Ministerie van Economische Zaken
en Klimaat

Terugblik Digital Trust Center 2023

Van weten naar doen

Inhoud

Voorwoord 2023

Bedrijven ‘van weten naar doen’ brengen

Afgelopen jaar hebben we het eerste lustrum van het Digital Trust Center (DTC) gevierd. Ruim vijf jaar geleden zijn we gestart met anderhalve man en een paardenkop (figuurlijk gesproken). Met als missie ‘ondernemend Nederland cyberweerbaar maken’ en de hoofdtaken ‘informatie geven’ en ‘samenwerkingsverbanden stimuleren’.

De missie en taken staan nog steeds als een huis, maar het DTC van nu is niet meer het DTC van toen. Waar we begonnen met alleen een website, hebben we nu ook een actieve DTC Community, social media kanalen en informeren we via webinars. De 6 samenwerkingsverbanden zijn uitgegroeid tot een ecosysteem van 60 samenwerkingsverbanden. En het aantal interactieve tools is uitgebreid van 1 naar 9, afgestemd op het beoogde volwassenheidsniveau, de omvang of productieproces van een bedrijf. Ook hebben we de laatste twee jaar een nieuwe dienst voor bedrijven gelanceerd: de DTC Notificatiedienst. We waarschuwen individuele bedrijven als we als overheid kennis hebben van een concrete kwetsbaarheid of dreiging. Vol trots *spoiler* ik dat er inmiddels al meer dan 156.000 notificaties zijn verzonden.

Dit alles doen we momenteel met 25 mensen: cyberadviseurs en -specialisten, relatiemanagers, communicatieprofessionals en staf. Er is dus veel veranderd in de afgelopen vijf jaar. Het jaarbericht dat voor je ligt, maakt inzichtelijk wat we in 2023 bereikt hebben. ‘Bedrijven van weten naar doen brengen’ was het motto van 2023. Als we dáárin slagen, dragen we bij aan het vergroten van de cyberweerbaarheid.

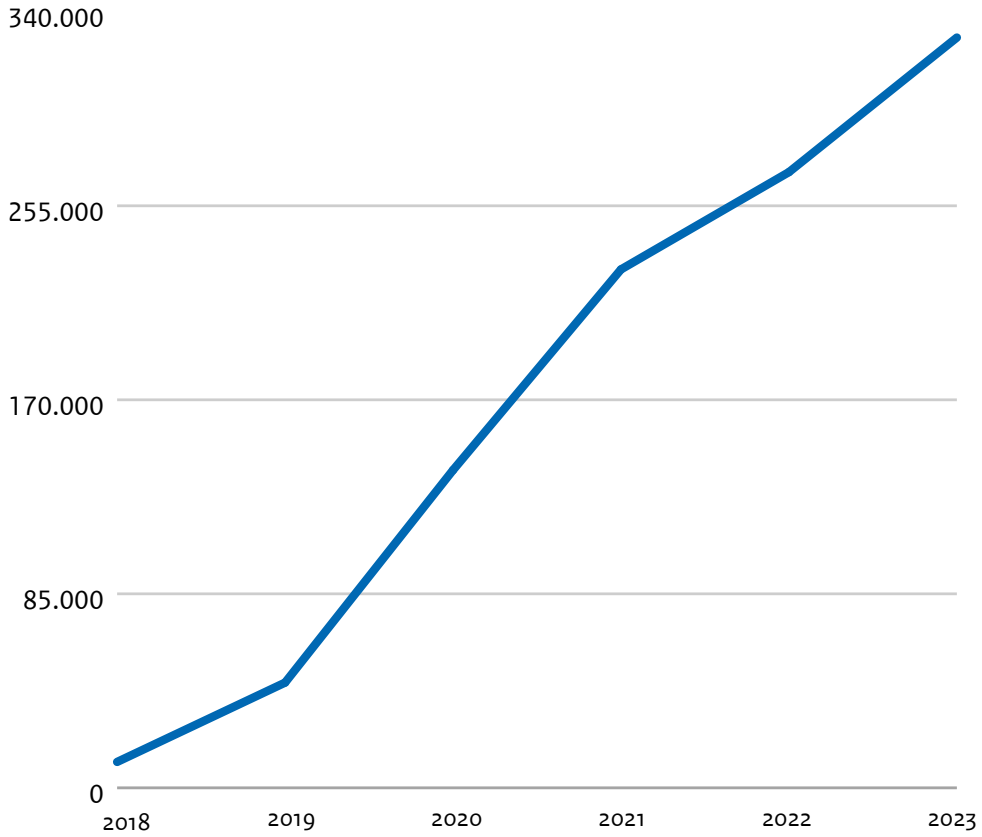
Een andere uitdaging is meer organisatorisch van aard: de start van de integratie van het DTC met het NCSC en het CSIRT-DSP. Met als motto’s *‘best of three worlds’* en ‘tijdens de verbouwing gaat de verkoop gewoon door’. Want ook in 2024 willen we een stijgende lijn zien in het bereik van ondernemers en in het activeren van bedrijven. En in 2024 houden we ook vast aan leveren wat we beloven en van buiten naar binnen blijven kijken. Geen ‘Haagse stolp’ maar juist een transparante organisatie zijn die sterk verbonden is met alle initiatieven en bedrijven die ook aan de slag willen met ‘ondernemend Nederland cyberweerbaar maken’.

