Stichting
Connect2Trust

In reactie op internetconsultatie:

Stichting Connect2Trust
KvK: 75171848

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

Minister van Justitie & Veiligheid
Turfmarkt 147
2511 DP Den Haag

Datum
28 maart 2025

Betreft: Consultatie Concepttekst CyberBeveiligingsBesluit

Excellentie,

Op 20 februari 2025 ontving de Stichting Connect2Trust van de Directeur Wetgeving en Juridische Zaken voor consultatie het CyberBeveiligingsBesluit (hierna: CBB) waarin de regels uit de CyberBeveiligingsWet (hierna: CBW) worden uitgewerkt voor bijvoorbeeld zorgplicht en opleidingen. Met de CBW en daarmee verbonden CBB geeft Nederland invulling aan de regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (PbEU 2022, L 333). De Stichting Connect2Trust heeft de conceptteksten van het CBB, de daarbij behorende Nota van Toelichting en de Ministeriële Regelingen aan de organisaties die bij haar zijn aangesloten, voorgelegd en alle reacties van die organisaties in dit advies samengebracht. Bij deze reacties is ook de laatste versie van de CBW en de daarbij behorende Memorie van Toelichting, meegenomen waarover de Raad van State op 24 februari 2025 haar advies heeft gepubliceerd.

Op 23 mei 2024 heeft de Minister van Justitie & Veiligheid de 'Toekomstvisie uitgebracht voor het verbeteren van publiek-private samenwerking bij het verhogen van de cyberweerbaarheid van organisaties'[1] (hierna: Toekomstvisie) welke op 23 mei 2024 is uitgebracht. Deze Toekomstvisie maakt onderdeel uit van de Nederlandse Cybersecurity Strategie 2022-2028 waarin wordt gesteld dat, in samenwerking met private partners, een bouwplan wordt opgesteld dat het kabinet in staat stelt om samen met het bedrijfsleven zoveel mogelijk organisaties binnen het Koninkrijk digitaal weerbaarder te maken. De Stichting Connect2Trust heeft aan zowel de totstandkoming van de toekomstvisie, als de lopende uitwerking van het bouwplan, een aanzienlijke bijdrage geleverd. In tegenstelling tot eerdere versies van de CBW, is in de laatste versie van de CBW, noch in de daarbij behorende Memorie van Toelichting of het daaruit voortvloeiende CBB of Nota van Toelichting, een verwijzing naar de Toekomstvisie te vinden. De Stichting Connect2Trust sluit zich daarom nadrukkelijk aan bij het (derde) advies van de Raad van State dat op 24 februari 2025 is gepubliceerd en zich richt op het Ministerie van Justitie en Veiligheid als uitvoeringscoördinator:

- *RvS Advies #3: Een nadere toelichting op de wijze waarop invulling wordt gegeven aan de coördinerende taak en de (mede)betrokkenheid van de minister van Justitie en Veiligheid*

Het CBB biedt, naar mening van Connect2Trust, onvoldoende duidelijkheid over de verdeling van verantwoordelijkheden bij de uitvoering van de vijf kernfuncties in de Toekomstvisie[2]. Dit betreft onder andere:

- De rol van vrijwillige CSIRT's conform de kamerbrief betreffende het herinrichten van het stelsel met een nationale en sectorale CSIRT's in Nederland[3] welke op 19 april 2023 is uitgebracht;

[1] https://www.rijksoverheid.nl/documenten/rapporten/2024/05/23/tk-bijlage-rapport-toekomstvisie-cyberweerbaarheidsnetwerk
[2] De vijf kernfuncties vastgesteld in de Toekomstvisie zijn: "Informatiedeling", "Doelwit- en slachtoffernotificatie", "Incidentafhandeling", "Kennisuitwisseling" en "Opleiden, Trainen en Oefenen"
[3] https://www.rijksoverheid.nl/documenten/rapporten/2023/04/19/csirt-stelsel-een-beleidskader-voor-het-herinrichten-van-het-stelsel-met-een-nationale-en-sectorale-csirts-in-nederland

- De rol van de partijen betrokken bij de publiek-private samenwerking in het CyberWeerbaarheidsNetwerk dat het resultaat is van de hiervoor genoemde Toekomstvisie welke op 23 mei 2024 is uitgebracht;

