Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 980

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 23 februari 2023

Zoals toegezegd in mijn Kamerbrief van 7 februari 2022 (Kamerstuk 26 643, nr. 817), informeer ik u hierbij over de voortgang van het Digital Trust Center (DTC) en de realisatie van de gestelde doelen.

In deze brief wordt achtereenvolgens ingegaan op de toezeggingen uit voornoemde Kamerbrief, alsmede de voortgang van de informatiedienst, de integratie van het DTC, het CSIRT voor digitale diensten (CSIRT-DSP) en het Nationaal Cyber Security Centrum (NCSC), het wetsvoorstel bevordering digitale weerbaarheid bedrijven en de moties van het lid Rajkowski over een mkb-keurmerk[1] en een structurele cyberoefenagenda[2] voor het niet-vitale bedrijfsleven. Daarnaast zal er aandacht worden besteed aan de ambities van het DTC voor het komende jaar.

Het DTC levert met haar activiteiten tevens een bijdrage aan diverse actiepunten zoals genoemd in het Actieplan (pijler 1) behorende bij de Nederlandse Cybersecurity Strategie (NLCS)[3] en in de Strategie Digitale Economie (pijler 5)[4]. U zult in het najaar integraal worden geïnformeerd over de voortgang van de NLCS en over de voortgang van de Strategie Digitale Economie.

Resultaten 2022

De missie van het DTC om ondernemend Nederland cyberweerbaar te maken is ook in 2022 onverminderd aan de orde. Met de hoofdtaken informatie en advies, en het aanjagen van samenwerking als vaste ankerpunten, lag de focus dit jaar op het door ontwikkelen en opschalen van de DTC-dienstverlening voor het niet-vitale bedrijfsleven in

[1] Kamerstuk 36 200 VII, nr. 60.
[2] Kamerstuk 36 200 VII, nr. 61.
[3] Kamerstuk 26 643, nr. 925.
[4] Kamerstuk 26 643, nr. 941.

kst-26643-980
ISSN 0921 - 7371
's-Gravenhage 2023

Nederland. In de bijlage bij deze brief wordt schematisch een overzicht gegeven van de gestelde en behaalde doelen en de ambities voor het komende jaar.

Vergroten bereik en interactie

Om de cyberweerbaarheid van ondernemend Nederland te vergroten, is het allereerst van belang te zorgen dat het nut en de noodzaak van cyberweerbaarheid onder de aandacht wordt gebracht van de doelgroep van het DTC. Daarom zet het DTC zich in om het bereik van haar communicatiekanalen te laten groeien. Ook in het afgelopen jaar is het aantal bezoekers op de website van het DTC toegenomen, waarbij duidelijk een piek wordt gezien in het aantal bezoekers bij cyberincidenten. Een voorbeeld hiervan waren de kritieke kwetsbaarheden in Microsoft Windows in januari 2022. Ook de campagne om security.txt te promoten als standaard voor het melden van cyberincidenten zorgde voor een piek. Over deze campagne leest u meer onder de kop «informatiedienst».

Het streven voor 2022 was in totaal 230.000 bezoeken. Met meer dan 260.000 websitebezoeken is deze doelstelling ruimschoots gehaald. Voor het komende jaar wordt ingezet op 300.000 bezoeken. Dit aantal is niet een doel op zich, maar wel een belangrijk meetinstrument om te bepalen hoeveel ondernemers bereikt kunnen worden. Het DTC gaat daarom de website verder optimaliseren en verrijken met informatie en advies. Hierbij is het van belang dat bezoekers snel inzicht en antwoorden krijgen op de vragen die ze hebben om hun cyberweerbaarheid te vergroten.

Ook het bereik op de sociale mediakanalen LinkedIn en Twitter is verder gegroeid. In totaal mag het DTC hiermee rekenen op meer dan 10.000 volgers.