Michel Verhagen, *manager Digital Trust Center*

5 jaar DTC

Vijf jaar DTC betekent vijf jaar groei. Op verschillende manieren heeft het DTC zich ingezet om het Nederlandse bedrijfsleven veiliger te maken. Om deze doelgroep van 2,3 miljoen bedrijven op maat te bedienen is het productenportfolio breder en dieper geworden. En ook aan het vergroten van het bereik is hard gewerkt.

Grafiek 1: Ontwikkeling DTC-websitebezoeken



336.187
Websitebezoeken in 2023

13.438
Volgers op social media (LinkedIn, X, en Mastodon)

2.855
Leden op DTC Community

9
Interactieve cyberveiligheidstools

>600
Webpagina's

60
Cybernetwerk van samenwerkingsverbanden

20.573
Gebruik van tools en quizzen in 2023

156.921
Waarschuwingen voor kwetsbare systemen bij bedrijven

20
Cyber alerts over kwetsbare software

Van weten naar doen

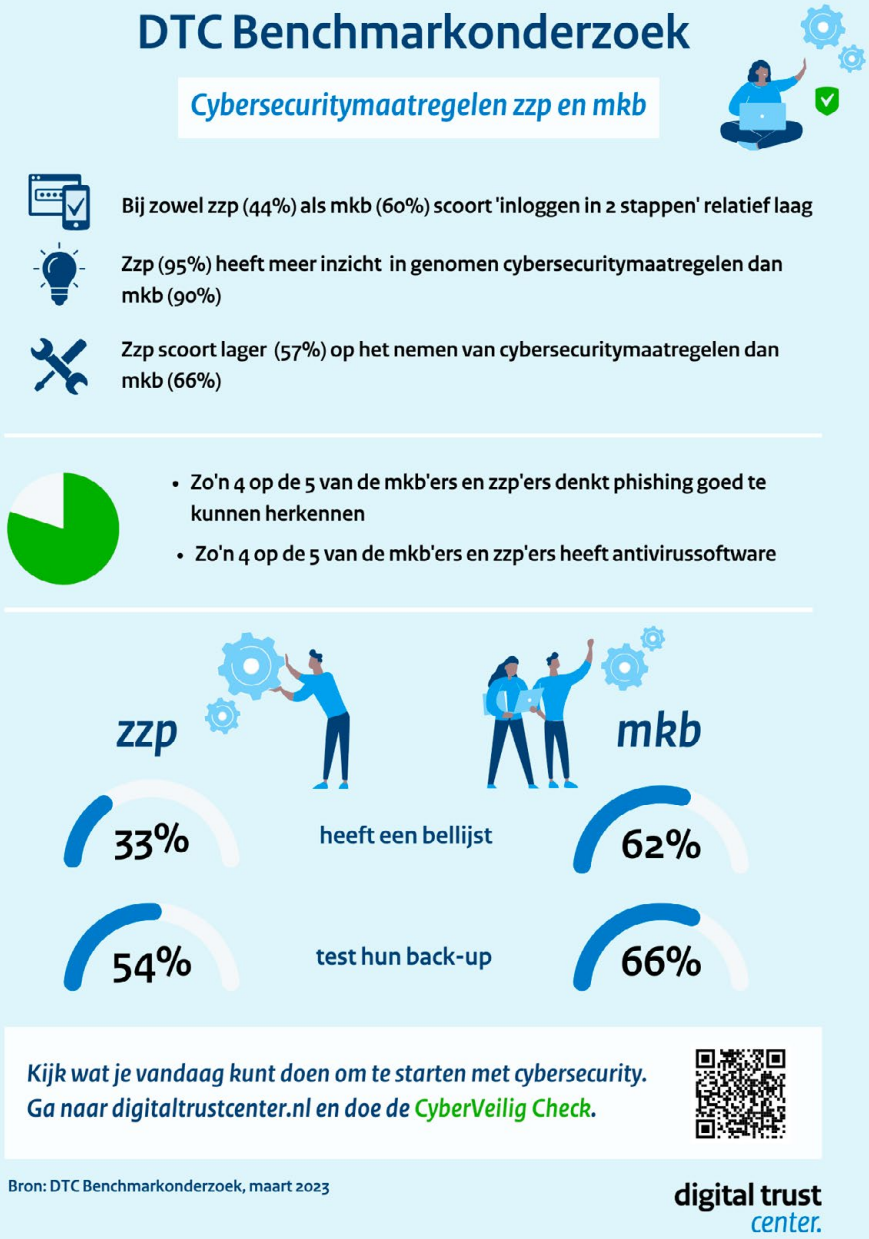
Veel kleine bedrijven zijn onvoldoende cyberweerbaar

Jaarlijks brengt het DTC via onderzoek in kaart wat de huidige staat van cyberweerbaarheid bij het bedrijfsleven is. Het CBS-onderzoek naar ICT-kenmerken bij bedrijven, het DTC Benchmark onderzoek en de data die uit de tools Basisscan Cyberweerbaarheid en CyberVeilig Check komen, tonen aan dat er nog genoeg ruimte voor verbetering is als het gaat om cybermaatregelen die ondernemend Nederland treft. Zo was het opvallend dat tweefactorauthenticatie bij zowel zzp'ers als mkb'ers onder de minst nageleefde maatregelen viel.

