Stichting
Connect2Trust

In reactie op internetconsultatie:

Stichting Connect2Trust
Otter 22
5251 GR Vlijmen
KvK: 75171848

I www.connect2trust.nl
E info@connect2trust.nl

Datum / Tijd
22 augustus 2021

Ministerie van Economische Zaken & Klimaat
T.a.v. Mevrouw mr. drs. M.C.G. Keijzer
Bezuidenhoutseweg 73
2594 AC Den Haag

Betreft: Consultatie Conceptvoorstel Wet Bevordering Digitale Weerbaarheid Bedrijven

Excellentie,

Op 28 juni 2021 ontving de Stichting Connect2Trust bericht van het Digital Trust Center (DTC) informatie m.b.t. de gevraagde consultatie van het conceptvoorstel Wet Bevordering Digitale Weerbaarheid Bedrijven. De stichting heeft uw conceptvoorstel voorgelegd aan haar deelnemers en alle reacties in dit advies samengebracht.

Als eerste wil de Stichting Connect2Trust benadrukken dat zij, ten principale, positief staat tegenover ieder ministerie dat de digitale weerbaarheid van Nederland probeert te vergroten. De snelle groei van het DTC bevestigt de toegevoegde waarde van het geven van informatie en advies in combinatie met het stimuleren van samenwerkingsverbanden. Tegelijkertijd dient deze groei zorgvuldig te worden afgestemd met alle gerelateerde ontwikkelingen op Europees en nationaal niveau, in zowel de publieke als private sector.

De Stichting Connect2Trust is van mening dat uw conceptvoorstel afbreuk doet aan de structuur en transparantie die de Wbni door middel van schakelorganisaties zoals sectorale computercrisisteams en OKTT's probeert aan te brengen in de opbouw van het Landelijk Dekkend Stelsel (LDS). Uw kamerbrief van 02 juni 2021 inzake de voortgang van het Digital Trust Center[1] geeft aan dat "er wordt gewerkt aan de voorwaarden om een aanwijzing als OKTT mogelijk te maken" als onderdeel van het LDS. Op dit moment maken 10 organisaties onderdeel uit van het LDS: IBD, Z-CERT, WM-CERT en SURF-CERT als sectoraal computercrisisteam, en de Vereniging Abuse Information Exchange, Stichting Nationale Beheersorganisatie Internetproviders (NBIP), Stichting Cyber Weerbaarheidscentrum Brainport (CWB), Cyberveilig Nederland, FERM en de Stichting Connect2Trust als OKTT[2]. Uw conceptvoorstel bevat geen enkele afbakening hoe de taken van de informatiedienst van het Digital Trust Center zich verhoudt met het delen van dreigings- en incidentinformatie door de bestaande schakelorganisaties in het LDS. De zinsnede "Deze informatie wordt kosteloos aangeboden" in de Memorie van Toelichting lijkt zelfs een concurrerende positie te suggereren die, indien correct, mogelijk strijdig is met de Wet Markt & Overheid

Het ontbreken van een dergelijke afbakening vergroot niet alleen het risico dat organisaties in Nederland meerdere keren dezelfde dreigings- en incidentinformatie ontvangen, het doet ook afbreuk aan de rollen en taken van de andere departementen in zowel de uitvoerende en toezichthoudende taken. Vitale bedrijven, sectorale computercrisisteams en OKTT's kijken naar de gehele ketenweerbaarheid voor de continuïteitsborging. Door ongevraagd en zonder enige inkadering niet-vitale bedrijven te verzoeken tot

