Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

36 560 XIII Jaarverslag en slotwet Ministerie van Economische Zaken en Klimaat 2023

Nr. 8 **BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 19 juni 2024

Hierbij zend ik u de antwoorden op de vragen van de vaste Tweede Kamer commissie van Economische Zaken en Klimaat over het Jaarverslag EZK 2023 in het kader van het V-100 evenement (2024D22199, ingezonden 30 mei 2024).

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

kst-36560-XIII-8
ISSN 0921 - 7371
's-Gravenhage 2024

V-100 thema (7): Cyberweerbaarheid, mkb en data-encryptie.

1
Het Digital Trust Center (DTC) zet in op het delen van kwetsbaarheidsinformatie met door DTC gesubsidieerde stichtingen en samenwerkingsverbanden die deze informatie commercieel beschikbaar stellen. Dat heeft tot gevolg dat publiek beschikbare beveiligingsinformatie alleen te verkrijgen is door bedrijven die daarvoor betalen. Volgens informatie van het DTC betreft het hier minder dan 1% van het aantal bedrijven in Nederland. Bent u zich bewust van deze situatie, in hoeverre acht u dit wenselijk en zo nee, ziet u mogelijkheden dit te veranderen?

Antwoord
Ik ben mij bewust van de situatie dat sommige samenwerkingsverbanden op deze manier opereren. Zoals aangegeven in de vraag is mijn beeld dat het in minder dan 1% van de gevallen voor komt. Cybersecurity samenwerkingsverbanden waar bedrijven lid van worden bieden overigens vaak ook andere diensten en producten zoals tools met praktische adviezen en kennis.

Ik hecht eraan te benadrukken dat het werken via samenwerkingsverbanden niet de enige manier is voor bedrijven om informatie te ontvangen van het DTC over digitale dreigingen en kwetsbaarheden. Het is onjuist dat publiek beschikbare beveiligingsinformatie alleen te verkrijgen is voor bedrijven die daarvoor betalen. Het DTC verspreidt informatie op verschillende wijzen. In de eerste plaats wordt algemene ernstige dreigingsinformatie verspreid via de eigen kanalen, waaronder de website en de online community. Ook worden doelgroep-berichten hiervoor ingezet.

In de tweede plaats kan het DTC bedrijven individueel waarschuwen bij een ernstige kwetsbaarheid, op het moment dat herleid kan worden welke bedrijven specifiek kwetsbaar zijn in het betreffende geval (zogenoemd ongevraagd notificeren). Tot slot, heeft het DTC een pilot met ongeveer vijftig bedrijven. Deze bedrijven hebben gegevens over hun systemen bij het DTC aangeleverd, zodat er matching plaats kan vinden op deze systemen en de dreigingsinformatie die bij het DTC bekend is (zogenoemd gevraagd notificeren). Deze pilotdeelnemers worden nu gekoppeld aan de ontwikkeling van het online portaal van het Nationaal Cyber Security Centrum met het oog op de integratie van de organisaties. In dit portaal kunnen bedrijven via een Mijn NCSC account hun gegevens aanleveren, zodat voornoemde matching sneller en effectiever kan plaatsvinden op de bij het NCSC bekende informatie.

Het totaal aantal mogelijk kwetsbare systemen waarvoor de informatiedienst, sinds de start in juni 2021, notificaties verstuurde aan bedrijven (gevraagd en ongevraagd) is ruim 258.000. Dit komt vooral op het conto van de «ongevraagde» waarschuwingen over kwetsbaarheden bij het bedrijfsleven. Het DTC notificeerde over bijna 140.000 bedrijfsspecifieke cyberdreigingen in 2023.

2
In hoeverre denkt u dat de cyberweerbaarheid te verhogen is door bedrijven te verplichten zich te verzekeren tegen digitale dreigingen (naar analoge van traditionele risico's als brand, inbraak of aansprakelijkheid) en in hoeverre overweegt u een dergelijke verplichting?

