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
29 juni 2024

Betreft: Consultatie Conceptvoorstel Cyberbeveiligingswet

Excellentie,

Op 21 mei 2024 ontving de Stichting Connect2Trust van de Directeur Wetgeving en Juridische Zaken voor consultatie 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) (Cyberbeveiligingswet, hierna CBW). De stichting heeft uw conceptvoorstel voorgelegd aan haar deelnemers en alle reacties in dit advies samengebracht.

De stichting heeft deze consultatie bezien in samenhang met twee beleidsstukken welke eerder door uw ministerie aan de Tweede Kamer zijn toegezonden. Dit betreft toekomstvisie voor het verbeteren van publiek-private samenwerking bij het verhogen van de cyberweerbaarheid van organisaties[1] welke op 23 mei 2024 is uitgebracht, en het beleidskader voor het herinrichten van het stelsel met een nationale en sectorale CSIRT's in Nederland[2] welke op 19 april 2023 is uitgebracht als bijlage bij de kamerbrief over de integratie van het DTC, CSIRT DSP en NCSC. Gezamenlijk geven deze documenten inzicht in de wijze waarop Nederland invulling zal geven aan de Europese Richtlijn (EU) 2022/2555 (hierna te noemen: NIS2) en de rol die de Stichting Connect2Trust hierin zal gaan vervullen.

De Stichting Connect2Trust staat ten principale positief tegenover uw voorstel en de wijze waarop met ons is samengewerkt bij de totstandkoming van onderdelen daarvan rondom de verbetering van het uitwisselen van dreigings- en incidentinformatie door middel van een verbeterde publiek-private samenwerking. Op het uitwisselen van dreigings- en incidentinformatie zijn in Nederland twee wetten van kracht: de Wet beveiliging netwerk- en informatiesystemen (WBNI)[3] geldend van 01-12-2022 t/m heden, en de Wet bevordering digitale weerbaarheid bedrijven (WBDWB)[4]. De laatste is op 19 maart 2024 aangenomen door de Tweede Kamer waarna de Eerste Kamercommissie wacht op het uitbrengen van de nota n.a.v. het tweede verslag waardoor deze ontbreekt in de verwijzing in de slotbepalingen (hoofdstuk 17) van de CBW.

De CBW richt zich primair op de sectoren zoals beschreven in de NIS2 en de organisaties die daarin binnen de gestelde criteria vallen en de rol van de overheid daarin en vervangt daarmee de WBNI. De CBW bevat echter ook taken voor het centrale contactpunt die in Nederland worden uitgevoerd door het NCSC waartoe ook het DTC en CSIRT DSP (zullen) behoren. De Stichting Connect2Trust is dan ook van mening dat hiermee ook de noodzaak voor de WBDWB komt te vervallen of deze ter minste dient te worden herschreven op basis van de

[1] *https://www.rijksoverheid.nl/documenten/rapporten/2024/05/23/tk-bijlage-rapport-toekomstvisie-cyberweerbaarheidsnetwerk*
[2] *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*
[3] *https://wetten.overheid.nl/BWBR0041515/2022-12-01*
[4] *https://www.eerstekamer.nl/wetsvoorstel/36270_wet_bevordering_digitale?&df2=ka*

definitieve CBW en het huidige goedkeuringsproces door de Eerste Kamercommissie per onmiddellijke ingang dient te worden beëindigd.