Wat opvalt in de statistieken is dat de persoonlijke verhalen en adviezen van ondernemers die te maken hebben gehad met een cyberincident veel worden gelezen en reacties oproepen op social media. Ook het komende jaar zetten we daarom in op het aan het woord laten van ondernemers.

De groei van de DTC community, welke in 2021 in gang is gezet, heeft in 2022 doorgezet. Het totaal aantal leden op de community stond eind 2022 op 1.608 leden. Hiermee is de target van 1.000 leden ruimschoots gehaald. Ook stijgt de activiteit op de community. Zo zijn er vele discussies gestart en blogs geschreven. Voor het komende jaar wordt gestreefd naar 2.000 leden.

Waar eind 2021 het DTC een webinar over de Log4j actualiteit organiseerde, heeft het dit jaar een webinar verzorgd over de cyberrisico's die de oorlog in Oekraïne met zich mee brengt. Hierin is samengewerkt met het NCSC. Het webinar is ruim 4.500 keer bekeken en ook voor het komende jaar zullen we deze manier van informatievoorziening inzetten bij dergelijke actualiteiten.

Hoewel het vergroten van cyberweerbaarheid start met het bereiken van de doelgroep, is het uiteraard cruciaal om de bedrijven vervolgens daadwerkelijk aan de slag te laten gaan met cybersecurity. Belangrijk is dan om zicht te hebben op de factoren die een bedrijf tot actie brengen. TNO heeft om die reden opdracht gekregen om een grondig onderzoek te starten naar een gedragsinterventiekader. Het onderzoek zal gedurende dit jaar en volgend jaar plaatsvinden. De resultaten (verwacht in Q2 2024) gaan helpen om inzicht te krijgen hoe een gedragsverandering teweeg te brengen om zo ondernemers van weten naar doen te brengen.

Gebruik van de tools

Op de website van het DTC worden diverse interactieve tools aangeboden om ondernemers te stimuleren met hun cyberweerbaarheid aan de slag te gaan. De tools zijn zodanig ingestoken dat er voor diverse doelgroepen een passende tool beschikbaar is. Zo is er bijvoorbeeld de Basisscan Cyberweerbaarheid voor bedrijven die willen toetsen of ze de basis op orde hebben qua cybersecurity-maatregelen. Er is ook een tool beschikbaar voor bedrijven die een security check willen doen op hun procesautomatisering, hiervoor is meer ICT-kennis vereist. Deze tools worden met (samenwerkingsverbanden van) bedrijven ontwikkeld om zo aan te sluiten op hun behoeften. Vervolgens worden ze met de samenwerkingsverbanden en branches onder de aandacht gebracht van individuele bedrijven.

In het afgelopen jaar zijn de tools in totaal 8.100 keer gebruikt. Dit jaar wordt ingezet op het activeren van de zzp'er en mkb'er die nog weinig stappen gezet hebben in hun digitale veiligheid.[5] Het DTC heeft hiervoor een laagdrempelige tool ontwikkeld, met de werknaam de «CyberVeilig Check». Deze tool geeft de kleinere ondernemer begrijpelijke instructies voor basismaatregelen die vandáág genomen kunnen worden. Wie klaar is met de eerste set maatregelen, kan door met de tweede set maatregelen van de op maat gemaakte actielijst. Deze tool zal in het voorjaar worden aangeboden aan zzp-ers en MKB. Ook de inzet en het gebruik van deze tools draagt er aan bij dat de ondernemer daadwerkelijk aan de slag kan met zijn of haar cyberweerbaarheid.

