Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 742

BRIEF VAN DE STAATSSECRETARIS VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 december 2020

In mijn brief van 18 februari 2020[1] heb ik u geïnformeerd over de uitkomsten van de evaluatie van het Digital Trust Center (DTC). Ook heb ik in die brief toegezegd u in het najaar te berichten over de voortgang van de implementatie van de aanbevelingen uit deze evaluatie en over de voortgang in de realisatie van de gestelde doelen. Hierbij informeer ik u conform mijn toezegging.

Implementatie aanbevelingen evaluatie

Het onderzoeksbureau Kwink heeft in haar evaluatie van het DTC een viertal aanbevelingen gedaan:
- Werk in een volgende fase van het DTC toe naar vergroting van bereik/effect.
- Monitor het succes van het platform en pas toekomstige beslissingen hierop aan.
- Creëer de voorwaarden waaronder relevante dreigingsinformatie gedeeld kan worden met grote/volwassen, niet-vitale bedrijven.
- Versterk de samenwerking tussen het DTC en het NCSC door te werken aan een gevoel van gezamenlijkheid en door de samenwerking regelmatig te evalueren.

Realisatie van de aanbevelingen

Het afgelopen jaar is het overgrote deel van bovengenoemde aanbevelingen gerealiseerd. Met name het bereik van DTC is sterk vergroot door veel meer bezoeken én bezoekers aan de website dan in de eerste twee jaar en ook doordat inmiddels al 31 samenwerkingsverbanden zich hebben aangesloten bij het DTC. Met het inrichten van een informatiedienst zijn de eerste stappen gezet om het delen van concrete dreigingsinformatie met cybervolwassen bedrijven mogelijk te maken. Ook zijn er

[1] Kamerstuk 26 643, nr. 668

kst-26643-742
ISSN 0921 - 7371
's-Gravenhage 2020

afspraken gemaakt tussen DTC en NCSC die tot verdergaande samenwerking leiden, onder andere afspraken over gezamenlijke invullen van themabijeenkomsten en activiteitenkalender en elkaar opzoeken op de werkvloer. Om het mogelijk te maken voor het NCSC om meer informatie over dreigingen en incidenten te delen met het DTC werkt mijn ministerie momenteel aan de voorwaarden om een aanwijzing als organisatie, zoals bedoeld in artikel 3, tweede lid, onderdeel a, Wet beveiliging netwerk- en informatiesystemen (Wbni), een zogenaamde OKTT[2], mogelijk te maken. In de bijlage[3] vindt u een overzicht van de realisatie van de concrete doelen voor 2020[4]. Ik licht in deze brief er een vijftal uit om u een beter beeld te geven.

1. Groei aantal bezoeken en bezoekers website

Het streven was in totaal 100.000 bezoeken voor de periode 2018–2020. Huidige realisatie voor die gehele periode is 184.000 bezoeken aan de website, waarvan 146.000 unieke bezoekers[5]. Vanaf de start op 8 juni 2018 zijn de aantallen bezoeken (afgerond) resp. 11.000 in 2018, 46.000 in 2019 en 127.000 in 2020.Voor de komende periode van drie jaar is minimaal 150.000 bezoeken *per jaar* het streven waarbij ook gestuurd zal worden op daadwerkelijke activering (bijvoorbeeld invullen van de basisscan en andere interactieve tools). Extra aandacht zal hierbij gegeven worden aan het bereiken van mkb en zzp'ers. Deze ambitie sluit naadloos aan op een van de aanbevelingen uit het WODC-rapport over informatie uitwisseling binnen het Landelijk Dekkend Stelsel (LDS[6]), nl. vergroot de vindbaarheid van het DTC onder deze doelgroep. Het DTC zal hierbij zowel inzetten op de eigen vindbaarheid als het benutten van de bij DTC aangesloten samenwerkingsverbanden en andere intermediaire organisaties die dicht bij de ondernemer staan.

2. Verbetering gebruikersvriendelijkheid platform

Dit platform is recent voorzien van een veiligere en gebruiksvriendelijkere tweefactor-authenticatie waardoor gebruik van het platform laagdrempeliger is geworden. Ook is in het verlengde van de geconstateerde behoefte gestart met samenwerkingsruimtes op het platform waarin samenwerkingsverbanden en individuele bedrijven in een vertrouwde, besloten omgeving informatie onderling kunnen uitwisselen. Het streefgetal van 250 gebruikers is helaas nog niet gerealiseerd, de teller staat per 30 november 2020 op bijna 100. Om te komen tot een succesvol platform en community, zal er extra geïnvesteerd worden in het werven van (mede)gebruikers, het actief modereren van de community en het aanbieden van extra informatief materiaal en interactiemogelijkheden.

