Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 817

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 7 februari 2022

In mijn brief aan uw Kamer d.d. 16 december 2020 over de voortgang van het Digital Trust Center (DTC)[1] is aangekondigd u eind 2021 te berichten over de voortgang van het DTC in de realisatie van de gestelde doelen. Hierbij informeer ik u conform deze toezegging.

In het Regeerakkoord staat de ambitie verwoord van centraal gecoördineerde structurele samenwerking tussen publieke en private organisaties om sneller en makkelijker informatie te delen over digitale kwetsbaarheden en «hacks» (Kamerstuk 35 788, nr. 77). Het DTC wordt hierbij genoemd als één van de partijen die hier een rol heeft te vervullen, uiteraard in goede samenwerking met het Nationaal Cybersecurity Centrum (NCSC), bedrijven en wetenschappers. Deze brief informeert u over de bijdrage die het DTC heeft geleverd en gaat leveren aan deze informatiedeling. Achtereenvolgens besteed ik hierbij aandacht aan de strategie, het bereik, de samenwerking met andere organisaties, delen van specifieke dreigingsinformatie met individuele bedrijven en kennisopbouw. Tenslotte komt ook kort de voortgang van het Cyber Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP) ter sprake.

Strategie 2021–2023: verbreden, verdiepen en verankeren

2021 markeerde de aftrap van de strategie voor de periode 2021–2023. Vanuit de hoofdtaak informatie en advies en de hoofdtaak stimuleren van samenwerking lag in 2021 de focus op:

- vergroten van het bereik van het DTC
- het verbreden en bestendigen van het netwerk van cyberweerbaarheidsverbanden
- de start van een nieuwe dienst voor het delen van specifieke dreigingsinformatie met individuele bedrijven

[1] Kamerstuk 26 643, nr. 742.

kst-26643-817
ISSN 0921 - 7371
's-Gravenhage 2022

- kennisopbouw over de stand van zaken over de cyberweerbaarheid van de doelgroep niet-vitale bedrijven

In de bijlage van de Kamerbrief van 16 december 2020 zijn bovenstaande ambities vertaald naar concrete doelstellingen. Het afgelopen jaar is het overgrote deel van de gestelde doelstellingen gerealiseerd. Zo is het DTC in september 2021 gestart met een nieuwe dienst voor het delen van specifieke dreigingsinformatie met individuele, niet-vitale bedrijven. Het starten van deze nieuwe dienst in de zomer van 2021 werd mede mogelijk door de aanwijzing krachtens de Wet beveiliging netwerk- en informatiesystemen (Wbni) als organisatie die objectief kenbaar tot taak heeft om andere organisaties of het publiek te informeren over voor hen relevante digitale dreigingen en incidenten (OKTT). Met deze OKTT-aanwijzing is het voor het DTC mogelijk geworden in ruimere zin dreigingsinformatie te ontvangen van het NCSC. Uw Kamer is hier bij brief van 2 juni jl. ook over geïnformeerd.[2]

Verhoogd bereik en online interactie met doelgroep niet-vitaal bedrijfsleven

Groei in bezoekersaantallen van de DTC-website en interactie sociale media

Door het jaar heen zien we een consistente stroom aan bezoekers van de DTC-website, met pieken in bezoekersaantallen bij cyberincidenten zoals Log4j. Het streven was in totaal 150.000 bezoeken voor de periode 1 januari 2021 tot en met 31 december 2021. Realisatie voor deze periode is 227.123 bezoeken aan de website, waarvan 172.252 unieke bezoekers. Daarmee is de voorgenomen doelstelling ruim behaald. Daarnaast is het bereik van DTC op sociale media flink gegroeid: op LinkedIn telt DTC 5.162 volgers (t.o.v. 3.333 in 2020), op Twitter 1.634 (t.o.v. 728 in 2020). Daarbij laten de statistieken zien dat met name berichten over algemene dreigingsinformatie goed gedeeld en bekeken worden.