Subsidieregeling cyberweerbaarheid

In het najaar 2022 is de subsidieregeling Cyberweerbaarheid weer opengesteld om samenwerking tussen ondernemers op het gebied van cybersecurity te stimuleren. De beoordelingscommissie heeft in de beoordeling met name gelet op samenwerkingsverbanden die een regio of sector vertegenwoordigen waar op dit moment nog weinig sprake is van samenwerking op het gebied van cyberweerbaarheid. Dit heeft geresulteerd in zes nieuwe projecten, waarmee het totaal aantal samenwerkingsverbanden medio januari op 52 is gekomen[6]. Ook dit najaar zal deze subsidieregeling worden opengesteld. Het bedrag wat hiervoor beschikbaar is zal met € 800.000,- iets lager liggen dan voorgaande jaren (€ 1.000.000). De reden hiervoor is dat het DTC het eerder gestelde doel van 50 samenwerkingsverbanden inmiddels heeft gerealiseerd en daarom dit jaar meer gaat inzetten op de synergie tussen de samenwerkingsverbanden, in plaats van enkel uitbreiding van het netwerk. Dat laatste zal uiteraard nog steeds plaatsvinden, maar de onderlinge kennisdeling in het huidige netwerk zal de focus krijgen.

Het resterende deel van het oorspronkelijke bedrag van deze subsidieregeling zal worden ingezet om ondernemers, met name zzp'ers en klein-MKB, te stimuleren en te ondersteunen bij basismaatregelen die nu belangrijk zijn om te nemen. Een voorbeeld hiervan is de ontwikkeling van de hiervoor genoemde «CyberVeilig Check» en het stimuleren van het gebruik van deze tool door ondernemers.

---

[5] CBS, cybersecuritymonitor 2021, te raadplegen op: Cybersecuritymonitor 2021 (cbs.nl).

[6] De volgende projecten hebben subsidie ontvangen: Hoornse Ondernemers Compagnie (HOC), Synthesis Information Technology, Techniek Nederland, CyberAnt B.V., Stichting Samenwerken aan Schema in Nederland, en Stichting Cyber Chain Resilience Consortium (CCRC).

Voortgang informatiedienst

Juni 2022 is de Kamer geïnformeerd over de start van de informatiedienst van het DTC.[7] De informatiedienst houdt zich specifiek bezig met het waarschuwen van bedrijven over specifieke digitale dreigingen om ze in staat te stellen actie te ondernemen. Deze dienstverlening is een concrete invulling van de maatschappelijke behoefte en wens van het bedrijfsleven om Nederlandse bedrijven te waarschuwen over digitale dreigingen.

De informatiedienst is sinds september 2021 operationeel en heeft in totaal ruim 8.100 waarschuwingen uitgestuurd.[8] Het gaat hierbij om «ongevraagd notificeren». Dit zijn notificaties voor individuele bedrijven waar het DTC nog geen relatie mee heeft. Na het achterhalen van de contactgegevens van deze bedrijven, waarschuwt het DTC, telefonisch of per mail over de betreffende digitale dreiging. Deze waarschuwing bevat ook relevant handelingsperspectief toegespitst op de betreffende dreiging.

Naast deze vorm van waarschuwen, is het DTC vorig jaar een pilot gestart met 57 bedrijven uit negen sectoren om «gevraagd» te notificeren. In de pilot controleert het DTC of de door de pilotdeelnemer aangeleverde bedrijfsgegevens- zoals IP-adressen, domeinnamen en AS-nummers – voorkomen in relevante dreigingsinformatie die bij het DTC en NCSC bekend is. Wanneer er een match wordt gevonden, wordt de pilotdeelnemer geautomatiseerd op de hoogte gesteld van deze specifieke dreiging. Bij deze notificatie wordt ook aangegeven wat eventuele vervolgacties kunnen zijn. Het is aan de pilotdeelnemer zelf om te beoordelen of het (zelf of via een ICT-dienstverlener) de geadviseerde mitigerende acties uitvoert of dat het andere maatregelen treft. Het DTC werkt hierin nauw samen met het NCSC. De pilot is succesvol verlopen en loopt door tot maart 2023. Om ook andere bedrijven uit de doelgroep van het DTC op deze wijze te kunnen informeren is het van belang om deze dienstverlening na afloop van de pilot te continueren en verder op te schalen. Daarom zal «gevraagd notificeren» een structurele dienst worden van het DTC voor alle bedrijven. De startdatum van deze dienst zal op een later moment worden bepaald.

Zoals hierboven aangegeven is het DTC in oktober 2022 een campagne gestart rondom «Security.txt». Dit is een eenvoudig tekstbestand met contactgegevens dat ondernemers op hun webserver kunnen plaatsen. Door dit te doen wordt het voor cybersecurityonderzoekers, en dus ook voor de informatiedienst van het DTC gemakkelijker de juiste persoon binnen een bedrijf te bereiken op het moment dat er sprake is van een dreiging. Door hier actief campagne op te voeren samen met een groot aantal ambassadeurs is het aantal bedrijven dat dit tekstbestand op hun webserver heeft staan, gegroeid naar 77.809.[9] We blijven dit, in samenwerking met tientallen bedrijven, promoten.

Voortgang wetsvoorstel bevordering digitale weerbaarheid bedrijven

In de Kamerbrief van 7 februari 2022[10] is aangegeven dat, om de taken en bevoegdheden van het DTC wettelijk te borgen, wordt gewerkt aan het wetsvoorstel bevordering digitale weerbaarheid bedrijven. Het

---

[7] Kamerstuk 26 643, nr. 864.
[8] Peildatum: 7 februari 2023.
[9] Bron: SIDN Labs, te raadplegen op: {Hyperlink: https://stats.sidnlabs.nl/nl/web.html#security%20policy%20(security.txt)}.
[10] Kamerstuk 26 643, nr. 817.

wetsvoorstel is een belangrijke voorwaarde om de doelstelling in het coalitieakkoord (Bijlage bij Kamerstuk 35 788, nr. 77) te realiseren om vanuit de overheid sneller en makkelijker informatie te delen met niet-vitale bedrijven over digitale kwetsbaarheden en «hacks». Het wetsvoorstel is 9 december jl. (Kamerstuk 36 270) voor behandeling aan de Kamer aangeboden. Door de Kamer is op 20 januari jl. (Kamerstuk 36 270, nr. 5) verslag uitgebracht over dit wetsvoorstel. De nota naar aanleiding van het verslag met betrekking tot dit wetsvoorstel wordt parallel aan u verzonden. Ik kijk uit naar een spoedige behandeling van het wetsvoorstel door de Kamer.

Voortgang integratie DTC, CSIRT voor digitale diensten en NCSC

Zoals in de Kamerbrief[11] van 7 september 2022 met betrekking tot de voorgenomen integratie van het DTC, het CSIRT voor digitale diensten en het NCSC is aangekondigd, is de integratie van het CSIRT voor digitale diensten en het NCSC voorzien in 2024, en de integratie met het DTC in 2026. In de aanloop naar de volledige integratie wordt er op steeds meer terreinen samengewerkt. Ook voor de lopende ontwikkelingen op producten en diensten geldt dat we daarin de onderlinge afstemming zoeken met het oog op de integratie.

Uitvoering moties (cyber oefenagenda niet-vitaal en keurmerk MKB)

Naar aanleiding van het wetgevingsoverleg van 14 november 2022[12] zijn twee moties aangenomen (Handelingen II 2022/23, nr. 28, item 9) waarin het DTC wordt gevraagd een rol te spelen. Dit betreft de motie van het lid Rajkowski c.s. waarin de regering wordt verzocht «om in samenwerking met het DTC, brancheorganisaties en regionale partners een structurele cyber oefenagenda te ontwikkelen met daarin cyberoefeningen specifiek gericht op niet-vitale bedrijven»[13] en de motie van het lid Rajkowski c.s. waarin de regering wordt verzocht «om in overleg te treden met het DTC en betrokken brancheorganisaties om te komen tot een eenduidig mkb-keurmerk voor IT-leveranciers om mkb'ers beter te ondersteunen bij het vormen van hun cybersecuritybeleid».[14]

Ten aanzien van de laatstgenoemde motie met betrekking tot het mkb-keurmerk is er een startnotitie opgesteld en zijn er afspraken gepland met de relevante partijen die reeds hebben nagedacht over een dergelijk keurmerk of kennis hebben van bestaande Nederlandse en Europese wetgeving en certificeringschema's, bijvoorbeeld het Europees Agentschap voor cyberbeveiliging (ENISA) en betrokken brancheorganisaties. Daarnaast is een geschikte partij nodig voor de ontwikkeling, uitgifte en onderhoud van het keurmerk. Aangezien een keurmerk (of certificering) een instrument is van en voor marktpartijen, is het DTC als overheidsorganisatie hier niet voor geschikt. Er wordt in de uitwerking nagedacht over twee mogelijke sporen, namelijk enerzijds een mkb-keurmerk voor bedrijven zoals beschreven in de motie (gericht op de eigen digitale weerbaarheid), anderzijds een keurmerk voor ICT-dienstverleners (gericht op de cybersecurity van de ICT-producten en diensten die zij aanbieden) zoals in het verslag van het wetgevingsoverleg Begrotingsonderdelen van het Ministeries van Binnenlandse Zaken (BZK), Economische Zaken en Klimaat (EZK) en Justitie en Veiligheid (JenV) van 14 november 2022

---

[11] Kamerstuk 26 643, nr. 927.
[12] Kamerstukken 36 200 VII, 36 200 XIII en 36 200 VI, nr. 116.
[13] Kamerstuk 36 200 VII, nr. 61.
[14] Kamerstuk 36 200 VII, nr. 60.

beschreven staat.[15] Op basis van de inventarisatie en consultatie met brancheorganisaties naar de behoeften in de markt, zal dit jaar worden gestart met de publiek-private ontwikkeling van het keurmerk. Qua vormgeving moet het keurmerk aansluiten op het Europese raamwerk van cybersecurity certificering onder de Europese cyberbeveiligingsverordening.[16]

Het DTC werkt ook aan de uitvoering van de motie van het lid Rajkowski c.s. om een structurele cyberoefenagenda te ontwikkelen met daarin cyberoefeningen gericht op het niet-vitale bedrijfsleven. De eerste stappen in de uitvoering van de motie zien op het uitvragen van de behoefte en het inventariseren van het aanbod van cyberoefeningen. Het uitvragen van de behoefte gebeurt door middel van het uitzetten van een flitspeiling onder mkb'ers. Ook zal er 14 maart 2023 in samenwerking met VNO-NCW een sessie met brancheorganisaties plaatsvinden. Daarnaast vinden er gesprekken plaats met verschillende aanbieders van cyberoefeningen. Op basis van deze uitkomsten zullen vervolgstappen worden genomen.

CSIRT voor digitale diensten

Hierbij wil ik u ook informeren over de voortgang van het CSIRT voor digitale diensten, dat sinds de oprichting op 1 januari 2019 het aangewezen CSIRT is voor online marktplaatsen, online zoekmachines en cloud computerdiensten op basis van de Wet beveiliging netwerk- en informatiesystemen. Het CSIRT voor digitale diensten zet zich in om uitval van netwerk- en informatiesystemen van deze digitale dienstverleners te voorkomen, de gevolgen van een uitval te beperken en te ondersteunen om de integriteit van systemen te verhogen. Deze digitale dienstverleners moeten incidenten met aanzienlijke gevolgen voor hun dienstverlening melden.[17] Het CSIRT voor digitale diensten verleent bijstand bij dergelijke incidenten.[18]

Het CSIRT voor digitale diensten heeft zich organisatorisch doorontwikkeld en een aantal relevante diensten uitgebreid. In 2022 heeft het CSIRT voor digitale diensten 61 incidenten in behandeling gehad, ten opzichte van 62 zaken in 2021, 42 zaken in 2020 en 6 zaken in 2019. Deze zaken betreffen bijvoorbeeld informatie over kwetsbare systemen waarna het verantwoordelijke contact is geïnformeerd zodat deze actie kon ondernemen. In 2022 is de doelgroep over 4.952 kwetsbare systemen geïnformeerd, in 2021 was dit 5.637. Deze informatie komt onder meer uit ontvangen meldingen en van partners zoals het NCSC, CSIRT's uit de Europese Unie (EU) en onderzoekers.

