Informatie-uitwisseling landelijk dekkend stelsel cybersecurity

Managementsamenvatting

Projectnummer:
2019.151

Publicatienummer
2019.151-2008

Datum:
Utrecht, 14 oktober 2020

Auteurs:
ir. ing. Reg Brennenraedts, MBA
prof. dr. Rudi Bekkers
Jessica Kats, MSc.
mr. drs. Melvin Hanswijk
Roma Bakhyshov, MSc.
ir. Wazir Sahebali
Roos Jansen, MSc.

Managementsamenvatting

Onze maatschappij is in toenemende mate afhankelijk van informatie- en telecommunicatietechnologie (ICT), en wordt daarmee ook steeds kwetsbaarder voor dreigingen op het gebied van cybersecurity.[1] Nederlandse inlichtingen- en veiligheidsdiensten, de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), het Nationaal Cybersecurity Centrum (NCSC) en de politie signaleren een zorgwekkende toename van digitale dreigingen. Bovendien blijft de weerbaarheid achter ten opzichte van de ontwikkeling van de dreiging.

Nederland onderkent deze kwetsbaarheid: in de Nederlandse Cyber Security Agenda (NCSA) luidt de eerste ambitie: 'Nederland heeft zijn digitale slagkracht op orde'.[2] Deze wordt als volgt toegelicht: "*Om daadkrachtig te kunnen reageren op de toename van de digitale dreiging, moeten overheidspartijen en private organisaties in Nederland samenwerken en beschikken over adequate capaciteiten en middelen*."[3] Een van de doelstellingen daarbij luidt: "*Er wordt een landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden ingericht waarbinnen informatie over cybersecurity breder, efficiënter en effectiever wordt gedeeld tussen publieke en private partijen. Dit dekkende stelsel heeft tot doel de slagkracht van publieke en private partijen te versterken*."[4]

De keuze van Nederland voor een decentrale vormgeving gaat gepaard met het risico dat de overheid een minder goed inzicht heeft als het gaat om het *bereik* van informatie over digitale veiligheid. Dat mindere inzicht speelt vooral voor de niet-vitale partijen. Momenteel speelt bij het Ministerie van Justitie en Veiligheid (JenV) dan ook de vraag of informatie over cybersecurity nog breder, efficiënter[5] en effectiever kan worden gedeeld tussen publieke en private partijen, en de vraag wat er nog gedaan kan worden om tot een landelijk dekkend stelsel van cybersecurity te komen.

In dit onderzoek hanteren we het volgende uitgangspunt met betrekking tot het landelijk dekkend stelsel van cybersecuritysamenwerkingsverbanden: het ideaal van een landelijk dekkend stelsel is gerealiseerd als elke partij in Nederland wordt 'bereikt' en toegang heeft tot de cybersecurity-informatie waar hij behoefte aan heeft. Partijen worden door het stelsel 'bereikt' indien ze weten waar ze terecht kunnen in geval van vragen over of problemen met cybersecurity.

Het onderliggend onderzoek beoogt inzichten op te leveren voor het zojuist gestelde probleem, en heeft de volgende overkoepelende onderzoeksvraag: *Welke doelgroepen met betrekking tot de niet-vitale partijen worden nu nog niet bereikt, op welke wijze - en via welke vakdepartementen - zou dat wel lukken en wat moet daar concreet voor gebeuren?*

Om de overkoepelende vraag en opgestelde deelvragen te beantwoorden zijn een aantal verschillende onderzoeksmethoden ingezet: documenten- en data-analyse, gesprekken met experts en andere betrokkenen, dataverzameling bij doelgroepen (interviews, survey), en

---

[1] Cybersecuritybeeld Nederland CSBN 2019.

[2] Nederlandse Cyber Security Agenda (NCSA), p. 17.

[3] Idem, p. 19.

[4] Idem, p. 19.

[5] Met efficiënter wordt vooral bedoeld in kwalitatieve zin, voor wat betreft de wijze van organisatie, dus niet kwantitatief, financieel.

een landenvergelijking. Daarna is middels een integrale analyse alle opgehaalde informatie bij elkaar gebracht en antwoord gegeven op de onderzoeksvragen.

