Ministerie van Economische Zaken

> Retouradres Postbus 20401 2500 EK Den Haag

Cyber Security Raad
Postbus 20301
2500 EH DEN HAAG

**Directoraat-generaal Economie en Digitalisering**
Directie Digitale Economie

**Bezoekadres**
Bezuidenhoutseweg 73
2594 AC Den Haag

**Postadres**
Postbus 20401
2500 EK Den Haag

**Overheidsidentificatienr**
00000001003214369000

T 070 379 8911 (algemeen)
F 070 378 6100 (algemeen)
www.rijksoverheid.nl/ez

**Behandeld door**
[redacted]

**Ons kenmerk**
DGED-DE / 89956703

Datum 25 november 2024
Betreft Beleidsreactie CSR advies 'Verkleinen van de Cyberweerbaarheidskloof'

Geachte co-voorzitters,

Hierbij bied ik u mede namens de minister van Justitie en Veiligheid (JenV) de beleidsreactie aan op het advies van de Cyber Security Raad (CSR) 'Verkleinen van de Cyberweerbaarheidskloof'. Op 4 juni jl. heeft de CSR het adviesrapport overhandigd aan de toenmalig minister van Economische Zaken en Klimaat, Micky Adriaansens.[1] In deze beleidsreactie wordt nader ingegaan op welke wijze vanuit de ministeries Justitie en Veiligheid (JenV) en Economische Zaken (EZ) invulling zal worden gegeven aan de aanbevelingen die gedaan zijn door de CSR om de cyberweerbaarheidskloof te verkleinen bij het midden- en kleinbedrijf (mkb).

De minister van JenV en ik bedanken de CSR voor dit advies. Het mkb is de motor van de Nederlandse economie. Daarmee is de digitale weerbaarheid van het mkb essentieel voor het verdienvermogen van Nederland. Daarmee is het een belangrijk onderwerp voor de raad om aandacht aan te besteden. Het gesignaleerde beeld dat er grote verschillen zijn tussen bedrijven die hun cyberweerbaarheid op orde hebben en achterblijvers bij wie dit nog niet het geval is, is herkenbaar. In met name het mkb zijn relatief veel achterblijvers. Publiek-private samenwerking is daarbij de hoeksteen van de aanpak. Door niet alleen voor, maar ook mét ondernemers te werken kunnen we gezamenlijk stappen zetten. In de op 28 oktober jl. gepubliceerde Voortgangsrapportage Nederlandse Cybersecuritystrategie (NLCS) 2024 is het belang hiervan ook door het kabinet onderstreept.[2] De aanbevelingen in het advies spreken ons aan. Wij zien dit als een bevestiging van de reeds ingezette publiek-private koers. Het is goed om op basis van een extern adviesrapport te constateren dat wij geen grote thema's over het hoofd zien. Het advies bevat suggesties voor vervolgstappen die wij aan boord willen nemen. Daarbij ook de uitnodiging om ons de komende jaren in CSR-verband scherp te houden op nieuwe ontwikkelingen zodat het overheidsbeleid daarop in kan blijven spelen. Het cybersecurity landschap is per slot van rekening continu aan verandering onderhevig.

[1] https://www.cybersecurityraad.nl/actueel/nieuws/2024/06/05/minister-verwelkomt-advies-cyberweerbaarheid-mkb.
[2] Kenmerk 2024Z17074.

**Directoraat-generaal**
**Economie en Digitalisering**
Directie Digitale Economie

**Ons kenmerk**
DGED-DE / 89956703

Als opvolging op het CSR-advies is op 24 oktober jl. is in samenwerking met de CSR een publiek-private bijeenkomst georganiseerd, waarin de adviezen van de CSR, de lopende initiatieven vanuit de overheid en de eventuele witte vlekken zijn besproken. Tijdens de bijeenkomst is aan de hand van drie thema's – het cyberweerbaarheidsnetwerk, de harmonisatie van hulpmiddelen en de behoeften rondom standaarden, keurmerken en wetgeving – met vertegenwoordigers van de overheid, intermediaire organisaties, kennisinstellingen en het bedrijfsleven een constructief gesprek gevoerd over gezamenlijke wensen en behoeften. Tijdens deze bijeenkomst is aangegeven dat veel van de CSR-adviezen en lopende initiatieven voor de aanwezige partijen herkenbaar waren. Ook zijn er verschillende waardevolle suggesties geopperd die in deze beleidsreactie zijn meegenomen.