[1] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2021/06/02/kamerbrief-voortgang-digital-trust-center/voortgang-digital-trust-center.pdf
[2] https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds

het aanleveren van informatie t.b.v. het delen van dreigings- en incidentinformatie bemoeilijkt het conceptvoorstel de mogelijkheid om de informatiedeling in te richten aan de hand van ketens indien deze, zoals veelal gebruikelijk, de grens van vitaal- en niet-vitaal overschrijden. Diezelfde ketenweerbaarheid staat ook centraal in de nieuwe Europese NIS2 Directive die, in aanvulling op digitale dienstverleners, nog aanvullende sectoren in scope betrekt ter voorkoming van digitale ontwrichting. Ook deze inkadering ontbreekt in uw conceptvoorstel waardoor het niet als toekomst-vast wordt beschouwd. Het eerste advies van de Stichting Connect2Trust is daarom om, in overleg met de andere ministeries in het algemeen en het Ministerie van Justitie & Veiligheid in het bijzonder, tot een inkadering te komen van de doelgroepen binnen het LDS waarop deze wet betrekking heeft op basis van transparante en gedragen criteria.

De Memorie van Toelichting stelt dat het Digital Trust Center, naast de samenwerking binnen de overheid en met formele partners zoals benoemd in de Wbni, ook samenwerkingen kan aangaan met organisaties buiten de rijksoverheid zoals maatschappelijke organisaties, onderzoeksinstituten, onderwijsinstellingen, cybersecurity bedrijven, decentrale overheden en onafhankelijke cyber security onderzoekers, t.b.v. het verkrijgen en delen van relevante informatie over digitale dreigingen, kwetsbaarheden en incidenten. Ook hier ontbreekt wederom de inkadering van taken hoe deze samenwerkingen zich verhouden tot de bestaande taken van bijvoorbeeld het Nationaal Cyber Security Centrum (NCSC). Uw conceptvoorstel introduceert hiermee een multi-loket gedachte waarin samenwerkende organisaties op meerdere plaatsen binnen de Rijksoverheid dezelfde bevindingen moeten melden. In het Anti-Abuse Netwerk wordt gezamenlijk door zowel het DTC, NCSC en onderzoekers gezocht naar oplossingen om dergelijke situaties te voorkomen of mogelijke blokkades te adresseren. Het tweede advies van de Stichting Connect2Trust is dan ook, om 1-loket voor alle meldingen te borgen in de Wbni, zodat in doorgifte aan alle OKTT's waaronder het Digital Trust Center, kan worden voorzien.

De Memorie van Toelichting stelt verder dat er geen verplichting bestaat voor bedrijven in Nederland om gebruik te maken van de informatie van het ministerie van EZK, of een bevoegdheid tot vordering van gegevens die benodigd zijn t.b.v. het verstrekken van dreigings- en incidentinformatie. In artikel 3 van het conceptvoorstel ontbreekt deze vrijblijvendheid m.b.t. het verstrekken van gegevens volledig en geeft daardoor een onjuist beeld van het wettelijk mandaat dat voortvloeit uit deze wet. Het derde en laatste advies van de Stichting Connect2Trust is dan ook om deze vrijblijvendheid en vrijwilligheid expliciet in de wet op te nemen. Een specifieke vraag hierbij is of het Ministerie van Economische Zaken & Klimaat kan bevestigen dat de genomen maatregelen ter beveiliging van de ontvangen informatie op minimaal hetzelfde niveau is als van het NCSC. Dit betreft zowel juridische maatregelen als uitvoerende maatregelen m.b.t. het gebruik van (gedeelde) hardware, software en infrastructuur binnen uw ministerie.

Samengevat adviseert de Stichting Connect2Trust om (1) in overleg met de andere ministeries in het algemeen en het Ministerie van Justitie & Veiligheid in het bijzonder, tot een inkadering te komen van de doelgroepen binnen het LDS waarop deze wet betrekking heeft op basis van transparante en gedragen criteria, (2) de 1-loket voor alle meldingen te borgen in de Wbni, zodat in doorgifte aan alle OKTT's kan worden voorzien, (3) om deze vrijblijvendheid en vrijwilligheid expliciet in de wet op te nemen m.b.t. het voldoen aan verzoeken m.b.t. het aanleveren van gegevens.

Namens de deelnemers van de Stichting Connect2Trust,
Het bestuur van Connect2Trust