeren van het werk van ICT-dienstverleners om mkb-organisaties te helpen bij het verhogen van hun cyberweerbaarheid. Het is de bedoeling hiermee het mkb te ondersteunen in het verbeteren van de cyberweerbaarheid van de organisatie (de «basis op orde te brengen») door makkelijk een betrouwbare aanbieder te kunnen kiezen. Voor meer informatie over dit mkb-keurmerk verwijs ik naar mijn recente Kamerbrieven.[21]

Maar ik deel ook de zorgen over de wildgroei binnen de digitale markt. Naast goede nationale initiatieven ben ik daarom van mening dat we ons primair moeten richten op aansluiting op de Europese ontwikkelingen.

---

[16] https://bio-overheid.nl/ICO-Wizard/.
[17] Onderzoek contractuele afspraken cybersecurity, pagina 19.
[18] Kamerstuk 26 643, nr. 925.
[19] Onderzoek contractuele afspraken cybersecurity, pagina 20.
[20] De motie Rajkowski c.s. 36200-VII-60.
[21] Kamerstuk 26 643, nr. 1068 en Kamerstuk 26 643, nr. 1143.

Internationaal opererende bedrijven zijn qua administratieve lasten en *level playing field* het meest gebaat bij het halen van certificeringen die in heel Europa geldig zijn. Dat is ook een van de redenen waarom er op Europees niveau de *Cybersecurity Act* (Cyberbeveiligingsverordening, CSA) tot stand is gekomen. De CSA creëert een Europees geharmoniseerd stelsel van cyberbeveiligingscertificering voor ICT-producten, -diensten en -processen. Het doel van de verordening is om door middel van een geharmoniseerde certificatiesystematiek de cybersecurity in Europa aan te jagen en tegelijkertijd de (digitale) interne markt te versterken. Zoals aangegeven in de NLCS draagt het kabinet in samenwerking met private partijen bij aan de ontwikkeling en adoptie van Europese cybersecuritycertificeringschema's voor ICT-producten, diensten en processen. Dit gebeurt onder meer via de publiek-private Online Trust Coalitie (OTC) en via de Europese standaardisatieorganisatie CEN/CENELEC. Voorbeelden zijn het recent gepubliceerde schema voor *Common Criteria*[22] en de nog in ontwikkeling zijnde schema's voor clouddiensten en 5G-technologie.

3. Het ondersteunen van bedrijven bij digitale incidenten

Het rapport adviseert een sociaal vangnet te creëren waar organisaties terecht kunnen wanneer zij ernstige digitale schade lijden.[23]

De informatiedienst van het DTC houdt zich specifiek bezig met het waarschuwen van bedrijven over digitale dreigingen om ze in staat te stellen actie te ondernemen, maar een bedrijf is en blijft zelf verantwoordelijk voor het actief beheren en versterken van zijn digitale veiligheid. De overheid speelt hierin een rol maar neemt uitdrukkelijk niet de verantwoordelijkheid van bedrijven over. De markt voorziet namelijk in *incident response,* met commerciële cybersecuritydiensten zoals hulp bij response en herstel bij hacks en/of schade. We hebben goede cybersecuritybedrijven in Nederland en de markt kan beter schalen dan de overheid. Toch is het voor bedrijven niet altijd eenvoudig om de weg te vinden naar instanties die ondersteuning bieden.
In het Actieprogramma Veilig Ondernemen wordt geconstateerd dat er behoefte is aan handelingsperspectief voor ondernemers nadat zij slachtoffer zijn geworden van cybercrime.[24] Er wordt dus een noodzaak gezien om hiermee aan de slag te gaan. Het project «Ontwerpen en testen van een incident response keten voor het mkb bij slachtofferschap van online criminaliteit» is een City Deal Lokale weerbaarheid Cybercrime project dat van start is gegaan om incident response voor het mkb te verkennen en een response structuur te ontwerpen, waarin contractuele aspecten meegenomen worden. Daarnaast wordt nu vanuit de NLCS gewerkt aan de doorontwikkeling van het Landelijk Dekkend Stelsel (LDS) dat overzicht moet geven waar organisaties bij welk probleem of oplossing terecht kunnen. U wordt daar voor de zomer door de Minister van Justitie en Veiligheid over geïnformeerd.

