Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1143

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 8 maart 2024

Zoals toegezegd in mijn Kamerbrief van 23 februari 2023,[1] informeer ik u hierbij over de voortgang van het Digital Trust Center (hierna: DTC) en het Computer Security Incident Response Team voor digitale diensten (hierna: CSIRT-DSP).

In deze brief wordt aan de hand van vier speerpunten ingegaan op de ambities van 2023 en de realisatie daarvan. In de voornoemde Kamerbrief zijn de vier speerpunten benoemd: van weten naar doen, de basis op orde, synergie in samenwerkingsverbanden en instrumenten, en tot slot het vergroten van bereik en impact. Alle activiteiten die het DTC ontplooit zijn opgehangen aan een of meerdere van deze speerpunten. Het DTC draagt ook bij aan de uitvoering van de Nederlandse Cybersecuritystrategie (NLCS)[2] en Pijler 5 van de Strategie Digitale Economie (SDE).[3]

Daarnaast zal deze brief stilstaan bij onder andere de moties van Kamerlid Rajkowski over een keurmerk voor het midden- en kleinbedrijf (hierna: mkb) en een structurele oefenagenda voor het niet-vitale bedrijfsleven,[4] het wetsvoorstel bevordering digitale weerbaarheid bedrijven (hierna: Wbdwb), de voortgang bij het CSIRT-DSP en de integratie van het DTC en het CSIRT-DSP met het Nationaal Cyber Security Centrum (hierna: NCSC).

Resultaten 2023

Het DTC heeft het afgelopen jaar weer meer ondernemers bereikt dan het jaar ervoor, door de inzet van een breed scala aan activiteiten, waaronder de inzet van tools, een aanvullende subsidieregeling en professionalisering van de dienstverlening. Een belangrijk onderdeel hiervan is het

[1] Kamerstuk 26 643, nr. 980.
[2] Kamerstuk 26 643, nr. 925.
[3] Kamerstuk 26 643, nr. 941.
[4] Kamerstuk 36 200 VII, nr. 60 en Kamerstuk 36 200 VII, nr. 61.

kst-26643-1143
ISSN 0921 - 7371
's-Gravenhage 2024

delen van informatie over specifieke cyberdreigingen en incidenten met bedrijven. De gestelde ambities van 2023 zijn behaald. Ook dit jaar zal het DTC deze activiteiten voortzetten en verder uitbreiden om bedrijven te ondersteunen in het verhogen van hun digitale weerbaarheid. Aan de hand van de vier speerpunten worden de ambities van 2023 en de realisatie daarvan uiteengezet.

Speerpunt 1: Van weten naar doen

Het DTC heeft veelvuldig ingezet op het onder de aandacht brengen van de basismaatregelen waarmee ondernemers hun cyberweerbaarheid kunnen vergroten. De basismaatregelen zijn een belangrijke eerste stap voor ondernemers om meer digitaal weerbaar te worden. Zoals aangegeven in de voortgangsbrief van 23 februari 2023[5] zet ik ook in op een gedragsverandering zodat ondernemers ook daadwerkelijk maatregelen treffen om digitaal weerbaar te worden.

Om meer inzicht te krijgen in de factoren die een ondernemer aanzet of weerhoudt om cybersecuritymaatregelen te nemen, heeft het DTC op 1 september 2023 TNO de opdracht gegeven om een onderzoek te starten naar gedrag. Vanwege de grootte van de doelgroep is besloten hier een onderverdeling in aan te brengen. Hierbij is een tweetal zaken onderzocht. Allereerst wat de behoeften zijn van bedrijven ten aanzien van producten en diensten vanuit het DTC. Ten tweede, op welke manier zij het beste benaderd en ondersteund kunnen worden. De resultaten worden verwacht in Q2 2024.

Voor kleine ondernemers die het nemen van cybermaatregelen uitstellen of niet nemen, bijvoorbeeld wegens financiële knelpunten, is de subsidieregeling *Mijn Cyberweerbare Zaak*[6] gerealiseerd met een totaalbudget van € 300.000. Deze regeling is een pilot. Van de aanschafwaarde en/of implementatiekosten werd maximaal 50% gedekt tot een maximum van € 1.250. De subsidieregeling was na drie weken overtekend en wordt geëvalueerd. In de evaluatie wordt onderzocht of de subsidieregeling in 2024 opnieuw beschikbaar kan worden gesteld. De resultaten worden eveneens in Q2 verwacht.