De invulling van de coördinerende taak betreft ook de wijze waarop de Minister van Justitie en Veiligheid om zal gaan met de uitvoering van meerdere wetten in opdracht van twee verschillende ministers. Enerzijds is dit de CBW en CER in opdracht van de Minister van Justitie en Veiligheid, anderzijds is dit de Wet Bevordering Digitale Weerbaarheid Bedrijven. Deze bundeling van taken wordt veroorzaakt door het opgaan van het Digital Trust Center in het Nationaal Cyber Security Centrum (NCSC) per 1 januari 2026. Ook deze bundeling roept bij de Stichting Connect2Trust vragen op die onbeantwoord blijven in de CBW en het CBB:

- Op welke wijze gaat de Minister van Justitie en Veiligheid de coördinatie inrichten tussen beide opdrachtgevers?
- Op basis van welk afwegingskader wordt de prioriteit voor ieder van de kernfuncties bepaald bij uitvoering van beide wetten vanaf 1 januari 2026 door het NCSC?
- Welke rol speelt het CWN, voortkomend uit de Toekomstvisie, in relatie tot de uitvoering van deze beide wetten door het NCSC vanaf 1 januari 2026?

Het voorgaande raakt ook een ander advies van de Raad van State, dat als vierde duidelijke taakafbakening adviseert tussen vakministers en zelfstandige bestuursorganen om problemen door overlapping van bevoegdheden te vermijden. Als grootste cross-sectorale non-profit organisatie binnen het huidige Landelijk Dekkend Stelsel, is de stichting Connect2Trust van mening dat er niet alleen taakafbakening benodigd is tussen vakministers en zelfstandige bestuursorganen, maar ook tussen de diverse vakministers. Dit is met name relevant voor organisaties die:

A. In meerdere sectoren actief zijn die onder de CBW vallen;
B. Zowel in sectoren actief zijn die onder de CBW vallen, als in andere sectoren;
C. Organisaties die zowel zijn aangewezen als onderdeel van de vitale infrastructuur en tevens als essentieel of belangrijk gekenmerkt zouden kunnen worden.

In het rapport betreffende het herinrichten van het stelsel met een nationale en sectorale CSIRT's in Nederland welke op 19 april 2023 is uitgebracht werden tussen de 10.600 en 11.600 organisaties verwacht op wie de NIS2 van toepassing zou zijn[4]. In haar reactie heeft de stichting Connect2Trust toen gevraagd om aan te geven hoeveel van deze organisaties in meerdere sectoren actief zijn waardoor de getallen mogelijk een vertekend beeld geven. In de Nota van Toelichting is dit aantal teruggebracht naar 8.100 organisaties maar ontbreekt iedere verwijzing naar een sector of iedere andere onderbouwing van dit getal ontbreekt ondanks dat het om een aanzienlijke reductie van 24% tot 30% gaat. Connect2Trust wil graag een antwoord op de volgende vragen:

I. Welke diensten van het NCSC m.b.t. de uitvoering van de NIS2-taken worden dienovereenkomstig ook met 24% tot 30% gereduceerd conform de bijgestelde getallen?
II. Hoe zijn de getallen verdeeld over de verschillende sectoren waarop de NIS2 van toepassing is en hoeveel van deze aantallen zijn in meerdere NIS2 sectoren actief en zo ja, welke?

Ook van het gehanteerde aantal personen, kosten per persoon en uurtarief ontbreekt iedere grondslag. Vanwege het ontbreken van iedere toelichting op het genoemde aantal van 8.100 organisaties, kan het ook zijn dat organisaties per sector extra kosten moeten maken omdat (bijvoorbeeld) vakministers besluiten tot aanvullende eisen rondom de vereiste maatregelen als onderdeel van de zorgplicht. De stichting Connect2Trust is van mening dat, vanwege deze mogelijkheid van aanvullende vereisten per vakminister, er bij de genoemde getallen ook nadrukkelijk moet worden aangegeven dat dit een ondergrens betreft op basis van schattingen en aannames. Dit geldt onverminderd ook voor het aantal benodigde personen en uren aangezien er niet wordt aangegeven

[4] *Economische Zaken (3.000) Binnenlandse Zaken en Koninkrijksrelaties (500), Infrastructuur en Waterstaat (4.500), Volksgezondheid, Welzijn en Sport (1.500 – 2.000) en Landbouw, Natuur en Voedselkwaliteit (1.000 – 1.500).*

waarom dit de resultante zou zijn van een gap assessment en de daaruit voortvloeiende “aanpassing van bestaande en het invoeren van nieuwe werkprocessen” zoals omschreven in de Nota van Toelichting.

