Evaluatie programma Digital Trust Center

Eindrapport

20 januari 2020

Ir. Bill van Mil
Pauline Modderman, MSc.
Frederique Uyterlinde, MSc.

KWINK GROEP

Samenvatting

Dit rapport betreft een evaluatie van het programma Digital Trust Center (DTC). Het DTC heeft als missie het niet vitale bedrijfsleven weerbaarder te maken tegen cyberdreigingen. De doelgroep van het DTC bestaat uit circa 1,8 miljoen bedrijven in Nederland die niet behoren tot de vitale infrastructuur en Rijksoverheid.

Aanleiding

Begin 2018 is het ministerie van Economische Zaken en Klimaat (EZK) samen met het ministerie van Justitie en Veiligheid (JenV) gestart met het programma Digital Trust Center. Het programma loopt van 2018 tot en met 2020. Ook na afloop van het programma is er structureel geld beschikbaar voor het voortzetten van de activiteiten. In het kader van de verdere voortzetting vindt het DTC het belangrijk om haar inspanning te evalueren en te toetsen in hoeverre het DTC in staat is geweest haar doelgroep te bereiken en te voorzien van nuttige en praktische informatie. Deze evaluatie vormt tevens input voor de besluitvorming over de toekomst van het DTC, waarover de Tweede Kamer begin 2020 wordt geïnformeerd.

Onderzoeksvragen en aanpak

De centrale onderzoeksvraag van dit onderzoek is: *Welke bijdrage heeft het programma Digital Trust Center geleverd (in de eerste twee jaren) aan de cyberweerbaarheid van ondernemend Nederland en wat is er voor nodig om deze bijdrage te vergroten?*

Het DTC heeft bij de centrale onderzoeksvraag drie subvragen meegegeven:

1. In hoeverre zijn de doelstellingen zoals genoemd in de Kamerbrief van 17 juni 2019 gehaald?[1]
2. Hoe is de samenwerking vormgegeven met het Nationale Cyber Security Centrum?
3. Hoe is de samenwerking vormgegeven met overige stakeholders?

De evaluatie heeft plaatsgevonden in de periode november 2019 tot en met januari 2020. Voor het beantwoorden van de onderzoeksvragen is een data- en documentenanalyse uitgevoerd en hebben 30 interviews plaatsgevonden met vertegenwoordigers van het DTC, het ministerie van EZK, het Nationaal Cyber Security Centrum (NCSC), de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), bij het DTC aangesloten samenwerkingsverbanden en brancheorganisaties, en overige stakeholders (zie bijlage 1 voor een overzicht van de gesprekspartners).

Conclusies

Hierna geven we een samenvatting van de belangrijkste conclusies ten aanzien van de onderzoeksvragen.

Hoofdvraag: Welke bijdrage heeft het DTC geleverd (in de eerste twee jaren) aan de cyberweerbaarheid van ondernemend Nederland en wat is er voor nodig om deze bijdrage te vergroten?

Het DTC heeft in korte tijd een organisatie opgezet die zich met een klein team richt op de doelgroep van 1,8 miljoen niet-vitale bedrijven in Nederland. Het DTC heeft een bijdrage geleverd aan de cyberweerbaarheid van ondernemend Nederland door informatie en advies te geven (hoofdtaak 1) en door samenwerkingsverbanden te stimuleren (hoofdtaak 2).

- **Informatie- en adviesfunctie:** Het DTC heeft een website en verschillende producten ontwikkeld. De informatie en producten van het DTC worden over het algemeen goed ontvangen en voorzien in een behoefte van bedrijven. De informatie en producten zijn met name geschikt voor het MKB en zzp-ers. De informatie en producten sluiten niet goed aan op de informatiebehoefte en vragen van grote/volwassen bedrijven. Voorts heeft het DTC een interactief platform opgezet welke eind november 2019 live is gegaan in een opstartfase.

[1] Het betreft Kamerstuk 26643, nr. 616.

Uit de evaluatie zijn signalen naar voren gekomen die erop wijzen dat er een kans is dat het platform in de praktijk door een beperkter aantal bedrijven gebruikt gaat worden dan waarvoor het bedoeld was: een interactieve omgeving waarin bedrijven, samenwerkingsverbanden en experts hun kennis kunnen delen en vermeerderen. Wanneer het platform volledig in gebruik is genomen zal duidelijk worden in hoeverre het inderdaad wel of niet voorziet in een behoefte van bedrijven.

- **Aanjaagfunctie samenwerkingsverbanden:** Het DTC heeft samenwerkingsverbanden aan zich verbonden en faciliteert deze onder andere door het verstrekken van informatie en adviezen, het faciliteren van productontwikkeling en kennisdeling, en door middel van subsidieverstrekking. We concluderen hierover het volgende:
    - De ondersteuning van het DTC sluit grotendeels aan bij de behoefte van de samenwerkingsverbanden.
    - Het DTC kan nog meer van meerwaarde zijn voor de samenwerkingsverbanden door meer praktische tools te ontwikkelen, waarmee bedrijven daadwerkelijk tot actie kunnen overgaan om hun cyberweerbaarheid te vergroten.
    - Het DTC is voor samenwerkingsverbanden met veel grote/volwassen, niet-vitale bedrijven in hun achterban van minder toegevoegde waarde, omdat deze samenwerkingsverbanden met name behoefte hebben aan actuele (dreigings)informatie van het NCSC. Het NCSC kan deze informatie (nog) niet altijd met het DTC delen.
    - Het DTC monitort of evalueert niet de *effecten* van de activiteiten van de samenwerkingsverbanden. De lessen die uit de ervaringen van de samenwerkingsverbanden kunnen worden getrokken, kunnen nog meer worden opgeschaald zodat ze van meerwaarde zijn voor een grotere groep bedrijven, waaronder bedrijven die geen lid zijn van een samenwerkingsverband.

De bijdrage van de bovengenoemde activiteiten van het DTC aan de cyberweerbaarheid van ondernemend Nederland is lastig te meten. Er zijn allerlei andere factoren van invloed op de cyberweerbaarheid van bedrijven, zoals andere programma's en organisaties. Daardoor is de toerekenbaarheid van effecten aan het DTC lastig vast te stellen. Uit recente cijfers van het CBS *(Statistiek ICT-gebruik bedrijven 2019*) blijkt wel dat DTC-bedrijven (bedrijven die zich hebben aangesloten bij een samenwerkingsverband) wat bewuster met ICT-veiligheid om lijken te gaan dan een groep vergelijkbare bedrijven. Ook uit deze cijfers kunnen echter geen conclusies over de bijdrage van het DTC getrokken worden.

Subvraag 1: In hoeverre zijn de doelstellingen zoals genoemd in de Kamerbrief van 17 juni 2019 gehaald?

In de Kamerbrief zijn negen doestellingen en ambities opgenomen. Zeven van deze doelstellingen zijn volledig gehaald, waarvan twee met vertraging. Een doelstelling is deels gehaald. Van de doelstelling om het DTC door te ontwikkelen tot een "one-stop-shop voor het niet-vitale bedrijfsleven" is niet vast te stellen of deze gehaald is, omdat deze doelstelling niet SMART is gemaakt en het daardoor niet helder is wat het zijn van een one-stop-shop inhoudt.

Subvraag 2: Hoe is de samenwerking vormgegeven met het Nationale Cyber Security Centrum?

Goede samenwerking met het NCSC is cruciaal voor het slagen van het DTC. Het DTC en het NCSC hebben op verschillende manieren samengewerkt. De samenwerking tussen het NCSC en het DTC kent ook knelpunten, waardoor er sprake was van een moeilijke start van de samenwerking. Een lastige factor in de samenwerking is dat het NCSC persoonsgegevens niet mag delen met het DTC, doordat het DTC geen wettelijke grondslag heeft om persoonsgegevens te ontvangen en te verwerken, het DTC specifieke dreigingsinformatie niet kan uitsluiten voor de Wet openbaarheid van bestuur (Wob) en het DTC niet is

aangewezen als OKTT (in de zin van Wbni, art. 3.2[2]). Beide organisaties zijn wel overtuigd van het belang van een goede samenwerking en er is en wordt ook gewerkt aan het verbeteren van de samenwerking.

Subvraag 3: Hoe is de samenwerking vormgegeven met overige stakeholders?

Het DTC werkt veel en intensief samen met allerlei partijen (brancheorganisaties, platforms en kennisinstituten) en heeft daardoor een goed netwerk op het terrein van cyberweerbaarheid. Mede hierdoor is er veel draagvlak en een gevoel van eigenaarschap voor het DTC onder relevante stakeholders. Op sommige punten kan de samenwerking tussen het DTC en andere partijen nog worden geïntensiveerd. Zo kan het DTC nog meer aansluiten bij al bestaande initiatieven (zoals congressen en campagnes) van samenwerkingspartners. Op deze wijze kunnen veel bedrijven bereikt worden en hoeft het DTC minder zelf te ontwikkelen. Ook kan het DTC meer informatie delen met andere organisatieonderdelen van het ministerie van EZK, zodat de informatie die het DTC tot haar beschikking heeft bijvoorbeeld gebruikt kan worden bij het opstellen van beleid.

Aanbevelingen

Op grond van het onderzoek bevelen we het DTC het volgende aan:

1. We bevelen het DTC aan in een volgende fase van het DTC toe te werken naar vergroting van het bereik/effect.
   a. Door doelgroepen te segmenteren en vervolgens per segment te bezien waar ‘grote klappers’ kunnen worden gemaakt. Dit kan bijvoorbeeld door intensief samen te gaan werken met de drie brancheorganisaties met de grootste achterban of door aanwezig te zijn op congressen waar veel bedrijven uit de doelgroep van het DTC komen.
   b. Door gebruik te maken van gedragsinzichten *(behavourial insights)* aangaande specifieke doelgroepen: wat is er nodig om bedrijven echt hun gedrag te laten aanpassen?
   c. Door meer informatie te verzamelen die zicht geeft op de effecten van de activiteiten van het DTC. Het DTC houdt al veel informatie bij over de eigen activiteiten en die van samenwerkingsverbanden. Om meer zicht te krijgen op de effecten van deze activiteiten raden we het DTC aan meer informatie onder gebruikers te verzamelen en voorbeelden te verzamelen die een beeld geven van wat de ondersteuning door het DTC oplevert voor samenwerkingsverbanden.
2. Grote/volwassen, niet-vitale bedrijven hebben behoefte aan specifieke dreigingsinformatie, maar ontvangen deze informatie momenteel nog niet altijd. We bevelen aan dat voorwaarden gecreëerd worden waaronder relevante dreigingsinformatie gedeeld kan worden met grote/volwassen, niet-vitale bedrijven.
3. Een goede samenwerking tussen het DTC en het NCSC is cruciaal. We bevelen aan de samenwerking tussen het DTC en het NCSC te versterken door te werken aan een gevoel van gezamenlijkheid en door de samenwerking regelmatig te evalueren.
4. Het is lastig om vooraf de inschatting te maken in hoeverre bedrijven het platform daadwerkelijk zullen gaan gebruiken. We bevelen het DTC daarom aan om het succes van het platform te monitoren en toekomstige (investerings)beslissingen daarop aan te passen. Voorts bevelen we aan realistisch te zijn in de verwachtingen over de deelname aan het platform en de inzet van tijd en middelen door het DTC daarop aan te passen: mocht uit het monitoren van het platform blijken dat het platform in de behoefte van slechts een zeer klein aantal bedrijven voorziet, dan dient ook de mogelijkheid om te stoppen met het platform of alleen een ‘light’ versie aan te bieden overwogen te worden.

[2] De Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) is sinds 9 november 2018 van kracht. Instanties die zijn aangewezen als OKTT in de zin van Wbni, art. 3.2, zijn bevoegd verkregen gegevens over dreigingen en incidenten met betrekking tot bepaalde netwerk- en informatiesystemen te delen met een selectie van andere organisaties.

Inhoud

1. Inleiding

In dit hoofdstuk beschrijven we allereerst de aanleiding van deze evaluatie. Vervolgens lichten we de onderzoeksvragen van de evaluatie en de gehanteerde onderzoeksmethoden toe. We sluiten dit hoofdstuk af met een leeswijzer.

