Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 616

BRIEF VAN DE STAATSSECRETARIS VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 17 juni 2019

In mijn brief van 26 juni 2018[1] heb ik toegezegd u begin 2019 opnieuw te informeren over waar het Digital Trust Center (hierna: DTC) staat. Met deze brief informeer ik u mede namens de Minister van Justitie en Veiligheid hierover. Achtereenvolgens ga ik in op de resultaten van 2018 en de speerpunten voor 2019, de voortgang op de twee hoofdtaken van DTC, de samenwerking binnen en buiten de overheid en tot slot de organisatie en de evaluatie.

Resultaten 2018 en speerpunten 2019

*H*et DTC is in 2018 goed van start gegaan en heeft haar eerste concrete bijdrages geleverd aan veilig digitaal ondernemen. De programma-organisatie staat en er is een relevant netwerk tot stand gekomen. In juni 2018 is de website (www.digitaltrustcenter.nl) met vijf basisprincipes voor veilig digitaal ondernemen live gegaan. Momenteel zijn er 10 samenwerkingsverbanden (clusters van niet-vitale bedrijven die hun cyberweerbaarheid willen vergroten) verbonden aan het DTC. Begin 2019 is een keuze gemaakt voor een leverancier van het digital trust platform. Dit platform dient als digitale interactieve ontmoetingsplaats voor bedrijven, samenwerkingsverbanden en experts die cybersecurity kennis willen delen en vermeerderen. Daarnaast komen er via het platform mogelijkheden voor communities (sectoraal, regionaal, thematisch) om informatie afgeschermd te delen.

De 5 basisprincipes van veilig digitaal ondernemen:
1. *Inventariseer kwetsbaarheden: breng jouw (digitale) risico's in kaart en maak back-ups;*
2. *Kies veilige instellingen: kies de instellingen die passen bij jouw (digitale) risico's;*

[1] Kamerstuk 26 643, nr. 545.

kst-26643-616
ISSN 0921 - 7371
's-Gravenhage 2019

3. *Voer updates uit: leveranciers leveren regelmatig updates, installeer die meteen of zet automatisch updaten aan;*
4. *Beperk toegang: verleen bewust en passende toegang tot systemen en data;*
5. *Voorkom virussen en andere malware: zorg voor gepaste maatregelen (zoals een antivirusprogramma) en stimuleer veilig gedrag bij medewerkers.*

Ook heeft de samenwerking met het Nationaal Cybersecurity Centrum (NCSC) van het Ministerie van Justitie en Veiligheid in 2018 handen en voeten gekregen en wordt informatie en ervaring gedeeld. Dit laatste heeft onder meer geresulteerd in handreikingen voor samenwerking in sectoren, regio's en ketens die door het DTC beschikbaar zijn gesteld aan haar doelgroep. Hiermee wordt concreet invulling gegeven aan de ambities zoals deze zijn neergelegd in de Nederlandse Digitaliseringstrategie (NDS)[2] en de Nederlandse Cybersecurity Agenda (NCSA)[3].

De grote opgave voor het DTC voor 2019 is vraag naar en aanbod van informatie en kennis over digitaal veilig ondernemen bij elkaar te brengen. Hiertoe zijn de volgende drie speerpunten voor 2019 vastgesteld:
1. Uitbreiden van het netwerk van samenwerkingsverbanden ten behoeve van kennisdeling in regio, per sector en op thema's (voorkomen, herkennen en reageren);
2. Versterking van de samenwerking tussen het DTC en het NCSC waarbij gekeken zal worden naar synergie in het verrichten van activiteiten en verdere onderlinge informatie-uitwisseling ten behoeve van de onderscheidenlijke doelgroepen.
3. Doorontwikkeling en het promoten van de website en het platform plus het aanbieden van extra tools om het niet-vitale bedrijfsleven te bereiken en te helpen weerbaarder te worden tegen cyberdreigingen.