Hoewel het vergroten van cyberweerbaarheid begint bij het bereiken van de doelgroep, is het vooral belangrijk dat bedrijven daadwerkelijk aan de slag gaan met hun cyberweerbaarheid. Daarom stond 2023 in het teken van gedragsverandering: **Van weten naar doen.** Aan de hand van drie activiteiten is hierin een flinke stap gezet. Speciaal voor de kleinere bedrijven is de CyberVeilig Check voor mkb en zzp ontwikkeld. Met verschillende bewustwordingscampagnes is de ondernemer gewezen op een concreet en haalbaar handelingsperspectief en ook is de Mijn Cyberweerbare Zaak-subsidie gelanceerd.

CyberVeilig Check voor zzp en mkb

Speciaal voor ondernemers die qua cybersecurity nog niet veel kennis en ervaring hebben, heeft het DTC de CyberVeilig Check ontwikkeld. Een laagdrempelige tool die ondernemers een concrete actielijst geeft met basismaatregelen die zij zélf vandaag nog kunnen nemen om hun cyber-weerbaarheid te vergroten.



Bewustwordingscampagnes

Daarnaast zijn er diverse campagnes gevoerd over de onderwerpen Online fraude, Starten met cybersecurity, Ondernemersverhalen en Mijn Cyberweerbare Zaak. Alle campagnes zijn erop gericht om ondernemers met laagdrempelige producten en tools te bereiken, bewust te maken en aan te zetten tot actie. Voor de Online Fraudecampagne zijn er bijvoorbeeld een informatiepagina, Fraude Fabels en een Fraude Quiz ontwikkeld om ondernemers te attenderen op de verschillende manieren van online fraude waar ze zakelijk mee te maken kunnen krijgen.

Mijn Cyberweerbare Zaak – subsidieregeling pilot

Via de nieuw ontwikkelde subsidieregeling 'Mijn Cyberweerbare Zaak' is getest of het wegnemen van een financieel knelpunt kleinere ondernemers aanzet tot het nemen van de hoognodige cybersecuritymaatregelen. Kleine bedrijven tot 50 medewerkers zijn in oktober in de gelegenheid gesteld om een subsidie aan te vragen voor de kosten van de aanschaf en implementatie van cruciale cyberweerbaarheidsmaatregelen. Na drie weken openstelling was het subsidiebudget van €300.000 al overtekend. We gaan deze subsidieregeling mogelijk in 2024 opnieuw beschikbaar stellen wanneer de evaluatie van deze pilot daar aanleiding toe geeft.

Hoe krijgen we ondernemers van weten naar doen?

Om meer inzicht te krijgen in de DTC-doelgroep, heeft het DTC ook een gedragsonderzoek laten uitvoeren door TNO. De voorlopige resultaten zijn gepresenteerd tijdens de ONE Conference en bij de Overheidsbrede Cyberwebinars. Het onderzoek biedt inzicht in het aantal en de soorten organisaties en hun barrières en overtuigingen die het nemen van cyber-securitymaatregelen belemmeren. Het onderzoeksrapport wordt in het eerste kwartaal van 2024 gepubliceerd.

DTC Notificatiedienst

Waarschuwingsdienst voor doelwitten en slachtoffers van cyberaanvallen

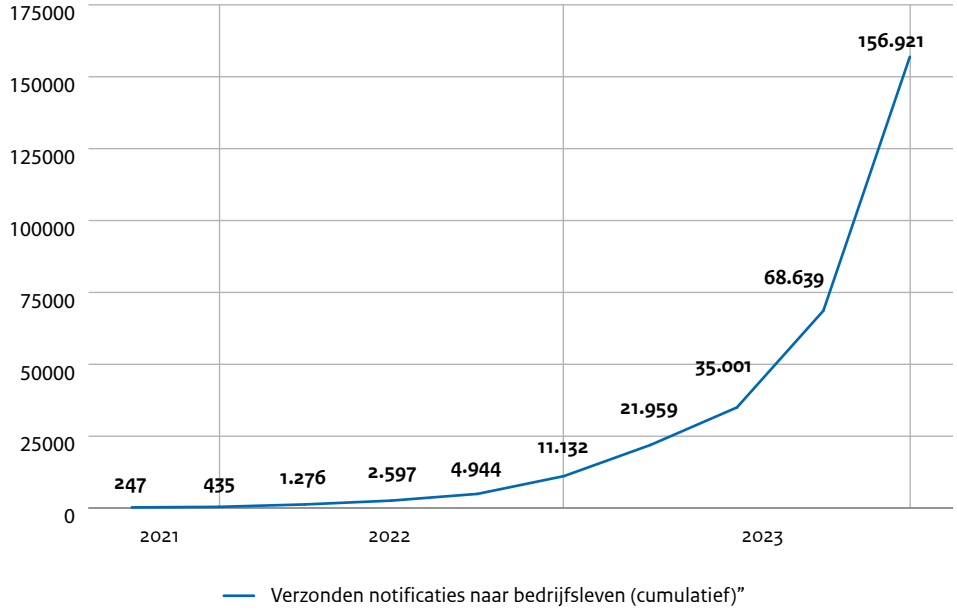
Dagelijks ontvangt de overheid informatie over kwetsbare of gehackte systemen. Dit kan bijvoorbeeld gaan over software waar een fout in zit, systemen waarop door cybercriminelen malware is geïnstalleerd, of systemen die elk moment misbruikt kunnen worden voor een ransomwareaanval. Deze informatie ontvangt de overheid van beveiligingsonderzoekers, ethische hackers en binnen- en buitenlandse partners. Het is essentieel om deze informatie snel bij het bedrijf te krijgen dat slachtoffer of mogelijk doelwit is. Het bedrijf kan dan actie ondernemen om schade te voorkomen of verkleinen.