In de CBW wordt in 16 artikelen (te weten artikel 3[5], 17[6], 18[7], 23[8], 24[9], 26[10], 33[11], 37[12], 45[13], 52[14], 64a[15], 68[16], 69[17], 79[18], 80[19] en 89[20]) verwezen naar (mogelijke) nadere (invulling van) regelgeving door middel van een "Maatregel van Bestuur" door de bevoegde autoriteit zoals aangewezen in artikel 16 van de CBW. Hierdoor ontstaat de mogelijkheid dat verschillende kerndepartementen hier op verschillende wijze invulling aan geven. Een voorbeeld hiervan is Artikel 18 lid 2 van de NIS2 dat nadere invulling geeft aan de zorgplicht zoals omschreven in het lid 1 van de NIS1 welke is overgenomen als in CBW Artikel 23 lid 1. Lid 4 van de CBW vervangt het tweede lid van de NIS2 echter door een Maatregelen van Bestuur "waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren en type entiteiten" waarbij het Europees recht voorschrijft dat deze tenminste de maatregelen van de NIS2 lid 2 dienen te bevatten. De Stichting Connect2Trust is bezorgd over de onduidelijkheid omtrent de aanvullende tijd die ieder kerndepartement krijgt voor de uitwerking daaraan en daarmee verbonden het effectieve moment van inwerkingtreding van de wet binnen een sector. De Stichting Connect2Trust adviseert daarom om te streven naar een zo groot mogelijke harmonisatie in de CBW tussen sectoren, subsectoren en type entiteiten, door (zoals in genoemd voorbeeld), de maatregelen van NIS2 lid 2 als minimale beveiligingsmaatregelen toe te voegen aan CBW artikel 23 lid 4, met een mogelijkheid voor aanvullende maatregelen d.m.v. een Maatregel van Bestuur.

Veel organisaties in Nederland vallen onder één of meerdere van de sectoren zoals omschreven in artikel 16. Dit betekent dat zij te maken hebben met meerdere bevoegde autoriteiten die zich richten op dezelfde bedrijfsvoering(processen) binnen één entiteit. De CBW heeft echter geen artikel (of lid) dat beschrijft hoe entiteiten hiermee moeten omgaan in het geval van bijvoorbeeld de verschillende, of conflicterende, invulling van maatregelen zoals hiervoor beschreven, maar ook bij nakoming van de meldplicht en toezicht. De Stichting Connect2Trust adviseert daarom een artikel (of lid) toe te voegen aan de CBW met daarin een procedure waarmee bij meerdere bevoegde autoriteiten, er één leidende bevoegde autoriteit kan worden vastgesteld door een entiteit.

De CBW introduceert in Artikel 77 een bestuurlijke boete in het geval van een overtreding. Dit onderschrijft de noodzaak van de hiervoor beschreven procedure m.b.t. één leidende bevoegde autoriteit, maar ook voor alle organisaties de noodzaak tot scherpe en eenduidige definities. Deze ontbreken echter in Artikel 27 lid 2 van de CBW als het gaat om de definitie van "significant" welke in de NIS2 (artikel 6) is gedefinieerd als "een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerk- en informatiesystemen van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van aanzienlijke materiële of immateriële schade", maar in CBW Artikel 27 lid 2 wordt vervangen door (a) een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of (b) andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken." Zonder enige definitie (of drempelwaarde) wat

[5] *Artikel 3 (uitvoering uitvoeringshandelingen, gedelegeerde handelingen en richtsnoeren)*
[6] *Artikel 17 (aanwijzing en taken CSIRT)*
[7] *Artikel 18 (aanwijzing en taken coördinator bekendmaking kwetsbaarheden)*
[8] *Artikel 23 (zorgplicht)*
[9] *Artikel 24 (sectorspecifieke rechtshandelingen)*
[10] *Artikel 26 (governance)*
[11] *Artikel 33 (sectorspecifieke rechtshandelingen)*
[12] *Artikel 37 (nadere regels over meldingen van significante incidenten)*
[13] *Artikel 45 (informatieverstrekking ten behoeve van nationale register)*
[14] *Artikel 52 (samenwerking en informatie-uitwisseling tussen instanties)*
[15] *Artikel 64a (bijzondere persoonsgegevens)*
[16] *Artikel 68 (controlefunctionaris)*
[17] *Artikel 69 (beveiligingsscan)*
[18] *Artikel 79 (beveiligingsscan)*
[19] *Artikel 80 (gerichte beveiligingsaudit)*
[20] *Artikel 89 (wijziging Telecommunicatiewet)*

wordt bedoeld met “ernstig”, “operationele verstoring”, “veroorzaken” of “aanzienlijke materiële of immateriële schade”. De Stichting Connect2Trust adviseert om te streven naar zoveel mogelijk harmonisatie bij het vaststellen van deze definities, maar met behoud van de mogelijkheid voor sectorspecifieke invulling door verschillende bevoegde autoriteiten waar nodig.