Verhoogde inzet op DTC online community heeft vruchten afgeworpen

De doelstelling van 250 leden voor de DTC online community is ruim gepasseerd, de teller staat per 31 december 2021 op 739. Met het actief modereren van de community is ook de interactie op het platform aanzienlijk verhoogd. Het doel is dat het DTC in 2022 deze groei vasthoudt door huidige inzet te behouden en gebruikersvriendelijkheid van het platform nog beter te maken.

Inzet op gedragsverandering met interactieve online tools en evenementen

Met de (door)ontwikkeling en publicatie van nieuwe content, interactieve tools en door deelname en organisatie van diverse (online) evenementen heeft het DTC ook ingezet op gedragsverandering omtrent cyberweerbaarheid bij de DTC doelgroep met het bieden van handelsperspectief (van weten dat het speelt naar daadwerkelijk stappen nemen).

Het DTC biedt ondernemers een portfolio aan interactieve online tools om hun cyberweerbaarheid te toetsen en hun kennis te vergroten:
- De DTC basisscan is een zelfevaluatie die ondernemers kunnen invullen om te meten in hoeverre hun cyberweerbaarheid strategie voldoet aan de door het DTC vastgestelde vijf basis principes van cyberweerbaarheid. De doelstelling voor in totaal 4.000 compleet

[2] Aanhangsel Handelingen II 2020/21, nr. 2760.

ingevulde basisscans voor de periode van 2019 t/m 2021 is per 31 december 2021 behaald met een realisatie van 4.140 ingevulde scans.
- De tweede tool is het risicoclassificatiemodel. Deze tool is in opdracht van de Ministeries van Economische Zaken en Klimaat (EZK) en Justitie en Veiligheid (JenV) ontwikkeld door het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en door het DTC gepubliceerd op 12 januari 2021. Uw Kamer is hier met de brief van 30 november jl over de voortgang van de Roadmap veilige Hard- en Software eerder over geïnformeerd.[3] Per 31 december 2021 is deze tool 5.070 keer volledig ingevuld.
- Daarnaast is op 5 juli 2021 de Security Check Procesautomatisering gelanceerd. Deze is ontwikkeld in samenwerking met diverse partijen. Met de Security Check Procesautomatisering kunnen organisaties snel in kaart brengen waar mogelijke risico's bij geautomatiseerde productieprocessen zitten, maar ook welke beschermingsmaatregelen zij hiertegen kunnen nemen. Tot 31 december 2021 is deze check 1.241 keer gebruikt.

Voor 2022 stelt het DTC het doel dat alle tools gecombineerd minstens 10.000 keer gebruikt worden. Om dit doel te realiseren zal het DTC inzetten op periodieke promotie van deze tools bij de doelgroep niet-vitaal bedrijfsleven. Ook staat op de agenda van 2022 om de doelmatigheid van de vijf basisprincipes[4] te evalueren. Hiervoor zal DTC waar mogelijk samenwerken met het NCSC. Aan de hand van deze evaluatie zullen interactieve tools zoals de basisscan en risicoklasse-analyse eventueel worden aangepast.

Het DTC heeft in 2021 met de organisatie van twee webinars, één voor de doelgroep brancheverenigingen en één gericht op ICT-dienstverleners, haar banden aangehaald met samenwerkingspartners om de naamsbekendheid van het DTC te vergroten. Met de organisatie van deze twee webinars, georganiseerd in samenwerking met respectievelijk VNO-NCW en MKB-Nederland en NLdigital, was het mogelijk om de beschikbare kennis, tools en diensten van het DTC toe te lichten aan sub-doelgroepen van beide ondernemersorganisaties. Het DTC heeft samen met het NCSC en CSIRT-DSP op 15 december 2021 ook een webinar georganiseerd over de ernstige kwetsbaarheid Log4j. Deze voorzag in een grote behoefte aan actuele informatie en is door meer dan 4.000 bezoekers bekeken. Gelet op de positieve evaluatie vanuit de deelnemers en de grote opkomst bij deze webinars is het DTC voornemens meer van zulke webinars te organiseren in 2022. Door middel van persbriefings heeft het DTC ook de media geïnformeerd over haar activiteiten, zodat deze de relevante ontwikkelingen in de diensten van het DTC kon delen met een breder publiek.