Als er bij de overheid informatie bekend is over een cyberdreiging voor een organisatie of bedrijf in Nederland, dan verzendt de overheid een waarschuwingsbericht (notificatie). De waarschuwing kan gericht zijn aan de netwerkeigenaar of de (eind)gebruiker van het kwetsbare systeem.

Bijna 140.000 keer gewaarschuwd in 2023

De DTC Notificatiedienst heeft afgelopen jaar een duidelijke groei doorgemaakt. Het aantal kwetsbaarheden waarvoor gewaarschuwd (ofwel genotificeerd) wordt, is de afgelopen maanden substantieel gegroeid. Deze groei is mede mogelijk gemaakt doordat het CSIRT-DSP, het NCSC en het DTC in de zomer van 2023 de krachten zijn gaan bundelen en intensief zijn gaan samenwerken op het gebied van slachtoffer- en doelwitnotificatie. Het DTC heeft het proces van notificeren verbeterd en verder geautomatiseerd wat de efficiëntie ten goede komt.

Grafiek 2: Aantal waarschuwingen voor kwetsbare systemen bij Nederlandse bedrijven



Sinds de start in de zomer van 2021 zijn er 156.921 waarschuwingen richting bedrijven en organisaties gegaan. De stijgende lijn laat zien dat de DTC Notificatiedienst qua impact gegroeid is. Er is veel geautomatiseerd en er zijn meer relevante bronnen ontsloten. Naar verwachting zet deze trend zich in 2024 ook voort omdat er over nog meer soorten kwetsbaarheden genotificeerd gaat worden.

'Ongevraagde' notificaties
'Ongevraagde' notificaties zijn de incidentele waarschuwen over kwetsbaarheden die zonder afspraak verzonden worden naar individuele bedrijven of hun netwerkeigenaren. In één notificatie zitten vaak meerdere IP-adressen wanneer een netwerkeigenaar gewaarschuwd wordt voor meerdere eindgebruikers.

'Gevraagde' notificaties
De ruim 50 (grote) bedrijven waarmee het DTC een paar jaar geleden een pilot voor 'gevraagde' notificaties startte, worden nog steeds genotificeerd als daar aanleiding toe is. In een aantal gevallen worden waarschuwingsberichten herhaald wanneer een pilot-bedrijf geen actie heeft ondernomen en de melding nog openstaat.

Aantal kwetsbaarheden waarop het DTC notificeert groeit

Het aantal kwetsbaarheden waarop genotificeerd wordt, is in de loop van het jaar gestegen. In 2023 stuurden we ongevraagde notificaties voor circa 135 verschillende kwetsbaarheden. Voor gevraagde notificaties ligt dat rond de 160 kwetsbaarheden. Om netwerkeigenaren niet te overladen met notificaties worden waarschuwingen voor dezelfde kwetsbaarheid bij meerdere IP-adressen gebundeld in één bericht. De netwerkeigenaren kunnen de waarschuwing met handelingsperspectief vervolgens doorsturen naar de betrokken eindgebruikers.

