Aan de voorzitter en (plv.) leden van de
Vaste Kamercommissie Digitale Zaken van de
Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Briefnummer
25-123119

Onderwerp
Inbreng Commissiedebat Online veiligheid en cybersecurity d.d. 5 februari a.s.

Den Haag
22 januari 2025

Telefoonnummer
+31 703490347

E-Mail
gielens@vnoncw-mkb.nl

Geachte dames en heren,

Er zijn veel ontwikkelingen die gericht zijn op het vergroten van de cyberweerbaarheid. Dat is goed nieuws want 1 op de 5 ondernemers wordt - nog los van de huidige hybride dreiging - jaarlijks getroffen door cybercriminaliteit. Cybercrime leidt tot miljoenen euro's aan schade bij burgers en bedrijven. Daarnaast is vergroting van de cyberweerbaarheid zeer urgent met oog op de permanente en almaar toenemende hybride dreiging. De Nederlandse samenleving is verregaand gedigitaliseerd; COVID-19 heeft dit proces verder versneld. Dit biedt allerlei kansen maar maakt ons ook extra kwetsbaar bij hybride dreiging zoals cyberaanvallen, sabotage van (vitale) processen etc. Dit vraagt om extra inzet, vanuit zowel het bedrijfsleven als de overheid.

Vanuit VNO-NCW en MKB-Nederland willen wij u graag een aantal punten meegeven voor het Commissiedebat Online veiligheid en cybersecurity van 5 februari a.s. om de cyberweer-baarheid van het bedrijfsleven en daarmee de maatschappij als geheel verder te versterken:

1. Verbeter informatiedeling over dreigingen en kwetsbaarheden
2. Zorg ervoor dat het nieuwe Nationaal Cybersecurity Centrum herkenbaar blijft voor het mkb
3. Draag zorg voor opvolging van de aanbevelingen vanuit de cyberoefening ISIDOOR IV
4. Zorg voor een voortvarende en efficiënte implementatie van de NIS2-richtlijn met focus op lerend vermogen
5. Implementeer alle komende wetgeving en acties op het gebied van cybersecurity alvorens tot nieuwe te komen

1. Verbeter informatiedeling over cyberdreigingen en kwetsbaarheden

Het is belangrijk dat (vitale) bedrijven structureel van inlichtingeninformatie worden voorzien zodat zij hun verantwoordelijkheid op het gebied van cyberweerbaarheid kunnen pakken en invullen. Onderdeel van de Nederlandse Cybersecuritystrategie (2022-2028) is de realisatie van het zogenoemde 'Cyclotron platform'. Met dit platform moet de informatiedeling op het gebied van cyberdreigingen en kwetsbaarheden tussen (vitale) bedrijven/organisaties en de overheid (inclusief inlichtingendiensten) verbeterd worden. In het Regeerprogramma is de ambitie uitgesproken om het platform in 2027 gerealiseerd te hebben.

Gezien de almaar toenemende digitale dreiging, met name vanuit statelijke actoren, is onze klemmende oproep om het platform Cyclotron versneld - dus eerder dan 2027 - te realiseren, in uiteraard nauwe samenwerking met het bedrijfsleven. Hierbij is het advies om te kijken naar de succesfactoren van het project Melissa waarin partijen zoals politie, Openbaar Ministerie, het Nationaal Cybersecurity Centrum en Cyberveilig Nederland succesvol samenwerken om ransomware te bestrijden. Alleen met een goede informatievoorziening vanuit de inlichtingendiensten over dreigingen en kwetsbaarheden kunnen bedrijven/organisaties tijdig de juiste tegenmaatregelen treffen ten einde de continuïteit van hun (vitale) diensten en daarmee van de samenleving te borgen.