**Leeswijzer**
Deze brief geeft allereerst een overzicht van de drieledige hoofdlijnen van het CSR advies, alvorens de concrete aanbevelingen worden uiteengezet. Vervolgens wordt ingegaan op de aanbevelingen en de opvolging daarvan.

**CSR-Advies inzake de cyberweerbaarheid van het Nederlandse mkb**
De hoofdlijnen van het CSR advies luidden als volgt:

1. Realiseer een gerichte, structurele en uniforme aanpak om de cyberweerbaarheid van het mkb te verbeteren. Vanuit publiek-privaat partnerschap en onder regie van de Rijksoverheid kan hiermee meer samenhang tussen verschillende initiatieven ontstaan. Ook kan zo de samenwerking binnen de verschillende netwerken en tussen netwerken onderling worden vergroot.
2. Zorg voor passende hulpmiddelen voor het mkb via bekende en toegankelijke kanalen, om elke organisatie in staat te stellen een optimaal cyberweerbaarheidsniveau te bereiken. Die hulpmiddelen variëren van basismaatregelen en metrieken voor het in kaart brengen van weerbaarheidsniveaus, tot hulp bij de uitvoering van risicoanalyses.
3. Stimuleer bedrijven om hun cyberweerbaarheid te verhogen en maatregelen te (laten) nemen ter verbetering. Maak daarbij gebruik van de genoemde aanpak, aangeboden hulpmiddelen en bestaande producten van ICT- en telecomleveranciers. Aankomende EU-wetgeving heeft daarbij weliswaar een aanjagende werking, maar heeft slechts op een gedeelte van het mkb betrekking.

Langs deze drie hoofdlijnen geeft de raad een aantal algemene adviezen voor verbetering.

De raad adviseert in het kader van een *gerichte, uniforme, structurele aanpak* aan de ministers JenV en EZ gezamenlijk:

1. Werk vanuit de huidige samenwerking van het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC) en het Computer Security Incident Response Team voor digitale diensten (CSIRT-DSP) stapsgewijs toe naar één loket en kenniscentrum in de nieuwe organisatie, dat ook gerichte ondersteuning aan het mkb biedt. Stimuleer daarbij ook doelwit- en

slachtoffernotificatie voor het mkb en het doen van meldingen en/of aangiften. Geef extra aandacht aan een adequate inzet van middelen hiervoor.
2. Bundel de krachten van organisaties via uitbouw van het 'netwerk van netwerken' in publiek-private samenwerking (waarbij groot klein helpt) en geef daarin ook vertrouwde partners van het mkb een plek, zoals accountants en de Kamer van Koophandel (KvK). Naast de ontwikkeling van informatie- en kennisproducten voor het mkb is het gebruik van standaard beschikbare oplossingen van ICT- en telecomleveranciers cruciaal.
3. Initieer vanaf 2025 een jaarlijkse meting van de cyberweerbaarheid van het mkb en het effect van genomen maatregelen en initiatieven. Maak daarbij gebruik van de recent gepubliceerde nulmeting en koppel dit ook aan de jaarlijkse voortgangsrapportage van de NLCS. Ga daarbij specifiek in op de acties die betrekking hebben op het mkb.