Voortgang informatiedienst

In de brief van 23 februari 2023[7] bent u geïnformeerd over het delen van specifieke dreigingsinformatie door de informatiedienst van het DTC. Het afgelopen jaar heeft er een significante groei plaatsgevonden van het aantal kwetsbaarheden waarop genotificeerd wordt. Het totaal aantal notificaties dat de informatiedienst sinds de start in juni 2021 verstuurde aan bedrijven (gevraagd en ongevraagd) is ruim 156.000. Dit komt vooral op het conto van de «ongevraagde» waarschuwingen over kwetsbaarheden bij het bedrijfsleven. Het DTC notificeerde over bijna 140.000 bedrijfsspecifieke cyberdreigingen in 2023.

Speerpunt 2: Basis op orde

Om ondernemers te ondersteunen in het nemen van basismaatregelen is aan het begin van 2023 de *Cyberveilig Check voor zzp en mkb* gelanceerd. De *Cyberveilig Check voor zzp en mkb* is gericht op ondernemers die nog niet veel kennis en ervaring hebben op het gebied van cybersecurity. Deze

[5] Kamerstuk 26 643, nr. 980.
[6] https://zoek.officielebekendmakingen.nl/stcrt-2023-26170.html; https://www.digitaltrustcenter.nl/toolkit-mijn-cyberweerbare-zaak.
[7] Kamerstuk 26 643, nr. 980.

laagdrempelige tool geeft ondernemers een concrete actielijst met basismaatregelen waarmee zij zélf direct aan de slag kunnen. De *Cyberveilig Check voor zzp en mkb* is in 2023 in totaal 6.842 keer ingevuld. Het DTC blijft ook in 2024 *De Cyberveilig Check voor zzp en mkb* onder de aandacht brengen zodat zo veel mogelijk ondernemers deze tools benutten.

Ondersteunende campagnes

Om de verschillende DTC-initiatieven kracht bij te zetten zijn er het afgelopen jaar verschillende doelgroepgerichte bewustwordingscampagnes gevoerd. De campagnes waren gericht op online fraude, ervaringsverhalen van gehackte bedrijven, starten met je cybersecurity en de nieuwe subsidieregeling *Mijn Cyberweerbare Zaak* voor kleine ondernemingen. De DTC-campagnes zijn erop gericht om ondernemers met laagdrempelige producten en tools te bereiken, bewust te maken en aan te zetten tot actie.

Informeren en adviseren over NIS2

De implementatiedeadline voor de nieuwe Europese richtlijn voor Netwerk- en Informatiebeveiliging (de NIS2-richtlijn)[8] is 17 oktober 2024. Uw Kamer is op 31 januari 2024 geïnformeerd over de stand van zaken van de implementatie.[9] Zoals gemeld wordt, gelet op de benodigde vervolgstappen in het wetgevingstraject, de deadline niet gehaald. Het streven is de wetsvoorstel in het najaar van dit jaar aan uw Kamer aan te bieden.

Meer organisaties zullen onder de reikwijdte van de NIS2 gaan vallen en er komt een zorgplicht tot het nemen van beveiligingsmaatregelen en een meldplicht van incidenten. Het DTC werkt samen met de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), het NCSC en de Rijksinspectie Digitale Infrastructuur (RDI) om bedrijven te informeren die met de NIS2 te maken krijgen. Zo is op 5 oktober 2023 het webinar «De impact van NIS2 op jouw organisatie» georganiseerd. In 2024 gaat het DTC door met het bieden van handvatten, informatie en advies aan de bedrijven.