1.1. Aanleiding

Begin 2018 is het ministerie van Economische Zaken en Klimaat (EZK) samen met het ministerie van Justitie en Veiligheid (JenV) gestart met het programma Digital Trust Center (DTC). Het DTC heeft als missie het niet vitale bedrijfsleven weerbaarder te maken tegen cyberdreigingen. De doelgroep van het DTC bestaat uit circa 1,8 miljoen bedrijven in Nederland die niet behoren tot de vitale infrastructuur en Rijksoverheid. Hiertoe zijn twee hoofdtaken voor het DTC onderscheiden. De eerste hoofdtaak is een informatie- en adviesfunctie en betreft het informeren van ondernemend Nederland over cyberweerbaarheid en het geven van een handelingsperspectief omtrent actuele dreigingen en kwetsbaarheden. De tweede hoofdtaak is een aanjaagfunctie voor samenwerkingsverbanden (cyberweerbaarheidsnetwerken) en betreft het tot stand helpen brengen van een stelsel van intermediaire organisaties.

Het programma DTC loopt van 2018 tot en met 2020. Ook na afloop van het programma is er structureel geld beschikbaar voor het voortzetten van de hierboven genoemde activiteiten.[3] In het kader van de verdere voortzetting vindt het DTC het belangrijk om haar inspanning te evalueren en te toetsen in hoeverre het DTC in staat is geweest haar doelgroep te bereiken en te voorzien van nuttige en praktische informatie. Deze evaluatie vormt tevens input voor de besluitvorming over de toekomst van het DTC, waarover de Tweede Kamer begin 2020 geïnformeerd wordt.

1.2. Onderzoeksvragen

De centrale onderzoeksvraag van dit onderzoek is: *Welke bijdrage heeft het programma Digital Trust Center geleverd (in de eerste twee jaren) aan de cyberweerbaarheid van ondernemend Nederland en wat is er voor nodig om deze bijdrage te vergroten?*

Het DTC heeft bij de centrale onderzoeksvraag drie subvragen meegegeven:

1. In hoeverre zijn de doelstellingen zoals genoemd in de Kamerbrief van 17 juni 2019 gehaald?[4]
2. Hoe is de samenwerking vormgegeven met het Nationale Cyber Security Centrum?
3. Hoe is de samenwerking vormgegeven met overige stakeholders?

1.3. Onderzoeksmethoden

De evaluatie heeft plaatsgevonden in de periode november tot en met januari 2020. Voor het beantwoorden van de onderzoeksvragen zijn de volgende onderzoeksmethoden ingezet:

- Om in kaart te brengen welke bijdrage het DTC heeft geleverd aan de cyberweerbaarheid van ondernemend Nederland is allereerst een **data- en documentenanalyse** uitgevoerd naar de activiteiten en resultaten van het

[3] Zie: http://www.rijksbegroting.nl/2020/voorbereiding/begroting,kst264855_12.html

[4] Het betreft Kamerstuk 26643, nr. 616.

DTC. Hiertoe zijn interne documenten van het DTC, Kamerbrieven, en wet- en regelgeving bestudeerd. Ook is gebruik gemaakt van de CBS-cijfers uit *Statistiek ICT-gebruik bedrijven 2019.*[5]

- Vervolgens hebben 30 **interviews** plaatsgevonden met vertegenwoordigers van het DTC, het ministerie van EZK, het Nationaal Cyber Security Centrum (NCSC), de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), bij het DTC aangesloten samenwerkingsverbanden en brancheorganisaties, en overige stakeholders (zie bijlage 1 voor een overzicht van de gesprekspartners). In de gesprekken is ingegaan op de bijdrage van het DTC aan de cyberweerbaarheid van ondernemend Nederland en op de vormgeving van de samenwerking. Tevens vormden deze gesprekken input voor aanbevelingen om de bijdrage van het DTC aan de cyberweerbaarheid van ondernemend Nederland te vergroten.

Op basis van een analyse van de verzamelde informatie zijn conclusies en aanbevelingen geformuleerd. Om tot deze conclusies en aanbevelingen te komen is onderscheid gemaakt tussen feiten (die onomstotelijk vaststaan of beschrijvend van aard zijn), percepties van gesprekspartners (opvattingen van betrokken partijen die wij geïnterviewd hebben), en ons eigen oordeel.

1.4. Leeswijzer

In het vervolg van dit rapport lichten we in hoofdstuk 2 allereerst de totstandkoming en invulling van het programma DTC toe. Vervolgens behandelen we in hoofdstuk 3 de activiteiten, resultaten en samenwerking van het DTC. In hoofdstuk 4 gaan we in op het doelbereik van het DTC. Hoofdstuk 5 bevat tot slot onze conclusies ten aanzien van de onderzoeksvragen en aanbevelingen om de bijdrage van het DTC aan de cyberweerbaarheid van ondernemend Nederland te vergroten.

De bijlagen bij het rapport bevatten een overzicht van de gesprekspartners (bijlage 1) en een samenvatting van de CBS-cijfers uit *Statistiek ICT gebruik bedrijven 2019* (bijlage 2).

[5] Zie: https://www.cbs.nl/nl-nl/maatwerk/2019/50/ict-kenmerken-bedrijven-digital-trust-center.

2. Het programma Digital Trust Center

In dit hoofdstuk introduceren we het programma Digital Trust Center. We lichten kort de totstandkoming van het programma toe en beschrijven de missie, hoofdtaken en doelgroep van het programma. Ook gaan we in op de governance van het DTC. We geven eerst de feitelijke informatie weer en beschrijven daarna de beelden van gesprekspartners. In dit hoofdstuk formuleren we geen conclusies, omdat we deze onderwerpen als achtergrondinformatie hebben opgenomen en er geen onderzoeksvragen met betrekking tot deze onderwerpen hoeven te worden beantwoord.

Wat zijn de feiten?

Totstandkoming DTC

Op Prinsjesdag 2017 is bekend geworden dat het DTC zou worden opgericht. Hiermee gaf het Kabinet invulling aan de motie Hijink/Tellegen[6] en het advies van de Cyber Security Raad[7] om een centrum op te richten om niet-vitale bedrijven en maatschappelijke organisaties te informeren en adviseren over, en concrete hulp en ondersteuning te bieden bij, het verbeteren van hun cyberweerbaarheid.

Na Prinsjesdag zijn de plannen voor het DTC verder uitgewerkt door een kernteam van EZK en medewerkers van het NCSC. Stakeholders binnen en buiten de overheid zijn bij dit proces betrokken geweest middels een klankbordgroep, drie ronde tafelconferenties en bilaterale gesprekken met het bedrijfsleven.[8]

Begin 2018 is het DTC opgericht in de vorm van een programma binnen het ministerie van EZK. Het Programmaplan Digital Trust Centre 2018-2020 is opgesteld voor een periode van drie jaar. Voor deze periode is gekozen omdat de inschatting was dat het drie jaar zou duren voordat een aantal vraagstukken en de vormgeving van het DTC voldoende zouden zijn uitgekristalliseerd.[9] Het DTC heeft thans 12 medewerkers (11 fte) in dienst.

In het Programmaplan Digital Trust Centre 2018-2020 wordt aangegeven dat ruim voor het eind van het driejarige programma een besluit moet worden genomen over het al dan niet voortzetten van het Digital Trust Center en in welke hoedanigheid. In de Kamerbrief van 17 juni 2019 geeft de Staatssecretaris van EZK aan dat de Tweede Kamer hierover in het tweede kwartaal van 2020 wordt geïnformeerd.[10]

Missie, hoofdtaken en ambities

De missie van het DTC is om ondernemend Nederland in staat te stellen haar weerbaarheid tegen cyberdreigingen te vergroten. De visie die het DTC daarbij heeft geformuleerd is: "*Het DTC is de betrouwbare en onafhankelijke partner die verbindt en zorgt voor een netwerk voor ondernemend Nederland en samenwerking op het gebied van cybersecurity*". Het DTC wil werken vanuit de waarden betrouwbaar, vindbaar en onafhankelijk (van commercie).[11]

Om de missie te realiseren zijn twee hoofdtaken voor het DTC onderscheiden:

1. Het informeren en het geven van een handelingsperspectief omtrent actuele dreigingen en kwetsbaarheden (informatie- en adviesfunctie);
2. Een stelsel van intermediaire organisaties tot stand helpen brengen (aanjaagfunctie samenwerkingsverbanden).

[6] Kamerstuk 26643, nr. 474.
[7] Cyber Security Raad (2017). *Naar een dekkend stelsel van informatieknooppunten.*
[8] Ministerie van EZK (2017). *Programmaplan Digital Trust Centre 2018-2020*, p. 5.
[9] Ministerie van EZK (2017). *Programmaplan Digital Trust Centre 2018-2020*, p. 5.
[10] Kamerstuk 26643, nr. 616.
[11] Ministerie van EZK (2017). *Programmaplan Digital Trust Centre 2018-2020*, p. 8.

In het Programmaplan Digital Trust Centre 2018-2020 worden ten aanzien van deze hoofdtaken de volgende ambities geformuleerd:[12]

1. Hoofdtaak 1: Een platform dat actuele, begrijpelijke en relevante informatie beschikbaar stelt over cyberdreigingen en hoe te handelen, zowel bij incidenten als ter bevordering van de weerbaarheid in structurele zin.
2. Hoofdtaak 2: Een landelijk dekkend stelsel van informatieknooppunten voor ondernemend Nederland op het gebied van cybersecurity.

Doelgroep

De doelgroep van het DTC bestaat uit circa 1,8 miljoen bedrijven in Nederland die niet behoren tot de vitale infrastructuur en Rijksoverheid. Deze doelgroep bevat 1,4 miljoen bedrijven waar één persoon werkzaam is (veelal zzp'ers) en bijna 400 duizend bedrijven met twee tot 100 medewerkers.[13] Bedrijven in vitale sectoren, zoals banken of energiebedrijven, behoren niet tot de doelgroep van het DTC. Deze bedrijven hebben het NCSC als samenwerkingspartner binnen de Rijksoverheid.[14]

Governance en financiering

Het DTC is als programma ondergebracht bij het Directoraat-generaal Bedrijfsleven en Innovatie (DG B&I), directie Digitale Economie. De Staatssecretaris van EZK is politiek opdrachtnemer vanuit het Kabinet.[15] Op de begroting van het ministerie van EZK is jaarlijks €2,5 miljoen beschikbaar gesteld voor de activiteiten van het DTC. De minister van JenV is politiek medeverantwoordelijk voor de realisatie van de ambities van het DTC, omdat ook aan het ministerie van JenV een budget ter beschikking is gesteld en zij het coördinerend ministerie is voor cybersecurity.[16] Op de begroting van het ministerie van JenV is structureel €1 miljoen beschikbaar voor het stroomlijnen van informatie ten behoeve van niet-vitale bedrijfsleven en het opzetten en onderhouden van contacten met het DTC en de verschillende samenwerkingsverbanden die zullen gaan ontstaan.

Wat zeggen gesprekspartners?

Gesprekspartners onderstrepen het belang van het bestaan van een organisatie die is gericht op het vergroten van de cyberweerbaarheid van niet-vitale bedrijven. Hierbij benoemen gesprekspartners de behoefte van deze bedrijven aan ondersteuning op het gebied van cyberweerbaarheid. Ook benadrukken ze de noodzaak om de bewustwording van niet-vitale bedrijven ten aanzien van cyberweerbaarheid te vergroten.

Gesprekspartners waarderen de manier waarop het DTC zich in korte tijd heeft (door)ontwikkeld. Hierbij benadrukken ze vaak de (grote) omvang van de doelgroep in verhouding tot de (kleine) omvang van het DTC. Gesprekspartners waarderen de energie en het enthousiasme waarmee het DTC met deze uitdaging aan de slag is gegaan.

Sommige gesprekspartners geven aan dat grote/volwassen niet-vitale bedrijven op dit moment 'buiten de boot vallen'. Deze bedrijven vallen buiten de doelgroep van het NCSC en tegelijkertijd zijn hun vragen en behoeften van een dusdanig technische aard dat ze het expertiseniveau van het DTC overstijgen.

[12] Ministerie van EZK (2017). *Programmaplan Digital Trust Centre 2018-2020*, p. 9.
[13] Zie: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/81589ned/table?ts=1575384717323.
[14] Zie: https://www.ncsc.nl/over-ncsc.
[15] Ministerie van EZK (2017). *Programmaplan Digital Trust Centre 2018-2020*, p. 17.
[16] Ministerie van EZK (2017). *Programmaplan Digital Trust Centre 2018-2020*, p. 17.