Antwoord

De markt van cyberverzekeringen is nog in ontwikkeling. De keuze of een cyberverzekering voor een bedrijf toegevoegde waarde heeft, is gebaseerd op een risicoafweging. De meerwaarde van een verzekering zal groter worden wanneer een bedrijf afhankelijk is van digitale systemen en de informatie in die systemen voor de bedrijfsvoering. Ook maakt het afsluiten van een cyberverzekering een ICT-omgeving niet per definitie veiliger. Het al dan niet afsluiten van een cybersecurityverzekering is onderdeel van de eigen verantwoordelijkheid van bedrijven voor hun digitale weerbaarheid. Daarom zie ik geen aanleiding om over te gaan tot een verplichting.

Het Digital Trust Center (DTC) verwijst naar vijf basisprincipes voor veilig digitaal ondernemen. Deze zijn opgesteld om ondernemers te helpen de basisbeveiliging in te laten stellen. Ondernemers die de 5 basisprincipes opvolgen, vergroten hun weerbaarheid tegen cyberrisico's die de bedrijfsvoering kunnen verstoren. Daarnaast heeft het DTC de Risicoklasse-indeling Veiligheid voor digitale veiligheid op haar website staan. Dit is een risicoclassificatiemodel voor het mkb, ontwikkeld onder leiding van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en in samenwerking met een breed scala belanghebbenden, onder andere het verbond van verzekeraars.

3
Nederland is buiten de top-10 vestigingsklimaat beland voor start-ups en scale ups. In hoeverre overweegt u belastingvoordelen of een voorkeursbeleid bij het inhuren van Nederlandse start-ups/scale-ups op gebied van digitale weerbaarheid op deze positie te verbeteren?

Antwoord
Het Ministerie van EZK heeft als één van de prioriteiten het verbeteren van het vestigingsklimaat voor alle typen bedrijven (startups, MKB en grootbedrijf). Daar zetten we ons dagelijks voor in en dat zal EZK ook in de toekomst blijven doen. Dit is aangegeven in de Kamerbrief Strategische agenda voor het ondernemingsklimaat in Nederland (2022), evenals in de Kamerbrief Startups en scale-ups als motor voor transities en groei (2023). Daar is primair ingezet op het verbeteren van toegang tot talent, financiering, kennis, internationale markten en netwerken en de overheid. Er wordt hierbij geen apart voorkeursbeleid gevoerd voor bepaalde groepen startups en scale-ups, zoals bijvoorbeeld bepaalde sectoren. Ik overweeg ook geen aparte belastingvoordelen of voorkeursbeleid bij het inhuren van Nederlandse startups of scale-ups op het gebied van digitale weerbaarheid. Deze startups en scale-ups worden op dezelfde wijze ingehuurd als alle andere bedrijven, conform de algemeen geldende inkoop- en aanbestedingsregels.

4
Generatieve AI wordt al ingezet voor cyber-aanvallen. De huidige maatregelen lijken vooral gericht op het opleiden van MKB'ers tot cybersecurity-specialist.
Wat wordt er concreet nu gedaan rondom generatieve AI en hoeveel geld is hiervoor gereserveerd? In hoeverre hebben deze investeringen resultaat en hoe worden deze gemeten?

Antwoord
AI, waaronder generatieve AI, verandert het digitale dreigingslandschap; als technologie voor aanvallen (bijvoorbeeld de inzet van generatieve AI voor phishing), en door aanvallen op AI-systemen zelf (bijvoorbeeld het beïnvloeden of verstoren van Large Language Models). Cybersecurity van AI-systemen en het gebruik van AI technologie in cyberaanvallen krijgt steeds meer aandacht van overheidspartijen. Daarnaast biedt AI ook een

kans voor innovatie om cybersecuritytoepassingen te versterken voor geautomatiseerde verdediging van cyberaanvallen.