Ook stelt Connect2Trust dat de gestelde verwachting omtrent een eenmalige tijdsbesteding voor registratie in de Nota van Toelichting onjuist is. Immers, artikel 28 lid 3 vraagt ook om het aanleveren van domeinnamen die aan snelle veranderingen onderhevig kunnen zijn. Het onderhouden van de geregistreerde gegevens is daarom een structurele taak geworden en dient derhalve ook zo te worden opgenomen in tabel 2. Met betrekking tot het verstrekken van diezelfde domeinnamen genoemd in artikel 28 lid 3 van het CBB, wil Connect2Trust ook graag een verduidelijking omtrent de interpretatie van de tekst. Het gaat dan met name om een definitie wat wordt beschouwd als een essentiële of belangrijke “haar” domeinennamen in het licht van recent wetenschappelijk onderzoek dat constateert dat de WHOIS-database als betrouwbare bron voor validatie van het eigendom van een domeinnaam, afneemt. De stichting Connect2Trust verzoekt daarom om een nadere toelichting wanneer een domein als eigendom moeten worden beschouwd en daarmee mogelijk als een aan te leveren gegeven, zoals bedoeld in artikel 28 lid 3 van het CBB.

Als laatste punt van aandacht met betrekking tot de regeldruk wijst Connect2Trust op een afwijking in de gehanteerde tarieven in tabel 1 en 2 (€ 54 en € 77) wat beneden het tarief van € 80 ligt dat bijvoorbeeld door het Digital Trust Center wordt gehanteerd bij haar subsidieregeling cyberweerbaarheid en dat al ruim beneden het marktgemiddelde voor cybersecurity experts ligt. Bij toepassing van dit tarief stijgen de incidentele kosten met 34,1% per bedrijf en de structurele kosten met 3% waarbij het opvalt dat er geen enkele kosten voor inrichting en uitvoering van de meldplicht zijn vermeld. De Stichting Connect2Trust stelt dat zonder deze toelichting en nadere onderbouwing, de genoemde aantallen een onjuiste representatie zijn van de te verwachten kosten.

Ter besluit van onze reactie komt de stichting Connect2Trust nog een laatste maal terug op het eerdergenoemde Toekomstvisie. Deze toekomstvisie voorziet ook “opleiden, trainen en oefenen” als kernfunctie voor het CyberWeerbaarheidsNetwerk. Toch ontbreekt ook in artikel 22 iedere relatie met de toekomstvisie of het CyberWeerbaarheidsNetwerk. Connect2Trust zou daarom graag zien dat de trainer ook de kennis en inzichten kan overbrengen en toepassen die binnen het CyberWeerbaarheidsNetwerk worden gedeeld. Deze verbintenis zou als extra vereiste kunnen worden toegevoegd aan artikel 22 lid 2 van het CBB. Ook vragen enkele aangesloten organisaties zich af waarom de vereisten in artikel 22 lid 1 van “onafhankelijkheid” en “gekwalificeerd” zich in de Nota van Toelichting (onder tabel 1) worden vertaald als “uit te voeren door een externe partij” terwijl dit bij de artikelsgewijze toelichting niet staat vermeld. Connect2Trust verzoekt dan ook om meer consistentie in deze teksten.

De Stichting Connect2Trust onderschrijft de adviezen zoals gegeven door de Raad van State en de zorgen zoals verwoord door het MKB-panel. Met dit advies hebben wij getracht, op constructieve wijze, het ontbreken van het CyberWeerbaarheidsNetwerk evenals grondslagen en definitief, onder de aandacht te brengen en vertrouwen op een goede verwerking hiervan in de eerstvolgende versies van het CWB en CBB.

Namens de aangesloten organisaties bij de Stichting Connect2Trust,

Het bestuur van de Stichting Connect2Trust