2. Zorg ervoor dat het nieuwe Nationaal Cybersecurity Centrum herkenbaar blijft voor het mkb

Ambitie is dat eind 2025 de integratie van het Nationaal Cyber Security Centrum (NCSC), het Digitale Trust Center (DTC) en het CSIRT voor Digitale Dienstverleners gereed is. VNO-NCW en MKB-Nederland zien deze integratie als een positieve ontwikkeling met veel potentie om de cybersecuritykennis en -kunde in Nederland te bundelen en naar een hoger niveau te tillen. Hierbij dient wel één zeer belangrijk uitgangspunt voor ogen te worden gehouden: de nieuwe geïntegreerde organisatie moet herkenbaar zijn en blijven voor het mkb. Waar vitale aanbieders veelal behoefte hebben aan snelle levering van ruwe inlichtingeninformatie, hebben mkb-ondernemers behoefte aan concrete handelingsperspectieven en laagdrempelige tools, zoals nu op een pragmatische wijze door het DTC wordt gegeven. Mkb-ondernemers hebben immers vaak minder kennis en middelen om zich voldoende te wapenen tegen cybercriminelen en dienen dus op een andere wijze bediend te worden dan bijvoorbeeld (grote) vitale bedrijven. Het is dan ook van belang dat de huidige werkwijze van het DTC door de vernieuwde organisatie wordt overgenomen, inclusief de succesvolle DTC-Community, een laagdrempelig platform waar private- en publieke partners in alle openheid met elkaar in gesprek kunnen gaan over o.a. slachtofferschap van cyberaanvallen en de lessons learned.

3. Draag zorg voor opvolging van de aanbevelingen vanuit de cyberoefening ISIDOOR

Eind 2023 vond voor de vierde keer de nationale cyberoefening ISIDOOR IV plaats. Met 120 deelnemende organisaties vanuit de publieke- en private kant werd de onderlinge samenwerking, informatie-uitwisseling en opschaling van de nationale crisisstructuur beoefend. Het in PPS-verband doorleven van een cyber-crisisscenario en beoefenen van de crisisrepons is zeer waardevol. Wij pleiten ervoor dat dit in de toekomst wordt voortgezet waarbij ook wordt gekeken naar oefeningen voor specifiek mkb-bedrijven.
Het evaluatierapport van ISIDOOR IV bevat veel concrete en nuttige aanbevelingen. Wij pleiten ervoor dat de aanbevelingen ook daadwerkelijk worden opgepakt, met in het bijzonder de volgende twee zaken. De onderlinge informatievoorziening tussen sectoren en het Rijk ten tijde van een (dreigende) crisis moet verbeterd worden. Aan de de zijde van het bedrijfslevens is vooral behoefte aan een overkoepelend situatiebeeld van hoe Nederland er op dat moment voor staat. Dit in verband met ketenafhankelijkheden en effecten. Het NCSC die bij de individuele sectoren de beelden ophaalt, zou hier een rol in kunnen en moeten spelen. Daarnaast is gebleken dat het noodzakelijk is om te komen tot een afwegingskader bij schaarste aan hulp en bijstand. Bij (dreigende) grootschalige cyberincidenten/crises ontstaat er al snel filevorming bij het NCSC maar ook bij cybersecurity dienstverleners. Het is noodzakelijk dat wanneer de nationale veilighied in het geding is of dreigt te raken, de overheid over de juiste bevoegdheden beschikt om waar nodig te kunnen prioriteren, ook richting cybersecurity dienstverleners. Hierbij zou bv. kunnen worden gesteld dat essentiële aanbieders onder de komende Cyberbeveiligingswet met voorrang geholpen dienen te worden. In verband met een gelijk speelveld, zou dit idealiter op Europees niveau geregeld moeten worden.