3. Toename aantal samenwerkingsverbanden

Eind 2018 waren er 7 samenwerkingsverbanden aangesloten bij het DTC, eind 2019 17 en op dit moment staat de teller op 31. Het streefgetal van 30 is al in oktober gehaald. Hiermee is het netwerk voor bedrijven en ook het bereik van het LDS voor cyberweerbaarheid zoals beoogd flink uitgebreid en verstevigd. In vele branches en regio's hebben bedrijven elkaar en de samenwerking op het thema cybersecurity gevonden. De samenwerkings-

---

[2] Raadpleegbaar via www.tweedekamer.nl

[3] Organisatie met OKTT-aanwijzing: Organisatie die objectief kenbaar tot taak (OKTT) heeft andere organisaties of het publiek te informeren over dreigingen en incidenten voor zover deze gegevens betrekking hebben op en relevant zijn voor netwerk- en informatiesystemen van organisaties uit de doelgroep van de OKTT organisatie.

[4] Stand van zaken 30-11-2020

[5] Meetperiode 8-06-2018 tot 30-11-2020

[6] WODC onderzoek informatie uitwisseling binnen het LDS, december 2020

verbanden worden gekenmerkt door een breed spectrum aan activiteiten van bewustzijn vergroten, gezamenlijke trainingen en onderling delen van kennis tot monitoring van cyberdreigingen. De achterban en doelgroepen variëren van zzp'er tot niet-vitaal grootbedrijf.

4. Inrichting informatiedienst

Momenteel werkt het DTC aan het inrichten van een informatiedienst voor het delen van concrete dreigingsinformatie. Hierdoor wordt het mogelijk voor het DTC om specifieke kwetsbaarheids- en dreigingsinformatie te delen met niet-vitale Nederlandse bedrijven. Deze stap is een waardevolle aanvulling op het groeiende landschap van OKTT's en computercrisis-teams[7] en maakt het mogelijk om meer organisaties te voorzien van voor hen relevante informatie. Om zulke dreigingsinformatie, in het bijzonder persoonsgegevens, te kunnen verwerken en delen conform privacywet-geving, werkt mijn ministerie aan een juridische basis voor het DTC in de vorm van een wetsvoorstel. Doel is om begin 2021 te starten met deze informatiedienst. Naast de samenwerking met het NCSC zal de informatie-dienst ook aansluiting en afstemming zoeken met initiatieven in de markt voor informatieontsluiting. Een voorbeeld hiervan is het Anti Abuse Netwerk (AAN).

5. Ontwikkeling risicoklasse model

In samenwerking met het CCV (Centrum voor Criminaliteitspreventie en Veiligheid), het Verbond van Verzekeraars, Cyberveilig Nederland, VNO-NCW en MKB-Nederland, de politie, NLdigital, het CIO Platform Nederland en Partnering Trust is een model uitgewerkt dat het mogelijk maakt voor bedrijven om te achterhalen welke maatregelen ze dienen te treffen gelet op de risicoklasse waar zij toe behoren. Hierbij is een praktisch instrument ontwikkeld die door het DTC zal worden aange-boden. Het model dat gebaseerd is op de vijf basisprincipes van het DTC,[8] brengt meer uniformiteit en helderheid in de cybersecurity maatregelen die van bedrijven worden verwacht. Het model is in de praktijk getest en zal medio januari 2021 beschikbaar zijn.

Strategie 2021–2023: verdiepen, verbreden en verankeren

Voor de hoofdtaak *informatie en advies* is het strategisch doel het bereik van het DTC te vergroten. Tevens wil het DTC ook meer aanzet geven tot gedragsverandering en het aanreiken van een concreet handelingsper-spectief. Waar nodig zullen hiertoe nieuwe, interactieve instrumenten voor worden ontwikkeld.

In aanvulling op de meer generieke informatievoorziening zal met de nieuwe informatiedienst het aanbod voor niet vitale bedrijven stapsgewijs worden uitgebreid door het verstrekken van notificaties over concrete dreigingen en kwetsbaarheden en door het bieden van handelingsper-spectief. De verantwoordelijkheid voor het daadwerkelijk nemen van maatregelen blijft echter bij het niet vitale bedrijfsleven zelf. Bij de informatiedienst van het DTC zal nauw samengewerkt worden met het NCSC.

Voor de hoofdtaak *stimuleren van samenwerking*, is de inzet om in de komende drie jaar het netwerk van cyberweerbaarheidsverbanden te completeren én te bestendigen. De subsidieregeling zal hierop worden aangepast waarbij extra gestuurd zal worden op de effectiviteit van de

[7] Zoals bedoeld in artikel 3, tweede lid, Wbni.
[8] https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen

samenwerkingsverbanden en het beter benutten van elkaars kennis en ervaringen. Ook zal de samenwerking van het DTC met zakelijke partners voor mkb en zzp'ers, zoals verzekeraars, banken, accountants, IT-dienstverleners en brancheorganisaties worden geïntensiveerd. Het idee hierbij is om veilig digitaal ondernemen steeds meer de norm en integraal onderdeel te laten zijn van hedendaags ondernemerschap. Tevens draagt het DTC ook in de komende jaren bij aan de implementatie van het MKB-actieplan, de roadmap veilige hard- en software en het regionaal economisch beleid.