Pentest legt ernstige kwetsbaarheid bij DTC bloot

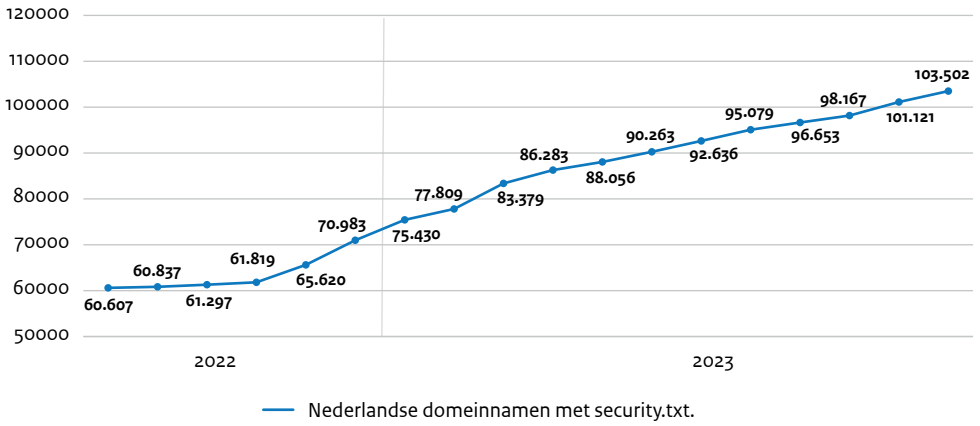
Bij een pentest die het DTC en CSIRT-DSP lieten uitvoeren op hun IT-systemen is door een CCV pentest keurmerk securitybedrijf een ernstige kwetsbaarheid ontdekt. In eerste instantie leverde de pentest niets op, van buitenaf was binnendringen niet mogelijk. Daarop heeft het DTC de pentesters toegang verleend tot één van de systemen en gevraagd om te testen of er na toegang kwaadaardige handelingen mogelijk zijn. Dat bleek het geval te zijn. In webapplicatie Best Practical Request Tracker (RT) bleek het voor de pentester mogelijk om zich voor te doen als een RT-gebruiker en om specifieke e-mailbijlagen te downloaden. De vondst in dit ticketsysteem was extra alarmerend omdat het een zogenoemde zero-day kwetsbaarheid betrof; een kwetsbaarheid die nog niet bekend was bij de leverancier van de webapplicatie. Veel securityteams, CERT's en CSIRT's maken gebruik van dit open source ticketsysteem voor het loggen, opvolgen en monitoren van gemelde cyberincidenten.

Om ervoor te zorgen dat deze zwakke plek in dit belangrijke IT-systeem snel opgelost kon worden, is er contact opgenomen met het Nationaal Cyber Security Centrum (NCSC) door middel van de Coordinated Vulnerability Disclosure-procedure. Het NCSC heeft contact gezocht met de leverancier van de webapplicatie om de problemen onder de aandacht te brengen. Er is vervolgens met alle betrokken partijen en de leverancier hard gewerkt om een beveiligingsupdate (patch) mogelijk te maken.

Security.txt op 'Pas toe of leg uit'-lijst

Het DTC zoekt dagelijks naar de beste en snelste manier om organisaties op de hoogte te stellen van digitale kwetsbaarheden. Het valt soms niet mee om de juiste persoon of afdeling binnen een organisatie te contacteren. Security.txt helpt hierbij. Het DTC heeft zich daarom ingezet om deze internetstandaard RFC9116 op de 'Pas toe of leg uit'-lijst te krijgen. Na een zorgvuldig afwegingsproces is deze standaard op de 'Pas toe of leg uit'-lijst gekomen en daarmee verplicht geworden voor overheidsorganisaties. Heeft jouw bedrijf of organisatie nog geen security.txt? Overweeg om dit ook voor jouw organisatie beschikbaar te maken via een gemakkelijk stappenplan.

Grafiek 3: Nederlandse domeinnamen met security.txt



In oktober 2022 heeft DTC in een campagne met veel ambassadeurs opgeroepen om security.txt te gaan gebruiken.

DTC Community

De DTC Community biedt bedrijven de mogelijkheid om actuele en relevante cybersecurity informatie, tips en *best practices* uit te wisselen. Dat allemaal op een onafhankelijk, niet-commercieel en veilig platform. Daarnaast is er een NIS2-themaruimte, waar leden met elkaar in gesprek gaan over de aankomende wetgeving.

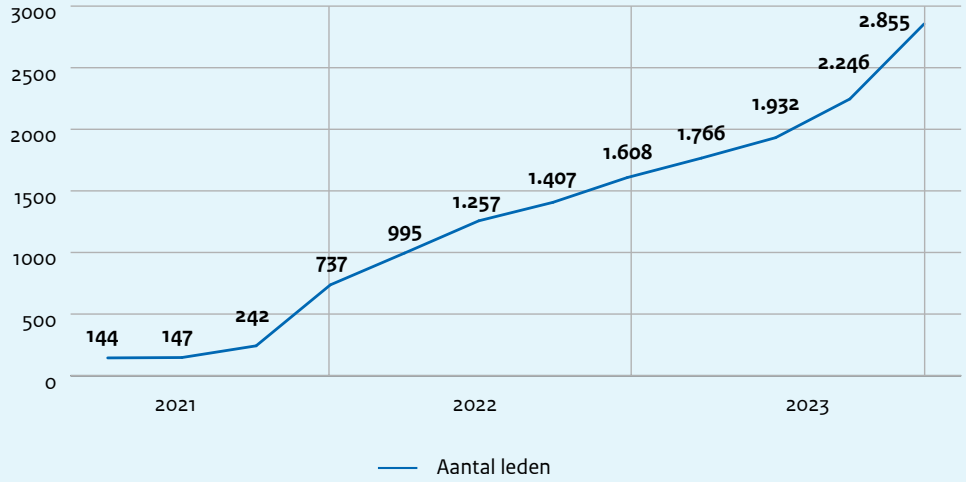
Uitbreiding van de DTC Community

Onze DTC Community heeft een indrukwekkende groei doorgemaakt. Sinds de start in 2021 hebben 2.855 bedrijven en organisaties zich aangesloten bij het cybersecurityforum. Een groot deel van de leden (19%) is ondernemer, CEO of directeur. Ook CISO's zijn goed vertegenwoordigd met 23%. Daarnaast zijn er veel IT-managers, systeembeheerders, consultants, engineers en CTO's actief op de community. Deze diversiteit onderstreept de relevantie van de DTC Community in verschillende sectoren.