Vanuit de kennis- en innovatiedoelstellingen van de Nederlandse Cybersecuritystrategie wordt er op dit moment een verkennend onderzoeksproject uitgevoerd door TNO over de impact van AI op cybersecurity, nu en in de toekomst. De conclusies van deze studie zullen, in samenhang met andere projecten, bijdragen aan de opbouw van handelingsperspectief voor burgers, bedrijven en overheid over AI en cybersecurity.

5a
Projecten zoals GPT-NL en OpenKAT worden door de overheid gefinancierd.
Is er bij deze projecten rekening gehouden met (verwachtingen ten aanzien van) de kwaliteit van het GPT-NL model gezien het lage budget wat hiervoor is gereserveerd?

Antwoord
GPT-NL is deels bekostigd via het Faciliteiten Toegepaste Onderzoek (FTO). Het FTO investeert in hoogwaardige en toekomstbestendige faciliteiten voor onderzoek, die van belang zijn voor het ontwikkelen van innovatieve producten en diensten. Het gaat hierbij om de ondersteuning van een faciliteit die open staat voor partners die met data en kennis willen bijdragen of toepassingen willen ontwikkelen op basis van GPT-NL. De aanvraag is conform de door de aanvragers ingediende begroting en gevraagde financiering vanuit FTO gehonoreerd. OpenKAT maakt geen gebruik van het GPT-NL model.

5b
In hoeverre gaat GPTNL concurreren met LLM's als ChatGPT4o en LLama70b?

Antwoord
GPT-NL is een initiatief dat is opgezet om de kennis en technologie op het gebied van taalmodellen in Nederland te versterken. Dit draagt bij aan het aantrekken en behouden van AI-talent en versterkt de digitale open strategische autonomie. Het doel is niet om te concurreren met andere taalmodellen, zoals GPT-4 of LLama. Het geldt ook niet als vervanging. Er wordt met GPT-NL gebouwd aan een alternatief van Nederlandse bodem op basis van beschikbare (Nederlandstalige) data, waarbij kennisopbouw in Nederland plaatsvindt.

5c
Zijn deze initiatieven vanuit de overheid rechtmatig of is hier sprake van concurrentie met de markt (zie Wet markt & overheid)?

Antwoord
GPT-NL is geen marktproduct maar een «faciliteit» om onderzoek naar taalmodellen mogelijk te maken. Exploitatie van deze faciliteit moet voldoen aan staatsteunregels (AGVV). Er is dus geen sprake van ongeoorloofde concurrentie met de markt. OpenKat is tijdens de Coronapandemie ontwikkeld, omdat er op dat moment geen product bestond wat voldeed aan de eisen om het Coronacheck-stelsel veilig te houden. OpenKat droeg daarmee bij aan het uitvoeren van een wettelijke taak en is tegen integrale kostprijs gerealiseerd. Hiermee voldoet de ontwikkeling van OpenKAT aan de eisen van de Wet markt en overheid.

5d
Worden er Nederlandse startups en scale-ups betrokken bij de ontwikkeling van deze projecten?

Antwoord
Deze faciliteit zal ontwikkeld en beheerd worden door TNO, SURF en NFI. Gebruik staat open voor iedereen, ook startups en scale-ups. Niet economisch gebruik door universiteiten is gratis. Voor economisch gebruik van deze faciliteit zal een marktconform tarief worden gerekend. OpenKAT wordt open-source ontwikkeld door het Ministerie van VWS volgens een community-aanpak. Vanuit de OpenKAT community dragen publieke- en private partijen, klein of groot, bij aan de (door)ontwikkeling van het product.

5e
Hoe zorgt de overheid voor een beheer-ecosysteem, waarin de verantwoordelijkheid binnen de keten wordt geadresseerd zodra het project de eerste resultaten heeft opgeleverd?