[3] Kamerstuk 26 643, nr. 801.
[4] Zie DTC website voor een overzicht van de 5 basisprincipes: De 5 basisprincipes van veilig digitaal ondernemen | Digital Trust Center (Min. van EZK).

MKB en haar informatiedienstverleners informeren over Log4j

In de laatste maand van 2021 dook misschien wel de ernstigste kwetsbaarheid van het hele jaar op. Op vrijdag 10 december 2021 werd het DTC in de ochtend door het NCSC geïnformeerd dat Apache beveiligingsupdates beschikbaar had gesteld voor een ernstige kwetsbaarheid in Apache Log4j 2, welke ook bekend staat als «Log4Shell». Uit diverse bronnen bleek dat heel veel organisaties gebruik maken van deze open source-bibliotheek. Dit maakte deze kwetsbaarheid in potentie zeer dreigend. Deze kwetsbaarheid raakte de doelgroep van zowel het DTC als het CSIRT-DSP.

Het CSIRT-DSP heeft zijn doelgroep direct geïnformeerd en gewaarschuwd via een doelgroepenbericht. Die middag heeft het DTC een partnerbericht uitgestuurd richting partners en samenwerkingsverbanden over de ernst van de kwetsbaarheid en beschikbaar handelsperspectief. Ook is er een nieuwsbericht geplaatst op de website gevolgd door berichtgeving op sociale media en de DTC Community.

Gezien de aard van Log4j was het voor veel ondernemers niet mogelijk om zelf direct de nodige updates uit te voeren. Veel ondernemers waren afhankelijk van hun softwareleverancier of externe IT-dienstverlener om de nodige updates door te voeren. Gezien de cruciale rol van softwareleveranciers, heeft het DTC daarom op zaterdag 11 december, na overleg met het NCSC, contact gehad met NLdigital zodat zij nog diezelfde dag hun leden, waaronder softwareleveranciers, konden informeren over de Log4j kwetsbaarheid.

Het was in deze periode cruciaal om zo veel mogelijk mensen te informeren over de kwetsbaarheid in Log4j, en hen te helpen bij het nemen van mitigerende maatregelen. In de dagen die volgden hebben het DTC en CSIRT-DSP diverse keren hun doelgroepen opnieuw geïnformeerd als er relevante nieuwe informatie beschikbaar was. Daarnaast organiseerde het DTC en NCSC samen een IT-informatiesessie over de kwetsbaarheid Log4j. In een livestream van 45 minuten werd door verschillende experts van het NCSC en het DTC de problematiek rondom deze kwetsbaarheid geduid. Daarnaast was er de mogelijkheid om vragen te stellen. Deze sessie is door meer dan 4000 bezoekers bekeken.

Het DTC verwacht de komende maanden meer duidelijkheid over de daadwerkelijke gevolgen van de Log4j kwetsbaarheid. Door de nauwe samenwerkingen tussen het DTC, NCSC en CSIRT-DSP was het mogelijk om snel te handelen en de kwetsbare doelgroepen te informeren. Het belang van een goed ingericht partnernetwerk werd ook bevestigd. Met de organisatie van de online informatiesessie was het mogelijk om ook veel ondernemers en ICT-dienstverleners direct te woord te staan en vragen te beantwoorden. Het DTC en NCSC hebben de intentie om in geval van een ernstige dreiging weer een dergelijke sessie te organiseren. Het DTC en NCSC gebruiken de input vanuit de informatiesessie ook voor de ontwikkeling van een gezamenlijk Log4j informatieproduct, te publiceren in de eerste helft van 2022.

Verbreden en bestendigen netwerk cyberweerbaarheidsverbanden

Het DTC-netwerk van cyberweerbaarheidsverbanden helpt bedrijven de cyberweerbaarheid te vergroten en de risico's in de keten te verkleinen. Per 31 december 2021 telt het DTC 37 samenwerkingsverbanden, waarmee de doelstelling voor 50 samenwerkingsverbanden eind 2023 goed haalbaar lijkt. Hiermee draagt het DTC ook bij aan de vorming van een Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden zoals opgenomen in de Nederlandse Cybersecurity Agenda (NCSA).