3. Activiteiten, resultaten en samenwerking

In dit hoofdstuk gaan we eerst in op de activiteiten en resultaten van het DTC. We bespreken per hoofdtaak de activiteiten die zijn uitgevoerd en wat de resultaten zijn van deze activiteiten. Daarnaast beschrijven we de wijze waarop het DTC samenwerkt met het NCSC en overige stakeholders. We geven steeds eerst de feitelijke informatie weer en daarna de beelden van gesprekspartners. Vervolgens bespreken we onze conclusies ten aanzien van het betreffende onderwerp.

3.1. Hoofdtaak 1: Informatie- en adviesfunctie

Wat zijn de feiten?

Ten aanzien van hoofdtaak 1 is de volgende ambitie geformuleerd: "*Ook bedrijven die (nog) niet aangesloten zijn bij een intermediaire organisatie moeten worden ondersteund. Voorzien wordt deze groep te bereiken via een te ontwikkelen digitaal platform. De ondersteuning van het DTC, in samenwerking met het NCSC, zal zich richten op het verbeteren van de cybersecurity in algemene zin en het informeren en het geven van een handelingsperspectief omtrent actuele dreigingen en kwetsbaarheden*."[17]

Website

Het DTC is in 2018 gestart met het ontwikkelen van een website, die in de zomer van 2018 live is gegaan. Op de website worden informatie en adviezen gedeeld waarmee ondernemingen aan de slag kunnen ten behoeve van het vergroten van hun cyberweerbaarheid. Onder meer de volgende producten en diensten worden op de website aangeboden:

- **Artikelen:** Op de website zijn artikelen beschikbaar over verschillende onderwerpen op het gebied van cyberweerbaarheid.
- **Handleidingen:** Voor verschillende onderwerpen heeft het DTC handleidingen of stappenplannen opgesteld waarin ondernemers stap voor stap worden begeleid in een bepaalde handeling om de cyberweerbaarheid te verhogen. Voorbeelden zijn de handleiding Apps updaten op je mobiele apparaat, de handleiding Internet of Things (IoT) en het stappenplan Basisbeveiliging router instellen.
- **Handreikingen:** In samenwerking met samenwerkingsverbanden en het NCSC heeft het DTC vijf handreikingen opgesteld met daarin tips, adviezen en concrete handvatten voor samenwerkingsverbanden. Het betreft handreikingen over de volgende onderwerpen: het starten van een cybersecurity samenwerkingsverband, het opstellen van een samenwerkingsovereenkomst, het ontwikkelen van een cybsersecurity scan, social media tips, en het organiseren van een cybersecurity roadshow.
- **Infographic:** Het DTC heeft een infographic gemaakt met daarin vijf basisprincipes van veilig digitaal ondernemen. Ondernemers die de vijf basisprincipes opvolgen, vergroten hun weerbaarheid tegen cyberrisico's die de bedrijfsvoering kunnen verstoren.
- **Factsheets:** Het DTC heeft twee factsheets gemaakt over informatiedeling binnen de keten. De factsheets zijn gebaseerd op de resultaten van een

[17] Kamerstuk 26643, nr. 474.

onderzoek dat TNO uitvoerde in opdracht van het ministerie van EZK naar cybersecurity-informatiedeling voor samenwerkingsverbanden. Daarbij is TNO ook gevraagd een herbruikbare cybersecurity toolbox te ontwerpen. In 2018 heeft hiervoor, in samenwerking met het DTC, een pilot met het Cyber Weerbaarheidscentrum Brainport (CWB) plaatsgevonden.

- **Basisscan Cyberweerbaarheid:** Het DTC heeft een scan ontwikkeld die ondernemers inzicht geeft in de digitale veiligheid van hun bedrijf. Na het invullen ontvangt de invuller een rapport waarin per basisprincipe wordt weergegeven in hoeverre de basis op orde is en waarin adviezen worden gegeven om de cyberweerbaarheid te vergroten.
- **Nieuwsberichten:** Op de website worden nieuwsberichten gedeeld over actuele dreigingen of andere relevante ontwikkelingen op het gebied van cyberweerbaarheid.
- **Ondernemersverhalen:** Op de website worden ervaringsverhalen van ondernemers gedeeld. Er worden succesverhalen gedeeld en er wordt gedeeld welke lessen uit de ervaringen kunnen worden getrokken. Het DTC hoopt ondernemers elkaar met ervaringsverhalen te laten inspireren en aan te moedigen de cyberweerbaarheid naar een hoger plan te tillen.

Het DTC probeert ondernemers ook te bereiken met informatie en adviezen via de social media kanalen. Het DTC heeft een LinkedIn-pagina en een Twitter-account waar wekelijks berichten op worden gedeeld.

Digitaal platform

Voorts is het DTC in 2018 gestart met het ontwikkelen van een digitaal platform. Het is de bedoeling dat het platform een interactieve omgeving wordt waarin bedrijven, samenwerkingsverbanden en experts hun kennis kunnen delen en vermeerderen. In het Programmaplan Digital Trust Centre 2018-2020 is de ambitie uitgesproken een platform te ontwikkelen waarop "*actuele, begrijpelijke en relevante informatie beschikbaar wordt gesteld over cyberdreigingen en hoe te handelen, zowel bij incidenten als ter bevordering van de weerbaarheid in structurele zin*."[18] Het streven is om 80% van de samenwerkingsverbanden begin 2020 hierop te hebben aangesloten en 500 deelnemers eind 2020 op het platform te hebben.[19]

De ontwikkeling van het platform heeft vertraging opgelopen, met name doordat het ontwikkelen van de IT (met de nodige eisen aan veiligheid en het vertrouwelijk kunnen delen van informatie) ingewikkeld is. De ambitie was aanvankelijk om het platform eind 2018 live te laten gaan.[20] Deze ambitie is later bijgesteld naar het derde kwartaal van 2019.[21] Uiteindelijk is eind november 2019 het platform live gegaan in een opstartfase. In deze fase hebben 25 deelnemers toegang gekregen tot het platform. Deze deelnemers zijn bijvoorbeeld contactpersonen van samenwerkingsverbanden en partijen uit de programmaraad. Het is de bedoeling dat een aantal van deze deelnemers als ambassadeurs bijdragen aan het tot een succes maken van het platform door het vervullen van verschillende taken. Zo zullen zij nieuwe leden welkom heten en hen wegwijs maken op het platform. Ook hebben ze een taak in het aanjagen van de discussie, het beantwoorden van vragen en het delen van interessante evenementen.

Wat zeggen gesprekspartners?

Gesprekspartners zijn over het algemeen positief over de kwaliteit van de producten van het DTC en over de informatie op de website van het DTC. Ze geven aan dat er over relevante onderwerpen informatie wordt verstrekt en dat de informatie op een duidelijke en toegankelijke manier is verwoord.

Een kanttekening die echter wel regelmatig door gesprekspartners wordt gemaakt is dat de informatie erg algemeen van aard is. De informatie en producten van het DTC zijn daardoor vaak geformuleerd op basisniveau en niet (of in ieder geval minder) geschikt voor grote/volwassen bedrijven. Er is volgens

[18] Ministerie van EZK (2017). *Programmaplan Digital Trust Centre 2018-2020*, p. 9.
[19] Kamerstuk 26643, nr. 616.
[20] Kamerstuk 26643, nr. 545.
[21] Kamerstuk 26643, nr. 616.

veel gesprekspartners dan ook behoefte aan meer gedifferentieerde informatie, aangepast naar de omvang en het volwassenheidsniveau van een bedrijf. Veel gesprekspartners benadrukken hierbij de grootte en de diversiteit van de doelgroep van het DTC. Gesprekspartners geven aan (de explicitering van) een focus of strategie ten aanzien van het bereiken van de doelgroep te missen. Ook geven gesprekspartners regelmatig aan dat de informatie op de website vooral informerend is. Zij hebben behoefte aan meer praktische tools en meer handvatten waarmee een ondernemer daadwerkelijk tot actie over kan gaan. De Basisscan Cyberweerbaarheid wordt hierbij soms als positief voorbeeld genoemd van het soort tool waar bedrijven behoefte aan hebben.

De meeste gesprekspartners twijfelen aan de mate waarin zij of hun achterban van het platform gebruik zullen gaan maken. Hiervoor worden verschillende redenen genoemd:

- Toegankelijkheid inlogmethode: Sommige gesprekspartners uiten de zorg dat de gekozen inlogmethode, eHerkenning, de toegankelijkheid van het platform belemmert. Zij hebben de indruk dat bedrijven terughoudend zijn om medewerkers toegang te verlenen tot de eHerkenning van het bedrijf. Overigens geeft het DTC zelf aan dat het mogelijk is eHerkenning met specifieke machtigingen toe te kennen aan medewerkers. Als bedrijven daarvan op de hoogte worden gesteld kan dit de zorg rondom de inlogmethoden dus mogelijk wegnemen.
- Veiligheid/vertrouwelijkheid: Gesprekspartners benadrukken vaak de gevoeligheid en vertrouwelijkheid van informatie rondom de cyberweerbaarheid van een bedrijf. Zij twijfelen daarom over de mate waarin bedrijven bereid zijn informatie over hun cyberweerbaarheid te delen. Een aantal keren is bijvoorbeeld genoemd dat bedrijven niet open zullen zijn in het delen van incidenten omtrent cyberweerbaarheid, omdat ze het idee hebben hierin zelf niet genoeg gedaan te hebben (met andere woorden: ze willen hun ‘vuile was’ niet buiten hangen). Deze twijfels worden versterkt door vragen die er bij gesprekspartners nog zijn rondom de beveiliging van het platform en de mate waarin men anoniem kan deelnemen aan de community op het platform. Gesprekspartners benoemen ook dat er terughoudendheid zal zijn in het delen van informatie, omdat bedrijven vrezen dat informatie van het platform kan worden opgevraagd via een Wob-verzoek.
- Onduidelijkheid toekomst platform: Gesprekspartners hebben vragen over de toekomstige eigenaar van het platform. Het is nog onduidelijk wat de status van het DTC zal zijn als het programma afloopt in 2020 en daarmee is het ook onduidelijk wat de toekomst van het platform zal zijn. Gesprekspartners denken dat helderheid over de toekomst van het DTC en het platform mogelijk kan bijdragen aan het verminderen van de onzekerheid en daarmee het verminderen van de terughoudendheid in het delen van informatie.
- Motivatie ondernemers: Veel gesprekspartners twijfelen of ondernemers voldoende gemotiveerd zullen zijn om actief informatie of ervaringen te delen. Ze verwachten dat ondernemers vooral op een laagdrempelige wijze informatie willen ontvangen en over het algemeen geen tijd en moeite zullen steken in het actief delen van hun ervaringen.
- Eigen platform: Enkele samenwerkingsverbanden hebben een eigen platform ontwikkeld. Het is voor hen vaak nog niet duidelijk of en hoe het DTC-platform van toegevoegde waarde gaat zijn in aanvulling op hun eigen platform.

Onze conclusies

In het kader van de informatie- en adviesfunctie heeft het DTC een website ontwikkeld. Op de website worden informatie en adviezen op het gebied van cyberweerbaarheid ontsloten. Ook heeft het DTC verschillende producten ontwikkeld die op de website worden aangeboden. De informatie en producten van het DTC worden over het algemeen goed ontvangen en voorzien in een behoefte van bedrijven. De informatie en producten richten zich voornamelijk op het basisniveau, en zijn daarmee met name geschikt voor het MKB en zzp-ers. Ze sluiten niet goed aan op de informatiebehoefte en vragen van grote/volwassen bedrijven.

Het platform bevindt zich sinds kort in een opstartfase. Er is een kans dat het platform in de praktijk door een beperkter aantal bedrijven gebruikt gaat worden dan waarvoor het bedoeld was: een interactieve omgeving waarin bedrijven, samenwerkingsverbanden en experts hun kennis kunnen delen en vermeerderen. Als het platform volledig in gebruik is genomen zal duidelijk worden in welke mate het voorziet in een behoefte van bedrijven. Duidelijkheid geven over de toegankelijkheid, vertrouwelijkheid en toekomst van het platform kan bijdragen aan het verminderen van de terughoudendheid van bedrijven om deel te nemen aan het platform.

3.2. Hoofdtaak 2: Aanjaagfunctie samenwerkingsverbanden

Ten aanzien van hoofdtaak 2 is de volgende ambitie geformuleerd: "*Het DTC beoogt de komende jaren het ontstaan van een stelsel van intermediaire organisaties tot stand te helpen brengen. Daarbij hangt de exacte ondersteuning die het DTC zal bieden af van de behoefte en het volwassenheidsniveau van een samenwerkingsverband*."[22] Het is tevens de ambitie om met het stelsel van intermediaire organisaties uiteindelijk een landelijk dekkend stelsel van informatieknooppunten te realiseren.[23]

Wat zijn de feiten?