Artikel 26 lid 2 spreekt over de benodigde kennis en vaardigheden voor de leden van de Raad van Bestuur omtrent de beveiliging van netwerk- en informatiesystemen. De NIS2 geeft hieromtrent in artikel 6 de volgende definitie van netwerk- en informatiesystemen:

a) een elektronische communicatienetwerk in de zin van artikel 2, punt1), van Richtlijn (EU)2018/1972;
b) elk apparaat of elke groep van onderling verbonden of verwante apparaten, waarvan er een of meer, op grond van een programma, een automatische verwerking van digitale gegevens uitvoeren, of
c) digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in punten a) en b) bedoelde elementen met het oog op de werking, het gebruik, de bescherming en het onderhoud ervan;

Lid a van NIS2 artikel 6 verwijst vervolgens naar de volgende definitie van elektronische communicatienetwerk in Richtlijn (EU)2018/1972: *de transmissiesystemen, al dan niet gebaseerd op een permanente infrastructuur of gecentraliseerde beheercapaciteit, en in voorkomend geval de schakel- of routeringsapparatuur en andere middelen, waaronder netwerkelementen die niet actief zijn, die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen waaronder satellietnetwerken, vaste (circuit- en pakketgeschakelde, met inbegrip van internet) en mobiele netwerken, elektriciteitsnetten voor zover deze voor overdracht van signalen worden gebruikt, netwerken voor radio- en televisieomroep en kabeltelevisienetwerken, ongeacht de aard van de overgebrachte informatie*.
Omwille van de duidelijkheid van de benodigde kennis en vaardigheden adviseert de Stichting Connect2Trust om een verduidelijking op te nemen in de Memorie van Toelichting wat precies met deze beide definities (“netwerk- en informatiesystemen” en “elektronische communicatienetwerk“) wordt bedoeld. De toevoeging van de zinsnede “*of gecentraliseerde beheercapaciteit”* suggereert bijvoorbeeld dat ook de netwerk en informatiesystemen bij leveranciers van publieke clouddiensten in scope zijn van een entiteit vallende onder de NIS2. De CBW stelt echter niet of een essentiële of belangrijke entiteit ook verantwoordelijk is voor de naleving van de voorgeschreven maatregelen in paragraaf 5.3.4. (a t/m j) bij deze leveranciers. De Stichting Connect2Trust adviseert daarom om de verantwoordelijkheid binnen deze voorgeschreven scope expliciet te omschrijven. Dit geldt vanzelfsprekend niet alleen voor kennis en vaardigheden, maar betreft ook alle andere verplichtingen zoals zijn uitgewerkt in de NIS2 en/of CBW.

Specifiek van toepassing op het gewenste niveau van kennis- en vaardigheden van de bestuurders is de vraag van de Stichting Connect2Trust waarom artikel 26 van toepassing is op *alle* bestuurders. Ten eerste is dit mogelijk incongruent met de wijze waarop een bestuur de taken wil verdelen. Zo is bijvoorbeeld een CFO verantwoordelijk voor de financiële bedrijfsvoering, en wordt daaromtrent van de andere bestuurders niet hetzelfde kennisniveau gevraagd. Ten tweede ontbreekt in de formulering van CBW artikel 26 lid 2 een normering aan welk niveau van kennis- en vaardigheden precies moet worden voldoen en, in het verlengde daarvan in CBW artikel 26 lid 5, aan welke eisen het verkregen certificaat moet voldoen. De Stichting Connect2Trust adviseert daarom dit artikel te nuanceren om een taakverdeling binnen het bestuur mogelijk te maken waarmee tegelijk ook voorkomen wordt dat meerdere bestuurders zich met zelfde risico’s bezig gaan houden en een (hoofd)eigenaar ontbreekt. Ook adviseert de Stichting Connect2Trust om de vaststelling van het gewenste niveau van kennis- en vaardigheden, in samenwerking met de bevoegde autoriteiten, op te nemen in de verdere uitwerking van de toekomstvisie voor het verbeteren van publiek-private samenwerking bij het verhogen van de cyberweerbaarheid van organisaties.