In 2021 lag de focus van het DTC niet alleen op het aanjagen van nieuwe samenwerkingsverbanden, maar ook op het verstevigen van het bestaande netwerk. Door middel van regulier persoonlijk contact en organisatie van maandelijkse digitale «inloopuren» heeft het DTC getracht bestaande samenwerkingsverbanden te ondersteunen ondanks het feit dat de aanhoudende coronacrisis fysieke bijeenkomsten onmogelijk maakte. Deze online-bijeenkomsten zijn goed bezocht door de samenwerkingsverbanden. Daarnaast is het DTC actief betrokken bij de City Deal «Lokale weerbaarheid Cybercrime (getekend 28 oktober 2020) waarbij het DTC met andere Ministeries (JenV en Binnenlandse Zaken en Koninkrijksrelaties), gemeenten, veiligheidsorganisaties, kennisinstellingen en private partijen samen aan de slag zijn gegaan om de cyberweerbaarheid te verhogen van burgers en bedrijven. Zo heeft het DTC een cybersecurity toolkit ontwikkeld speciaal voor gemeenten. Deze is beschikbaar gesteld via de DTC website. Bij het aanjagen van nieuwe samenwerkingsverbanden is er in 2021 ook gekeken naar welke sectoren en regio's ondervertegenwoordigd zijn in het huidige DTC netwerk. Vanuit die analyse is besloten om in 2022 in te zetten op de totstandkoming van een ISAC voor de topsectoren en een ISAC voor topinstituten. Het DTC werkt samen met TNO, en in afstemming met het NCSC, om dit te realiseren.

Subsidieregeling cyberweerbaarheid

Het openstellen van de subsidieregeling cyberweerbaarheid 2021 heeft er toe geleid dat er zes nieuwe projecten zullen starten in 2022 met als doel de cyberweerbaarheid van bedrijven te vergroten. De zes partijen die deze subsidie hebben ontvangen zijn: Stichting Dutch Institute for Vulnerability Disclosure (DIVD), Stichting ECP, Stichting The Hague Security Delta, MMOX, Synanta BV en Stichting Cyber Safety Noord Nederland. Voor het verder stimuleren van samenwerking op het gebied van cyberweerbaarheid zal na de zomer van 2022 de subsidieregeling cyberweerbaarheid opnieuw worden opengesteld. Bij het uitzetten van deze regeling zal worden gekeken hoe de sectoren en regio's waar nog weinig samenwerkingsverbanden zijn, extra kunnen worden gestimuleerd om met voorstellen te komen.

Start van dienst voor delen specifieke dreigingsinformatie

Het DTC deelt sinds de zomer 2021 bij het DTC bekende specifieke dreigingsinformatie met individuele niet-vitale bedrijven. Sinds de zomer zijn er 15 verschillende aanleidingen geweest om dergelijke bedrijven te notificeren, waarbij het DTC 361 bedrijven direct gewaarschuwd heeft voor een ernstige cyberdreiging.

Pilot «gevraagd notificeren»

Om ook bij grootschalige cyberdreigingen die duizenden individuele bedrijven raakt tijdig te kunnen waarschuwen, onderzoekt het DTC de

schaalbaarheid van deze service. Daarom loopt er parallel aan de uitrol van deze dienst voor ongevraagd notificeren een pilot «gevraagd notificeren». Met een testgroep van 57 bedrijven wordt in een pilot van 12 maanden onderzocht of deze «waarschuwingsdienst» geautomatiseerd kan worden. De bedrijven die deelnemen aan de pilot vertegenwoordigen negen sectoren[5] om zo een representatieve weerspiegeling van het bedrijfsleven te simuleren. Het NCSC draagt bij aan het succes van deze pilot door, met inachtneming van het wettelijk kader van het NCSC, bij het NCSC beschikbare informatie over dreigingen en kwetsbaarheden die relevant is voor de deelnemers aan de DTC-pilot te delen met het DTC. Het DTC vult deze informatie aan door openbare bronnen aan te sluiten op de bestaande infrastructuur om zo in staat te zijn de bedrijfstechnische gegevens te matchen met kwetsbaarheden en dreigingen die openbaar bekend zijn. Tot op heden zijn er in de pilot 6 bedrijven geautomatiseerd genotificeerd omtrent diverse kwetsbaarheden.