Antwoord
De criteria die door de overheid/EZK zijn gesteld voor de selectie van voorstellen die in aanmerking komen voor financiering uit het Faciliteiten Toegepast Onderzoek (FTO) zien juist ook op de verantwoordelijkheden binnen de keten na oplevering van de eerste resultaten. Door de onafhankelijke adviescommissies is hierop scherp toegezien. OpenKAT is open source, wat wil zeggen dat het niet alleen door VWS gebouwd en gefinancierd wordt. Naast eigen ontwikkeling door VWS kent OpenKAT een brede community met bijdragen van andere organisaties, zoals Kennisnet, Z-CERT, BDO en anderen die de inzet van ontwikkelaars financieren en zo bijdragen aan de software. Het Ministerie van VWS heeft op dit moment de overkoepelende rol in de aansturing van het project en beheert daarmee de ontwikkeling onder een EUPL licentie. Gezocht wordt naar een andere partij die per 1 januari 2025 het structurele beheer, generieke doorontwikkeling en community management duurzaam kan overnemen.

6
In sectoren zoals brandveiligheid, automotive en beveiligingsbedrijven is het vanzelfsprekend dat je met goedgekeurde/gecertificeerde bedrijven samenwerkt en je als gebruiker geen specialist hoeft te worden om het product te gebruiken. De huidige maatregelen rondom cybersecurity en AI lijken er op gericht om het MKB op te leiden als specialist i.p.v. concrete oplossingen voor de problematiek te komen. Hoe maken we het MKB vanzelfsprekend veilig?

Hoe kan een MKB'er zekerheid krijgen op het feit dat zij voldoet aan de gestelde veiligheidseisen? Als parallel met de auto-industrie valt er veel te leren: i) je bent verplicht verzekerd; ii) je hebt een zorgplicht om met een veilige auto de weg op te gaan; iii) je rijdt in een gecertificeerd type voertuig dat door een gecertificeerde partij is gekeurd en door een gecertificeerde partij is geproduceerd; en iv) mensen zijn (zo goed als) gestopt met rijden onder invloed toen verzekeraars verklaarden dat je in dat geval onverzekerd rondrijdt.

Antwoord
Er zijn verschillende ontwikkelingen die het midden- en kleinbedrijf vanzelfsprekend veiliger zullen maken. Naar aanleiding van de motie van het lid Rajkowski c.s. is de regering verzocht «om in overleg te treden met het Digital Trust Center (DTC) en betrokken brancheorganisaties om te komen tot een eenduidig mkb-keurmerk, om mkb-organisaties beter te ondersteunen bij het vormen van hun securitybeleid» (Kamerstuk 36 200 VII, nr. 60). Het certificeren van het werk van ICT-dienstverleners zal mkb-organisaties 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. Eind 2023 is voor de ontwikkeling van het keurmerk een subsidie aan het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) gegeven. De ontwikkeling van het keurmerk zal naar verwachting een doorlooptijd hebben van twee jaar. Het keurmerk zal eind 2025/begin 2026 geïntroduceerd kunnen worden. Daarnaast worden in de EU cybersecurity certificeringschema's ontwikkeld voor verschillende categorieën ICT-producten, diensten en processen zoals voor clouddiensten. Bedrijven kunnen in de toekomst bij hun ICT-aanbieder daarnaar vragen.

Daarnaast zal de Cyber Resilience Act (CRA) cybersecurityeisen gaan stellen aan álle producten met digitale elementen (alle hard- en software) die in de Europese Unie op de interne markt wordt gebracht (inwerkingtreding vanaf 2027). De CRA introduceert bovendien een zorgplicht voor fabrikanten om ook na de verkoop, gedurende de hele verwachte gebruiksduur van het product, veiligheidsupdates te verstrekken bij kwetsbaarheden. De CRA voorziet daarnaast in een meldplicht voor fabrikanten bij actief misbruikte kwetsbaarheden en incidenten. Producten die vanaf medio 2027 niet voldoen aan de cybersecurityeisen kunnen door de Rijksinspectie Digitale Infrastructuur (RDI) van de markt worden gehaald. Dit betekent dat mkb-bedrijven die digitale producten gebruiken er van op aan kunnen dat die producten standaard veilig zijn.