4. Zorg voor een voortvarende en efficiënte implementatie van de NIS2-richtlijn met focus op lerend vermogen

VNO-NCW en MKB-Nederland zien de NIS2-richtlijn als belangrijke wetgeving om de digitale weerbaarheid van Europa te vergroten. Wij roepen onze leden sinds ruime tijd op om proactief aan de slag te gaan met de eisen uit de richtlijn. Op dit moment wordt door het Rijk hard gewerkt aan implementatie van de richtlijn, via de Cyberbeveiligingswet (Cbw). Wij pleiten voor een voortvarende en efficiënte implementatie en met name uitvoering van de richtlijn. Er zijn straks bedrijven/organisaties die als gevolg van hun activiteiten met twee verschillende toezichthouders voor hun zorg- en meldplicht onder de Cbw te maken krijgen. In het kader van de lastendruk aan zowel de zijde van bedrijven als de overheid, is het van groot belang dat dubbele toezichtlasten worden voorkomen. Uitgangspunt moet zijn dat één toezichthouder - daar waar het zwaartepunt van de essentiële processen ligt - de regie neemt en de andere toezichthouder informeert. Daarnaast geldt in algemene zin dat het in te richten toezicht transparant, redelijk en éénduidig moet zijn.
Een ander aandachtspunt is het implementatietermijn. De NIS2-richtlijn kent geen implementatietermijn. Zodra de Cbw van kracht gaat (verwachting is Q3 van dit jaar), dienen bedrijven/organisaties aan hun zorg- en meldplicht te voldoen. Dat is ook de reden waarom wij onze leden oproepen om nu al aan de slag te gaan. Echter, een aantal zaken is nog onduidelijk, waaronder de exacte reikwijdte van de Cbw. Dit geldt met name voor bedrijven/organisaties met complexe bedrijfsstructuren. Daarnaast wordt de zorgplicht op dit moment nader uitgewerkt in de AMvB onder de Cbw. De precieze eisen zijn nu dus nog niet geheel duidelijk. Wij gaan ervan uit dat betrokken toezichthouders hier rekening mee houden. Dit betekent concreet dat zodra de wet van kracht gaat, vanuit het toezicht wordt ingezet op lerend vermogen (en niet tot het direct opleggen van sancties) en - analoog aan de werkwijze in omliggende landen - bedrijven /organisaties de benodigde tijd krijgen voor het behalen van certificaten en het uitvoeren van audits als bewijsvoering voor het nakomen van hun zorgplicht.

5. Implementeer alle komende wetgeving en acties op het gebied van cybersecurity alvorens tot nieuwe te komen

Afgelopen tijd is op het gebied van cybersecurity een flinke inhaalslag gemaakt ten aanzien van wet- en regelgeving op het gebied van cybersecurity. De ambitie van de Europese Commissie is zichtbaar. De Cyber Resilience Act (CRA), Radioapparatenrichtlijn, Cybersecurity Act (CSA), NIS2-richtlijn, en de Digital Operational Resilience Act (DORA) zijn enkele voorbeelden.
VNO-NCW en MKB-Nederland zien van veel van deze wetten en regels de meerwaarde in: Europa is kwetsbaar en de cyberweerbaarheid moet - vooral in het licht van de huidige geopolitieke situatie - in de hele EU naar een hoger niveau. Tegelijkertijd moet er ook ruimte zijn voor een goede- en samenhangende implementatie van wet- en regelgeving, en voor evaluatie. Wij pleiten er dan ook voor om de wetgeving die nu in de pijplijn zit eerst goed te implementeren en evalueren alvorens met nieuwe/aanvullende wetgeving te komen. Daarnaast is het van belang dat kleine en micro-bedrijven ondersteuning vanuit de overheid krijgen. Hierbij gaat het bv. om vereenvoudigde technische documentatie bij implementatie van de CRA voor veiligere digitale producten.

Ik hoop u hiermee voldoende te hebben geïnformeerd. Mocht u nog vragen hebben, dan kunt u contact opnemen met beleidssecretaris Sabine Gielens van VNO-NCW en MKB-Nederland, gielens@vnoncw-mkb.nl.

Met vriendelijke groet,

drs. F.W. Vijselaar
Algemeen directeur VNO-NCW

L.J. Visser
Algemeen directeur MKB-Nederland