Bestendigen taken en bevoegdheden van het DTC

Om de taken en bevoegdheden van het DTC wettelijk te borgen wordt gewerkt aan het wetsvoorstel Bevordering digitale weerbaarheid bedrijven (Wbdwb). Het wetsvoorstel is in de zomer van 2021 in consultatie geweest. De reacties worden momenteel verwerkt en de nodige toetsen zijn of worden doorlopen. Het streven is om Q1 2022 de ministerraad te passeren en de stukken aan de Raad van State aan te bieden. Vooruitlopend op het wetvoorstel, dat de juridische basis van het DTC nader regelt, is het mogelijk voor het DTC om dreigingsinformatie te kunnen ontvangen, verwerken en delen met niet-vitale bedrijven.

Kennisopbouw omtrent doelgroep niet-vitaal bedrijfsleven

Om de cyberweerbaarheid van het niet-vitale bedrijfsleven te verhogen is het van belang dat het DTC een goed beeld heeft van het huidige kennisniveau en de motivatie van de doelgroep ondernemend Nederland. Het DTC werkt samen met het CBS aan de vraagstelling van de jaarlijkse ICT-enquête. Resultaten laten zien dat bedrijven gekoppeld aan het DTC via een DTC-samenwerkingsverband hoger scoren in het nemen van cyberweerbaarheidsmaatregelen dan bedrijven zonder een band met het DTC. Voor 2022 zullen er op verzoek van het DTC in de ICT-enquête een aantal specifieke vragen worden meegenomen over phishing, om zo een beter beeld te krijgen van de mate waarin dit speelt en de consequenties hiervan bij ondernemend Nederland. In 2021 heeft het CBS op verzoek van het DTC ook een apart onderzoek uitgevoerd om de cyberweerbaarheid van ZZP-er doelgroep inzichtelijk te krijgen. Resultaten laten zien dat de cyberweerbaarheid van een ZZP-er sterk wisselt afhankelijk of een ZZP-er eigen opdrachten heeft, of alleen gebruikt maakt van de ZZP-er constructie om full-time gedetacheerd bij een grotere organisatie te werken. De resultaten van 2021 worden gebruikt als nulmeting en dit onderzoek wordt in aangepaste vorm uitgezet in 2022 om beter inzicht te krijgen in de mogelijke rol van DTC om de ZZP-doelgroep te ondersteunen. Daarnaast wordt in het jaarlijks terugkerende trendonderzoek dat in het kader van de bewustwordingscampagne «Alert Online» wordt uitgevoerd, zowel het vitale als te niet-vitale bedrijfsleven meegenomen. In dit onderzoek wordt gekeken naar kennis, houding en gedrag van ondernemers.

[5] Deelnemende bedrijven worden geclassificeerd onder sectoren: 1) gezondheidszorg en welzijn, 2) handel en dienstverlening, 3) ICT, 4) landbouw, natuur en visserij 5) media en communicatie 6) onderwijs, cultuur en wetenschap 7) techniek, productie en bouw 8) transport en logistiek 9) overig.

Uit eigen tools is het voor het DTC mogelijk om ook steeds meer inzichten te krijgen in het kennisniveau van ondernemend Nederland op gebied van cyberweerbaarheid. In 2021 zijn de eerste stappen gemaakt om de data die verzameld wordt vanuit de DTC-tools te vergelijken met het CBS-gemiddelde. Doel is om in 2022 inzicht in eigen data uit tools verder door te ontwikkelen zodat het DTC en haar samenwerkingspartners meer diepgaande kennis hebben van de cyberweerbaarheid van de doelgroep en zo gericht (informatie)producten kunnen ontwikkelen en doorontwikkelen.