In een samenwerkingsverband werken ondernemers samen met andere organisaties aan het vergroten van de cyberweerbaarheid, binnen en tussen niet-vitale branches, sectoren en regio's. Het DTC heeft tot doel deze samenwerkingsverbanden te stimuleren en te ondersteunen. Onder samenwerkingsverbanden verstaat het DTC "*een samenwerking van twee of meer partijen die zich organiseren met als doel samen de cyberweerbaarheid van ondernemend Nederland te vergroten en waarbij commerciële doelstellingen ondergeschikt zijn*".[24] Het DTC maakt onderscheid tussen drie soorten samenwerkingsverbanden:

1. Samenwerkingsverbanden met een DTC-subsidie;
2. Samenwerkingsverbanden zonder DTC-subsidie;
3. Information Sharing and Analysis Centers (niet-vitale ISAC's).[25]

Samenwerkingsverbanden met subsidie

Samenwerkingsverbanden kunnen een subsidie aanvragen via de subsidieregeling cyberweerbaarheid. Het doel van deze regeling is om nieuwe netwerken te creëren waar leden kennis en kunde op het terrein van cyberweerbaarheid gaan toepassen. De maximale subsidie per project is €200.000,-. De subsidieregeling loopt via de Rijksdienst voor Ondernemend Nederland (RVO). De Adviescommissie cyberweerbaarheid adviseert over de rangschikkingscriteria en selecteert de voorstellen die in aanmerking komen voor de subsidieregeling. In het kader van de subsidieregeling zijn twee vormen van samenwerking mogelijk:

1. Meerdere ondernemingen stellen gezamenlijk een cyberweerbaarheidsplan op. Het samenwerkingsverband bestaat uit minimaal twee en maximaal acht deelnemers en heeft als doel het behartigen van de belangen van ondernemingen die niet actief zijn in de vitale sectoren.
2. Een verband met een rechtspersoonlijkheid (bijvoorbeeld een stichting) dat tot doel heeft de behartiging van cyberweerbaarheid van niet-vitale ondernemingen, kan een subsidieaanvraag indienen. De stichting is dan de ontvanger van de subsidie. Samenwerking met minstens twee ondernemingen is verplicht.

[22] Kamerstuk 26643, nr. 474.
[23] Ministerie van EZK (2017). *Programmaplan Digital Trust Centre 2018-2020*, p. 9.
[24] Intern document DTC, december 2019.
[25] DTC (2019). *Jaarwerkplan 2019,* p. 12.

In 2018 zijn 15 subsidieaanvragen ingediend, waarvan er zes zijn gehonoreerd. In 2019 zijn 18 subsidieaanvragen ingediend, waarvan 12 voldeden aan de gestelde eisen en uiteindelijk zeven aanvragen zijn gehonoreerd. Eén samenwerkingsverband heeft bezwaar aangetekend tegen het subsidiebesluit van de RVO en is daardoor (nog) niet aangesloten bij het DTC. Dat betekent dat 12 samenwerkingsverbanden die subsidie ontvangen eind 2019 aan het DTC zijn verbonden.

Samenwerkingsverbanden dienen na afloop van ieder projectjaar te rapporteren over de voortgang van hun project. Hiervoor moet gebruik worden gemaakt van een model voor voortgangsrapportages van de RVO.[26] Een samenwerkingsverband geeft hierin aan hoe de projectactiviteiten vorderen en wat de stand van zaken is. Er wordt onder andere gevraagd naar knelpunten, successen en externe ontwikkelingen. Daarnaast wordt gevraagd om wijzigingen door te geven die gerelateerd zijn aan de voortgang, bijvoorbeeld op financieel, inhoudelijk of organisatorisch vlak. Ook worden samenwerkingsverbanden gevraagd om een vooruitblik. Voorafgaand aan de subsidieronde van 2019 heeft de adviescommissie een verslag ontvangen van de voortgang van de activiteiten van de samenwerkingsverbanden die reeds subsidie ontvangen.

Samenwerkingsverbanden zonder subsidie

Het DTC verbindt ook samenwerkingsverbanden aan zich die geen subsidie hebben aangevraagd of geen subsidie toegekend hebben gekregen. Het samenwerkingsverband dient een plan op te stellen ten aanzien van de wijze waarop het samenwerkingsverband de cyberweerbaarheid binnen dan wel buiten het verband gaat vergroten. Informatiedeling moet een belangrijk onderdeel van dit plan zijn. Eind 2019 zijn drie samenwerkingsverbanden zonder subsidie bij het DTC aangesloten en vermeld op de website.[27]

Naast samenwerkingsverbanden kunnen ook brancheorganisaties zich aansluiten bij het DTC. Eind 2019 zijn vijf brancheorganisaties aangesloten en vermeld op de website als samenwerkingsverband.[28]

Niet-vitale ISAC's

ISAC's betreffen een vrijwillige samenwerking tussen partijen in een sector met als doel het vertrouwelijk delen van informatie en analyses over dreigingen, incidenten, kwetsbaarheden, maatregelen en leerpunten op het gebied van digitale veiligheid.[29] In het Jaarwerkplan 2019 schrijft het DTC dat in 2019 een aantal niet-vitale ISAC's zullen worden overgedragen vanuit het NCSC aan het DTC.[30] Het betreft de ISAC Pensioenen, ISAC Verzekeraars, ISAC Media en ISAC Legal. Dit wordt ook gecommuniceerd in de Kamerbrief van 17 juni 2019. De ISAC's zijn nog niet als samenwerkingsverband aan het DTC verbonden en er zijn nog geen werkafspraken bestendigd met de ISAC's. Wel heeft in november 2019 overdracht van contactgegevens vanuit het NCSC plaatsgevonden en is het DTC in november 2019 reeds met één van de ISAC's in gesprek over de mogelijkheden voor aansluiting bij het DTC.

Ondersteuning samenwerkingsverbanden

De wijze waarop het DTC samenwerkingsverbanden ondersteunt verschilt, afhankelijk van de behoeften van het verband. De ondersteuning die het DTC in 2019 aan samenwerkingsverbanden heeft geboden is als volgt:

- **Informatievoorziening**:
    - Overzicht nieuwsberichten NCSC: Het NCSC stuurt het DTC dagelijks een nieuwsbrief met daarin nieuwsberichten. Het DTC clustert de

[26] Zie: https://www.rvo.nl/subsidies-regelingen/subsidiespelregels/subsidiespelregels-ministerie/ministerie-van-economische-zaken-en-klimaat.
[27] Het betreft de volgende samenwerkingsverbanden: Connect2Trust, Ferm, Noord Holland Samen Veilig.
[28] Het betreft de volgende brancheorganisaties: Transport en Logistiek Nederland, Adfiz, PZO, FHI en Techniek Nederland.
[29] Kamerstukken 26643, nr. 560.
[30] DTC (2019). *Jaarwerkplan 2019,* p. 12.

berichten die relevant zijn voor haar doelgroep en verstuurt deze op vrijdag naar aangesloten samenwerkingsverbanden. In 2019 verstuurde het DTC dit overzicht 52 keer.
    - Start of Week: De *Start of Week* is een actueel en informatief nieuwsoverzicht samengesteld door het DTC op het gebied van digitaal ondernemen. De *Start of Week* wordt verstuurd naar aan het DTC verbonden samenwerkingsverbanden. De *Start of Week* kan gevoelige informatie bevatten. Om op een eenduidige wijze te definiëren wat er met de informatie mag gebeuren, maakt het DTC gebruik van het zogenoemde Traffic Light Protocol (TLP).[31] Via een TLP-aanduiding wordt aangegeven wat een samenwerkingsverband wel en niet met de informatie mag doen. In 2019 verstuurde het DTC 32 keer een *Start of Week.*
    - Dreigingsinformatie en kwetsbaarheden: Naast de *Start of Week* worden er ook incidentele berichten verstuurd naar aangesloten samenwerkingsverbanden ten aanzien van kwetsbaarheden of actuele dreigingsinformatie.
- **Begeleiding en ondersteuning**: Het DTC heeft zogenaamde 'relatiemanagers'. Het relatiemanagement van het DTC biedt, wanneer daar behoefte aan is, één op één ondersteuning aan samenwerkingsverbanden. Dit doen zij bijvoorbeeld door advies te geven over het aanvragen van een subsidie, door het geven van presentaties bij (de achterban van) het samenwerkingsverband en door mee te denken over en mee te werken aan de ontwikkeling van producten van de samenwerkingsverbanden.
- **Ontwikkeling tools:** Het DTC werkt met verschillende samenwerkingsverbanden aan het ontwikkelen van nieuwe tools. Zo ontwikkelde het DTC in samenwerking met Stichting Cyberweerbaarheid Noord-Nederland en Cyberweerbaarheid Limburg de handreiking 'Ontwikkel een cybersecurity scan'. In samenwerking met het Cyber Weerbaarheidscentrum Brainport en TNO heeft een pilot plaatsgevonden waarin onderzoek is gedaan naar het ontwerpen van een herbruikbare cybersecurity-informatiedeling toolbox. Op basis hiervan zijn twee factsheets ontwikkeld over informatiedeling binnen de keten.
- **Netwerk van samenwerkingsverbanden**: Het DTC biedt ook ondersteuning door individuele samenwerkingsverbanden met elkaar in contact te brengen. Daarnaast heeft het DTC in januari en september 2019 netwerkbijeenkomsten georganiseerd, bestemd voor de aan het DTC verbonden samenwerkingsverbanden en brancheorganisaties die initiatieven vertonen op het gebied van cyberweerbaarheid. Beide bijeenkomsten zijn bezocht door circa 30 deelnemers. De eerste bijeenkomst is door deelnemers gewaardeerd met het cijfer acht. De twee bijeenkomst is niet middels een evaluatieformulier gewaardeerd. Het DTC is voornemens elke zes maanden een netwerkbijeenkomst te organiseren.
- **Landingspagina op de website van het DTC:** Samenwerkingsverbanden die officieel zijn aangesloten bij het DTC worden vermeld op de website van het DTC. Elk samenwerkingsverband heeft een eigen pagina met informatie over de doelstelling, activiteiten en resultaten tot nu toe.

Wat zeggen gesprekspartners?

Veel gesprekspartners (zowel gesprekspartners die zelf zijn aangesloten bij een samenwerkingsverband als andere gesprekspartners) zien meerwaarde in het werken met samenwerkingsverbanden. Genoemd is dat het DTC via de samenwerkingsverbanden bedrijven kan bereiken (de achterbannen van de samenwerkingsverbanden). Ook is genoemd dat de samenwerkingsverbanden actief communiceren over het feit dat ze als samenwerkingsverband zijn aangesloten bij het DTC, wat bijdraagt aan de naamsbekendheid van het DTC. Wel zijn enkele gesprekspartners kritisch op de relatief grote hoeveelheid aandacht die het DTC geeft aan de samenwerkingsverbanden. Deze gesprekspartners benadrukken dat er ook veel bedrijven *niet* zijn aangesloten bij samenwerkingsverbanden. Ze twijfelen of deze groep bedrijven voldoende

[31] Zie: https://www.digitaltrustcenter.nl/start-of-week.

aandacht krijgt in verhouding tot de bedrijven die wel zijn aangesloten bij een samenwerkingsverband.

Samenwerkingsverbanden zijn positief over het enthousiasme en de benaderbaarheid van het DTC. Vaak benoemen samenwerkingsverbanden dat zij goed contact hebben met de relatiemanagers van het DTC. Ook waarderen samenwerkingsverbanden de ondersteuning die door het DTC wordt geboden. Met name de *Start of Week* wordt door veel samenwerkingsverbanden gewaardeerd en gebruikt in de communicatie richting de eigen achterban. Ook geven samenwerkingsverbanden vaak aan dat het DTC een waardevolle rol vervult als verbindende partij. Het in contact brengen van samenwerkingsverbanden en het organiseren van fysieke bijeenkomsten wordt door veel samenwerkingsverbanden gewaardeerd. Samenwerkingsverbanden die subsidie hebben ontvangen geven aan dat de subsidie een versnellend effect heeft gehad op de ontwikkeling en implementatie van hun plannen. Met versnellend effect wordt erop gedoeld dat de subsidie er niet zozeer toe heeft geleid dat activiteiten zijn uitgevoerd die anders niet waren uitgevoerd, maar dat activiteiten (bijvoorbeeld het ontwikkelen van een product) door de subsidie wel sneller zijn uitgevoerd.