"De DTC Community is hét cybersecurity forum van Nederland."

- Michel Verhagen, manager DTC

Grafiek 4: Ondernemers en IT-professionals aangesloten bij DTC Community



Kennisdeling en Samenwerking

"Via de DTC Community vergroot ik mijn netwerk, deel ik actuele kennis en leer ik van anderen."

Binnen de DTC Community hebben we een omgeving gecreëerd voor het delen van actuele cybersecurity-informatie, tips en *best practices*. De DTC Community is er voor iedereen die aan de slag wil met cybersecurity. Van starters tot professionals. Het platform heeft zich ontwikkeld tot een centrale hub waar IT-professionals, CISO's en ondernemers elkaar helpen, kennis uitwisselen en gezamenlijk werken aan een digitaal weerbaar Nederland. Zo kun je vragen stellen aan experts in dit vakgebied; bijvoorbeeld over awareness, ransomware of incident response.

"Door dreigingsinformatie te ontvangen kan ik onze systemen snel updaten wanneer dat nodig is."

NIS2-themaruimte

Een belangrijke toevoeging aan de DTC Community is de NIS2-themaruimte, waar leden met elkaar in gesprek gaan over de aankomende wetgeving. Deze ruimte dient als een waardevol forum voor discussies en het delen van inzichten over de gevolgen van deze wetgeving op de verschillende organisaties, klanten en (toe)leveranciers.

Berichten en interactie

"Als CISO wil ik via betrouwbare bronnen op de hoogte zijn van wat er speelt."

In 2023 zijn de berichten op de DTC Community bijna 30.000 keer gelezen. Daarnaast zijn er in dit jaar 44 cyber alerts over urgente kwetsbaarheden gepubliceerd door het DTC en door securitybedrijven. En stel je een vraag aan community leden? Dan heb je vaak al binnen een uur meerdere reacties en adviezen ontvangen van mede-ondernemers of cybersecurity professionals.

Wat we horen van leden

We hebben waardevolle feedback ontvangen van onze leden, waarbij zij benadrukken dat de DTC Community niet alleen een bron van betrouwbare informatie is, maar ook een platform voor netwerken en samenwerken.

Vooruitblik DTC Community

In 2024 zullen we vooral inzetten op het aantrekken van meer leden door middel van een doorlopende campagne. Daarnaast is het altijd van belang om de DTC Community te voorzien van actuele, relevante content. Zowel vanuit de leden, het DTC en organisaties waar we veel mee samenwerken. Uiteraard blijven we in de tussentijd het platform verbeteren, met nieuwe functionaliteiten en verbeterde designs. Daarnaast verkennen we de mogelijkheid om de community óók offline – tijdens een fysieke bijeenkomst – samen te brengen.

Tenslotte kijken we met de DTC Community natuurlijk ook uit naar de integratie met het NCSC en het CSIRT-DSP. Hoe de community er dan precies uit komt te zien is nog niet zeker, maar we weten wél dat er behoefte is aan kennisdeling en dat we samen nog meer organisaties kunnen bereiken en bedienen.

"Ondernemers, IT-professionals en experts komen samen op de DTC Community. Ze zijn ontzettend behulpzaam en leden reageren vaak binnen enkele minuten op elkaars vragen. Ik ben trots dat we met het Digital Trust Center dit onafhankelijke platform hebben laten groeien tot een community met meerwaarde voor leden en bedrijven. Met behulp van de DTC Community maken bedrijven elkaar weerbaarder tegen cyberdreigingen. Dat is toch fantastisch?"

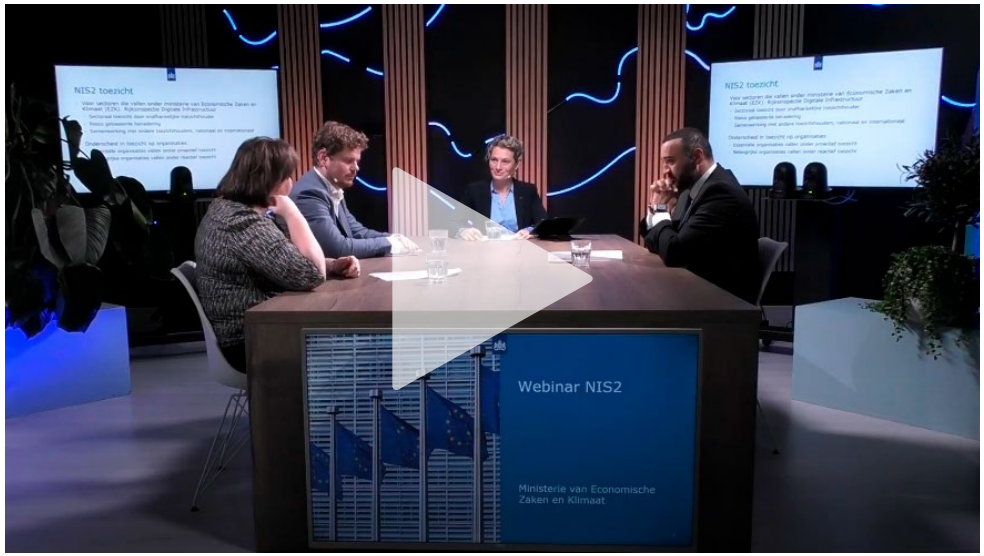
- Irene van der Zanden, manager DTC Community