Speerpunt 3: Synergie in samenwerkingsverbanden en instrumenten

In 2023 is de onderlinge samenwerking tussen samenwerkingsverbanden (regionaal en sectoraal) vergroot. Er is onder meer gewerkt aan de gezamenlijke ontwikkeling van informatieproducten die passen bij de behoefte van de doelgroep. Dit heeft als doel het creëren van kennisrijke netwerken waar ondernemers terecht kunnen. Het totale aantal samenwerkingsverbanden dat nu is aangesloten bij het DTC komt begin dit jaar uit op 60.[10] Daarnaast wordt onderling kennis uitgewisseld tussen ondernemers in de online DTC-community waarbij 3.540 leden zijn aangesloten.

In 2024 wordt extra ingezet op het vergroten van de synergie tussen de bestaande samenwerkingsverbanden. Zo heeft bijvoorbeeld de samenwerking van Agrifood met de MKB Cvber Campus geleid tot de Agro Cyberscan, die specifiek is ontwikkeld voor de agrarische sector. Momenteel wordt door het DTC in samenwerking met vier samenwerkingsverbanden (Samen Digitaal Veilig, de MKB Cyber Campus, CYRA en

[8] https://eur-lex.europa.eu/legal-content/nl/ALL/?uri=CELEX:32022L2555.
[9] Kamerstuk 22 112, nr. 3868.
[10] https://www.digitaltrustcenter.nl/overzicht-van-samenwerkingsverbanden.

The Cyber Partners) en het Ministerie van Infrastructuur en Waterstaat een Cybertools hulpkaart ontwikkeld. Hierop staan de verschillende tools die de DTC samenwerkingsverbanden aanbieden.

Het afgelopen jaar is de subsidieregeling *Cyberweerbaarheid* weer opengesteld om samenwerkingen tussen ondernemers op het gebied van cybersecurity te stimuleren. De onafhankelijke beoordelingscommissie heeft hierbij specifiek gelet op het versterken van bestaande initiatieven met nieuwe projecten en daarnaast is gekeken naar sectoren waar extra samenwerking wenselijk is. Er was in totaal € 800.000 beschikbaar met een maximum van € 200.000 per project. Van de 23 ingediende plannen zijn dit jaar zes[11] projecten gehonoreerd. Vanwege het feit dat er nog voldoende inbreng is van goede projecten zal de subsidieregeling ook in 2024 worden voortgezet. In 2024 zal een totaalbedrag van € 600.000 beschikbaar komen met een maximumbedrag van € 150.000 per project. Deze wijziging van de subsidieregeling biedt ruimte om samenwerkingsverbanden te blijven stimuleren en om nieuwe instrumenten te ontwikkelen zoals *Mijn Cyberweerbare Zaak*.

Naast de subsidieregelingen is in september 2023 een pilot gestart waarmee projecten die in de DTC samenwerkingsverbanden ontstaan worden ondersteund. Drie opdrachten hebben een bedrag ontvangen van € 20.000 om hun projectvoorstellen in het kader van «van weten naar doen: activeer de ondernemer» uit te voeren. Dit heeft onder meer geresulteerd in interactieve klikbare video's op verschillende basis cybersecurity onderwerpen. Vanwege de grote belangstelling vanuit de samenwerkingsverbanden wordt het budget van de pilot van opdrachtverstrekkingen in 2024 verder uitgebreid naar een budget van € 400.000.

Speerpunt 4: Bereik en impact vergroten: het DTC als katalysator

Het DTC zet in op het vergroten van het bereik en de impact van producten, diensten en tools die het DTC aanbiedt om zo steeds meer ondernemers te helpen cyberweerbaar te worden. Het streven voor 2023 was 300.000 bezoeken op de website. De website is in 2023 meer dan 330.000 keer bezocht. Deze doelstelling is daarmee ruimschoots behaald. Met 20.573 ingevulde zelfscans en tools is het gebruik ervan door bedrijven ten opzichte van het jaar ervoor verdubbeld. De in april 2023 gelanceerde *CyberVeilig Check voor zzp en mkb* had met 33% het grootste aandeel in het gebruik van de 11 interactieve tools. Op dit platform wordt niet alleen informatie gebracht, maar wordt ook input gehaald waar het DTC mee aan de slag kan. Denk aan het aanvullen van tips en adviezen en het verkrijgen van input op producten, diensten en kanalen van het DTC. Ook wordt er inzicht verkregen in het situationeel beeld vanuit de leden. Door middel van de antwoorden kan het DTC analyseren wat de impact was van deze ernstige kwetsbaarheid in het bedrijfsleven en in hoeverre de handelingsperspectieven hebben geholpen de impact ervan te beperken.