Ook kan een bedrijf zich tegen incidenten verzekeren. Hulp bij incidenten zoals ransomware is een onderdeel van deze verzekeringen. Het rapport wijst ook op de rol van cybersecurityverzekeringen.[25] Daarbij verwijs ik graag naar de NLCS. Hierin is opgenomen dat het Ministerie van Justitie en Veiligheid, samen met het Ministerie van EZK en het Ministerie van

---

[22] https://digital-strategy.ec.europa.eu/nl/library/implementing-regulation-adoption-european-common-criteria-based-cybersecurity-certification-scheme.
[23] Onderzoek contractuele afspraken cybersecurity, pagina 26 en pagina 28 – stap 7.
[24] https://www.rijksoverheid.nl/documenten/rapporten/2022/12/14/tk-bijlage-actieprogramma-veilig-ondernemen-2023–2026, pagina 6.
[25] Onderzoek contractuele afspraken cybersecurity, pagina 28 – stap 8.

Financiën, verkent welke rol verzekeraars zouden kunnen spelen in het kader van gevolgschade van cyberincidenten.[26]

Maar, voorkomen is beter dan genezen. De onderzoekers geven aan dat veel organisaties, voornamelijk in het midden- en klein bedrijf, beperkte (financiële) middelen hebben om in te zetten voor het inbouwen van cybersecuritymaatregelen. Daarbij speelt ook het tekort aan technisch personeel.[27]

Dit onderken ik. Zoals aangegeven in mijn brief van 8 maart jl. is er voor kleine ondernemers die, bijvoorbeeld wegens financiële knelpunten, cybermaatregelen uitstellen of niet nemen, door het DTC de subsidieregeling «Mijn Cyberweerbare Zaak»[28] gerealiseerd met een totaalbudget van € 300.000.[29] Deze regeling is een pilot. Van de aanschafwaarde en/of implementatiekosten wordt maximaal 50% gedekt tot een maximum van € 1.250. De subsidieregeling was na drie weken overtekend en wordt geëvalueerd. In de evaluatie wordt onderzocht of de subsidieregeling in 2024 opnieuw beschikbaar kan worden gesteld. De resultaten worden in Q2 verwacht. Bovendien heeft het achterblijven van het mkb bij het verhogen van hun cyberweerbaarheidsniveau, de zogenaamde «cyberweerbaarheidskloof», ook de aandacht van de Cyber Security Raad, die op verzoek van de Minister van Justitie en Veiligheid een advies hierover voorbereid. Dit advies wordt dit voorjaar verwacht.

Tot slot

Het onderzoek naar contractuele afspraken over cybersecurity in b2b-relaties maakt onderdeel uit van het actieplan van de NLCS. Belangrijke doelstelling in de NLCS is daarnaast om fabrikanten met een zorgplicht meer verantwoordelijkheid te laten dragen voor de digitale veiligheid van producten. Met de cybersecurityeisen onder de RED en de CRA wordt dit op Europees niveau wettelijk vastgelegd, zodat gebruikers (bedrijven en consumenten) erop kunnen vertrouwen dat digitale producten die in de Europese Unie op de markt komen veilig zijn. Hiervoor zijn consumenten en zakelijke gebruikers dan niet langer alleen afhankelijk van de contractuele afspraken die zij hebben kunnen afspreken, en wordt voor de fabrikanten een *level playing field* binnen de Europese markt gecreëerd. Over de verdere voortgang van de diverse acties zal u verder worden geïnformeerd bij de jaarlijkse voortgangsbrief van de NLCS in het najaar.

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

---

[26] https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022–2028/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022–2028.
[27] Onderzoek contractuele afspraken cybersecurity, pagina 19.
[28] https://zoek.officielebekendmakingen.nl/stcrt-2023–26170.html; https://www.digitaltrustcenter.nl/toolkit-mijn-cyberweerbare-zaak.
[29] Kamerstuk 26 643, nr. 1143.