NIS2

De cyberwereld stond in 2023 onder andere in het teken van de *Network and Information Security directive*, oftewel NIS2-richtlijn. Deze richtlijn is vastgesteld door de Europese Unie. Op dit moment wordt binnen de Rijksoverheid gewerkt aan de nationale implementatie door deze richtlijn om te zetten naar Nederlandse wetgeving. De richtlijn heeft impact op meerdere type bedrijven; essentieel en belangrijk én de leveranciers in de keten van deze essentiële en belangrijke entiteiten. Duizenden bedrijven in Nederland zullen eind 2024 aan deze richtlijn moeten voldoen. Daarmee gaat de richtlijn de doelgroep van het DTC raken. Een deel van de DTC-doelgroep zal een NIS2-bedrijf worden. Naast deze groep zullen ook veel bedrijven indirect bijvoorbeeld via de keten, te maken krijgen met de wetgeving die voortkomt uit NIS2.

Om deze doelgroep te informeren over de aankomende wetgeving organiseerde het DTC samen met beleidsmedewerkers van het Ministerie van Economische Zaken en Klimaat op 5 oktober het webinar '[De impact van NIS2 op jouw organisatie]'. In het webinar vertelden EZK-beleidsmedewerkers wat de NIS2-richtlijn is en wat voor impact deze richtlijn heeft op bedrijven in Nederland. Het DTC gaf in dit webinar uitleg over welke maatregelen organisaties nu kunnen nemen ter voorbereiding op de NIS2-richtlijn, omdat het ook nu al van belang is dat organisaties aan de slag gaan met het verhogen van hun cyberweerbaarheid. Er staan een aantal maatregelen in de richtlijn waar bedrijven nu al mee aan de slag kunnen, bijvoorbeeld het uitvoeren van een risicoanalyse.

In 2024 gaat het DTC door met het bieden van handvatten, informatie en advies aan de bedrijven die te maken krijgen met de NIS2-richtlijn. In samenwerking met andere overheidsorganisaties zoals het NCSC en RDI worden diverse communicatiemiddelen ontwikkeld met als doel zoveel mogelijk organisaties te helpen bij het verhogen van hun cyberweerbaarheid. Wat sowieso geldt: of je bedrijf wel of niet, direct of indirect aan deze wet moet gaan voldoen: het is altijd verstandig om je cyberweerbaarheid naar een hoger niveau te brengen.



DTC-netwerk in beeld

In de dynamische wereld van cybersecurity is samenwerken de sleutel tot overleven. Door samen de krachten te bundelen en kennis te delen, speelt het DTC een sleutelrol bij het versterken van de digitale veerkracht. Onze partners en samenwerkingsverbanden zijn hierin onmisbaar. In 2023 heef het DTC 12 nieuwe samenwerkingsverbanden verwelkomd. Daarmee is het totale aantal unieke samenwerkingsverbanden in 2023 op 60 uitgekomen.

Aan het woord: Samenwerkingsverband CCRC

Het Cyber Chain Resilience Consortium (CCRC) is een non-profit platform waar publieke en private organisaties en hun toeleveranciers, cross sectoraal samenwerken om zich te beschermen tegen cyberaanvallen in de keten door het uitvoeren van laagdrempelige cybercrisis oefeningen voor managers en directie.

In het afgelopen jaar hebben we meer dan 150 deelnemers mogen verwelkomen tijdens onze Cyber Boost sessies. Dit waren voornamelijk IT-managers, CEO's , CFO's, en (C)ISO's van het MKB en groot zakelijk die d.m.v. het managen van een 3 uur durende gesimuleerde cybercrisis met meer

hands-on ervaring en concrete handvaten terug naar hun organisaties gingen. Daarnaast hebben we het boek "Cybercrisis: Geen Paniek - Handboek Oefenen van een Cybercrisis", verschillende *whitepapers* en een crisiskaart gepubliceerd.

Dit succes is mede mogelijk gemaakt door de versnelling die CCRC doorgemaakt heeft, dankzij de waardevolle steun en samenwerking met het DTC. Het DTC-netwerk en de betrokken relatiemanager speelden een sleutelrol bij het realiseren van onze missie. Door diverse samenwerkingsverbanden kregen we de kans om onze aanpak te delen, wat resulteerde in meerdere succesvolle opdrachten. Nu we dankzij de hulp van het DTC goed op stoom zijn, kijken we vol vertrouwen uit naar 2024 waar we onze scope verbreden op het beheersen van *business continuity management*, waarbij cybercrisisoefeningen een essentieel onderdeel vormen van onze aanpak.