Naast deze speerpunten vindt er een aantal verkenningen plaats die de basis kunnen vormen voor nieuwe activiteiten van het DTC. Deze verkenningen vinden plaats in nauwe samenwerking met de partners van het DTC. Een voorbeeld hiervan is een recente eerste verkenning naar welke rol gemeentes kunnen vervullen als het gaat om het bereiken van bedrijven in hun gemeente, al of niet georganiseerd in winkeliersverenigingen en ondernemersverenigingen. De resultaten hiervan zullen gedeeld worden met de VNG.

Voortgang hoofdtaak 1: informatie en advies

De inhoud van de website van het DTC wordt periodiek vernieuwd. Hierbij wordt de volgende indeling gehanteerd: voorkomen (bijvoorbeeld «wat zijn sterke wachtwoorden?»), herkennen (bijvoorbeeld «hoe herken ik phishing e-mails?») en reageren (bijvoorbeeld «gehackt, wat nu?»). De website en de nieuwe inhoud wordt onder de aandacht gebracht van de doelgroep met behulp van gerichte online campagnes. De ambitie is eind 2019 minimaal 30.000 bezoekers te hebben gehad en eind 2020 minimaal 100.000 bezoekers.

De website was een eerste stap. De tweede stap is het digital trust platform. Het live gaan van het platform is voorzien in het derde kwartaal van 2019. Hiermee krijgen de samenwerkingsverbanden een digitale ontmoetingsplaats en kan kennisdeling vertrouwd, gericht en sneller plaats vinden. Het streven hier is begin 2020 80% van de samenwerkings-

[2] Kamerstuk 26 643, nr. 541.
[3] Kamerstuk 26 643, nr. 536.

verbanden aangesloten te hebben op het platform en eind 2020 te komen tot een actieve community van 500 deelnemers.

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. Verder zal er samen met de samenwerkingsverbanden worden gewerkt aan de inzet van in de praktijk beproefde scans voor bedrijven, onder meer met inzet van studenten. Dit heeft als voordeel dat de geleverde expertise betaalbaar is voor het MKB. Tevens wordt hierdoor de aansluiting van onderwijs op praktijkvraagstukken verbeterd en schaarse kennis ontwikkeld. Ook zal er separaat onderzoek plaats vinden 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. Dit betreft de inhoud van de berichtgeving maar ook het communicatiekanaal dat wordt ingezet om de doelgroep te bereiken. De resultaten worden aan het einde van dit jaar verwacht.

Voortgang hoofdtaak 2: samenwerking stimuleren

In mijn brief van 19 september 2018[4] heb ik u geïnformeerd over de zes nieuwe samenwerkingsverbanden die tot stand zijn gekomen met behulp van de subsidieregeling cyberweerbaarheid die het DTC in het voorjaar van 2018 in de markt heeft gezet. Al eerder werd er samengewerkt met Cyberweerbaarheid Centrum Brainport (Eindhoven). Sindsdien is er een drietal samenwerkingsverbanden bij gekomen: FERM (bedrijvencluster in de Rotterdamse haven), CYSSEC (bedrijvencluster op Schiphol) en Connect2Trust (multi-sectoraal cluster van vijftien bedrijven).
Op 1 april 2019 is een nieuwe ronde gestart van de subsidieregeling die tot doel heeft nieuwe samenwerkingsverbanden op het gebied van cybersecurity te faciliteren. Bij sluiting op 13 mei jl. waren er 18 nieuwe aanvragen voor subsidie ingediend. De toekenningen zullen in juli dit jaar bekend worden gemaakt. Naar verwachting levert dit minimaal vijf nieuwe samenwerkingsverbanden op. Doordat ook andere samenwerkingsverbanden, waaronder niet-vitale Information Sharing and Analysis Centres (ISAC's), zich naar verwachting zullen aansluiten bij het DTC, is als ambitie geformuleerd dat er eind 2019 twintig samenwerkingsverbanden zijn aangesloten bij DTC. Onder een ISAC wordt verstaan een vrijwillige samenwerking tussen partijen in een sector met als doel het vertrouwelijk delen van informatie en analyse over dreigingen, incidenten, kwetsbaarheden, maatregelen en leerpunten op het gebied van digitale weerbaarheid.