De raad adviseert in het kader van het aanbieden van *passende hulp*:

Aan de ministers van JenV en EZ gezamenlijk:
4. Geef de nieuwe centrale fusieorganisatie het voortouw om in publiek-private samenwerking het aanbod van hulpmiddelen ter verhoging van de cyberweerbaarheid beter af te stemmen op de behoefte van het mkb. Laat dit in overleg met onder andere MKB-Nederland oppakken. Zet voor eind 2024 een harmonisatie daarvan in gang, gericht op een beperking van het huidige aantal verschillende hulpmiddelen.
5. Werk op vrijwillige basis toe naar standaardisatie van hulpmiddelen en maak deze zo laagdrempelig mogelijk. Daarvoor zijn verschillende mogelijkheden, zoals CyRa (Cyber Rating). Stimuleer ook het gebruik van bestaande OT-standaarden en de generieke ISO27001 beveiligingsstandaard (als mogelijke top-up op CyRa), en meet de effectiviteit van deze hulpmiddelen. Houd hierbij rekening met (toekomstige) EU-keurmerken en implementeer zo spoedig mogelijk aankomende EU-regelgeving voor veilige producten en diensten.
6. Stimuleer het gebruik van (gedifferentieerde) hulpmiddelen en het nemen van basismaatregelen binnen sectoren. Een toegankelijke handreiking gericht op brancheorganisaties is daarvoor essentieel. Dit geldt ook voor de beveiliging van Operationele Technologie (OT)-systemen[3] binnen het mkb; baseer deze zoveel mogelijk op standaard beschikbare oplossingen. Maak hierbij gebruik van bestaande samenwerkingsverbanden.

Aan de minister van EZ:
7. Zie erop toe dat de al in gang gezette ontwikkeling van een kwaliteitskeurmerk voor ICT-leveranciers (in samenwerking met het DTC en brancheorganisaties) wordt geëffectueerd, inclusief cybersecurityeisen, en dat het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) de uitvoering daarvan voortvarend ter hand neemt. Harmoniseer indien mogelijk een dergelijk keurmerk met toekomstige EU-ontwikkelingen op dit gebied.

[3] Ofwel Industrial and Automation Control Systems, IACS.

De raad adviseert in het kader van *het stimuleren en aanzetten tot handelen*:

Aan de ministers van JenV en EZ gezamenlijk:

8. Overweeg de start van een brede maatschappelijke publiekscampagne in samenwerking met private partijen. De overkoepelende boodschap is daarbij dat ook ondernemers zich moeten aanpassen aan de verder digitaliserende samenleving, met cybersecurity als belangrijk aandachtspunt. Maak daarbij ook gebruik van het TNO-onderzoek 'Veilig Digitaal Ondernemen' om gedrag effectief te kunnen beïnvloeden.
9. Zet in op een tijdige doorvertaling van de nieuwe Netwerk en Informatiebeveiligingsrichtlijn (NIS2-richtlijn) in Nederland en stimuleer specifiek het mkb in het nemen van maatregelen om aan deze eisen te kunnen voldoen. Geef daarbij ook aandacht aan bedrijven die niet vallen onder de huidige Wet bescherming netwerk- en informatiesystemen (Wbni) of toekomstige NIS2, waarbij de aanstaande wetgeving (Wet bevordering digitale weerbaarheid bedrijven (Wbdwb))[4] voor informatiedeling en ondersteuning als uitgangspunt geldt.