Artikel 9, 10, 11, 13 en 14 spreken allen over het aanwijzen van een essentiële of belangrijke entiteit bij regeling of besluit van de bevoegde autoriteit. Het gebruik van het woord “aanwijzen” in combinatie met de woorden “regeling” en “besluit” maakt niet duidelijk of een entiteit van één (of meerdere) bevoegde autoriteit(en) een aanwijzingsbesluit (per brief) kan verwachten, of bijvoorbeeld een zelfevaluatie zoals aangeboden wordt door

RDI [21] kan worden beschouwd als regeling waarmee een aanwijzingsbesluit (per brief) niet zal worden verzonden. De Stichting Connect2Trust verzoekt daarom een nadere toelichting op de nemen in de CBW met de geharmoniseerde wijze waarop deze aanwijzingen zullen geschieden.

De Memorie van Toelichting spreekt in paragraaf 5.6.5 over organisaties die op grond van de WBNI zijn aangewezen als OKTT. Dit betreffen, naast de Stichting Connect2Trust, de Vereniging Abuse Information Exchange, Stichting Nationale Beheersorganisatie Internetproviders (NBIP), Stichting Cyber Weerbaarheidscentrum Brainport (CWB), Cyberveilig Nederland, FERM en de NL CISO Circle of Trust. “Met het intrekken van de WBNI komen die aanwijzingen te vervallen. Deze voormalige Organisaties die fungeren als schakelorganisatie voor een achterban van aanbieders (hierna: schakelorganisaties) kunnen onder het regime van de CBW onder omstandigheden worden gekwalificeerd als een relevante partij als bedoeld in artikel 17, tweede lid, onderdeel b van de CBW[22]. Dit maakt het voor schakelorganisaties mogelijk om samenwerkingsrelaties tot stand te brengen met CSIRT’s (CBW artikel 17 lid 6) en met hen vertrouwelijke gegevens te verstrekken (CBW Artikel 65 lid 2) teneinde de doelstellingen van de CBW te verwezenlijken”. De CBW, noch de Memorie van Toelichting of de toekomstvisie voor het verbeteren van publiek-private samenwerking bij het verhogen van de cyberweerbaarheid van organisaties, geven echter inzicht wat er wordt bedoelt met “onder omstandigheden” als omschreven in de Memorie van Toelichting. Hiermee is er geen schriftelijke zekerheid of, en zo ja door welke bevoegde autoriteit, de bestaande OKTT’s (tevens toekomstige schakelorganisaties) ook als zodanig zullen worden gekwalificeerd. Omdat dit wel mondeling is toegezegd tijdens het OKTT overleg (georganiseerd door NCSC/NCTV) van 21 mei jl., adviseert de Stichting Connect2Trust daarom dit ook op te nemen in de Memorie van Toelichting alsook de “omstandigheden” in de Memorie van Toelichting nader te specificeren.

Diverse OKTT’s (tevens toekomstige schakelorganisaties) verrichten ook andere CSIRT taken zoals genoemd in artikel 17 lid 2 onder lid c, d en f in artikel 17. De Stichting Connect2Trust adviseert om, in aanvulling op de verplichte taak voor een schakelorganisatie genoemd in artikel 17, tweede lid, onderdeel b van de CBW, ook de mogelijkheid op te nemen dat ook deze activiteiten kunnen worden gecontinueerd door de schakelorganisaties, mits dit in goede afstemming geschiedt met de sectorale CSIRT en het NCSC als nationaal contactpunt.