Tegelijkertijd is er bij veel samenwerkingsverbanden behoefte aan andere of meer intensieve ondersteuning. Veel samenwerkingsverbanden geven aan dat zij graag zouden beschikken over meer praktische tools en handvatten die hun achterban kan gebruiken in het daadwerkelijk overgaan tot actie om de cyberweerbaarheid te vergroten. Daarnaast geven samenwerkingsverbanden met veel grote/volwassen, niet-vitale bedrijven in hun achterban aan dat het DTC hen op dit moment nog niet goed kan ondersteunen. De vragen die zij hebben vergen specialistische kennis die niet bij het DTC aanwezig is. Ze hebben bovendien voornamelijk behoefte aan actuele (dreigings)informatie vanuit het NCSC, maar deze informatie kan het NCSC (nog) niet altijd met het DTC delen. Het NCSC deelt wel actuele dreigingsinformatie zonder persoonsgegevens met het DTC. Dreigingsinformatie met persoonsgegevens mag het NCSC echter niet delen met het DTC, doordat het DTC geen wettelijke grondslag heeft om persoonsgegevens te ontvangen en te verwerken (zie paragraaf 3.3.1.).

Zowel door samenwerkingsverbanden met subsidie als door brancheorganisaties worden regelmatig zorgen over de toekomst geuit. Veel samenwerkingsverbanden werken aan een business case voor het moment dat de subsidie die zij van het DTC ontvangen stopt, maar er is nog onzekerheid over de vraag in hoeverre de samenwerkingsverbanden daadwerkelijk zullen blijven bestaan zonder de subsidie van het DTC.

Enkele gesprekspartners uit de Adviescommissie cyberweerbaarheid (die de subsidieaanvragen van samenwerkingsverbanden hebben behandeld) zijn kritisch op de kwaliteit van de plannen die worden ingediend voor een subsidieaanvraag. Met name in de tweede subsidieronde was de verwachting dat er nieuwe of innovatieve voorstellen zouden worden ingediend en dat de kwaliteit van de voorstellen van een hoger niveau zouden zijn. Aan deze verwachting werd volgens deze gesprekspartners niet voldaan. Ook zijn gesprekspartners binnen en buiten de Adviescommissie kritisch op het ontbreken van een evaluatie van de activiteiten en resultaten van samenwerkingsverbanden. Er kan volgens hen meer worden gestuurd op het monitoren van resultaten en effecten van de activiteiten van samenwerkingsverbanden. Op basis daarvan kunnen lessen en *best practices* in kaart worden gebracht die vervolgens breed kunnen worden gedeeld en opgeschaald. Ook geven gesprekspartners aan dat deze inzichten vervolgens kunnen worden gebruikt bij de selectie van toekomstige samenwerkingsverbanden.

Onze conclusies

Het DTC heeft samenwerkingsverbanden aan zich verbonden en faciliteert deze onder andere door het verstrekken van informatie en adviezen, het faciliteren van productontwikkeling en kennisdeling, en door middel van subsidieverstrekking. De ondersteuning van het DTC sluit grotendeels aan bij de behoefte van de samenwerkingsverbanden.

Het DTC kan nog meer van meerwaarde zijn voor de samenwerkingsverbanden door meer praktische tools te ontwikkelen, waarmee bedrijven daadwerkelijk tot actie kunnen overgaan om hun cyberweerbaarheid te vergroten. Het DTC is voor samenwerkingsverbanden met veel grote/volwassen bedrijven in hun achterban van minder toegevoegde waarde, omdat deze samenwerkingsverbanden met name behoefte hebben aan actuele (dreigings)informatie van het NCSC. Het NCSC kan deze informatie (nog) niet altijd met het DTC delen. Het NCSC deelt wel actuele dreigingsinformatie zonder persoonsgegevens met het DTC. Dreigingsinformatie met persoonsgegevens mag het NCSC echter niet delen met het DTC, doordat het DTC geen wettelijke grondslag heeft om persoonsgegevens te ontvangen en te verwerken (zie paragraaf 3.3.1.).

De samenwerkingsverbanden die subsidie ontvangen dienen zich te verantwoorden over de activiteiten die zij met de subsidie hebben ondernemen. Echter, het DTC monitort of evalueert niet de *effecten* van de activiteiten van de samenwerkingsverbanden. De lessen die uit de ervaringen van de samenwerkingsverbanden kunnen worden getrokken, kunnen nog meer worden opgeschaald zodat ze van meerwaarde zijn voor een grotere groep bedrijven, waaronder bedrijven die geen lid zijn van een samenwerkingsverband.

3.3. Samenwerking

3.3.1. Samenwerking met het NCSC

Wat zijn de feiten?

In het Programmaplan Digital Trust Centre 2018-2020 staat beschreven dat goede samenwerking met het NCSC cruciaal is voor het slagen van het DTC.

Nadat is besloten het DTC op te richten is het NCSC betrokken geweest bij het verder uitwerken van de plannen voor het DTC. Ook daarna heeft samenwerking tussen het NCSC en het DTC plaatsgevonden. Zo heeft het NCSC inhoudelijke expertise ingebracht en bijvoorbeeld meegedacht over het door het DTC ontwikkelde platform (zie paragraaf 3.1 voor meer informatie over het platform). Verder heeft een medewerker van het NCSC plaatsgenomen in de beoordelingscommissie die de aanvragen voor subsidie voor samenwerkingsverbanden heeft beoordeeld. De leden van de beoordelingscommissie hebben op persoonlijke titel plaatsgenomen in de commissie. Ook maakt het NCSC onderdeel uit van de programmaraad van het DTC. Afgesproken is dat het DTC informatie die het van het NCSC kan ontvangen, zal omzetten in informatie die het niet-vitale bedrijfsleven in staat zal stellen om meer cyberweerbaar te worden.[32] Het NCSC deelt inderdaad informatie voor het niet-vitale bedrijfsleven met het DTC, die het DTC onder andere opneemt in de *Start of Week* die naar samenwerkingsverbanden wordt gestuurd. In de *Start of Week* wordt ingegaan op ontwikkelingen rondom de samenwerkingsverbanden en specifieke onderwerpen op het gebied van cyberweerbaarheid die voor ondernemend Nederland van belang zijn, bijvoorbeeld kwetsbaarheden die in veelgebruikte software zijn ontdekt.

Op de begroting van het ministerie van JenV is structureel €1 miljoen beschikbaar voor het stroomlijnen van informatie ten behoeve van het niet-vitale bedrijfsleven en het opzetten en onderhouden van contacten met het DTC en de verschillende samenwerkingsverbanden die zullen gaan ontstaan voor het niet-vitale bedrijfsleven. Het NCSC heeft aangegeven dat deze extra middelen ook hiervoor zijn ingezet.

De samenwerking tussen het NCSC en het DTC kent een aantal knelpunten. Het NCSC mag persoonsgegevens niet delen met het DTC, doordat het DTC geen wettelijke grondslag heeft om persoonsgegevens te ontvangen en te verwerken, het DTC specifieke dreigingsinformatie niet kan uitsluiten voor de Wet

[32] Kamerstuk 26643, nr. 616.

openbaarheid van bestuur (Wob) en het DTC niet is aangewezen als OKTT (in de zin van Wbni, art. 3.2[33]).

Meer generieke informatie of specifieke informatie zonder persoonsgegevens wordt in beginsel door het NCSC met het DTC gedeeld. Het NCSC heeft geen nadere meldingen gedaan over hoeveel informatie met persoonsgegevens het NCSC niet met het DTC maar rechtstreeks met de CERT's en OKTT's of in uitzonderlijke gevallen de getroffen organisaties zelf heeft gedeeld, en dit is dus ook niet bekend.

Cultuurverschillen en onduidelijke samenwerkingsafspraken hebben er aan bijgedragen dat de samenwerking tussen het DTC en het NCSC op een zeker moment tijdelijk is vastgelopen. De cultuurverschillen liggen vooral in de wijze van omgaan met informatie. Waar het DTC vooral gericht is op het zoveel en zo breed mogelijk delen van informatie met het bedrijfsleven, is het NCSC (gegeven het karakter van de informatie, de herkomst van de informatie en de bovenliggende privacy wetgeving) eerder gericht op het zo specifiek en gericht mogelijk delen van cybersecurity-informatie.

Nadat de samenwerking tussen het DTC en het NCSC tijdelijk was vastgelopen, hebben het DTC en het NCSC gewerkt aan het verbeteren van de samenwerking. Zo hebben zij twee externe adviseurs, die wel betrokken zijn bij de organisaties, gevraagd de ontstane knelpunten te inventariseren, te analyseren en te komen met oplossingsrichtingen. Mede naar aanleiding hiervan is het contact tussen het NCSC en het DTC op directieniveau geïntensiveerd, is er een aantal gesprekken geweest tussen medewerkers van het NCSC en het DTC en zijn er concept-samenwerkingsafspraken opgesteld. Ten tijde van deze evaluatie waren deze samenwerkingsafspraken nog niet definitief, maar werd er volgens het NCSC en het DTC al wel conform de gedachte uit deze samenwerkingsafspraken samengewerkt. Vanaf eind 2019 onderzoeken NCSC en DTC op welke wijze het DTC aangewezen kan worden als OKTT.

Wat zeggen gesprekspartners?

Gesprekspartners van binnen en buiten het DTC en het NCSC benadrukken het belang van goede samenwerking tussen de twee organisaties. Gesprekspartners buiten het DTC benoemen bijvoorbeeld het belang van de informatie van het NCSC voor het bedrijfsleven. Sommige medewerkers van het DTC benoemen dat ze graag meer gebruik zouden maken van de expertise van het NCSC, aangezien het DTC nog niet zo lang geleden gestart is en de jarenlange kennis en ervaring van het NCSC bruikbaar kan zijn.

Veel gesprekspartners (bedrijven, brancheorganisaties en andere stakeholders) hebben het beeld dat het NCSC informatie niet of laat met het DTC deelt. Een indicatie die ze hiervoor hebben is dat bedrijven of de pers soms al informatie van het NCSC heeft, terwijl het DTC deze informatie pas op een later moment naar buiten brengt. Ook benoemen verschillende gesprekspartners de verschillen tussen het NCSC en het DTC, die het volgens gesprekspartners soms lastig maken voor de twee organisaties om effectief samen te werken. Tot slot hebben verschillende gesprekspartners het beeld dat de 1 miljoen die op de begroting van het ministerie van JenV beschikbaar is gesteld om het DTC en de samenwerkingsverbanden te ondersteunen rechtstreeks naar het NCSC is gegaan. Deze gesprekspartners geven vervolgens aan dat voor hen onduidelijk is wat er is gedaan met de €1 miljoen. Deze gesprekspartners benoemen dat het NCSC in hun ogen voor dit budget meer had kunnen doen.

Onze conclusies

Goede samenwerking met het NCSC is cruciaal voor het slagen van het DTC. Het DTC en het NCSC hebben op verschillende manieren samengewerkt. De samenwerking tussen het NCSC en het DTC kende een moeizame start en is op

[33] De Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) is sinds 9 november 2018 van kracht. Met organisaties die zijn aangewezen als OKTT in de zin van Wbni, art. 3.2, kan het NCSC verkregen gegevens delen over dreigingen en incidenten met betrekking tot voor hun relevante netwerk- en informatiesystemen . Deze OKTT's kunnen deze informatie weer delen met aangesloten organisaties.

enig moment ook tijdelijk vastgelopen. Beide organisaties zijn overtuigd van het belang van een goede samenwerking en er is en wordt ook gewerkt aan het verbeteren van de samenwerking. Zo zijn er gesprekken geweest tussen medewerkers van het NCSC en het DTC waarin afspraken zijn gemaakt en zijn er concept-samenwerkingsafspraken op papier gezet. Hiermee is de samenwerking, nadat deze tijdelijk was vastgelopen, verbeterd. Ook is de verwachting dat de samenwerking verder zal verbeteren als het NCSC en het DTC de gemaakte afspraken in de praktijk zullen brengen.

3.3.2. Samenwerking met overige stakeholders

Wat zijn de feiten?