**Beleidsreactie op de aanbevelingen**
In deze brief zal op volgorde op de verschillende aanbevelingen worden ingegaan.

**Aanbeveling 1, 2 en 3** in het kader van een *gerichte, uniforme, structurele aanpak*

*Eén loket: Integratie van het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC) en het Computer Security Incident Respons Team voor digitale diensten (CSIRT-DSP)*
De ingezette integratie van het NCSC, het DTC en het CSIRT-DSP zal in de toekomst zorgen voor één loket voor alle bedrijven. De organisaties werken al nauw samen en de integratie richting één organisatie op 1 januari 2026 ligt op schema. Tijdens de workshop op 24 oktober jl. is meegegeven dat het van belang is dat de vernieuwde NCSC organisatie op basis van behoefte werkt en zorgt voor goede aansluiting tussen partners en producten. Meer concreet moet de vernieuwde NCSC-organisatie herkenbaar zijn en blijven voor het mkb, de huidige DTC-community behouden blijven en uitgebreid worden. Daarbij dient de vernieuwde organisatie in te spelen op de specifieke behoeften van het mkb, namelijk, het bieden van concrete adviezen met handelingsperspectief. Deze input nemen we ter harte. Het centraal stellen van de doelgroep is één van de leidende principes van de vernieuwde organisatie. Tegelijkertijd blijft de winkel open tijdens de verbouwing. Hierbij dan ook de uitnodiging aan het bedrijfsleven om ons scherp te houden in de dagelijkse samenwerking en in de CSR.

*Netwerk van netwerken: toekomstvisie Cyberweerbaarheidsnetwerk en Cyclotron*
De kabinetsvisie op de tweede aanbeveling om een 'netwerk van netwerken' uit te bouwen op het gebied van publiek-private samenwerking is eerder dit jaar uitgewerkt in de toekomstvisie op de doorontwikkeling van het Landelijk Dekkend

[4] De Wet bevordering digitale weerbaarheid bedrijven is per 1 oktober 2024 in werking getreden.

Stelsel tot het Cyberweerbaarheidsnetwerk.[5] Deze toekomstvisie dient als basis voor het uit te werken bouwplan voor de publiek-private samenwerking ten behoeve van het verhogen van de cyberweerbaarheid van organisaties. Op 11 september en 22 oktober jl. hebben de eerste twee publiek-private bijeenkomsten plaatsgevonden om het bouwplan verder uit te werken. Het netwerk van meer dan 60 samenwerkingsverbanden van het DTC wordt hierin ook meegenomen. Het DTC zal in 2025 een verkenning starten om de contacten met de door de CSR genoemde intermediairs zoals brancheorganisaties, banken, boekhouders of accountants meer te benutten en te faciliteren. Zij kunnen een extra bijdrage leveren aan de cyberweerbaarheid van hun klanten, veelal mkb-bedrijven. In de workshop van 24 oktober jl. is naar voren gekomen dat het zinvol en effectief is om de bestaande contactpunten die kleine ondernemers hebben aan te grijpen om hen te wijzen op de noodzaak van cyberweerbaarheid en handelingsperspectief te bieden. Naast de brancheorganisatie zou dat de KvK, boekhouder, accountant, financieel adviseur, bank enzovoort kunnen zijn. Deze mogelijkheid wordt ook meegenomen en verkend. Er wordt ook gekeken naar het betrekken van lokale partijen en initiatieven, welke een belangrijke rol kunnen hebben in het versterken van de cyberweerbaarheid van het mkb. De bestaande samenwerking tussen het DTC en de KvK wordt voortgezet en er wordt blijvend gezocht naar innovatieve mogelijkheden om cybersecurity dicht bij de ondernemer te krijgen.

Daarnaast wordt door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het NCSC gewerkt aan het programma Cyclotron. Cyclotron is een publiek-privaat samenwerkingsplatform waar de politie, de diensten, het Openbaar Ministerie, het bedrijfsleven en de wetenschap aan deelnemen. Het doel is om op grotere schaal publiek-private informatie te delen, te analyseren en samen te werken, om gezamenlijk meer grip te krijgen op cyberdreigingen. Meer partijen kunnen zo profiteren van schaarse kennis en expertise, waaronder laagvolwassen en hoog volwassen organisaties. Het Cyclotron distributie- en communicatiecentrum is bij uitstek gericht om producten te ontwikkelen die relevant zijn voor minder volwassen bedrijven.