Daarnaast wordt er in paragraaf 5.6.4 van de Memorie van Toelichting ook stilgestaan bij de categorie relevante partijen. Hier betreft het echter niet specifiek de bestaande OKTT’s (tevens toekomstige schakelorganisaties). De relevantie van deze organisaties wordt vastgesteld op basis van de relevantie van de informatie van een CSIRT voor de cyberweerbaarheid van de partijen zelf of hun achterban. De reikwijdte van relevante partijen is op basis van deze paragraaf niet in te schatten. Omwille van de duidelijkheid m.b.t. de taken en verantwoordelijkheden van de bestaande OKTT’s (tevens toekomstige schakelorganisaties) in vergelijking met deze relevante partijen waarop CBW artikel 65 lid 2 ook van toepassing is, adviseert de Stichting Connect2Trust om meer onderscheid aan te brengen tussen deze twee typen organisaties.

De meldplicht in de CBW (artikelen 28 en 29) schrijft voor dat een essentiële entiteit of belangrijke entiteit een melding dient door te geven aan haar CSIRT en de bevoegde autoriteit. De Stichting Connect2Trust interpreteert deze artikelen dat deze meldingen door een entiteit zowel direct bij haar CSIRT en de bevoegde autoriteit kan worden gedaan, als op verzoek door haar CSIRT[23], of door een schakelorganisatie met gedeeltelijke CSIRT-taken[24]

[21] https://www.rdi.nl/actueel/nieuws/2023/10/18/lancering-zelfevaluatie-tool-nis2

[22] Het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie onder de betrokken essentiële entiteit of belangrijke entiteit en aan de bevoegde autoriteiten en andere relevante partijen over cyberdreigingen, kwetsbaarheden en incidenten, indien mogelijk in bijna-realtime;

[23] Conform beleidskader voor het herinrichten van het stelsel met een nationale en sectorale CSIRT's in Nederland 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

[24] Conform de de toekomstvisie voor het verbeteren van publiek-private samenwerking bij het verhogen van de cyberweerbaarheid van organisaties https://www.rijksoverheid.nl/documenten/rapporten/2024/05/23/tk-bijlage-rapport-toekomstvisie-cyberweerbaarheidsnetwerk

kan worden gedaan aan de omschreven autoriteiten in de CBW. Hiermee ontstaat de mogelijkheid van een one-stop-shop voor de verplichte meldingen van incidenten met daaraan verbonden een verlichting van taken voor een entiteit gedurende een cyberincident. De Stichting Connect2Trust adviseert daarom dit ook expliciet op te nemen in de CBW en daarbij ook aan te geven wie binnen een essentiële of belangrijke entiteit de bevoegdheid krijgt om deze melding ook te doen.

De entiteiten die volgende Artikel 4 lid 1 onder de CBW vallen dienen gevestigd te zijn in Nederland en in (of vanuit) Nederland diensten of activiteiten in (en buiten) Europa te verrichten. Veel van de organisaties die zijn aangesloten bij de Stichting Connect2Trust hebben ook (zuster-, moeder-, dochter) bedrijven die zijn gevestigd buiten Nederland maar binnen Europa. De CBW houdt op dit moment geen rekening met dergelijke multinationale bedrijven als het gaat om de registratie van een entiteit en het melden van incidenten. Vanuit de nationale soevereiniteit en het Europees recht is dit begrijpelijk maar onderschrijft dit eens te meer de hiervoor beschreven noodzaak tot het hebben van de optie tot kunnen registreren en/of melden via aangewezen CSIRT's of schakelorganisaties, zonder dat dit afbreuk doet aan de verantwoordelijkheid van een entiteit om bevestigen te verkrijgen dat deze registratie of melding ook correct is aangekomen in ieder land binnen Europa waar een entiteit is gevestigd waarop de NIS2 van toepassing is. De Stichting Connect2Trust adviseert daarom om in de CBW expliciet te beschrijven hoe multinationale organisaties uitvoering dienen te geven aan de registratie- en meldplicht buiten Nederland en Europa.

Namens de aangesloten organisaties bij de Stichting Connect2Trust,

Het bestuur van de Stichting Connect2Trust