Het DTC werkt met veel partijen samen. Zo werkt het DTC samen met andere organisatieonderdelen van het ministerie van EZK aan de implementatie van agenda's voor een duurzaam ondernemend Nederland. Dit geldt bijvoorbeeld voor de Nederlandse Digitaliseringsstrategie, de roadmap Digitaal Veilige Hard- en Software (DHVS) en het MKB-actieplan. Ook werkt het DTC samen met brancheorganisaties en platforms (waaronder VNO-NCW / MKB-Nederland, ECP, KVK, het CIO Platform Nederland, NLdigital, Cyberveilig Nederland, de Stichting Digitale Infrastructuur Nederland) en kennisinstituten (waaronder TNO, het CBS, het CPB, Saxion Hogeschool en de Haagse Hogeschool).

Tijdens het opzetten van het DTC is een klankbordgroep samengesteld met verschillende (branche)organisaties. Begin 2018 is de klankbordgroep omgezet in een programmaraad. De organisaties die zitting hebben in de programmaraad zijn het CIO platform Nederland, ECP, KVK, het NCSC, NLdigital, VNO-NCW en het ministerie van JenV. Het ministerie van EZK is voorzitter van de programmaraad. De belangrijkste taak van de programmaraad is te adviseren over de koers, het tempo en de prioriteiten van het DTC.

Met de samenwerkingspartners wisselt het DTC onder andere informatie uit (bijvoorbeeld over de behoefte van de doelgroepen van brancheorganisaties). Ook vindt er gezamenlijk productontwikkeling plaats.

Wat zeggen gesprekspartners?

Gesprekspartners benoemen dat het DTC veel samenwerkt en een goed netwerk heeft. De samenwerkingspartners zelf hebben vaak veel waardering voor de prettige contacten met het DTC en geven aan dat er korte lijnen zijn. Veel samenwerkingspartners hebben een gevoel van eigenaarschap, mede door hun rol in de klankbordgroep en later in de programmaraad.

Veel samenwerkingspartners benoemen dat de samenwerking in een volgende fase nog kan worden geïntensiveerd. Zo kan het DTC volgens deze gesprekspartners nog meer aansluiten bij initiatieven van samenwerkingspartners (zoals campagnes en congressen), om zo meer bereik te genereren. Specifiek is door enkele gesprekspartners genoemd dat de samenwerking tussen andere organisatieonderdelen van het ministerie van EZK en het DTC kan worden geïntensiveerd. Het DTC haalt veel informatie op bij bedrijven, die goed gebruikt kan worden bij het maken van beleid door het ministerie van EZK. Het DTC en het ministerie van EZK kunnen volgens deze gesprekspartners meer doen aan informatie-uitwisseling.

Onze conclusies

Het DTC werkt veel en intensief samen met allerlei partijen en heeft daardoor een goed netwerk op het terrein van cyberweerbaarheid. Mede hierdoor is er veel draagvlak en een gevoel van eigenaarschap voor het DTC onder relevante stakeholders. De klankbordgroep en daarna de programmaraad dragen bij aan dat gevoel van eigenaarschap: een aantal organisaties heeft meegedacht over de plannen voor de oprichting van het DTC en heeft ook daarna een rol als klankbord vervuld. Op sommige punten kan de samenwerking tussen het DTC en andere partijen nog worden geïntensiveerd. Zo kan het DTC nog meer aansluiten bij al bestaande initiatieven (zoals congressen en campagnes) van

samenwerkingspartners. Ook kan het DTC meer informatie delen met andere organisatieonderdelen van het ministerie van EZK, zodat de informatie die het DTC tot haar beschikking heeft bijvoorbeeld gebruikt kan worden bij het opstellen van beleid.

4. Doelbereik

In dit hoofdstuk gaan we in op het doelbereik van het DTC. Paragraaf 4.1. bevat een overzicht van de doelstellingen die zijn geformuleerd in de Kamerbrief van 17 juni 2019 en de mate waarin het DTC deze doelstellingen heeft gehaald. In paragraaf 4.2. gaan we in op de bijdrage van het DTC aan de cyberweerbaarheid van ondernemend Nederland.

4.1. Doelstellingen Kamerbrief

In de Kamerbrief van 17 juni 2019 zijn doelstellingen en ambities voor het DTC opgenomen. Sommige van deze doelstellingen zijn heel goed meetbaar, omdat er een termijn en een streefgetal aan gekoppeld zijn. Andere doelstellingen zijn breder geformuleerd, waardoor het lastiger is vast te stellen of de doelstelling wel of niet is gehaald. Hierna lopen we bij de doelstellingen langs, waarbij we zover mogelijk ook hebben aangegeven in hoeverre de doelstelling is gehaald. Daarnaast hebben we een toelichting opgenomen over de mate waarin de doelstelling gehaald is.

Hoofdtaak 1: Informatie- en adviesfunctie

Doelstelling 1. De ambitie is eind 2019 minimaal 30.000 bezoekers op de website te hebben gehad en eind 2020 minimaal 100.000 bezoekers.
Doelstelling gehaald? Doelstelling volledig gehaald.
Toelichting. Op 31 december 2019 heeft de website van het DTC 46.149 unieke bezoekers geteld (totaal 57.479 bezoekers).

Doelstelling 2. Het live gaan van het platform is voorzien in het derde kwartaal van 2019. Het streven hier is begin 2020 80% van de samenwerkingsverbanden aangesloten te hebben op het platform en eind 2020 te komen tot een actieve community van 500 deelnemers.
Doelstelling gehaald? Doelstelling met vertraging gehaald.
Toelichting. In eerste instantie was het doel om het platform eind 2018 te lanceren.[34] In de Kamerbrief van 17 juni 2019 is de ambitie om het platform in het derde kwartaal van 2019 live te laten gaan opgenomen.[35] De ontwikkeling van het platform liep vertraging op, met name doordat het ontwikkelen van de IT (met de nodige eisen aan veiligheid en het vertrouwelijk kunnen delen van informatie) ingewikkeld was. In november 2019 is het platform live gegaan in een opstartfase, waarbij 25 deelnemers toegang hebben gekregen tot het platform.

[34] Kamerstuk 26643, nr. 545.

[35] Kamerstuk 26643, nr. 616.

Doelstelling 3. Om bedrijven inzicht te geven in waar ze staan op de ladder van veilig digitaal ondernemen en wat ze kunnen ondernemen om hun cyberweerbaarheid te verhogen, zal in het derde kwartaal van 2019 een assessment worden opgeleverd op basis van de eerder genoemde vijf basisprincipes van het DTC.
Doelstelling gehaald? Doelstelling met vertraging gehaald.
Toelichting. In het vierde kwartaal van 2019 (november) heeft het DTC de Basisscan Cyberweerbaarheid gelanceerd. Hiermee kunnen bedrijven aan de hand van 25 stellingen achterhalen hoe hun onderneming scoort op de vijf basisprincipes van veilig digitaal ondernemen. Eind 2019 hebben meer dan 1000 bedrijven de scan volledig ingevuld.

Doelstelling 4. Er zal samen met de samenwerkingsverbanden worden gewerkt aan de inzet van in de praktijk beproefde scans voor bedrijven, onder meer met inzet van studenten.
Doelstelling gehaald? Doelstelling volledig gehaald.
Toelichting. In samenwerking met Stichting Cyberweerbaarheid Noord-Nederland en Cyberweerbaarheid Limburg is de handreiking 'Ontwikkel een cybersecurity scan' tot stand gekomen. In deze handreiking staan adviezen en voorbeelden van actuele initiatieven binnen de huidige cyberweerbaarheid samenwerkingsverbanden rondom het ontwikkelen van een cybersecurity scan.[36]

Doelstelling 5. Er zal separaat onderzoek plaatsvinden om meer zicht te krijgen op de behoeftes van bedrijven als het gaat om informatie en handelingsperspectief. Dit onderzoek moet de mogelijkheid bieden binnen de grote groep van 1,6 miljoen bedrijven te komen tot meer gerichte advisering en meer maatwerk in communicatie.
Doelstelling gehaald? Doelstelling volledig gehaald.
Toelichting. Juli 2019 heeft het DTC een doelgroepenanalyse uitgevoerd, om inzicht te krijgen in de segmentering en behoefte van de doelgroep van het DTC, zodat het DTC in staat is prioriteiten te stellen en de effectiviteit en efficiency van haar instrumentarium te vergroten. Uit deze analyse volgt dat veel vragen nog open liggen, waardoor dit onderzoek niet direct heeft geleid tot meer gerichte advisering en maatwerk in communicatie.

Hoofdtaak 2: Aanjaagfunctie samenwerkingsverbanden

Doelstelling 6. De ambitie is dat eind 2019 twintig samenwerkingsverbanden zijn aangesloten bij het DTC.
Doelstelling gehaald? Doelstelling volledig gehaald.
Toelichting. Onder samenwerkingsverbanden verstaat het DTC alle mogelijke georganiseerde manieren van samenwerken. Het gaat erom dat organisaties met elkaar gaan samenwerken om zo weerbaarder te worden tegen cyberincidenten. In december 2019 had het DTC 20 samenwerkingsverbanden aan zich verbonden, die zijn vermeld op de website.[37]

[36] Zie: https://www.digitaltrustcenter.nl/handreiking-ontwikkel-een-cybersecurity-scan.

[37] Deze samenwerkingsverbanden zijn: 1. NIDV Cyberweerbaarheid DVI; 2. Adfiz; 3. Cyber Security Programma Noordzeekanaalgebied; 4. FERM; 5. Cybersecurity Centrum voor de Maakindustrie; 6. Cyber Weerbaarheidscentrum Brainport; 7. Nationale Beheersorganisatie Internet Providers; 8. Vergroting cyberweerbaarheid groentezaadveredelingsbedrijven; 9. CYSSEC; 10. GEU; 11. Federatie van technologiebranches; 12. Verhogen cyberweerbaarheid Beveiligingsinstallaties; 13. NuBno – de 8e disbalans; 14. Stichting Cyberweerbaarheid Noord-Nederland; 15. Noord Holland Samen Veilig; 16.

Samenwerking binnen en buiten de overheid

Doelstelling 7. Het kabinet heeft de ambitie het DTC door te ontwikkelen tot een “one-stop-shop voor het niet-vitale bedrijfsleven”.
Doelstelling gehaald? Niet meetbaar i.v.m. ontbreken operationalisering.
Toelichting. Met het ontwikkelen van het DTC tot een “one-stop-shop voor het niet-vitale bedrijfsleven” wil het kabinet recht doen aan de behoefte van het (niet-vitale) bedrijfsleven om één loket te hebben voor veilig digitaal ondernemen. Het is niet helder wat het zijn van een one-stop-shop inhoudt. In het Voortgangsbericht Digital Trust Center[38], wordt omschreven dat het DTC zich zal doorontwikkelen tot een one-stop-shop door de lancering van het interactieve platform. Omschreven is dat het platform onder andere *facts and figures,* richtsnoeren, tools en scans en *best practices* zal gaan bevatten welke als doel hebben het bedrijfsleven te voorzien van concreet handelingsperspectief. Het platform kan zo uitgroeien tot een dynamisch en interactief informatieknooppunt voor het niet-vitale bedrijfsleven. In de Kamerbrief van 17 juni 2019 is omschreven dat een onderdeel van het zijn van een one-stop-shop inhoudt dat het DTC de informatie die van het NCSC zal kunnen worden ontvangen, voor zover relevant voor de doelgroep van het DTC, omzet in informatie die het niet-vitale bedrijfsleven in staat zal stellen om meer cyberweerbaar te worden. Doordat niet helder is wat het zijn van een one-stop-shop inhoudt en doordat dit doel niet verder SMART is gemaakt, kan niet worden bepaald of deze doelstelling is bereikt.

Doelstelling 8. Het DTC zal informatie die van het NCSC zal kunnen worden ontvangen, voor zover relevant voor de doelgroep van het DTC, omzetten in informatie die het niet-vitale bedrijfsleven in staat zal stellen om meer cyberweerbaar te worden.
Doelstelling gehaald? Doelstelling deels gehaald, deels onbekend.
Toelichting. Het DTC ontvangt informatie van het NCSC en zet deze om in informatie voor het niet-vitale bedrijfsleven. Het DTC doet dit bijvoorbeeld in de *Start of Week* die naar samenwerkingsverbanden wordt gestuurd. Ook op de website heeft het DTC berichten met informatie van het NCSC gepubliceerd. We merken hierbij op dat uit de evaluatie signalen naar voren zijn gekomen dat het NCSC informatie (nog) niet altijd kan delen met het DTC. Het NCSC deelt actuele dreigingsinformatie zonder persoonsgegevens met het DTC. Dreigingsinformatie met persoonsgegevens mag het NCSC niet delen met het DTC, doordat het DTC geen wettelijke grondslag heeft om persoonsgegevens te ontvangen en te verwerken (zie paragraaf 3.3.1.) Het NCSC heeft geen nadere mededelingen gedaan over hoeveel informatie met persoonsgegevens het NCSC niet met het DTC, maar rechtstreeks met de CERT’s en OKTT’s of in uitzonderlijke gevallen organisaties zelf heeft gedeeld, en dit is dus onbekend.