Ondernemer aan het woord: Threadstone

"Wij bedienen vanuit de Techone groep meer dan 50.000 mkb-klanten in Nederland en gebruiken de CyberVeilig Check om basismaatregelen in kaart te brengen. Voor ons is de CyberVeilig Check waardevol omdat deze tool vanuit een onafhankelijke, publieke organisatie wordt geleverd. In de markt worden allerlei scans aangeboden, maar welke moet je als mkb'er nou vertrouwen en gebruiken?

Daarom helpen wij onze klanten met het doorlopen van de CyberVeilig Check, inclusief onze verdiepende vragen. Wij zijn van mening dat we hier als professioneel dienstverlener ook een zorgplicht richting onze klanten hebben."

- René van Etten, Threadstone Cyber Security

Vooruitblik naar de vernieuwde organisatie

Om de versnippering in het cybersecuritystelsel tegen te gaan, heeft het kabinet besloten om het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC) en het Computer Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP) te integreren in één centrale, zichtbare en effectieve cybersecurityorganisatie.

De integratie verloopt gefaseerd, in de eerste fase tot 1 oktober 2024 werken de organisaties al zoveel mogelijk samen. Zo is er een gezamenlijk loket geopend voor meldingen van dreigingen en kwetsbaarheden. Alle taken en processen moeten op 1 januari 2026 volledig geïntegreerd en geoptimaliseerd zijn. Enkele medewerkers van het NCSC, DTC en CSIRT-DSP vertellen hoe ze tegen de vernieuwde organisatie aankijken:

"Waar ik naar uitkijk in de vernieuwde organisatie? Om kennis en expertise te bundelen met mijn, nu nog (in-)directe, collega's om gezamenlijk doelgroep gedreven producten- en diensten te leveren. Dit zie ik als de kern. En natuurlijk om hét nationale CSIRT van Nederland te worden."

- Mike Henschen, securityanalist CSIRT-DSP

"Toenemende cyberdreigingen, met in het bijzonder cyberaanvallen als gevolg van ketenafhankelijkheid, maken de integratie van het NCSC, het DTC en het CSIRT-DSP naar een vernieuwde organisatie zo essentieel. Op die manier kunnen we met al onze kennis en capaciteit de volledige doelgroep van zowel rijk, vitaal als het bedrijfsleven beter bedienen."

- Erwin Hasenpflug,
cybersecurityadviseur DTC

"Het is een mooi vooruitzicht om straks één nationale cybersecurity organisatie vanuit de overheid te hebben, maar ik vind de weg ernaartoe minstens net zo waardevol. Want deze weg moet gezamenlijk bewandeld worden, niet alleen door de drie organisaties die samen gaan, maar samen met alle cybersecurity partners in het stelsel.

De weg zit niet zonder uitdagingen en dat is juist fijn, want in die uitdagingen zit de verbinding. En met elke verbinding die we samen maken, komen we steeds een stapje dichterbij een digitaal weerbaar Nederland. Hoe geweldig om hieraan te mogen bijdragen!"

- Ying Ying Lau,
strategisch relatiemanager samenwerken NCSC

“Elk veranderproces is uniek. In dit transitieprogramma brengen we drie cybersecurityorganisaties samen met ieder een eigen opgave, doelgroepen, werkwijzen én unieke kwaliteiten. We zoeken steeds naar het beste van die werelden én meer. Dat doen we vooral door nu al intensief samen te werken, op weg naar 2026.”

- Dora Horjus, transitiemanager de vernieuwde cybersecurityorganisatie

“Door samen te gaan als drie cyberorganisaties brengen we mensen en expertise bij elkaar waarmee we bedrijven van zzp-er tot vitaal grootbedrijf kunnen faciliteren cyberweerbaar te worden. Van buiten naar binnen werkend en met vertrouwen en collegialiteit als fundament maken we van 1 + 1 + 1 vijf.”

- Michel Verhagen, manager DTC

“Samenwerking wordt in de praktijk vaak genoeg in de weg gestaan door praktische bezwaren, belemmeringen en belangen. Het geeft me energie en vertrouwen om te zien dat we in de aanloop naar de vernieuwde organisatie al gezamenlijk ondervinden dat niks ons in de weg staat om echt samen te bouwen aan 1 krachtige nationale cybersecurity organisatie.”

- Corine Schipper-Derkse, waarnemend directeur NCSC

Colofon

DTC Terugblik
Editie 3 Jaargang 2023

Publicatiedatum
12 januari 2024

Hoofdredactie
Digital Trust Center

Productie
Digital Trust Center

Vormgeving
Xerox / OSAGE

Website
digitaltrustcenter.nl

Redactieadres
Postbus 20401 2500 EK Den Haag

Copyright
CCo 1.0 Universal

Volg ons via: