Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

32 637 Bedrijfslevenbeleid

Nr. 1068

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 18 september 2023

In de procedurevergadering van de vaste commissie voor Digitale Zaken van 5 juli 2023 is het kabinet verzocht uw Kamer te informeren over de uitvoering van een tweetal moties van het lid Rajkowski c.s. Het betreft respectievelijk de motie inzake een eenduidig mkb-keurmerk om het midden- en kleinbedrijf (mkb) beter te ondersteunen bij hun cybersecurity-beleid,[1] en de motie inzake het ontwikkelen van een structurele cyberoefenagenda.[2] Beide moties zijn aangenomen naar aanleiding van het wetgevingsoverleg van 14 november 2022 (Kamerstukken 36 200 VII, 36 200 XIII en 36 200 VI, nr. 116). In deze brief informeer ik u over de voortgang van de uitvoering van deze moties. Met deze brief geef ik ook uitvoering aan twee toezeggingen aan het lid Rajkowski over dezelfde materie, te weten toezegging van 14 november 2022 en toezegging van 22 maart 2023.

Uitvoering motie mkb-keurmerk

In de eerste motie van het lid Rajkowski c.s. wordt 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 security-beleid». De afgelopen tijd is ingezet op inventarisatie en consultatie met relevante partijen. Zoals ik heb aangegeven bij het Wetgevingsoverleg van 14 november 2022 heeft het ontwikkelen van certificering of keurmerk op Europees niveau mijn voorkeur, omdat Europese certificaten binnen het raamwerk van de Europese cyberbeveiligingsverordening (*Cyber Security Act, CSA)* in de gehele EU geldig zijn. Dit bevordert het gelijke speelveld en concurrentievermogen van bedrijven in Europa. Hierover is contact geweest met het Europees Agentschap voor cyberbeveiliging (ENISA), die thans cybercertificering onder het Europees raamwerk van de CSA

[1] Kamerstuk 36 200 VII, nr. 60.
[2] Kamerstuk 36 200 VII, nr. 61.

kst-26643-1068
ISSN 0921 - 7371
's-Gravenhage 2023

ontwikkelt. ENISA heeft te kennen gegeven dat de uitvoering van de genoemde motie past binnen de vormgeving van het Europese certificeringsstelsel.

Binnen Nederland is een inventarisatie gemaakt en heeft consultatie plaatsgevonden met relevante partijen[3] naar de behoeften in de markt. Daarbij heb ik geconstateerd dat verschillende organisaties vooral een meerwaarde zien in een keurmerk voor ICT-dienstverleners om het grootste effect te bereiken op het cybersecurity beleid van mkb-organisaties. Deze behoefte komt nadrukkelijk sterker naar voren dan bijvoorbeeld een keurmerk gericht op de mkb-organisaties zelf. Genoemde redenen hiervoor zijn dat «dé mkb'er niet bestaat» en dat met name de kleine(re) mkb-organisaties voor een belangrijk deel juist afhankelijk zijn van hun ICT-dienstverlener als het gaat om het verhogen van hun cyberweerbaarheid. Daarbij hebben de geraadpleegde partijen onderstreept dat een dergelijk keurmerk laagdrempelig, voor iedereen toegankelijk én betaalbaar dient te zijn, waarbij bij voorkeur aansluiting wordt gezocht bij bestaande initiatieven.

Ik ben voornemens de motie uit te laten voeren door ondersteuning van het initiatief Kwaliteitspreventie van het *Centrum voor Criminaliteitspreventie en Veiligheid (CCV)*, een onafhankelijke instantie, waarbij actief samengewerkt wordt met het DTC en onder meer het initiatief «Samen Digitaal Veilig» van VNO-NCW/MKB-Nederland. Uit de gevoerde gesprekken is namelijk gebleken dat hun initiatief het meest aansluit op de wens van de markt om te komen tot een keurmerk voor ICT-dienstverleners. Dit keurmerk biedt aan afnemende mkb-organisaties inzicht of de basismaatregelen van cybersecurity op orde zijn bij de dienstverlening van hun ICT-dienstverlener, zoals bij kantoorautomatisering. Daarnaast kan het keurmerk inzicht bieden aan mkb-organisaties of de betreffende ICT-dienstverlener gekwalificeerd is om bij te dragen aan de vormgeving van het eigen cybersecurity beleid. Omgekeerd biedt dit keurmerk ICT-dienstverleners de kans zich kwalitatief te onderscheiden.

