Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1277

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 februari 2025

Conform de Kamerbrief van 8 maart 2024,[1] informeer ik u hierbij over de voortgang van het Digital Trust Center (DTC). In deze brief wordt aan de hand van de vier speerpunten van het DTC uiteengezet welke inspanningen zijn gedaan en welke resultaten zijn behaald. Deze speerpunten zijn: van weten naar doen, de basis op orde, synergie in samenwerkingsverbanden en instrumenten, en tot slot het vergroten van bereik en impact.[2] Alle activiteiten die het DTC ontplooit zijn opgehangen aan een of meerdere van deze speerpunten. Het DTC draagt hiermee bij aan de uitvoering van de Nederlandse Cybersecuritystrategie (NLCS)[3] en Pijler 5 van de Strategie Digitale Economie (SDE).[4]

Daarnaast wordt in de brief onder andere stilgestaan bij de stand van zaken rond de uitvoering van de moties inzake het mkb-keurmerk, cyberoefenen en digitale hulpverlening. Tenslotte gaat de brief in op de aanstaande integratie met het Nationaal Cyber Security Centrum (NCSC).

Resultaten 2024

Het DTC heeft zich in 2024 met onverminderde energie ingezet om de 2,4 miljoen niet-vitale bedrijven digitaal weerbaarder te maken. Aan de hand van de eerdergenoemde speerpunten zal ik ingaan op de behaalde resultaten.

Speerpunt 1: Van weten naar doen

De activiteiten voor dit speerpunt zien op het stimuleren van ondernemers om daadwerkelijk aan de slag te gaan met het op orde brengen van hun

[1] Kamerstuk 26 643, nr. 1143.
[2] Kamerstuk 26 643, nr. 980 en Kamerstuk 26 643, nr. 1143.
[3] Kamerstuk 26 643, nr. 925.
[4] Kamerstuk 26 643, nr. 941.

kst-26643-1277
ISSN 0921 - 7371
's-Gravenhage 2025

cyberweerbaarheid. Het DTC probeert op diverse manieren de drempels om actie te ondernemen te verlagen.

Voortgang DTC Notificatiedienst

De DTC Notificatiedienst houdt zich bezig met het waarschuwen van bedrijven over specifieke digitale dreigingen om ze in staat te stellen actie te ondernemen. De DTC Notificatiedienst heeft in 2024 ruim 238.000 kwetsbare systemen van verschillende bedrijven genotificeerd over specifieke dreigingsinformatie. Het totaal aantal genotificeerde systemen dat sinds de start in juni 2021 verstuurd zijn aan bedrijven («gevraagd» en «ongevraagd») is ruim 394.000. Dit komt vooral op het conto van de «ongevraagde» waarschuwingen over kwetsbaarheden bij het bedrijfsleven. «Ongevraagd» notificeren verwijst naar notificaties voor individuele bedrijven waar het DTC nog geen directe relatie mee heeft. Na het achterhalen van de contactgegevens van deze bedrijven, waarschuwt het DTC over de betreffende digitale dreiging. Deze waarschuwing bevat ook relevant handelingsperspectief toegespitst op de betreffende dreiging. Bij «gevraagd» notificeren heeft een bedrijf relevante gegevens op voorhand aangeleverd. Door het verzenden van deze waarschuwingen kunnen ondernemers tijdig reageren om bijvoorbeeld een beveiligingslek of configuratiefout te herstellen. Zo kan worden voorkomen dat een kwetsbaarheid kan worden misbruikt door kwaadwillenden. De operationele processen rondom het gevraagd notificeren zijn inmiddels een geïntegreerd proces tussen de DTC Notificatiedienst en het NCSC, ongevraagd notificeren draait nog separaat bij het DTC. Sinds 1 oktober 2024 is onder andere deze taak wettelijk verankerd in de Wet bevordering digitale weerbaarheid bedrijven (Wbdwb).