*Meting cyberweerbaarheid en evaluatie Nederlandse Cybersecuritystrategie*
De derde aanbeveling om jaarlijks metingen te doen landt op dit moment op twee verschillende plekken. Eén van de manieren om zicht te krijgen op het huidige cyberweerbaarheidsniveau is het in kaart brengen van de cybermaatregelen voor een groep bedrijven.[6] Het Centraal Bureau voor de Statistiek (CBS) rapporteert jaarlijks middels de Cybersecuritymonitor over de meest actuele stand van zaken rond de cyberweerbaarheid van bedrijven en huishoudens in Nederland. Dat gebeurt hoofdzakelijk met CBS-cijfers over het aantal cybercrime-gerelateerde incidenten en de maatregelen die genomen worden om deze incidenten te voorkomen. Het overzicht van ICT-veiligheidsmaatregelen en -incidenten van Nederlandse bedrijven wordt uitgesplitst naar bedrijfsgrootte (waaronder het mkb) en bedrijfstak. De meest recente cybersecuritymonitor is gepubliceerd op

[5] https://www.nctv.nl/documenten/publicaties/2024/05/23/toekomstvisie-cyberweerbaarheidsnetwerk.
[6] Deloitte, Cyberweerbaarheidskloof. Aanbevelingen voor een cyberweerbaar mkb en het verkleinen van de cyberweerbaarheidskloof in Nederland, § 2.2.1.

28 juni 2024.[7] In deze meting ziet het CBS dat kleinere bedrijven minder cyberweerbaar zijn dan grote bedrijven. Op alle uitgevraagde (basis)maatregelen nemen kleine bedrijven minder actie dan grote bedrijven en dat maakt hen kwetsbaarder voor cyberincidenten. Naast de Cybersecuritymonitor doet het Wetenschappelijk Onderzoek- en Datacentrum momenteel in opdracht van het ministerie van JenV onderzoek naar mogelijke 'cybersecurity meetlatten'. Het uiteindelijke doel is om de weerbaarheid van organisaties in Nederland en het effect van beleid hierop beter te kunnen meten. Hierbij wordt ook gekeken naar mkb.

De tweede meting wordt uitgevoerd in het kader van de NLCS. De strategie is in 2022 opgesteld en zet uiteen hoe de betrokken publieke, private en wetenschapspartijen in zes jaar gezamenlijk toewerken naar een digitaal veilig Nederland. Deze inzet is concreet gemaakt in een onderliggend actieplan.[8] Een nulmeting heeft voor de NLCS inzichtelijk gemaakt wat de uitgangssituatie was voordat er met de strategie werd gestart en vormt de basis voor een tussentijdse evaluatie in 2025 en een eindevaluatie in 2028.[9]

**Aanbeveling 4, 5, 6 en 7** in het kader van het aanbieden van *passende hulp*

*De harmonisatie van hulpmiddelen ter verhoging van de cyberweerbaarheid*
Vanuit het DTC worden verschillende generieke producten aangeboden die bedrijven uit alle sectoren kunnen gebruiken om stappen te zetten ter verhoging van hun cyberweerbaarheid. Enkele voorbeelden zijn de Cyberveiligcheck voor zzp en mkb, de cyberoefengame met een ransomware scenario en veel verschillende informatieve webpagina's met handige tips om ondernemers (verder) op weg te helpen. Deze producten worden waar mogelijk in samenwerking met de doelgroep ontwikkeld om deze zo goed mogelijk aan te sluiten bij hun behoeften. Deze producten kunnen sectorspecifiek worden gemaakt. Hierbij is altijd kennis en expertise vanuit de sector vereist, welke voor een deel ligt bij de verschillende vakdepartementen, maar bijvoorbeeld ook bij brancheorganisaties. Ik nodig de partijen die behoefte hebben aan sectorspecifieke varianten uit om samen op te trekken. In termen van harmonisatie van hulpmiddelen worden in de aanloop naar de vorming van de vernieuwde NCSC-organisatie tools en producten steeds meer in nauwe samenwerking ontwikkeld. Een concreet voorbeeld hiervan is het samenvoegen van de verschillende basisprincipes voor de digitale weerbaarheid van organisaties tot één set aan basisprincipes.[10] De insteek hierbij is behoefte gestuurd te werk te gaan waarbij publiek-private samenwerking met partners zoals VNO-NCW en MKB-Nederland en gezamenlijke communicatie een belangrijke rol spelen. Het NCSC en het DTC zullen in 2025 samen kijken waar door gezamenlijke communicatie nog meer winst te behalen valt. De vraag om het concreet en praktisch toepasbaar te maken voor de ondernemer, bijvoorbeeld door het gebruik van templates, wordt daarin meegenomen.

---

[7] CBS, Cybersecuritymonitor 2023, 28 juni 2024.
[8] https://www.rijksoverheid.nl/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022---2023.
[9] Kamerstuk 5187852.
[10] https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen.

Daarnaast blijft het DTC zoeken naar mogelijkheden om hulpmiddelen op een laagdrempelige manier gedifferentieerd aan te bieden om zo het nemen van basismaatregelen binnen alle sectoren te stimuleren. Zo is het afgelopen jaar in samenwerking met de cultuursector een specifieke versie van de CyberveiligCheck ontwikkeld.[11] Voor dit soort samenwerkingen wordt ook gekeken naar het gebruik van bestaande DTC-samenwerkingsverbanden.

*Standaardisatie van hulpmiddelen*
Standaarden en keurmerken zijn primair instrumenten van de markt en er is veel waardering voor initiatieven uit het bedrijfsleven. Het zijn belangrijke instrumenten en het kabinet wil de ontwikkeling daarvan in het cybersecuritydomein stimuleren. Zo is de ontwikkeling van bijvoorbeeld het certificeringsmodel CyRa[12] financieel ondersteund met een subsidie vanuit het DTC. Echter, tijdens de bijeenkomst op 24 oktober jl. werd aangegeven dat een certificering als CyRa of een standaard als ISO27001 niet altijd voor het mkb toegankelijk en/of noodzakelijk is. De noodzaak is bijvoorbeeld afhankelijk van het risicoprofiel van de mkb-er en de bedrijven aan wie zij producten en diensten leveren. Er werd benadrukt dat eisen die NIS2-bedrijven/organisaties aan hun directe leveranciers gaan stellen, proportioneel en risico-gebaseerd moeten zijn. In het algemeen heeft het mkb veelal behoefte aan een lager instapniveau dan bovengenoemde standaarden, van waaruit ze (met hulp) verder kunnen groeien. Het DTC zal kijken op welke manier deze hulp mogelijk is.

In het kader van de uitvoering van de motie Rajkowski[13] wordt door het CCV publiek-privaat een keurmerk ontwikkeld voor ICT-dienstverleners ten behoeve van het mkb.[14] Dit keurmerk moet afnemers (mkb) een bepaalde mate van zekerheid geven. Bijvoorbeeld dat de gekozen ICT-dienstverlener betrouwbaar is, kwaliteit levert bij implementatie van basismaatregelen en gekwalificeerd is om bij te dragen aan de vormgeving van het cybersecurity-beleid. Het project wordt uitgevoerd met als doel het gemiddelde niveau van cybersecurity bij het mkb te verhogen. De ontwikkeling van het keurmerk verloopt conform de planning en wordt het naar verwachting eind 2025 afgerond.[15] In de workshop van 24 oktober jl. kwam naar voren dat een dergelijk keurmerk positief wordt ontvangen.

Daarnaast is belangrijk te voorkomen dat er een wildgroei ontstaat aan cyberbeveiligingscertificaten binnen de cybersecuritymarkt. Naast goede nationale initiatieven is het daarom belangrijk om de pijlen primair te richten op aansluiting op huidige en toekomstige Europese ontwikkelingen op het gebied van standaarden en certificering. 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. Immers, de huidige Europese markt

---

[11] https://tools.digitaltrustcenter.nl/cyberveilig-check-voor-cultuur/.
[12] https://cyberrating.nl/.
[13] Kamerstuk 36200 VII, nr. 60.
[14] Het CCV heeft ook met een subsidie van het ministerie van EZ en JenV in 2021 publiek-privaat een keurmerk ontwikkeld en gelanceerd voor pentesten (een cybersecuritydienst).
[15] kenmerk 2024Z17074, § II.1.3.