> *Stichting Cybersafety Noord-Nederland is samen met de noordelijke regionale overheden (gemeentes en de drie noordelijke provincies), ROC en HBO instellingen een project gestart gericht op het MKB. In dit project worden de volgende activiteiten verricht: organiseren van bewustmakingssessies, uitvoeren van security scans, inrichten van een security pool, opzetten van een security community en uitvoeren van cybercrisis oefeningen met ondernemers en bestuurders. Meer dan 500 bedrijven zijn inmiddels al bereikt.*

[4] Kamerstuk 26 643, nr. 560.

Samenwerking binnen en buiten de overheid

Het DTC werkt met het NCSC samen om bovengenoemde hoofdtaken uit te voeren. Het kabinet heeft de ambitie het DTC door te ontwikkelen tot een «one-stop-shop voor het niet-vitale bedrijfsleven» (Voortgangsbericht Digital Trust Center, Kamerstuk 26 643, nr. 545). Hiermee wil het kabinet recht doen aan de behoefte van het (niet-vitale) bedrijfsleven om één loket te hebben voor veilig digitaal ondernemen. Met het oog hierop is het gewenst dat het NCSC het DTC, met inachtneming van de geldende wettelijke kaders, zal voorzien van actuele en concrete informatie over dreigingen en incidenten of aanwijzingen daarvoor, voor zover deze informatie relevant is voor het niet-vitale bedrijfsleven. Zoals hierboven vermeld zal daarom worden beoordeeld of en in hoeverre het NCSC het DTC deze informatie gelet op de wettelijke kaders zal kunnen verstrekken. 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. Het DTC zal voor de distributie van deze informatie onder andere het DTC platform in zetten, uiteraard met inachtneming van de kaders die hiervoor op grond van de Algemene verordening gegevensbescherming (AVG) gelden.

Het DTC en het NCSC hebben als gezamenlijk doel Nederland weerbaarder te maken tegen cyberdreigingen. Het NCSC staat hierbij aan de lat voor de vitale sectoren en de rijksoverheid en het DTC voor het «niet-vitale bedrijfsleven», van zzp-er tot multinational. Het DTC zorgt voor de communicatie naar haar doelgroep. Hierbij benut het DTC niet alleen de kennis en ervaring ter zake van het NCSC, maar ook de kennis van de samenwerkingsverbanden die met het DTC verbonden zijn én de mix van haar communicatiekanalen (website, platform, social media en fysieke netwerkbijeenkomsten).

> *Cyber Weerbaarheidscentrum Brainport (Hightech industrie in Nederland) is een initiatief van een twintigtal grotere bedrijven uit Eindhoven, Brainport Development, Brainport Industries, BDO en de Provincie Noord-Brabant. Dit centrum biedt deelnemers de volgende producten: een security health check, een digitaal platform voor uitwisselen van best practices en kennis over dreigingen en kwetsbaarheden (hier wordt na lancering het digital trust platform voor gebruikt), deelname aan intervisiegroepen en een sectoraal dreigingsbeeld. Bovenop het standaardlidmaatschap biedt het centrum de mogelijkheid van gezamenlijk inkopen van security consultancy, awareness trainingen, incident response en forensisch onderzoek*

Het DTC werkt ook samen met andere organisatieonderdelen van het Ministerie van Economische Zaken en Klimaat aan implementatie van agenda's voor een duurzaam ondernemend Nederland. Dit geldt bijvoorbeeld voor de Nederlandse Digitaliseringsstrategie, de roadmap Digitale Veilige Hard en Software (DVHS) en het MKB-actieplan. Voor de Nederlandse digitaliseringsstrategie draagt het DTC bij aan het versterken van het fundament van Nederland Digitaal, in het bijzonder door digitale veiligheid en privacy op orde te krijgen. Voor de roadmap DVHS gaat het om de opvolging van metingen van TU Delft naar besmette IoT (Internet of Things)-apparaten door in gesprek te gaan met fabrikanten en andere stakeholders om maatregelen te treffen. Over de voortgang van alle maatregelen van de roadmap DVHS informeer ik u separaat. Voor het MKB-actieplan is de inzet om cybersecurity integraal onderdeel te laten zijn van de digitalisering van het bedrijfsleven. Ook met (de uitvoering van) het cybercrime- en cybersecuritybeleid van het Ministerie van Justitie

en Veiligheid zijn er veel raakvlakken: uiteraard geldt dat voor de Nederlandse Cyber Security Agenda maar ook met de integrale aanpak cybercrime en de jaarlijkse awareness-campagnes zoals Alert Online.