Gerichter bedienen van bedrijven

In opdracht van het DTC heeft TNO afgelopen jaar het onderzoeksrapport «Veilig Digitaal Ondernemen» opgeleverd.[5] De resultaten uit dit onderzoek bieden het DTC meer inzicht in de motivaties en barrières van ondernemers ten aanzien van het wel of niet vertonen van cyberveilig gedrag. De DTC-doelgroep is te verdelen in vijf gedefinieerde groepen: de Voorlopers, Uitbesteders, Overmoedigen, Machtelozen en Onverschilligen. Elk van deze subgroepen bestaat uit bedrijven van verschillende grootte en sector, maar met overeenkomsten op basis van motivaties en barrières. Deze inzichten worden meegenomen in de ontwikkeling van nieuwe, en de herijking van bestaande producten en diensten om deze nog gerichter en effectiever te laten aansluiten bij de behoeften en uitdagingen vanuit de doelgroep. Door ondernemersverhalen te publiceren en in de communicatie meer focus te leggen op het betrekken van intermediaire partijen die dicht bij ondernemers staan, streeft het DTC er in 2025 naar om alle doelgroepen binnen het niet-vitale bedrijfsleven te bereiken – inclusief degenen die aanvankelijk geen aanleiding zien om actie te ondernemen.
Verschillende door het DTC aangeboden tools bedienen op een gerichte manier de doelgroep. Met het recent gelanceerde startpunt[6] op de DTC-website kunnen ondernemers op een gemakkelijke manier de informatie vinden die voor hen is bedoeld. Ook kunnen ondernemers die werkzaam zijn binnen domeinen waarin operationele technologie (OT) een

[5] TNO, Veilig digitaal ondernemen. Inzicht in motivaties en barrières door doelgroepsegmentatie. Tineke Hof, Rick van der Kleij, Silke Mergler, april 2024.
[6] Het startpunt is de startpagina van de DTC-website. Op deze pagina kan de bezoeker aan de hand van zijn positie in één oogopslag de belangrijkste informatie zien.

rol speelt meer kennis opdoen middels de «Security Check Procesautomatisering».[7]

Mijn Cyberweerbare Zaak

Door «Mijn Cyberweerbare Zaak»[8] kunnen zzp'ers, micro- en kleine ondernemingen subsidie krijgen voor de kosten van de aanschaf en implementatie van één of meer belangrijke cyberweerbaarheidsmaatregelen. Na een positieve evaluatie, waaruit onder meer bleek dat deze subsidie de juiste doelgroep weet te bereiken en aanzet tot het doen van investeringen voor de digitale veiligheid van ondernemers, is de subsidieregeling tussen 2 september en 31 december 2024 opnieuw opengesteld met een subsidiebudget van € 1.000.000. Om de doelmatigheid te maximaliseren zijn er bij deze heropenstelling enkele verbeterpunten doorgevoerd; zo werden alleen aanvragen in behandeling genomen als deze waren voorzien van een betalingsbewijs in plaats van een offerte.

Speerpunt 2: Basis op orde

Om het Nederlandse bedrijfsleven cyberweerbaar te maken, is er een blijvende inspanning nodig om bedrijven te motiveren om in ieder geval de basis op orde te hebben. Deze inspanning levert het DTC op de volgende manieren.

Herijking van de vijf basisprincipes

Incidenten hebben regelmatig negatieve gevolgen wanneer ondernemers de basisbeveiligingsmaatregelen niet op orde hebben. Een ondernemer verhoogt de digitale weerbaarheid van zijn of haar onderneming door middel van de vijf basisprincipes van veilig digitaal ondernemen, die met relatief eenvoudige stappen te doorlopen zijn. De vijf basisprincipes van digitale weerbaarheid zijn 1) het in kaart brengen van risico's, 2) het bevorderen van veilig gedrag, 3) de bescherming van systemen, apparaten en applicaties, 4) toegangsbeheer en 5) voorbereiding op incidenten. De door het DTC geïntroduceerde basisprincipes zijn na een periode van zes jaar in samenwerking met het NCSC vernieuwd. Het betreft een raamwerk dat aandacht heeft voor de mens, techniek en de organisatie. Onder de vijf vernieuwde basisprincipes kunnen vervolgens specifieke maatregelen worden opgehangen die zijn toegespitst, bijvoorbeeld op het volwassenheidsniveau van een organisatie.