op het gebied van cyberbeveiligingscertificaten is versnipperd wat leidt tot wildgroei en fragmentatie. Dat is ook een van de redenen waarom er op Europees niveau de Cybersecurity Act (Cyberbeveiligingsverordening, CSA) tot stand is gekomen. De CSA verordening 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 cyberveiligheid in Europa aan te jagen en tegelijkertijd de (digitale) interne markt te versterken. Maar het omgekeerde kan gelden: nationale initiatieven kunnen, indien succesvol, op hun beurt weer waardevolle inspiratie zijn voor de Europese standaarden en certificeringsschema's van de toekomst. Daarom moeten nationale initiatieven goed aansluiten op het Europese raamwerk. Dat helpt om publiek en privaat goede Nederlandse initiatieven naar Europa te brengen zodat zij toekomstige Europese certificeringsschema's kunnen inspireren. De ervaring is dat Nederland goed is gepositioneerd in Europa om deze rol te vervullen.

**Aanbeveling 8 en 9** in het kader van *het stimuleren en aanzetten tot handelen*

*Brede maatschappelijke publiekscampagnes*
Op dit moment loopt er geen brede maatschappelijke publiekscampagne voor bedrijven met een overkoepelende boodschap die raakt aan de steeds verder digitaliserende samenleving waarmee ondernemers te maken krijgen, met cybersecurity als belangrijk aandachtspunt. Het DTC zet op dit moment in op meer gerichte campagnes om ondernemers te bereiken. Daarnaast komen in cybersecuritymaand oktober onder de vlag van Alert Online alle cybersecurityinitiatieven bij elkaar. Een netwerk van ruim 200 partners organiseert in oktober activiteiten gericht op hun klanten, medewerkers of achterban. Ten aanzien van grootschalige publiekscampagnes wordt vanuit de Rijksoverheid in breder verband ingezet op publiekscampagnes gericht op de digitale weerbaarheid van burgers. Voorbeelden zijn de campagnes 'Doe Je Updates' en 'Laat je niet interneppen'. De ervaring met het opzetten en uitvoeren van grootschalige publiekscampagnes is dat één boodschap zeer gericht moet zijn en over een langere tijd moet worden herhaald. Achter een (voor de cybersecurityprofessional) simpele slogan gaat voor de doelgroep van een campagneboodschap een complexere reeks communicatieve stappen schuil die mensen moet activeren op kennis, houding en gedrag. In het relatief onbekende cybersecuritydomein moet een campagne ook eerst meer kennis overbrengen over zaken in de digitale wereld dan bekende zaken in de fysieke wereld voordat de doelgroep wordt geactiveerd op het uiteindelijke doel van gedragsverandering. Ter illustratie, de achterliggende communicatieve stappen van de publiekscampagne 'Doe je updates' voor burgers bestaan uit: 1) wat is een slim apparaat? (kennis), 2) welke slimme apparaten heb ik in huis? (kennis), 3) wat is een update? (kennis), 4) waarom is dit belangrijk? (houding), en 5) hoe moet ik dat doen? (gedrag).

Doordat het mkb een erg diverse groep is, zal overheidscommunicatie vanuit een grootschalige publiekscampagne gericht op het mkb naar verwachting een zeer gering resultaat overleveren ten opzichte van de significante investering van

financiële middelen. Ook is tijdens de workshop van 24 oktober jl. geconcludeerd dat een meer gerichte campagne een beter effect zal geven dan een brede en grootschalige publiekscampagne. Het DTC onderzoekt daarom een campagnevorm die partijen meer mobiliseert en faciliteert. Onder de kapstok van een grote gestructureerde campagne waarbij een boodschap uitgedragen wordt, maar waarbij gebruik wordt gemaakt van de intermediair, zoals brancheorganisaties, banken, boekhouders of accountants, die dichter bij de ondernemer staan als vehikel om de boodschap over te brengen. Deze aanpak sluit aan op de door TNO gepubliceerde resultaten in hun onderzoek veilig digitaal ondernemen[16] en is ook tijdens de workshop van 24 oktober jl. veelvuldig genoemd. Door het betrekken van een partij die dicht bij de ondernemer staat, zoals de eerder genoemde brancheorganisaties, banken, boekhouders of accountants, kunnen ondernemers beter gemobiliseerd en gefaciliteerd worden.