Cyberweerbaarheid in Limburg; 17. Cyber Netwerk Drechtsteden; 18. Connect2Trust; 19. Transport en Logistiek Nederland; 20. Platform Zelfstandige Ondernemers.

[38] Kamerstuk 26 643, nr. 545.

Doelstelling 9. De verkenning naar samenwerking met gemeenten en in hoeverre zij een rol kunnen spelen in het bereiken van ondernemers.
Doelstelling gehaald? Doelstelling volledig gehaald.
Toelichting. Het DTC heeft in 2019 onderzocht in hoeverre gemeenten kunnen bijdragen aan cyberweerbaarheid in het MKB. In het onderzoek zijn vier gemeenten meegenomen.

4.2. Bijdrage aan cyberweerbaarheid ondernemend Nederland

De bijdrage van het DTC aan de cyberweerbaarheid van ondernemend Nederland is lastig te meten. Er zijn allerlei andere factoren van invloed op de cyberweerbaarheid van bedrijven, zoals andere programma's en organisaties. Daardoor is de toerekenbaarheid van effecten aan het DTC lastig vast te stellen. Het DTC heeft zelf dan ook geen zicht op haar precieze bijdrage aan de cyberweerbaarheid van ondernemend Nederland. Het DTC heeft wel inzicht in het aantal bezoekers op de website en het aantal keren dat producten worden gedownload en tools worden gebruikt. Het DTC heeft echter geen zicht op de mate waarin ondernemers op basis van de informatie en producten daadwerkelijk actie ondernemen om hun cyberweerbaarheid te vergroten. Ook heeft het DTC geen zicht op het aantal bedrijven dat wordt bereikt via de samenwerkingsverbanden.

Recente CBS-cijfers geven wel een mogelijke indicatie voor de bijdrage van het DTC aan de cyberweerbaarheid van ondernemend Nederland. Het CBS heeft op verzoek van het ministerie van EZK DTC-bedrijven (bedrijven die zich aangemeld hebben bij één van de samenwerkingsverbanden die aan het DTC zijn verbonden) opgenomen in de S*tatistiek ICT-gebruik bedrijven 2019.*[39] Op deze manier wordt inzicht verkregen in de ICT-kenmerken van deze DTC-bedrijven en kunnen deze kenmerken vergeleken worden met die van een referentiegroep van bedrijven. De referentiegroep is een groep bedrijven uit de S*tatistiek ICT-gebruik bedrijven 2019* die door herweging qua bedrijfstak en -grootte eenzelfde samenstelling heeft als de populatie DTC-bedrijven. Hierna bespreken we de belangrijkste punten uit de statistiek. In bijlage 2 hebben we een uitgebreidere samenvatting van de belangrijkste resultaten opgenomen.

Uit de S*tatistiek ICT-gebruik bedrijven 2019* komt naar voren dat DTC-bedrijven wat bewuster met ICT-veiligheid om lijken te gaan dan andere bedrijven. Zo maken DTC-bedrijven vaker gebruik van ICT-veiligheidsmaatregelen zoals authenticatie via een soft- of hardware-token en risicoanalyses, geven meer DTC-bedrijven vrijwillige cursussen aan hun personeel op het terrein van ICT-veiligheid, hebben meer DTC-bedrijven procedures omtrent ICT-veiligheid vastgelegd in een document en wordt dit document door DTC-bedrijven frequenter geactualiseerd in vergelijking met de bedrijven in de referentiegroep. Ook hebben DTC-bedrijven minder vaak dan bedrijven in de referentiegroep te maken gehad met ICT-incidenten.

Uit deze cijfers kunnen echter geen conclusies over de bijdrage van het DTC getrokken worden. Ten eerste omdat de toerekenbaarheid van deze effecten aan het DTC niet vastgesteld kan worden. Ten tweede omdat het goed mogelijk is dat er een bias in de onderzoeksresultaten zit. Immers, het is aannemelijk dat bedrijven die zich hebben aangesloten bij een samenwerkingsverband gemotiveerd zijn hun cyberweerbaarheid te vergroten. Dit geldt mogelijk in mindere mate voor de bedrijven in de referentiegroep.

[39] Zie: https://www.cbs.nl/nl-nl/maatwerk/2019/50/ict-kenmerken-bedrijven-digital-trust-center.

5. Conclusies en aanbevelingen

In dit hoofdstuk vindt u eerst in paragraaf 5.1 onze conclusies per onderzoeksvraag. Paragraaf 5.2 bevat onze aanbevelingen voor het DTC.

5.1. Conclusies

Hoofdvraag: Welke bijdrage heeft het DTC geleverd (in de eerste twee jaren) aan de cyberweerbaarheid van ondernemend Nederland en wat is er voor nodig om deze bijdrage te vergroten?

Het DTC heeft in korte tijd een organisatie opgezet die zich met een klein team richt op de doelgroep van 1,8 miljoen niet-vitale bedrijven in Nederland. Het DTC heeft een bijdrage geleverd aan de cyberweerbaarheid van ondernemend Nederland door informatie en advies te geven (hoofdtaak 1) en door samenwerkingsverbanden te stimuleren (hoofdtaak 2).

In het kader van de informatie- en adviesfunctie heeft het DTC een website en verschillende producten ontwikkeld (zoals de Basisscan Cyberweerbaarheid). De informatie en producten van het DTC worden over het algemeen goed ontvangen en voorzien in een behoefte van bedrijven. De informatie en producten zijn met name geschikt voor het MKB en zzp-ers, maar sluiten niet goed aan op de informatiebehoefte en vragen van grote/volwassen bedrijven. De derde hoofdactiviteit onder de informatie- en adviesfunctie is het opzetten van een interactief platform. Het platform is eind november 2019 live gegaan in een opstartfase. Er is een kans dat het platform in de praktijk door een beperkter aantal bedrijven gebruikt gaat worden dan waarvoor het bedoeld was: een interactieve omgeving waarin bedrijven, samenwerkingsverbanden en experts hun kennis kunnen delen en vermeerderen. Wanneer het platform volledig in gebruik is genomen zal duidelijk worden in hoeverre het inderdaad wel of niet voorziet in een behoefte van bedrijven.

Het DTC heeft samenwerkingsverbanden aan zich verbonden en faciliteert deze onder andere door het verstrekken van informatie en adviezen, het faciliteren van productontwikkeling en kennisdeling, en door middel van subsidieverstrekking. De ondersteuning van het DTC sluit grotendeels aan bij de behoefte van de samenwerkingsverbanden.

Het DTC kan nog meer van meerwaarde zijn voor de samenwerkingsverbanden door meer praktische tools te ontwikkelen, waarmee bedrijven daadwerkelijk tot actie kunnen overgaan om hun cyberweerbaarheid te vergroten.

Het DTC is voor samenwerkingsverbanden met veel grote/volwassen, niet-vitale bedrijven in hun achterban van minder toegevoegde waarde, omdat deze samenwerkingsverbanden met name behoefte hebben aan actuele (dreigings)informatie van het NCSC. Het NCSC kan deze informatie (nog) niet altijd met het DTC delen.

De samenwerkingsverbanden die subsidie ontvangen dienen zich te verantwoorden over de activiteiten die ze met de subsidie hebben ondernomen. Echter, het DTC monitort of evalueert niet de *effecten* van de activiteiten van de samenwerkingsverbanden. De lessen die uit de ervaringen van de samenwerkingsverbanden kunnen worden getrokken, kunnen nog meer worden opgeschaald zodat ze van meerwaarde zijn voor een grotere groep bedrijven, waaronder bedrijven die geen lid zijn van een samenwerkingsverband.

De bijdrage van de activiteiten van het DTC aan de cyberweerbaarheid van ondernemend Nederland is lastig te meten. Er zijn allerlei andere factoren van

invloed op de cyberweerbaarheid van bedrijven, zoals andere programma's en organisaties. Daardoor is de toerekenbaarheid van effecten aan het DTC lastig vast te stellen. Uit recente cijfers van het CBS *(Statistiek ICT-gebruik bedrijven 2019*) blijkt wel dat DTC-bedrijven (bedrijven die zich hebben aangesloten bij een samenwerkingsverband) wat bewuster met ICT-veiligheid om lijken te gaan dan een groep vergelijkbare bedrijven. Ook uit deze cijfers kunnen echter geen conclusies over de bijdrage van het DTC getrokken worden.

Subvraag 1: In hoeverre zijn de doelstellingen zoals genoemd in de Kamerbrief van 17 juni 2019 gehaald?

In de Kamerbrief zijn negen doestellingen en ambities opgenomen. Zeven van deze doelstellingen zijn volledig gehaald, waarvan twee met vertraging. Een doelstelling is deels gehaald. Zo heeft de website van het DTC meer dan 30.000 bezoekers gehad en heeft het DTC 20 samenwerkingsverbanden aan zich verbonden. Van de doelstelling om het DTC door te ontwikkelen tot een "one-stop-shop voor het niet-vitale bedrijfsleven" is niet vast te stellen of deze gehaald is, omdat deze doelstelling niet SMART is gemaakt en het daardoor niet helder is wat het zijn van een one-stop-shop inhoudt.

Subvraag 2: Hoe is de samenwerking vormgegeven met het Nationale Cyber Security Centrum?

Goede samenwerking met het NCSC is cruciaal voor het slagen van het DTC. Het DTC en het NCSC hebben op verschillende manieren samengewerkt. Zo is het NCSC vertegenwoordigd in de programmaraad van het DTC en deelt het NCSC informatie die het DTC in een *Start of Week* omzet en vervolgens deelt met samenwerkingsverbanden. De samenwerking tussen het NCSC en het DTC kent ook knelpunten, waardoor er sprake was van een moeilijke start van de samenwerking. Cultuurverschillen en onduidelijke samenwerkingsafspraken hebben eraan bijgedragen dat de samenwerking tussen het DTC en het NCSC op enig moment tijdelijk is vastgelopen.

Beide organisaties zijn overtuigd van het belang van een goede samenwerking en er is en wordt ook gewerkt aan het verbeteren van de samenwerking. Zo zijn er gesprekken geweest tussen medewerkers van het NCSC en het DTC waarin afspraken zijn gemaakt en zijn er concept-samenwerkingsafspraken op papier gezet. Hiermee is de samenwerking, nadat deze tijdelijk was vastgelopen, verbeterd. Ook is de verwachting dat de samenwerking verder zal verbeteren als het NCSC en het DTC de gemaakte afspraken in de praktijk zullen brengen.

Subvraag 3: Hoe is de samenwerking vormgegeven met overige stakeholders?

Het DTC werkt veel en intensief samen met allerlei partijen (brancheorganisaties, platforms en kennisinstituten) en heeft daardoor een goed netwerk op het terrein van cyberweerbaarheid. Mede hierdoor is er veel draagvlak en een gevoel van eigenaarschap voor het DTC onder relevante stakeholders. Tijdens het opzetten van het DTC is een klankbordgroep samengesteld met verschillende (branche)organisaties. Deze is in 2018 omgezet in een programmaraad. De klankbordgroep en daarna de programmaraad dragen bij aan het gevoel van eigenaarschap. Op sommige punten kan de samenwerking tussen het DTC en andere partijen nog worden geïntensiveerd. Zo kan het DTC nog meer aansluiten bij al bestaande initiatieven (zoals congressen en campagnes) van samenwerkingspartners. Op deze wijze kunnen veel bedrijven bereikt worden en hoeft het DTC minder zelf te ontwikkelen. Ook kan het DTC meer informatie delen met andere organisatieonderdelen van het ministerie van EZK, zodat de informatie die het DTC tot haar beschikking heeft bijvoorbeeld gebruikt kan worden bij het opstellen van beleid.

5.2. Aanbevelingen

1. Werk in een volgende fase van het DTC toe naar vergroting van het bereik/effect. Door doelgroepen te analyseren en te bezien waar 'grote klappers' kunnen worden gemaakt en door meer informatie te verzamelen die zicht geeft op de effecten van de activiteiten van het DTC.