Er is door het CSIRT voor digitale diensten afgelopen jaar geen verplichte melding ontvangen die aan de eisen van de meldplicht voldeed[19], in 2021 was dit 1 melding. Vrijwillige meldingen die binnen kwamen gingen over incidenten rond DDoS-aanvallen (eventueel met afpersing[20]), ransomware-aanvallen, phishing of uitval van systemen. Het CSIRT voor digitale diensten verspreidt wekelijks een situationeel beeld aan zijn

---

[15] Kamerstukken 36 200 VII, 36 200 XIII en 36 200 VI, nr. 116.

[16] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PbEU 2019, L151).

[17] Ingevolge art. 13, eerste lid, Wbni.

[18] Ingevolgde art. 4, vierde lid, Wbni.

[19] Uitvoeringsverordening (EU) 2018/151 van de Commissie van 30 januari 2018 tot vaststelling van toepassingsbepalingen voor Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad (PbEU 2018, L26/48).

[20] Ransom DDoS.

doelgroep over kwetsbaarheden, dreigingen en relevante gebeurtenissen van die week. Inmiddels zijn er 158 ontvangers die zich hebben ingeschreven, in 2021 waren dit nog 110. Verder neemt het CSIRT voor digitale diensten actief deel aan het EU CSIRTs Network.[21]

Er is in 2022 doorgebouwd aan de relatie met de doelgroep, brancheorganisaties en samenwerkingsverbanden. Omdat er geen register is van digitale dienstverleners moeten het CSIRT voor digitale diensten en de doelgroep naar elkaar op zoek om contact te leggen. Om de groei in werkzaamheden te kunnen ondersteunen is een incidentresponseplatform in gebruik genomen. Er zijn aanvullende bronnen, met voor digitale dienstverleners relevante dreigingsinformatie, toegevoegd en er wordt meer informatie via publiek-private samenwerkingsverbanden ontvangen en gedeeld.

Dit jaar staat in het teken van de integratie van het CSIRT voor digitale diensten en het NCSC welke uiterlijk in 2024 zijn beslag zal moeten krijgen.[22]

Ambities 2023

Voor 2023 zijn vier speerpunten benoemd waaraan de activiteiten en acties die binnen het DTC worden ontplooid zijn opgehangen. Dit zijn: van weten naar doen, de basis op orde, synergie in samenwerkingsverbanden en instrumenten en tot slot bereik en impact vergroten.

Van weten naar doen

In de afgelopen jaren heeft het DTC vooral ingezet op het onder de aandacht brengen van de basismaatregelen die ondernemers relatief gemakkelijk konden helpen om hun cyberweerbaarheid te vergroten. De groeiende bezoekersaantallen op de website, het aantal volgers op de sociale mediakanalen en het aantal leden van de community maken duidelijk dat het bereik van het DTC groeit en daarmee het aantal ondernemers dat kennis kan nemen van de informatie en adviezen van het DTC. Dat is goed nieuws maar uiteraard nog niet voldoende. Dit jaar wil ik ondernemers nog een stapje verder helpen. Niet enkel informeren en adviseren maar inzetten op een gedragsverandering zodat ondernemers ook daadwerkelijk maatregelen treffen om digitaal weerbaar te worden.

Basis op orde

Omdat cybercriminelen niet stil zitten en ondernemers hun dienstverlening steeds verder digitaliseren is het van belang dat de basis op orde komt. Dit wil zeggen dat er wordt gestreefd naar een basisniveau van cyberweerbaarheid van ondernemend Nederland. Hiertoe wordt gewerkt aan een instap tool die onderscheidend voor zzp en klein mkb concrete tips en maatregelen geeft die door deze doelgroepen vandaag kunnen worden genomen. Dit hangt nauw samen met de hierboven gewenste gedragsverandering.