*Implementatie van de NIS2-richtlijn en de Wet bevordering digitale weerbaarheid bedrijven*
Op 16 oktober jl. heeft de minister van JenV de Kamer geïnformeerd over de laatste stand van zaken rondom de implementatie van de NIS2-richtlijn (en de richtlijn weerbaarheid kritieke entiteiten (de CER-richtlijn) in de Cyberbeveiligingswet (Cbw).[17] Het streven is dat beide wetten in het derde kwartaal van 2025 in werking treden. Op de DTC website kunnen bedrijven meer informatie vinden over de NIS2-richtlijn,[18] ook biedt het DTC ondernemers en professionals de mogelijkheid om vragen over NIS2 te stellen via de DTC Community en de NIS2-samenwerkruimte.[19] De NCTV en het NCSC hebben daarnaast een pagina ingericht met de meest gestelde vragen en antwoorden over de Cyberbeveiligingswet. Die pagina krijgt een update wanneer meer informatie voor handen is.[20]

De DTC website biedt ook voor bedrijven die niet onder de huidige Wbni of toekomstige Cbw gaan vallen veel informatie en verschillende tools, welke veelal gericht zijn op het op orde krijgen van de basis op het gebied van cybersecurity. Hiernaast ontvangt het DTC dagelijks informatie over kwetsbare of gehackte systemen. Als deze informatie na controle wordt ingeschat als waardevol voor een Nederlands bedrijf, gaat het DTC over tot waarschuwen (notificeren) zodat het bedrijf hierop actie kan ondernemen. Dit houdt in de meeste gevallen in dat een e-mailbericht wordt verzonden naar het bedrijf. Als de informatie niet te herleiden is tot een specifiek bedrijf, dan wordt de netwerkeigenaar op de hoogte gebracht. In 2023 is er op deze manier ruim 140.000 keer genotificeerd, in 2024 staat de teller op ruim 150.000 notificaties.[21] Sinds 1 oktober 2024 is deze taak wettelijk verankerd in de Wet bevordering digitale weerbaarheid bedrijven.

---

[16] https://www.digitaltrustcenter.nl/sites/default/files/2024-05/TNO_2024_Veilig_digitaal_ondernemen_0.pdf.
[17] Kenmerk 2024Z16101.
[18] https://www.digitaltrustcenter.nl/nis2/startpunt.
[19] https://www.digitaltrustcenter.nl/community.
[20] https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/vragen-en-antwoorden.
[21] https://www.digitaltrustcenter.nl/dreigingsinformatie-ontvangen.

**Directoraat-generaal**
**Economie en Digitalisering**
Directie Digitale Economie

**Ons kenmerk**
DGED-DE / 89956703

**Tot slot**

Bovenstaande laat zien dat er al veel initiatieven lopen, maar ook dat er nog kansen zijn om de cyberweerbaarheid van bedrijven verder te versterken en de cyberweerbaarheidskloof te verkleinen. Vanuit onder meer het Actieprogramma Veilig Ondernemen 2023-2026 werken het DTC, het ministerie van EZ en het ministerie van JenV ook structureel samen met de politie en het bedrijfsleven om de cyberweerbaarheid van het mkb te verhogen. Het speelveld is blijvend in beweging en daardoor zal vraag en aanbod continu gemonitord moeten worden. De ingeslagen weg om in publiek-privaat verband verder te blijven werken aan het verhogen van de digitale weerbaarheid van het mkb wordt daarom doorgezet.

Dirk Beljaarts
Minister van Economische Zaken