Met ingang van 1 januari 2019 is het Computer Security Incident Response Team (CSIRT) voor digitale diensten (online zoekmachines, cloudcomputerdiensten en online marktplaatsen) ondergebracht bij het Ministerie van Economische Zaken en Klimaat. Dit vloeit voort uit de Wet beveiliging netwerk- en informatiesystemen (Wbni), die strekt tot uitvoering van de EU-richtlijn houdende maatregelen voor een hoog gemeenschappelijk niveau van de beveiliging van netwerk- en informatiesystemen in de Unie (NIB-richtlijn; EU) 2016/1148). Het CSIRT voor digitale diensten (CSIRT-DSP) is krachtens de Wbni voor wat digitale dienstverleners betreft belast met de in bijlage 1 van de NIB-richtlijn genoemde taken, waaronder het monitoren en reageren op incidenten en het zorgen voor waarschuwingen en verspreiding van informatie over risico's en incidenten. De Wbni regelt ook dat digitale dienstverleners incidenten met aanzienlijke gevolgen voor hun dienstverlening moeten melden bij het CSIRT-DSP. Met het oog hierop is er bij het CSIRT-DSP een meldpunt ingericht voor incidenten met aanzienlijke gevolgen bij digitale dienstverleners. Het CSIRT-DSP werkt samen met het NCSC, onder meer wat de deelname betreft aan het Europese netwerk van nationale CSIRTs. Hoewel de taken van dit CSIRT-DSP anders zijn dan die van het DTC en ook een andere basis hebben, is bij de praktische uitvoering hiervan gezocht naar synergie met het DTC. Deze is gevonden onder meer in gedeeld gebruik van huisvesting.

Naast de rijksoverheid zijn er ook samenwerkingstrajecten met stakeholders zoals VNO-MKB Nederland, Nederland ICT, Kamer van Koophandel, CIO Platform, ECP, Cyberveilig Nederland en Digitale Infrastructuur Nederland. Op het gebied van onderwijs en onderzoek werkt het DTC samen met kennisinstituten als TNO, CBS, CPB, Saxion en de Haagse Hogeschool. Het DTC hanteert hierbij als filosofie dat via samenwerking de weerbaarheid van het niet-vitale bedrijfsleven op een hoger peil kan worden gebracht en het cybersecurity-ecosysteem van kennisopbouw en kennisdeling structureel wordt versterkt.

Organisatie en evaluatie

Het DTC staat nu als programma-organisatie en is op sterkte. Samen met de stakeholders en de samenwerkingsverbanden wordt er gewerkt aan veiliger digitaal ondernemen. Eind 2019 start de evaluatie van het DTC. Deze evaluatie zal extern worden uitgevoerd en wordt in het eerste kwartaal van 2020 afgerond. Belangrijkste evaluatievraag is «in hoeverre is het DTC een succes als je kijkt naar het bereik en het effect van de activiteiten en hoe borgen we dit na afloop van het programma eind 2020?» Naast deze evaluatie van het DTC zal er ook gekeken worden naar de ervaringen met het eerste jaar van het CSIRT-DSP. Dat biedt de mogelijkheid voor gelijktijdige besluitvorming over de follow-up van het DTC en het CSIRT-DSP. De Tweede Kamer zal over de uitkomst van de evaluatie en de besluitvorming over de follow-up in het tweede kwartaal van 2020 worden geïnformeerd

De Staatssecretaris van Economische Zaken en Klimaat,
M.C.G. Keijzer