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 Justitie & Veiligheid
T.a.v. De heer prof. mr.
Turfmarkt 147
2511 DP Den Haag

Betreft: Consultatie Conceptvoorstel Wet Beveiliging Netwerk- en Informatiesystemen

Excellentie,

Op 21 juni 2021 ontving de Stichting Connect2Trust van de Directeur Wetgeving en Juridische Zaken ter advisering het conceptvoorstel tot wijziging van de Wet beveiliging netwerk- en informatiesystemen. De stichting heeft uw conceptvoorstel voorgelegd aan haar deelnemers en alle reacties in dit advies samengebracht.

De Stichting Connect2Trust staat ten principale positief tegenover uw voorstel omdat het meer structuur en transparantie geeft aan het verspreiden van dreigings- en incidentinformatie binnen Nederland door het NCSC als Nationaal Cyber Security Centrum. Deze structuur wordt geborgd in een Landelijk Dekkend Stelsel van schakelorganisaties c.q. cybersecurity samenwerkingsverbanden (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[1]. De Memorie van Toelichting stelt in artikel 2.1.2. dan ook terecht dat het LDS nog in opbouw verkeert.

Naarmate het aantal organisaties toeneemt dat onderdeel uitmaakt van het LDS, vergroot het risico dat organisaties in Nederland meerdere keren dezelfde dreigings- en incidentinformatie ontvangen. Dit creëert een aanzienlijke extra werklast voor cybersecurity medewerkers wat, vanwege de grote schaarste onder deze groep van medewerkers, maximaal voorkomen dient te worden. De toetsing van een schakelorganisatie als sectoraal computercrisisteam of OKTT, richt zich echter uitsluitend op de vaststelling dat uitwisseling van gegevens over dreigingen of incidenten verantwoord en gerechtvaardigd is. Het eerste advies van de Stichting Connect2Trust in reactie op deze consultatie, is daarom om de criteria voor toelating voor alle lopende en nieuwe aanvragen van organisaties tot aanwijzing als OKTT uit te breiden ter voorkoming van dergelijke doublures.

De sectorale computercrisisteams en OKTT's waaronder de Stichting Connect2Trust, verbonden in het Anti-Abuse Netwerk[2], hebben zich bereid verklaard om vanuit de private sector het voortouw te nemen tot het opstellen van deze aanvullende criteria als onderdeel van de realisatie van een nationaal clearinghouse. Dit clearinghouse biedt het NCSC de mogelijkheid om alle informatie eenduidig te verspreiden binnen het LDS, en tegelijkertijd organisaties de mogelijkheid om, naar behoefte, gericht dreigings- en incidentinformatie

[1] https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds
[2] https://www.abuse.nl/

(terug) te delen met elkaar en de overheid[3]. Ook kunnen de ontvangende (groepen van) aangesloten organisaties hier specifieke diensten voor ontwikkelen zoals bijvoorbeeld het inrichten van nieuwe samenwerkingsverbanden of gezamenlijke computercrisisteams. Het tweede advies van de Stichting Connect2Trust in reactie op deze consultatie, is dan ook om de inrichting van, en aansluiting op een dergelijk clearinghouse voor het LDS vanuit een publiek-private samenwerking te stimuleren als onderdeel van de opbouw van het LDS en daarmee integraal onderdeel te maken van de uitvoering van de Nationale Cyber Security Agenda (NCSA).

Met betrekking tot het delen van dreigings- en incidentinformatie is, in opdracht van het Anti-Abuse Netwerk, door Privacy Management Partners in 2021 onderzoek uitgevoerd naar het delen van abuse informatie middels een Legitimate Interest Assessment (LIA)[4]. Onder abuse informatie wordt verstaan: ongewenste configuraties, kwetsbaarheden en ongewenst gebruik. Het rapport concludeert het volgende:

- Voor zover de abuse informatie kwalificeert als persoonsgegevens (wat meestal niet het geval is), kan de informatie worden verwerkt op grond van artikel 6(1)(f) AVG (gerechtvaardigd belang). Een voorwaarde hiervoor is dat deze informatie wordt uitgesplitst naar de partij die de abuse kan verhelpen en dat deze zich netjes aan de basisvoorwaarden van de AVG houdt.
- Deze conclusie geldt niet als de abuse informatie kwalificeert als strafrechtelijke gegevens over daders
- Geaggregeerde informatie is -mits de groepsgrootte groot genoeg is- geen persoonsgegeven. Het verstrekken van geaggregeerde abuse informatie aan niet-aangesloten partijen valt dan ook niet onder de AVG, zodat er vanuit dat punt geen belemmeringen zijn om het te doen.

De conclusies van dit LIA-onderzoek, alsook de urgentie zoals aangegeven door de Cyber Security Raad[5], worden onderschreven door de Stichting Connect2Trust en haar deelnemers en vraagt een verdere nuancering van de Wbni hoe om te gaan wanneer dreigings- en incidentinformatie wel of geen persoonsgegeven betreffen. Het groot deel hiervan betreft immers geen persoonsgegevens. Sectorale computercrisisteams en OKTT's zijn getoetst op hun gerechtvaardigd belang voor het omgaan met die zeer kleine groep aan restdata. De inrichting van het eerder genoemde clearinghouse als centraal knooppunt voor informatiedeling biedt nog een aanvullend instrument dat ervoor kan zorgen dat persoonsgevoelige informatie gecontroleerd wordt gedeeld en niet verder wordt gedeeld met niet-relevante doelgroepen. Het derde, en tevens laatste advies van de Stichting Connect2Trust in reactie op deze consultatie, is om in de Wbni op basis van heldere en juridisch publiek getoetste criteria, aan te geven wanneer dreigings- en incidentinformatie een persoonsgegeven betreft. Het huidig wetsvoorstel biedt in dat geval in beide situaties voldoende basis voor het omgaan met deze informatie door de sectorale computercrisisteams en OKTT's.

Samengevat adviseert de Stichting Connect2Trust om (1) de criteria voor toelating voor alle lopende en nieuwe aanvragen van organisaties tot aanwijzing als OKTT uit te breiden ter voorkoming van het dubbel ontvangen van dreigings- en incidentinformatie, (2) de inrichting van, en aansluiting op een dergelijk clearinghouse voor het LDS vanuit een publiek-private samenwerking te stimuleren als onderdeel van de opbouw van het LDS verankerd in de NCSA, (3) in de Wbni aan te geven op basis van heldere en juridisch publiek getoetste criteria dreigings- en incidentinformatie een persoonsgegeven betreft.

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

[3] Zie ook de handvaten in de AAN-metrokaart: https://www.abuse.nl/2020/12/14/Metrokaart-december-2020.html
[4] https://www.abuse.nl/2021/07/13/AAN-publiceert-LIA.html
[5] https://www.cybersecurityraad.nl/documenten/adviezen/2021/02/22/csr-adviesbrief-inzake-het-versneld-delen-van-incidentinformatie