Onderzoek toont aan dat menselijk handelen een belangrijke rol speelt in veel cybersecurity-incidenten.[6] Daarom staat ook onderzoek naar de menselijke aspecten van cyberweerbaarheid bij DTC hoog op de agenda. Met die lens heeft het DTC in 2021 samen met NHL Stenden onderzoek gedaan naar de gedragsverandering die plaats vindt bij ondernemers na het doorlopen van de DTC-basisscan. Resultaten tonen aan de mate waarin deze tool leidt tot gedragsverandering afhankelijk is van het profiel van ondernemer en de cybervolwassenheid die hun bedrijf al heeft. In 2022 wil het DTC vervolg geven aan dit onderzoek door de basisscan aan te passen aan de verschillende profielen die naar voren kwamen uit dit onderzoek en door verder onderzoek te doen naar de menselijke gedragsfactoren die ondernemers beïnvloeden om op een bepaalde manier te handelen.

CSIRT-DSP

Ik maak met deze brief van de gelegenheid gebruik u ook te informeren over de voortgang van het CSIRT-DSP[7], dat sinds de oprichting op 1 januari 2019 het CSIRT is voor online marktplaatsen, online zoekmachines en cloud-computerdiensten. Het CSIRT-DSP zet zich in om uitval van netwerk- en informatiesystemen van deze digitale dienstverleners te voorkomen, de gevolgen van een uitval te beperken en te ondersteunen om de integriteit van systemen te verhogen. Deze digitale dienstverleners moeten incidenten met aanzienlijke gevolgen voor hun dienstverlening melden.[8] Het CSIRT-DSP verleent bijstand bij dergelijke incidenten.[9]

Het CSIRT-DSP heeft inmiddels organisatorisch vorm en inhoud gekregen en een aantal relevante diensten ontwikkeld. In 2021 heeft CSIRT-DSP 57 zaken in behandeling gehad, ten opzichte van 42 zaken in 2020 en 6 zaken in 2019.[10] Deze zaken betreffen bijvoorbeeld informatie over kwetsbare systemen waarna het verantwoordelijke contact is geïnformeerd zodat deze actie kon ondernemen. In 2021 is de doelgroep over 5.637 kwetsbare systemen geïnformeerd. Deze informatie komt onder meer uit ontvangen meldingen en van partners, zoals het NCSC, onderzoekers, of andere CSIRT's uit de EU.

Er is door het CSIRT-DSP afgelopen jaar 1 verplichte melding ontvangen die aan de eisen van de meldplicht voldeed. Dit betrof een uitval van een dienst door een DDoS-aanval. Deze melding heeft geleid tot een inspectie door de toezichthouder, Agentschap Telecom. Inmiddels zijn er aanpassingen gedaan door de digitale dienstverleners om een soortgelijke uitval in de toekomst te voorkomen. Vrijwillige meldingen die binnen kwamen gingen over incidenten rond DDoS-aanvallen (eventueel met afpersing[11]),

---

[6] De mens als schakel in cybersecurity | TNO.
[7] Computer Security Incident Response Team voor digitale diensten, art. 4, tweede lid, Wbni.
[8] Ingevolge art. 13, eerste lid, Wbni.
[9] Ingevolgde art. 4, vierde lid, Wbni.
[10] Stand van zaken 09-11-2021.
[11] Ransom DDoS.

ransomware-aanvallen, phishing of uitval van systemen. Het CSIRT-DSP verspreidt wekelijks een situationeel beeld aan zijn doelgroep over kwetsbaarheden, dreigingen en relevante gebeurtenissen van die week. Inmiddels zijn er 110 ontvangers die zich hebben ingeschreven. Verder neemt het CSIRT-DSP actief deel aan het EU CSIRTs Network.[12]

Er is in 2021 verder contact gezocht en gekregen met de doelgroep, brancheorganisaties en samenwerkingsverbanden. Omdat er geen register is van digitale dienstverleners moet het CSIRT-DSP en de doelgroep naar elkaar op zoek om contact te leggen. Om de groei in werkzaamheden te kunnen ondersteunen is het incidentresponseplatform doorontwikkeld. Er zijn inmiddels meer bronnen met voor digitale dienstverleners relevante dreigingsinformatie in gebruik genomen en er wordt meer informatie via publiek-private samenwerkingsverbanden ontvangen.