Het doel is om de website actueel te houden en aan te vullen met informatie en hulpmiddelen waar bedrijven behoefte aan hebben. Het eerdergenoemde onderzoek van TNO zal aanknopingspunten bieden hoe het DTC bedrijven nog beter kan ondersteunen.

[11] https://www.rvo.nl/subsidies-financiering/subsidieregeling-cyberweerbaarheid/publieke-samenvattingen-2023.

Uitvoering moties (mkb-keurmerk en cyberoefenen)

Op 18 september 2023[12] is de Kamer geïnformeerd over de voortgang van de motie Rajkowski inzake een eenduidig mkb-keurmerk om het mkb beter te ondersteunen bij hun cybersecuritybeleid en de motie Rajkowski over het ontwikkelen van een structurele cyberoefenagenda voor het niet-vitale bedrijfsleven in samenwerking met het DTC.[13]

Voor de motie over het mkb-keurmerk is ondersteuning gezocht bij het initiatief Kwaliteitspreventie van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV), een onafhankelijke instantie. De verwachting is dat de ontwikkeling van het keurmerk een doorlooptijd van 2 jaar zal hebben en eind 2025 gereed zal zijn. Het spreekt daarbij voor zich dat intensieve samenwerking met cybersecurityexperts, brancheorganisaties en overheidsinstanties zoals het DTC cruciaal is, om ervoor te zorgen dat het keurmerk nauwkeurig aansluit op de behoeften en uitdagingen van mkb organisaties.

In het kader van de motie over een structurele cyberoefenagenda is een informatiepagina online gezet met meer informatie over de verschillende soorten cyberoefeningen die bedrijven kunnen doen.[14] Naast informatie over wat cyberoefeningen zijn en waarom het van belang is om regelmatig te oefenen, worden er ook aanbevelingen gedaan aan ondernemers over hoe ze kunnen beginnen met oefenen. Ook is in de voortgangsbrief van het DTC op 23 februari 2023[15] toegezegd dat het DTC de mogelijkheid verkent om een eigen cyberoefening aan te bieden die partijen zelf – zonder begeleiding – kunnen uitvoeren. De verwachting is dat deze oefening, ondersteund door de tevens toegezegde campagne, in de eerste helft van dit jaar gelanceerd zal worden.

Voortgang wetsvoorstel bevordering digitale weerbaarheid bedrijven

Het wetsvoorstel bevordering digitale weerbaarheid bedrijven (hierna: Wbdwb) is op 9 december 2022 aan de Kamer aangeboden (Kamerstuk 36 270). Door de Kamer is op 20 januari 2023 verslag uitgebracht over dit wetsvoorstel. Hier heb ik op gereageerd door op 8 maart 2023 door u de nota naar aanleiding van het verslag aan te bieden.[16]

Het wetsvoorstel is een belangrijke voorwaarde om de doelstelling in het coalitieakkoord Rutte IV te realiseren om vanuit de overheid sneller en makkelijker informatie te delen met niet-vitale bedrijven over digitale kwetsbaarheden en «hacks». Daarnaast is de Wbdwb voorwaardelijk om vanuit de nieuwe nationale cybersecurityorganisatie, die ontstaat na de integratie van het DTC, het CSIRT-DSP en het NCSC, te borgen dat het niet-vitale bedrijfsleven voorzien blijft van algemene en specifieke informatie over cyberdreigingen en incidenten. Ik zie uit naar een spoedige behandeling van het wetsvoorstel door uw Kamer. De Kamerbehandeling is voorzien in de tweede week van maart 2024.

---

[12] Kamerbrief 26 643, nr. 1068.
[13] Het betreft de moties Rajkowski Kamerstuk 36 200 VII, nr. 60 en Kamerstuk 36 200 VII, nr. 61.
[14] https://www.digitaltrustcenter.nl/cyberoefenen.
[15] Kamerstuk 26 643, nr. 980.
[16] Kamerstuk 36 270, nr. 6.