Het CCV is een solide keuze met betrekking tot de ontwikkeling, uitgifte en het onderhoud van dit keurmerk. Sterke punten van CCV zijn de onafhankelijkheid en neutraliteit van de organisatie (geen winstoogmerk), de samenwerking met brancheorganisaties, toegang tot experts, en de bekendheid van en het vertrouwen in het CCV bij partijen. Dat het CCV de vormgeving van het keurmerk kan realiseren binnen de kaders van het CSA cybersecuritystelsel is eveneens een belangrijke factor.

Ik ben voornemens het CCV nog vóór het einde van dit jaar subsidie te verstrekken. De ontwikkeling van het keurmerk zal vervolgens naar verwachting een doorlooptijd hebben van twee jaar. Het spreekt voor zich dat intensieve samenwerking met cybersecurityexperts, brancheorganisaties en overheidsinstanties zoals het DTC cruciaal is, om ervoor te zorgen dat het keurmerk nauwkeurig aansluit op de behoeften en uitdagingen van mkb-organisaties. Het betrekken van diverse belanghebbenden zal ons gezamenlijk in staat stellen een inclusief en robuust keurmerk te ontwikkelen, dat een waardevolle bijdrage levert aan de digitale veiligheid van mkb-organisaties.

---

[3] VNO-NCW, NLdigital, Cyberveilig Nederland, CyberRAting (CYRA, initiatief van Cyber Weerbaarheidscentrum Brainport (CWB), TÜV en ASML voor de hightech maakindustrie en toeleveranciers), Cyberfundamentals (Cyberprofessionals geïnspireerd door het Britse Cyber Essentials), Samen Digitaal Veilig (SDV, project van VNO-NCW/MKB Nederland), CCV Kwaliteitsregeling en Stichting Koninklijk Nederlands Normalisatie Instituut (NEN).

Uitvoering motie structurele cyberoefenagenda niet-vitaal

In de tweede motie van het lid Rajkowski c.s. wordt de regering verzocht «om in samenwerking met het Digital Trust Center, brancheorganisaties en regionale partners een structurele cyberoefenagenda te ontwikkelen met daarin cyberoefeningen specifiek gericht op niet-vitale bedrijven». Om te achterhalen wat de behoefte van ondernemers is met betrekking tot cyberoefenen is er gestart met het uitzetten van een flitspeiling[4] onder ondernemers uit het mkb. 845 respondenten hebben de vragenlijst volledig ingevuld, waarvan de bedrijfsgrootte van de deelnemers redelijk gelijkmatig was verdeeld. De uitkomsten daarvan zijn op 15 maart 2023 gepubliceerd.[5] Uit deze flitspeiling komt naar voren dat een kwart van de ondernemers cyberoefeningen nuttig vindt voor hun bedrijf, terwijl de helft twijfelt over het nut van cyberoefeningen. Een kwart van de respondenten geeft aan het nut van cyberoefeningen voor hun bedrijf/organisatie niet in te zien. Uit de flitspeiling blijkt voorts dat bedrijven het best geholpen zijn met praktische handreikingen en oefeningen die toegankelijk en laagdrempelig zijn. Ook bleek dat van de groep mkb'ers die wél behoefte heeft aan oefeningen, de meerderheid binnen die groep de voorkeur heeft voor oefenen binnen de eigen organisatie. Aan oefenen samen met andere organisaties binnen de sector of regio is minder behoefte.

Daarnaast is er conform het motieverzoek op verschillende momenten contact geweest met VNO-NCW/MKB-Nederland en met verschillende brancheorganisaties. Uit die contacten kwam naar voren dat er bij hun leden nog veel winst te behalen is op het gebied van cybersecurity en meer specifiek op het onderwerp cyberoefenen. Vanuit de brancheorganisaties is de behoefte uitgesproken om een laagdrempelige cyberoefening te ontwikkelen die indien mogelijk op eenvoudige wijze sectorspecifiek te maken is. Hoe dichter het scenario bij de bedrijfsvoering komt van de ondernemers, hoe groter de kans op succes is.

Het DTC heeft op haar beurt ook haar samenwerkingsverbanden benaderd over hoe zij het nut en noodzaak van cyberoefenen onder de aandacht van hun achterban kunnen brengen, waarbij het DTC kan faciliteren bij de (totstandkoming van) content hiervoor. Tot slot hebben er gesprekken plaatsgevonden met verschillende aanbieders van cyberoefeningen, met als doel om te kijken in welke mate de markt al in cyberoefeningen voorziet, juist ook voor de kleinere ondernemer. Hieruit komt naar voren dat het aanbod uiteenloopt, onder andere qua doelgroep, aantal deelnemers per oefening, begeleiding bij de oefeningen, tijdsduur en kosten.