Hoe de verschillende partijen cybersecurity, en de verschillende aspecten daarvan, definiëren

Doordat er sprake is van een vrij jong en dynamisch domein, worden er door de diverse partijen veel verschillende definities van cybersecurity gehanteerd. Niet alleen het begrip 'cybersecurity', maar ook soortgelijke begrippen of beschrijvingen komen voor. De voornaamste overeenkomsten tussen definities is de focus op digitale weerbaarheid, maatregelen en nationale/digitale veiligheid. Verschillen liggen in de omvang van het begrip; het CBS houdt bijvoorbeeld de definitie aan van het CSBN, maar geeft wel extra context. Veel partijen laten zich überhaupt niet uit over de definitie van cybersecurity; ze geven aan wat je kunt doen (of wat zij voor je kunnen doen) om cyber secure te zijn, maar zij specificeren niet wat zij daaronder verstaan. Een onderscheid tussen overheid, private vitale en niet-vitale partijen is niet duidelijk zichtbaar.

De definitie van cybersecurity in Cybersecuritybeeld Nederland (CSBN) 2020[6] wordt aangehouden door de Nederlandse overheid en luidt: "*Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan. Die schade kan bestaan uit de aantasting van de beschikbaarheid, vertrouwelijkheid of integriteit van informatiesystemen en informatiediensten en de daarin opgeslagen informatie.*"[7]

De doelstellingen van het Nederlandse kabinet ten aanzien van cybersecurity

De doelstelling van het Nederlandse cybersecuritybeleid is de volgende: "*Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen.*"

Dit valt uiteen in zeven ambities:[8]

1. Nederland heeft zijn digitale slagkracht op orde.
2. Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein.
3. Nederland loopt voorop in het bevorderen van digitaal veilige hard- en software.
4. Nederland beschikt over weerbare digitale processen en een robuuste infrastructuur.
5. Nederland werpt door middel van cybersecurity succesvol barrières op tegen cybercrime.
6. Nederland is toonaangevend op het gebied van cybersecurity kennisontwikkeling.
7. Nederland beschikt over een integrale, publiek-private aanpak van cybersecurity.

Deze ambities gelden voor Nederland als geheel, waarbij publiek-private samenwerking als uitgangspunt geldt. Vitale sectoren vallen onder het Ministerie van Justitie en Veiligheid en de vakdepartementen, hier wordt ingezet op structurele en adaptieve risicobeheersing. Niet-vitale sectoren vallen onder het Ministerie van Economische Zaken en Klimaat. Onder het ministerie van EZK is in 2018 het Digital Trust Center (DTC) opgericht, een informatieknooppunt ingericht voor het niet-vitale bedrijfsleven.

---

[6] Het Cybersecuritybeeld Nederland (CSBN) biedt inzicht in dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid. Het CSBN wordt jaarlijks door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) vastgesteld.

[7] CSBN 2020, p. 48.

[8] Nederlandse Cyber Security Agenda (NCSA), p. 17.

De huidige inrichting van het Nederlandse cybersecurity-beleid

Het Nederlandse systeem laat zich het beste kenmerken als een decentraal en dynamisch systeem. Het is decentraal omdat het verschillende partijen kent voor het bereiken van de Rijksoverheid en private, vitale partijen (onder andere het NCSC) en voor het bereiken van niet-vitale partijen (onder andere het DTC), en vervolgens gebruik maakt van samenwerkingsverbanden, die een grote rol spelen in de daadwerkelijke verspreiding van informatie. In feite betreft het een netwerkbenadering, visueel weergegeven in **Fout! Verwijzingsbron niet gevonden.** in paragraaf **Fout! Verwijzingsbron niet gevonden.**. Het Nederlandse systeem is verder dynamisch omdat de samenwerkingsverbanden sterk in beweging zijn: regelmatig komen er nieuwe bij of verandert hun samenstelling en bereik.