CSIRT voor digitale diensten

Met deze brief wil ik u ook informeren over de voortgang van het CSIRT-DSP.[17] 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 weerbaarheid van systemen te verhogen. Deze digitale dienstverleners moeten incidenten met aanzienlijke gevolgen voor hun dienstverlening melden.

In 2023 heeft het CSIRT-DSP 81 incidenten behandeld. Deze zaken betreffen bijvoorbeeld incidentele informatie over kwetsbare, gecompromitteerde of onjuist geconfigureerde systemen, maar ook vrijwillige meldingen van incidenten door organisaties uit de doelgroep van het CSIRT-DSP. In 2023 heeft het CSIRT-DSP twee verplichte meldingen ontvangen. Informatie die het CSIRT-DSP heeft ontvangen wordt doorgezet naar de digitale dienstverleners om deze te waarschuwen over de (potentiële) dreiging en te voorzien van een handelingsperspectief. Door automatisch te notificeren heeft het CSIRT-DSP een groter aantal kwetsbaarheden in systemen genotificeerd dan de jaren ervoor. Afgelopen jaar waren dit er 417.561.

Voortgang integratie DTC, CSIRT voor digitale dienst en NCSC

In juni 2023 is uw Kamer geïnformeerd over de voortgang van de integratie van het DTC, het CSIRT-DSP en het NCSC.[18] Het afgelopen jaar heeft de integratie van het DTC met het NCSC steeds verder vorm gekregen. Belangrijke ontwikkelingen waren het aanstellen van een transitiemanager en het opstellen en verder vormgeven van de transitieopgave. Daarnaast wordt er onderling tussen het DTC en het NCSC al op verschillende manieren samengewerkt. Er wordt in teams, waarin alle disciplines van het DTC en het NCSC zijn vertegenwoordigd, langs vier werkstromen aan de transitie naar de vernieuwde cybersecurityorganisatie gewerkt. Tevens is de medezeggenschapsraad voor de vernieuwde nationale cybersecurityorganisatie ook op een gezamenlijke manier ingericht.

Daarnaast zijn het afgelopen jaar stappen gezet voor de integratie van het CSIRT-DSP en het NCSC. De securityspecialisten van het CSIRT-DSP zijn in 2023 voornamelijk werkzaam geweest op locatie bij het NCSC en hebben daar de samenwerking tussen beide partijen geïntensiveerd. Dit heeft bijvoorbeeld geleid tot een detachering van twee medewerkers van het CSIRT-DSP bij het NCSC om volledig als NCSC-medewerker mee te kunnen draaien gedurende de nationale cybercrisis oefening ISIDOOR IV die plaatsvond in november 2023. Deze detachering is succesvol verlopen en is een mooie proef voor de integratieplannen in 2024.

Voor zowel het DTC als het CSIRT-DSP geldt dat ook in het aankomende jaar de samenwerking met het NCSC steeds verder geïntensiveerd zal worden. Dit wordt beoogd middels de start van een cultuurtraject en het werken naar gezamenlijke producten. Uw Kamer wordt periodiek geïnformeerd over de voortgang van de transitie. Dit zal in de rapportage over de voortgang van de NLCS gebeuren.

---

[17] Sinds de oprichting op 1 januari 2019 het aangewezen CSIRT voor online marktplaatsen, online zoekmachines en cloud computerdiensten op basis van de Wet beveiliging netwerk- en informatiesystemen (Wbni).

[18] Kamerstuk 26 643, nr. 1058.

Tot slot

In 2023 zijn de nodige stappen door het DTC en het CSIRT-DSP gezet om bedrijven te ondersteunen in het verhogen van hun digitale weerbaarheid. In 2024 blijven de organisaties zich hiervoor inzetten. Het DTC blijft nauw samenwerken met bedrijven om te zorgen dat zij producten en diensten biedt waar bedrijven behoefte aan hebben en gebruik van maken. Ik ben voornemens om de Kamer begin volgend jaar weer te informeren over de voortgang van het DTC.

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