Hoewel het kabinet nadrukkelijk sympathie heeft voor de intentie achter de motie, blijkt uit de flitspeiling en de genoemde gesprekken met de brancheorganisaties dat een oefening zoals ISIDOOR, die opgezet is voor de rijksoverheid en vitale organisaties, in feite te complex en grootschalig is voor de gemiddelde mkb'er om aan mee te doen. Ook is de doelgroep niet-vitale bedrijven te divers voor één cyberoefenagenda. Alles afwegende kom ik daarom tot de conclusie dat het organiseren van structurele cyberoefeningen zoals ISIDOOR voor het niet-vitale bedrijfsleven niet de meest effectieve aanpak vormt. Tegelijkertijd vindt het kabinet het stimuleren van cyberoefeningen, juist voor het mkb, wel degelijk van belang. Daarom zullen er passende stappen genomen

[4] Een flitspeiling is een snelle steekproef, deze flitspeiling is tussen 14 en 24 februari 2023 uitgezet.

[5] https://www.rijksoverheid.nl/documenten/publicaties/2023/03/15/flitspeiling-ondernemers-cyberoefenen.

worden om niet-vitale bedrijven vooruit te helpen met cyberoefeningen. Het kabinet zet daarbij met name in op het versterken van de informatievoorziening en de advisering rondom cyberoefeningen. VNO-NCW/MKB-Nederland en verschillende brancheorganisaties onderschrijven deze lijn.

Informatie en advies over cyberoefeningen

Ondernemers die cyberoefeningen als nuttig zien, vinden het vaak lastig om zelf cyberoefeningen op te zetten of te bepalen waar ze moeten beginnen. Om de ondernemer daarbij te helpen is gekozen voor een stapsgewijze aanpak. Op korte termijn zal ondersteuning geboden worden bij het vinden van een passende cyberoefening via de DTC website. De website zal een pagina aanmaken met meer informatie over de verschillende soorten cyberoefeningen die bedrijven kunnen doen. Op deze informatiepagina zal het DTC naast informatie over wat cyberoefeningen zijn en waarom het van belang is om regelmatig te oefenen, ook aanbevelingen doen aan ondernemers over hoe ze kunnen beginnen met oefenen. Hierbij zal het DTC onder meer doorverwijzen naar platforms waar cyberoefeningen voor het niet-vitale bedrijfsleven te vinden zijn.

Daarnaast wordt er vanuit het DTC de mogelijkheid verkend om eigen cyberoefeningen aan te bieden die partijen zelf zonder begeleiding kunnen uitvoeren. Daarover vinden momenteel nog gesprekken plaats, waaronder met het Britse Nationaal Cyber Security Centrum om te leren van hun ervaringen en reeds ontwikkelde middelen. Er wordt in dat kader ook gekeken naar oefeningen die zich met name richten op ondernemers die starten met cyberoefeningen. Na het lanceren van de informatiepagina en het aanbieden van breder inzetbare cyberoefeningen is een mogelijke vervolgstap het (laten) ontwikkelen van sectorspecifieke cyberoefeningen, als uit overleg met brancheorganisaties en (regionale) samenwerkingsverbanden blijkt dat dat nodig is om ondernemers te laten oefenen. Bij de op te zetten activiteiten geldt dat de Wet Markt en Overheid in acht wordt genomen om marktverstoring te voorkomen.

Voor ondernemers die de relevantie van cyberoefeningen nog niet (voldoende) zien zal de informatiepagina tevens vergezeld gaan met een informatiecampagne in samenwerking met partners van het DTC, zoals de genoemde samenwerkingsverbanden en brancheorganisaties, om het belang van oefenen onder de aandacht te brengen bij ondernemers. Het is de bedoeling dat de ondernemer door deze campagne op de hoogte is van de (algemenere) informatie rondom cyberoefeningen die het DTC aanbiedt, maar ook leert dat er via de schakelorganisaties en brancheorganisaties ook sectorspecifieke informatie over cyberoefeningen te krijgen is.

Tot slot

De afgelopen periode zijn de gesprekken met private partners waardevol geweest. Duidelijk is dat zowel een keurmerk voor het mkb als initiatieven rondom het faciliteren van cyberoefeningen voor het niet-vitale bedrijfsleven aansluiten bij het streven naar een digitaal veilig Nederland. Dit stelt ondernemers in staat om hun eigen digitale weerbaarheid te versterken. Over de uitvoering van beide moties zal ik u blijven informeren bij de jaarlijkse voortgang van de NLCS.

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