Ter ondersteuning van beide hoofdtaken zal het DTC werken aan verdere kennisopbouw. Enerzijds zal er sprake zijn van eigen data verzameling en analyse, bijvoorbeeld bij het gebruik van de basisscan, bij bezoeken aan de website en door bevraging van de samenwerkingsverbanden. Hiermee kan een goed beeld worden gekregen van de behoeftes bij het niet vitale bedrijfsleven. Anderzijds zal hier de samenwerking worden opgezocht met het CBS, TNO en andere kennisinstellingen die ook relevante (kwantitatieve) data en meer inzicht in gedrag kunnen genereren. Een voorbeeld hiervan is de verbreding van de ICT-bedrijven-enquête van het CBS met een vragenset voor zzp'ers, een groep ondernemers waar nog weinig over bekend is als het om cybersecurity gaat. Deze kennisopbouw is belangrijk om de hoofdtaken goed te kunnen richten en ook feedback te verkrijgen over de effectiviteit van de activiteiten van het DTC.

Bovengenoemde strategie zal worden vertaald naar de werkplannen voor de komende jaren met de noodzakelijke prioritering en fasering, gelet op de beschikbare capaciteit en middelen.

CSIRT-DSP

Ik maak met deze brief van de gelegenheid gebruik u ook te informeren over de voortgang van het CSIRT-DSP[9], dat sinds de oprichting op 1 januari 2019 het CSIRT is voor online marktplaatsen, online zoekmachines en cloud computerdiensten waar deze aanbieders meldingen kunnen doen van incidenten met aanzienlijke gevolgen voor diens dienstverlening[10]. Het CSIRT-DSP wordt geacht bij dergelijke incidenten ook bijstand te verlenen[11]. Het CSIRT-DSP heeft inmiddels organisatorisch vorm en inhoud gekregen en een aantal relevante diensten ontwikkeld. In 2020 heeft ze 42 zaken in behandeling gehad, ten opzichte van 6 in 2019[12]. Deze zaken betreffen bijvoorbeeld informatie over kwetsbare systemen waarna het verantwoordelijke contact is geïnformeerd zodat deze actie kon ondernemen. Deze informatie komt van partners van het CSIRT-DSP zoals het NCSC, onderzoekers, of andere CSIRT's uit de EU. Er zijn door het CSIRT-DSP nog geen (verplichte) meldingen ontvangen die voldoen aan de minimumeisen van de meldplicht. De (vrijwillige) meldingen die wel binnen kwamen gingen over incidenten rond DDoS-aanvallen, phishing of uitval van systemen. Het CSIRT-DSP is gestart met het wekelijks informeren van zijn doelgroep over kwetsbaarheden, dreigingen en relevante gebeurtenissen van die week. Er is in 2020 meer contact gezocht en gekregen met de doelgroep, brancheorganisaties en samenwerkingsverbanden. Om de groei in werkzaamheden te kunnen ondersteunen is er een incidentresponse platform in gebruik genomen. Verder blijft het CSIRT-DSP zich doorontwikkelen en zijn dienstverlening verbeteren. Dit zal gebeuren door op zoek te gaan naar meer bronnen met

[9] Computer Security Incident Response Team voor digital service providers
[10] Ingevolge art. 13, eerste lid, Wbni.
[11] Ingevolgde art. 4, vierde lid, Wbni.
[12] Stand van zaken 30-11-2020

voor digitale dienstverleners relevante dreigingsinformatie en via publiek-private samenwerkingsverbanden.

Tot slot

Het DTC ligt op koers. Ook de komende jaren blijft het Ministerie van Economische Zaken en Klimaat (EZK) investeren in het vergroten van de cyberweerbaarheid en daarmee ook het verdienvermogen van het bedrijfsleven. Belangrijke onderdelen hierbij zijn het inrichten en het uitbouwen van de informatiedienst, het doorontwikkelen van het Digital Trust Platform en de community en het uitbreiden en bestendigen van de samenwerkingsverbanden van bedrijven op het gebied van cyberweerbaarheid. Hiermee wordt ook actief bijgedragen aan de doelstellingen en de realisatie van het LDS voor cybersecurity.

Veilig digitaal ondernemen moet uiteindelijk het nieuwe normaal worden, integraal onderdeel zijn van de bedrijfsvoering van bedrijven én van economisch beleid en bijbehorend instrumentarium. Bij de realisatie van deze ambitie zal de samenwerking gezocht worden met vele partijen, zowel privaat als publiek. Want ook hier geldt, alleen samen maak je het verschil en heb je een kans om cyberweerbaar te worden. In het najaar van 2021 zal ik u wederom informeren over de voortgang zodat u zicht op de realisatie houdt.

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