In de eerste fase van haar bestaan heeft het DTC zich met name gericht op 'daar waar de energie zit'. Bijvoorbeeld door samenwerkingsverbanden aan zich te verbinden die zich reeds georganiseerd hadden en die gemotiveerd waren (ook) samen te werken op het gebied van cyberweerbaarheid. Deze invalshoek was een logische en geschikte keuze voor het opbouwen van de organisatie en om de eerste stappen te zetten.

Voor de volgende fase raden we het DTC aan meer nadruk te leggen op het analyseren van wat er nodig is om bedrijven in staat te stellen cyberweerbaarder te worden, zodat vervolgens die activiteiten uitgevoerd kunnen worden waarmee het grootste bereik en het meeste effect wordt gerealiseerd. Het maken van een keuze voor activiteiten is hoe dan ook nodig, gezien de doelgroep van 1,8 miljoen bedrijven die het DTC met slechts 11 fte tracht te bereiken.

Wij bevelen het DTC aan om de volgende stappen te zetten:

- Doelgroepen segmenteren en vervolgens per segment bepalen wat nodig is om dit deel van de doelgroep in staat te stellen cyberweerbaarder te worden.
- Een analyse maken van met welke inspanningen zoveel mogelijk bedrijven bereikt kunnen worden. Oftewel: hoe kan het DTC 'grote klappers' maken? In de analyse kan bijvoorbeeld gekeken worden naar: Welke drie brancheorganisaties hebben de grootste achterban? Bij welke bestaande campagnes kan het DTC aansluiten? Op welke congressen komen veel bedrijven uit de doelgroep en waar kan het DTC dus het best ook een rol innemen?
- Gebruik maken van gedragsinzichten *(behavourial insights)* aangaande specifieke doelgroepen. Het is een uitdaging om bedrijven echt in actie te laten komen met activiteiten en producten van het DTC, in de zin van dat ze maatregelen op het gebied van cyberweerbaarheid gaan nemen. Het is daarom behulpzaam om bij het ontwikkelen van producten onderzoek te laten doen naar en vervolgens gebruik te maken van gedragsinzichten: wat is er nodig om bedrijven echt hun gedrag te laten aanpassen?
- Het zicht op het bereik en de effecten van activiteiten en producten van het DTC vergroten. De bijdrage van het DTC aan de cyberweerbaarheid van ondernemend Nederland is lastig te meten. Er zijn allerlei andere factoren van invloed op de cyberweerbaarheid van bedrijven, zoals andere programma's en organisaties. Daardoor is de toerekenbaarheid van effecten aan het DTC lastig vast te stellen. Wel zijn er verschillende manieren waarop het zicht op het bereik en de effecten vergroot kan worden. Het DTC houdt al veel informatie bij over de eigen activiteiten en die van samenwerkingsverbanden. Om meer zicht te krijgen op de effecten van deze activiteiten raden we het DTC ten eerste aan meer informatie onder gebruikers te verzamelen. Het DTC houdt bijvoorbeeld bij hoeveel bedrijven de Basisscan Cyberweerbaarheid hebben gedownload. Aanvullend hierop kan het DTC gebruikers vragen in hoeverre bedrijven hun gedrag ook daadwerkelijk hebben aangepast naar aanleiding van de scan. Ook kan het DTC gebruikersonderzoek uitvoeren onder de bedrijven die zijn aangesloten bij de samenwerkingsverbanden. Ten tweede kan het DTC voorbeelden verzamelen van wat de ondersteuning door het DTC oplevert voor samenwerkingsverbanden. Door middel van deze voorbeelden ontstaat meer zicht op hoe de activiteiten en producten bijdragen aan de beoogde effecten. Op deze wijze krijgt het DTC meer zicht op zijn bijdrage aan het vergroten van de cyberweerbaarheid van ondernemend Nederland. Met meer zicht op het bereik en de effecten kunnen vervolgens strategische keuzes gemaakt worden over het wel of niet doorontwikkelen van producten en het wel of niet uitvoeren of uitbreiden van activiteiten.

2. Creëer de voorwaarden waaronder relevante dreigingsinformatie gedeeld kan worden met grote/volwassen, niet-vitale bedrijven.

Grote/volwassen bedrijven die geen onderdeel uitmaken van de vitale infrastructuur vallen momenteel tussen wal en schip. Ze behoren niet tot de doelgroep van het NCSC (dat zich alleen richt op de vitale bedrijven) en de ondersteuning van het DTC is met name waardevol voor bedrijven die relatief nog minder volwassen zijn (vaak MKB). Grote/volwassen bedrijven hebben vaak zelf al veel kennis en ervaring op het gebied van cyberweerbaarheid, waardoor de informatie van het DTC te algemeen is.

Grote/volwassen, niet-vitale bedrijven hebben behoefte aan specifieke dreigingsinformatie, maar ontvangen deze informatie momenteel nog niet altijd. We bevelen daarom aan om te borgen dat de voorwaarden gecreëerd worden waaronder het DTC grote/volwassen, niet-vitale bedrijven kan voorzien van de dreigingsinformatie waar zij behoefte aan hebben.

3. Versterk de samenwerking tussen het DTC en het NCSC door te werken aan een gevoel van gezamenlijkheid en door de samenwerking regelmatig te evalueren.

Een goede samenwerking tussen het DTC en het NCSC is cruciaal. We bevelen daarom aan om verschillende stappen te zetten om de samenwerking tussen het DTC en het NCSC (weer) zo effectief mogelijk te laten verlopen. Sommige van deze stappen zijn reeds ingezet of opgenomen in de opgestelde concept-samenwerkingsafspraken.

Het is ons inziens belangrijk om te werken aan een gevoel van gezamenlijkheid onder de medewerkers van het DTC en het NCSC. Een manier om dit te bereiken is ervoor zorgen dat medewerkers elkaar kennen, door regelmatig gezamenlijke activiteiten te ondernemen. Gedacht kan worden aan kennissessies over een bepaald onderwerp of het samen werken aan een product. Ook het regelmatig werken in elkaars nabijheid kan bijdragen aan een gevoel van gezamenlijkheid.

Daarnaast bevelen we aan om regelmatig te evalueren of de gemaakte samenwerkingsafspraken in de praktijk gebracht worden en of hiermee de samenwerking naar wens van zowel het DTC als het NCSC verloopt.

4. Monitor het succes van het platform en pas toekomstige beslissingen daarop aan. Wees realistisch in de verwachtingen over de deelname aan het platform en pas de inzet van tijd en middelen door het DTC daarop aan.

Het is lastig om vooraf de inschatting te maken in hoeverre bedrijven het platform daadwerkelijk zullen gaan gebruiken. Wel zijn in de evaluatie twijfels over de meerwaarde van het platform en de mate waarin het platform gebruikt gaat worden naar voren gekomen.

We bevelen het DTC daarom aan om het succes van het platform te monitoren en toekomstige (investerings)beslissingen daarop aan te passen. Uiteindelijk is het belangrijk dat het DTC haar (beperkte) tijd en middelen steekt in die zaken die de grootste bijdrage leveren aan het in staat stellen van bedrijven om cyberweerbaarder te worden. Mocht uit het monitoren van het platform blijken dat het platform in de behoefte van slechts een zeer klein aantal bedrijven voorziet, dan dient ook de mogelijkheid om te stoppen met het platform of alleen een ‘light’ versie aan te bieden overwogen te worden. Een ‘light’ versie zou een omgeving kunnen bieden voor bedrijven om informatie aan te bieden, zonder dat het DTC zelf actief een rol speelt op het platform door het delen van informatie.

Bijlage I. Overzicht gesprekspartners

Rijksoverheid

- Digital Trust Center (DTC) (3 gesprekken)
- Ministerie van Economische Zaken en Klimaat (EZK)
- Nationaal Cyber Security Center (NCSC) (3 gesprekken)
- Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)

Samenwerkingsverbanden en brancheorganisaties

- Adfiz
- Connect2Trust
- Cyber Security Programma Noordzeekanaalgebied
- Cyber Weerbaarheidscentrum Brainport (CWB)
- Cybersecurity Centrum voor de Maakindustrie
- Cyberweerbaarheid Groentezadenveredelingsbedrijven
- Cyberweerbaarheid Limburg
- CYSSEC (Cybersecurity Synergie Schiphol Ecosysteem)
- FERM
- GEU (Groep Educatieve Uitgeverijen)
- Innovation Quarter
- Koninklijke Metaalunie
- Nationale Beheersorganisatie Internet Providers (NBIP)
- NIDV Cyberweerbaarheid DVI
- Noord Holland Samen Veilig
- NuBno – De 8e disbalans | Digitale Veiligheid in de Zorg
- Platform Zelfstandige Ondernemers (PZO)
- Stichting Cyberweerbaarheid Noord-Nederland

Overige stakeholders

- ECP|Platform voor de InformatieSamenleving
- CIO Platform Nederland
- Cyberveilig Nederland
- Deloitte
- Haagse Hogeschool
- MKB-Nederland
- NLdigital
- VNO-NCW

Bijlage 2: Samenvatting CBS Statistiek ICT-gebruik bedrijven 2019

Het CBS heeft op verzoek van het ministerie van EZK DTC-bedrijven (bedrijven die zich aangemeld hebben bij één van de samenwerkingsverbanden die aan het DTC zijn verbonden) opgenomen in de *Statistiek ICT-gebruik bedrijven 2019.* Het CBS heeft de ICT-kenmerken van DTC-bedrijven vergeleken met die van een referentiegroep van bedrijven. De referentiegroep is een groep bedrijven uit de *Statistiek ICT-gebruik bedrijven* die door herweging qua bedrijfstak en -grootte eenzelfde samenstelling heeft als de populatie DTC-bedrijven. Hierna hebben we een beknopte samenvatting opgenomen van de belangrijkste resultaten uit de *Statistiek ICT-gebruik bedrijven 2019*. De volledige resultaten zijn te vinden via deze link: https://www.cbs.nl/nl-nl/maatwerk/2019/50/ict-kenmerken-bedrijven-digital-trust-center.

- Op sommige aspecten van ICT-veiligheid zijn slechts kleine verschillen te zien tussen DTC-bedrijven en bedrijven in de referentiegroep. Voorbeelden zijn antivirussoftware (99 tegenover 97 procent), beleid voor sterke wachtwoorden (89 tegenover 81 procent) en het up-to-date houden van (besturings)software (98 tegenover 95 procent).
- Op andere aspecten van ICT-veiligheid zijn grotere verschillen te zien. Zo hebben de DTC-bedrijven in vergelijking met de bedrijven in de referentiegroep meer ICT-veiligheidsmaatregelen getroffen (zo maakt 79 procent van de DTC-bedrijven gebruik van authenticatie via soft- of hardware-token, tegenover 54 procent van de referentiegroep en maakt 78 procent van de DTC-bedrijven gebruik van risicoanalyses, tegenover 56 procent van de bedrijven in de referentiegroep), geven meer DTC-bedrijven vrijwillige cursussen aan hun personeel op het terrein van ICT-veiligheid (68 procent tegenover 44 procent), hebben meer bedrijven procedures omtrent ICT-veiligheid vastgelegd in een document (78 procent tegenover 51 procent) en wordt dit document frequenter geactualiseerd in vergelijking met de bedrijven in de referentiegroep (68 procent van de DTC-bedrijven heeft het document minder dan 12 maanden geleden gereviewed, tegenover 37 procent van de bedrijven in de referentiegroep).
- DTC-bedrijven hebben uiteindelijk ook iets minder vaak te maken gehad met ICT-incidenten (39 tegenover 51 procent) en lijken met name bij de incidenten door een aanval van buitenaf, beter in staat de kosten hiervan te beperken, in vergelijking met de bedrijven in de referentiegroep.
- Vijf procent van de DTC-bedrijven gebruikt de website van het DTC ten behoeve van cyberweerbaarheid. Voor de referentiegroep is dit zes procent.
- Van de bedrijven uit de populatie van de statistiek ‘ICT-gebruik bedrijven exclusief de DTC-bedrijven’, is acht procent bekend met het Digital Trust Center en geeft twee procent aan de website van het DTC wel eens bezocht te hebben. Voor de bedrijven uit de referentiegroep (bedrijfstakken en bedrijfsgrootteklassen van waaruit bedrijven daadwerkelijk deelnemen aan het DTC) zijn deze percentages respectievelijk 16 en zes procent.

KWINK groep B.V.
Nassaulaan 1
2514 JS Den Haag

www.kwinkgroep.nl