Het DTC kan dit niet alleen bereiken. Samenwerking met andere partijen om bijvoorbeeld een keurmerk voor het MKB te ontwikkelen zoals in de eerdergenoemde motie wordt gevraagd helpt hierbij.

---

[21] https://csirtsnetwork.eu/.

[22] Ik verwijs hiervoor nogmaals naar de Kamerbrief van 7 september 2022 jl. (Kamerstuk 26 643, nr. 927).

Synergie in samenwerkingsverbanden en instrumenten

Het DTC-netwerk bestaat op dit moment uit 52 samenwerkingsverbanden. Hoe groter het netwerk van samenwerkingsverbanden, hoe groter het bereik. Echter, vanaf dit jaar wil het DTC niet enkel inzetten op kwantiteit, maar ook op kwaliteit van de samenwerking tussen de verschillende initiatieven. Door meer te focussen op onderlinge samenwerking, kennisdeling en gezamenlijke ontwikkeling van informatieproducten die passen bij de behoefte van de doelgroep ontstaat er een beter netwerk met kennis waar ondernemers terecht kunnen en stijgt de weerbaarheid.

Bereik en impact vergroten: het DTC als katalysator

Aanvullend op bovenstaande speerpunten wordt ingezet op het vergroten van het bereik van het DTC en de impact van de producten, diensten en tools die het DTC aanbiedt om zo steeds meer ondernemers te helpen cyberweerbaar te worden. Begin volgend jaar zal ik u informeren over de resultaten die zijn geboekt.

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

Bijlage

Toezegging	Realisatie 31-12	Toelichting / vervolg
1. Kwantitatief		
Bezoeken DTC website 230.000 in 2022	Gerealiseerd (ruim 260.000)	Doelstelling 2023: 300.000
50 samenwerkingsverbanden eind 2023	In wording (48 samenwerkings-verbanden)	Doelstelling medio januari gehaald (52). Voor 2023 focus op meer synergie
Gebruik tools bij elkaar opgeteld 10.000	Niet gerealiseerd (realisatie 8.100)	Doelstelling 2023: 10.000
DTC Online community 1.000 deelnemers	Gerealiseerd (realisatie 1.608)	Doelstelling 2023: 2.000 deelnemers
2. Kwalitatief		
Samenwerkingsafspraken DTC en NCSC	Gerealiseerd	Samenwerking in de praktijk gebracht, integratieproces gestart.
Wetsvoorstel bevordering digitale weerbaar-heid bedrijven	In wording	Behandeling Tweede Kamer voorzien 1e helft 2023
CBS onderzoek cybersecurity ZZP-ers	Gerealiseerd	Onderzoek zal worden herhaald in 2023
Gedragsonderzoek	Gerealiseerd en uitgebreid	TNO onderzoek gestart naar een gedragsinterventiekader. Resultaten worden in 2024 verwacht
Nieuwe subsidieregeling cyberweerbaarheid	Gerealiseerd (6 nieuwe projecten)	Subsidieregeling zal opnieuw worden opengesteld Q3 2023
Informatiedienst voor concrete dreigingsinfor-matie (ongevraagd notificeren)	Gestart (realisatie 6.574 notificaties)	Dienst wordt voortgezet.
3. Extra / nieuw		
DTC pilot gevraagd notificeren	Pilot verlengd (realisatie 4.123 notificaties)	Continuering en opschaling gevraagd notificeren voorzien in Q2 2023
Webinars	Gerealiseerd	Instrument wordt ook in 2023 ingezet bij grote cyberincidenten
Motie MKB Keurmerk	Gestart	In uitvoering
Motie Cyberoefenplan niet-vitaal	Gestart	In uitvoering