Ook de AI-verordening stelt straks eisen aan AI-systemen die als product op de Europese interne markt worden gebracht. De aanbieder van een hoog risico AI-systeem moet onder andere risico's adresseren, ervoor zorgen dat het systeem cyberveilig is en maatregelen nemen om ervoor te zorgen dat de gebruikers van het systeem er op een veilige manier mee om kunnen gaan. Een hoog risico AI systeem mag enkel op de markt worden gebracht of in gebruik worden genomen, als aan alle eisen voldaan wordt. Het moet dan het CE-label dragen. Hierdoor kunnen MKB'ers die deze systemen kopen en gebruiken, erop vertrouwen dat deze naar verwachting werken en veilig zijn. Bovendien krijgen ze uitgebreide instructies voor gebruik, die ze ook verplicht moeten naleven. Als het personeel van een MKB'er met het AI-systeem aan de slag gaat, moet ervoor gezorgd worden dat zij weten hoe ze dat AI-systeem op de juiste manier moeten gebruiken. Indien nodig moeten ze daarvoor opgeleid worden. Hiermee heeft de ontwikkeling en het gebruik van AI grote gelijkenissen met het genoemde voorbeeld van de auto-industrie, waar ook een gedeelde verantwoordelijkheid bij fabrikanten (veilige auto's) en kopers (rijbewijs en veilig rijden) ligt.

Daarnaast wordt zoals aangegeven in vraag 4 een verkennend onderzoek uitgevoerd door TNO over de impact van AI op cybersecurity nu en in de toekomst.

7
Welke concrete doelen heeft u het DTC gesteld ten aanzien van cyberweerbaarheid van het MKB? Welke maatregelen heeft u getroffen om te zorgen dat het MKB wordt betrokken, de dienstverlening van DTC de MKB ook daadwerkelijk bereikt en hoe en worden doeltreffendheid van de activiteiten gemeten?

Antwoord
Het Digital Trust Center heeft twee hoofdtaken, namelijk i) bedrijven voorzien van betrouwbare en onafhankelijke informatie over digitale kwetsbaarheden en het geven van concreet handelingsadvies, en ii) het stimuleren van cybersecurity samenwerkingsverbanden tussen bedrijven. Hierbij ligt de focus van het DTC de komende jaren op vier speerpunten:

zorgen dat bedrijven de basis op orde hebben; ondernemers brengen van bewustzijn over cybersecurity-risico's naar handelen (van weten naar doen); het versterken van het netwerk van cybersecurity samenwerkingsverbanden en het bereik en impact te vergroten.

Dit wordt bereikt door middel van onder andere tools, waaronder de CyberVeilig Check, waarin ondernemers op een laagdrempelige manier worden geholpen aan de slag te gaan met hun cyberveiligheid. Om ondernemers daadwerkelijk te stimuleren om te komen van enkel weten, naar daadwerkelijke implementatie van maatregelen heeft het DTC vorig jaar de subsidie voor Mijn Cyberweerbare zaak verstrekt. Aanvullend stimuleert het DTC samenwerking tussen bedrijven door middel van de subsidieregeling cyberweerbaarheid. Daarnaast beschikt het DTC over een levendige online community met meer dan 4000 leden. Hierin kan op een laagdrempelige manier kennis, ervaring en adviezen worden uitgewisseld.

Jaarlijks meet het CBS in hoeverre bedrijven die middels een samenwerkingsverband zijn aangesloten bij het DTC meer maatregelen treffen om meer cyberweerbaar te worden. Tevens beschikt het DTC over meerdere manieren om feedback te vragen op de tools en overige producten en diensten die beschikbaar worden gesteld. Dit wordt nauw gemonitord en op basis van deze feedback worden producten en diensten aangepast of ontwikkeld. Daarnaast is er veel direct contact met de doelgroep om zo te blijven monitoren welke behoeftes er leven en hoe daar invulling aan te geven. Over de voortgang van alle activiteiten van het DTC bent u op 8 maart jl. geïnformeerd.[1]

[1] Kamerstuk 26 643, nr. 1143