CyberVeilig Check voor zzp en mkb

Om ondernemers te ondersteunen in het nemen van basismaatregelen is in 2023 de «Cyberveilig Check voor zzp en mkb» gelanceerd. Deze interactieve zelfscan is gericht op ondernemers die nog niet veel kennis en ervaring hebben op het gebied van cybersecurity. Tevens biedt de zelfscan ondernemers een concrete actielijst met basismaatregelen waarmee zij zélf (of met hulp) direct aan de slag kunnen. De «Cyberveilig Check voor zzp en mkb» is in 2024 meer dan 9.000 keer ingevuld. Ook in 2025 zal deze tool blijvend onder de aandacht gebracht worden, vooral om te stimuleren dat de kleinere bedrijven de basis op orde brengen met concrete en goed uitvoerbare cybermaatregelen.

[7] https://www.digitaltrustcenter.nl/tools/doe-de-security-check-procesautomatisering.
[8] https://www.digitaltrustcenter.nl/mijn-cyberweerbare-zaak-2023-positief-geevalueerd.

Voorbereiding op de Cyberbeveiligingswet

De herziene Europese Netwerk- en Informatiebeveiligingsrichtlijn (NIS2-richtlijn)[9] wordt geïmplementeerd in nationale wetgeving via de Cyberbeveiligingswet (Cbw). De Kamer is reeds door de Minister van Justitie en Veiligheid (JenV) geïnformeerd over het niet tijdig omzetten van de richtlijn en het dus niet halen van de implementatiedeadline van 17 oktober 2024.[10] Het streven is dat de wetgeving in het derde kwartaal van 2025 in werking zal treden. Het kabinet roept de circa 10.000 entiteiten die onder deze nieuwe wetgeving komen te vallen op om alvast voorbereidingen te treffen. Zo is er onder meer het NIS2-Startpunt om met toelichting en hulpmiddelen aan de slag te gaan met de tien maatregelen die de wet voorschrijft waar het gaat om de zorgplicht.[11] De nieuwe wetgeving heeft een indirecte impact op de toeleveranciers van de entiteiten die onder de wet vallen omdat zij aandacht moeten hebben voor digitale weerbaarheid van hun directe leveranciers. Om hen te helpen bij het aanpakken van ketenbeveiliging zijn met tips en adviezen uit de praktijk «Good Practices voor Ketenbeveiliging» samengesteld.[12] Voor organisaties die een overzichtelijke keten van leveranciers hebben, is een invulbare risicoinventarisatie beschikbaar waarin per leverancier de afhankelijkheden, afspraken en alternatieven kunnen worden vastgelegd.[13] In de online community van het DTC worden ook praktijkervaringen gedeeld door CISO's, IT-managers en bestuurders om elkaar te inspireren. Verderop in deze brief wordt uitgebreider ingegaan op de DTC Community.

Interactieve tools

Om ondernemers van weten naar doen te krijgen, moet de informatie laagdrempelig en gemakkelijk uitvoerbaar zijn. Als de intentie er is, moet het eenvoudig zijn om in actie te komen. Daarom heeft het DTC zo'n vijftien interactieve tools in het assortiment. Veelal zijn het geanonimiseerde zelfscans die een actielijst met handzame instructies opleveren. Dit jaar zijn er ook drie interactieve bestanden aan toegevoegd, waaronder een bellijst voor noodsituaties. De interactieve tools zijn in 2024 26.634 keer gebruikt.

Speerpunt 3: Synergie in samenwerkingsverbanden en instrumenten

Intensivering samenwerking tussen het DTC, het NCSC en samenwerkingsverbanden

Het afgelopen jaar is de onderlinge samenwerking tussen regionale en sectorale samenwerkingsverbanden verder vergroot. Ook is de samenwerking tussen het DTC en het NCSC met de samenwerkingsverbanden geïntensiveerd. Dit is onder meer nodig vanwege de naderende integratie van de organisaties, de zachte landing van de DTC-doelgroep bij het vernieuwde NCSC en de implementatie van de NIS2-richtlijn. Er is onder andere gewerkt aan de gezamenlijke ontwikkeling van informatieproducten die passen bij de behoefte van de doelgroepen.

Het DTC organiseert tevens evenementen waarbij de 64 samenwerkingsverbanden de gelegenheid krijgen om onderlinge contacten te intensi-

[9] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555.
[10] Kamerstuk 22 112, nr. 3968.
[11] https://www.digitaltrustcenter.nl/nis2/startpunt.
[12] https://www.digitaltrustcenter.nl/ketenbeveiliging-good-practices.
[13] https://www.digitaltrustcenter.nl/sites/default/files/2024-04/Handvat_voor_keteninventarisatie.pdf.

veren, met als doel het netwerk van samenwerkingsverbanden verder te versterken en te consolideren. De samenwerking tussen deze samenwerkingsverbanden resulteert in waardevolle initiatieven, zoals CYRA, dat mede is opgericht door drie samenwerkingsverbanden binnen het DTC: FERM, het Cyberweerbaarheidscentrum Brainport en de Cybercampus Noord.

Subsidieregeling Cyberweerbaarheid

Daarnaast is de subsidieregeling «Cyberweerbaarheid 2024–2025» opengesteld, gericht op het verhogen van de cyberweerbaarheid van bedrijven. Dit kunnen duurzame samenwerkingen zijn in de keten, regio, sector of branche. Er zijn vorig jaar vijf projectvoorstellen geselecteerd voor een subsidie. Het volledige bedrag is deze ronde verlaagd van € 800.000 naar € 600.000, waarbij er een maximum van € 150.000 in plaats van € 200.000 per project wordt uitgekeerd. Doordat drie inschrijvingen onvoldoende scoorden om de subsidie te kunnen toekennen, is het bedrag van € 600.000 niet opgegaan. In 2025 wordt de regeling op advies van de onafhankelijke adviescommissie geëvalueerd. Op basis daarvan zal worden bekeken of en op welke wijze de regeling voorgezet zal worden. Met de vijf nieuwe samenwerkingsverbanden uit deze subsidieronde zijn er op dit moment in totaal 68 DTC samenwerkingsverbanden.

Cyberweerbaarheidsnetwerk

Het DTC werkt ook nauw samen met het NCSC aan een bouwplan voor het Cyberweerbaarheidsnetwerk.[14] In het Cyberweerbaarheidsnetwerk werken publieke en private organisaties samen aan het verhogen van de cyberweerbaarheid en dragen op die manier bij aan de cyberweerbaarheid van heel Nederland. De samenwerking vindt plaats vinnen vijf functies: 1) informatiedeling, 2) doelwit- en slachtoffernotificatie, 3) incidentafhandeling, 4) kennisuitwisseling, en 5) opleiden, trainen en oefenen (OTO). Het streven is om in april 2025 het bouwplan op te leveren.

Speerpunt 4: Bereik en impact vergroten: het DTC als katalysator

Ondersteunende campagnes

De DTC-campagnes hebben als doel ondernemers te bereiken met laagdrempelige producten en tools, de bewustwording te vergroten en aan te zetten tot actie. Dit gebeurt onder meer aan de hand van interactieve video's en het oefenen van cyberincidenten. Vanwege het feit dat veel ondernemers denken dat ze geen doelwit zijn, blijft het DTC werken aan bewustwording via ervaringsverhalen van gehackte ondernemers.[15]

Voor de meer cybervolwassen bedrijven is er door middel van een campagne hulp aangereikt om zich voor te bereiden op de NIS2-richtlijn.[16] Veel inspanningen vanuit het DTC, zoals de campagnes op sociale media en de nieuwsberichten op de website, zijn erop gericht geweest om de subsidieregeling «Mijn Cyberweerbare Zaak» voor kleine ondernemers onder de aandacht te brengen. Door het delen van sectorspecifieke berichten waren brancheorganisaties en redacties van vakbladen meer bereid om deze subsidieregeling onder de aandacht te brengen bij de ondernemers in hun achterban. De toepassing van deze werkwijze zal in 2025 verder worden uitgebouwd.

---

[14] Kamerstuk 26 643, nr. 1176.
[15] https://www.digitaltrustcenter.nl/ondernemend-nederland-vertelt.
[16] https://www.digitaltrustcenter.nl/nis2/startpunt.

Bereik vergroot

Het DTC heeft het afgelopen jaar weer meer ondernemers bereikt dan het jaar ervoor, door de inzet van een breed scala aan activiteiten en communicatiekanalen. Aan de website zijn bijna 400.000 bezoeken gebracht, dit waren er 336.000 in 2023. De wereldwijde computerstoring na de Crowdstrike-update heeft tot een piek in informatiezoekers geleid. De sectorgerichte verspreiding van ruim 50 nieuwsberichten via PR-activiteiten heeft ook tot flink meer websitebezoeken geleid. Ook wisselen in de DTC Community meer dan 5.700 ondernemers online kennis uit. In 2025 wordt ook hier extra ingezet op het vergroten van de synergie tussen de bestaande samenwerkingsverbanden, onder andere door middel van eigen consultatieruimten en onderlinge informatie-uitwisseling.

Uitvoering moties (mkb-keurmerk, cyberoefenen en digitale hulpverlening)

In de Kamerbrief en Voortgangsrapportage NLCS 2024[17] is de Kamer geïnformeerd over de uitvoering van de motie Rajkowski inzake een eenduidig mkb-keurmerk om het mkb beter te ondersteunen bij hun cybersecuritybeleid en de motie Rajkowski over het ontwikkelen van een structurele cyberoefenagenda voor het niet-vitale bedrijfsleven in samenwerking met het DTC.[18]

Ter uitvoering van de motie inzake het mkb-keurmerk ontwikkelt het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) een keurmerk voor ICT-dienstverleners ten behoeve van het mkb. Het keurmerk geeft afnemers een bepaalde mate van zekerheid 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 doel is om het keurmerk aan het einde van het jaar te publiceren. Naar aanleiding van de motie over cyberoefenen kunnen ondernemers op de DTC website aan de slag met de toegezegde cyberoefening. Partijen kunnen deze zelf – zonder begeleiding – uitvoeren.[19] In het eerste kwartaal van 2025 zullen twee nieuwe varianten op de oefening worden gelanceerd. Hiermee is uitvoering gegeven aan de motie.

Het Centraal Bureau voor de Statistiek (CBS) zal voor de uitvoering van motie van het lid Kathmann in de jaarlijkse Cybersecuritymonitor onderzoeken hoeveel bedrijven hun digitale hulpverlening hebben ingericht en op welke manier.[20] In verband met de doorlooptijd van de metingen van het CBS zal dit vraagstuk terugkomen in de Cybersecurity-monitor van 2025. Het DTC heeft op zijn website informatie opgenomen voor het inrichten van digitale hulpverlening en brengt dit onder de aandacht bij ondernemers via het cybernetwerk en sociale media.[21] Hiermee is de motie opgenomen in de staande werkprocessen van het CBS en het DTC. Hiermee is uitvoering gegeven aan de motie en doe ik de motie af.

---

[17] Kamerbrief 26 643, nr. 1229.
[18] Het betreft de moties Rajkowski Kamerstuk 36 200 VII, nrs. 60 en 61.
[19] https://www.digitaltrustcenter.nl/cyberoefenen.
[20] Kamerstuk 36 270, nr. 9.
[21] https://www.digitaltrustcenter.nl/wie-verleent-digitale-hulpverlening.

Voortgang integratie DTC, CSIRT voor digitale diensten en NCSC

In maart 2024 is uw Kamer geïnformeerd over de aanstaande integratie van het DTC, het CSIRT-DSP en het NCSC.[22] Het afgelopen jaar zijn hierin weer verschillende stappen gezet, waaronder de realisatie van een visie op de vier rollen van de in te richten Nationale Cybersecurityorganisatie, of te wel het vernieuwde NCSC. De vier rollen van het vernieuwde NCSC zijn (1) nationaal CSIRT, (2) centraal kennis- en adviescentrum, (3) uitvoeringscoördinator en (4) sectoraal CSIRT. Deze visie en de implementatie ervan zijn belangrijke uitgangspunten in de herinrichting van de organisatie en de dienstverlening voor alle organisaties in Nederland. Een voorbeeld van de intensieve samenwerking tussen voornoemde partijen zijn de vijf gezamenlijke basisprincipes van digitale weerbaarheid, die nu gelijkluidend en op dezelfde manier worden uitgedragen. Om de verschillende producten en diensten goed te integreren werken verschillende teams van het DTC en het NCSC al op diverse manieren samen. Zo wordt in multidisciplinaire teams gewerkt aan het versneld en geautomatiseerd opleveren van doelwit- en slachtoffernotificaties, en kwetsbaarheden aan organisaties. Enkele doelen voor 2025 zijn het realiseren van een gezamenlijke adviesraad. Deze adviesraad bestaat uit externe stakeholders, onder andere uit het bedrijfsleven en het cybersecuritydomein. De raad wordt door de directie van het vernieuwde NCSC gevraagd om advies te geven over strategische onderwerpen, de richting van het vernieuwde NCSC en ontwikkelingen die spelen in het werkveld. Daarnaast staat 2025 in het teken van meer gezamenlijke communicatie naar doelgroepen en meer gezamenlijke producten. Ook zal de harmonisatie en integratie van alle taken, mensen en benodigde faciliteiten worden voorbereid zodat er vanaf 2026 een integrale, nieuwe cybersecurityorganisatie wordt gevormd waarin naadloos wordt samengewerkt. Denk daarbij bijvoorbeeld ook aan de ICT-infrastructuur, en tooling zoals de websites.

Een andere belangrijke ontwikkeling was de voorspoedige en bijna volledige integratie van het CSIRT-DSP. Vanaf 1 januari 2025 wordt de doelgroep van het CSIRT-DSP vanuit het NCSC bediend. Daarmee zijn de producten van het CSIRT-DSP geïntegreerd in de dienstverlening en operationele processen van het NCSC. De doelgroep is stapsgewijs meegenomen in de ontwikkeling en aanpassingen. Vanaf volgend jaar zal deze dienstverlening verder worden uitgebreid met onder andere toegang tot het MijnNCSC portaal, zodat informatie op maat beschikbaar kan worden gesteld.

Tot slot

In 2024 zijn de nodige stappen door het DTC en het CSIRT-DSP gezet om ondernemers te ondersteunen in het verhogen van hun digitale weerbaarheid. Deze werkwijze zal ook in 2025 worden voortgezet waarbij het DTC nauw blijft samenwerken met bedrijven om te zorgen dat zij producten en diensten biedt waar bedrijven behoefte aan hebben en gebruik van kunnen maken. Ook vanuit het vernieuwde NCSC zal de dienstverlening blijvend worden afgestemd met de verschillende doelgroepen aan bedrijven.

[22] Kamerstuk 26 643, nr. 1143.

Gezien de integratie van het DTC in het vernieuwde NCSC op 1 januari 2026 is dit de laatste aparte voortgangsbrief. De Kamer zal in de toekomst worden geïnformeerd over de voortgang van het vernieuwde NCSC via de jaarlijkse voortgangsbrief van de NLCS.

De Minister van Economische Zaken,
D.S. Beljaarts