Tot slot

2022 staat in het teken van het door ontwikkelen en opschalen van de DTC dienstverlening voor het niet-vitale bedrijfsleven van Nederland. Het DTC heeft zichzelf een aantal kwantitatieve doelen gesteld voor 2022 zodat gemonitord kan worden op de voortgang van haar activiteiten. In de bijlage bij deze brief staan deze opgesomd waarbij onderscheid wordt gemaakt in bereik via verschillende kanalen, het gebruik van tools, het aantal aangesloten samenwerkingsverbanden en het aantal genotificeerde bedrijven.

Met de doorontwikkeling van de informatiedienst ongevraagd notificeren en afronding en evaluatie van de pilot gevraagd notificeren zal het DTC haar vermogen om specifieke dreigingsinformatie te delen uitbreiden. Om deze doelen te bereiken zal ook de samenwerking tussen het DTC en NCSC, met inachtneming van de toepasselijke wettelijke kaders, verder worden uitgebreid op zowel operationeel, tactisch en strategisch niveau. Verder zal het DTC verder doorpakken in het beter inspelen op de behoeftes van haar doelgroep. Door analyse van de data uit eigen tools, onderzoek in samenwerking met het CBS en aanvullend kwalitatief onderzoek wil het DTC een duidelijk overzicht en inzicht krijgen van de cyberweerbaarheid van het niet-vitaal bedrijfsleven, handelingsperspectieven en activatie van deze doelgroep.
Het DTC ligt op koers. Ook de komende jaren zal het Ministerie van Economische Zaken en Klimaat blijven investeren in de cyberweerbaarheid van niet-vitale bedrijven om daarmee bij te dragen aan het verdienvermogen van ondernemend Nederland en de economische kansen van digitalisering daadwerkelijk te kunnen benutten.

Begin 2023 zal ik u wederom informeren over de voortgang zodat u zicht op de realisatie houdt.

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

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

Bijlage **Voortgang DTC**

Toezegging	Realisatie 31–12	Toelichting / vervolg
1. Kwantitatief		
Bezoeken DTC website 150.000 in 2021	Gerealiseerd (227.123)	Nieuw doel voor 2022 230.000 bezoeken
50 samenwerkingsverbanden eind 2023	In wording (realisatie 37)	Doelstelling ligt op koers
4.000 ingevulde basisscans in periode 2019–2021	Gerealiseerd (4.140)	Nieuw doel gebruik van alle tools bij elkaar opgeteld 10.000 in 2022
DTC Online community 250 deelnemers eind 2021	Gerealiseerd (739)	Nieuw doel 1.000 deelnemers eind 2022
2. Kwalitatief		
Aanwijziging DTC krachtens Wbni als OKTT	Gerealiseerd	Ruimere informatie-uitwisseling vanuit NCSC
Samenwerkingsafspraken DTC en NCSC	In wording	Samenwerking in de praktijk gebracht, afspraken dienen nog ondertekend te worden
Wetsvoorstel voor delen concrete dreigingsinformatie	In wording	Streven om in Q1 2022 de MR te passeren en de stukken aan de Raad van State aan te bieden
CBS onderzoek cybersecurity ZZPers	Gerealiseerd	Onderzoek zal worden herhaald in 2022
Gedragsonderzoek	Gerealiseerd	Publicatie van NHL Stenden onderzoek basis voor verder onderzoek naar gedragsfactoren.
Nieuwe subsidieregeling cyberweerbaarheid	Gerealiseerd (6 projecten)	Subsidieregeling zal opnieuw worden opengesteld Q3 2022
Informatiedienst voor concrete dreigingsinformatie (ongevraagd notificeren)	Gestart (361 notificaties)	Dienst wordt verder uitgebouwd
3. Extra / nieuw		
DTC pilot gevraagd notificeren	Gestart	Pilot wordt Q3 2022 afgerond en geëvalueerd
Webinar georganiseerd voor doelgroep brancheverenigingen en IT dienstverleners	Gerealiseerd	Instrument wordt ook in 2022 ingezet i.s.m. partners
Webinar Log4j	Gerealiseerd	Instrument wordt ook in 2022 ingezet bij grote cyberincidenten
Ontwikkeling feedbackloops uit eigen tools	In wording	DTC komt in 2022 met eigen bijdrages over ontwikkelingen in cybersecurity