Informatie-uitwisseling in het Nederlandse cybersecurity-stelsel, en mogelijke beperkingen daarbinnen

In de gegevensuitwisseling tussen de partijen staan twee typen informatie centraal, namelijk voorlichtingsinformatie en dreigingsinformatie, en door verschillen in de aard van deze categorieën, zijn ze onderworpen aan verschillende juridische regimes. Het is met name deze juridische component die de ruimte bepaalt om informatie daadwerkelijk te kunnen delen. Vooral het delen van dreigingsinformatie met niet-vitale partijen is momenteel beperkt, mede door beperkingen vanuit de AVG. De ruimte voor gegevensuitwisseling is mede afhankelijk van de institutionele setting, waar zo nodig aanpassingen gemaakt kunnen worden (zie verderop), maar is deels ook een kwestie van juridische interpretatie (bijvoorbeeld wanneer het gaat om de wettelijke taak van het DTC en de mogelijkheden die deze biedt binnen de AVG; of de vraag hoe om te gaan met de noodzakelijkheidstoets uit de AVG wanneer een samenwerkingsverband geen IP-adressen van de achterban kan aandragen; hoe breed het begrip 'vertrouwelijke informatie' uit de Wbni[9] moet worden uitgelegd en wat de bedoelingen van de wetgever waren bij de beperkingen aan het delen daarvan). Het valt buiten het bestek van dit onderzoek om een oordeel te vellen over de verschillende visies op de juiste juridische interpretaties. Wel verwachten we dat, als gevolg van de lopende discussie, er op de korte of middellange termijn meer consensus ontstaat over de (on)mogelijkheden van informatiedeling in de huidige setting. Hetzelfde geldt voor de mogelijkheden die kunnen ontstaan na aanpassingen in de institutionele omgeving, zoals het versterken van de wettelijke grondslag van het DTC in het kader van de AVG. Eventueel zou vervolgonderzoek meer specifiek op deze juridische vragen in kunnen gaan.

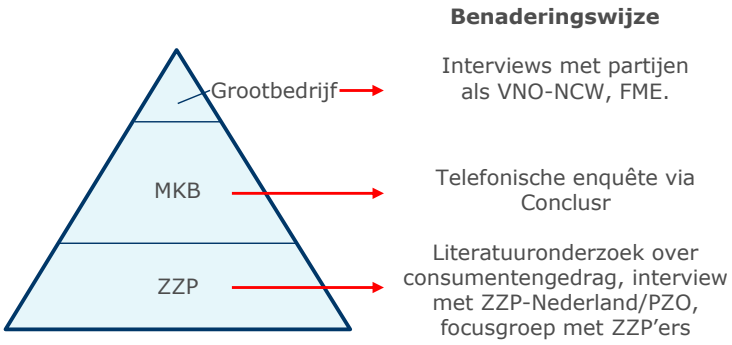
Informatiebehoeften van doelgroepen van niet-vitale bedrijven, en de mate waarin het huidige Nederlandse stelsel deze doelgroepen bereikt

Op basis van eigen dataverzameling, zie Figuur 1, concluderen we dat:

- ZZP'ers een diverse doelgroep zijn wat betreft zowel hun kennis over cybersecurity als hun behoefte aan (meer) kennis daarover. Er zijn ZZP'ers met een zeer duidelijke behoefte aan informatie over cybersecurity (die zij willen ontvangen via meerdere kanalen), zoals een basisscan van hun cybersecurity, benchmarking (hoe goed is hun cybersecurity ten opzichte van die van anderen?), en concrete handelingsperspectieven. In deze behoefte wordt volgens hen momenteel slechts zeer beperkt voorzien (en indien wel, dan door partijen die een zelfbelang hebben en waarbij de neutraliteit van de informatie mogelijk in het geding is). Opvallend is dat het DTC wel degelijk momenteel al in staat is om in een groot deel van deze behoefte te voorzien. Deze categorie bedrijven wordt echter nagenoeg niet bereikt door het DTC.

[9] Wet beveiliging netwerk- en informatiesystemen, deze wet beschrijft onder andere de taken en bevoegdheden van het NCSC.

- Een groot deel van het MKB geen behoefte heeft aan meer informatie over cybersecurity. De 16% die in de telefonische enquête aangaf hier wel behoefte aan te hebben, heeft wensen die grotendeels overeenkomen met die van de genoemde ZZP'ers. Zij hebben vooral behoefte aan algemene cybersecurity-informatie, bij voorkeur per e-mail, aan een manier om te testen of hun beveiliging in orde is en aan een betrouwbare bron waar zij informatie kunnen vinden.
- Bedrijven die beveiligingsdiensten afnemen bij ICT leveranciers een veel beperktere vraag hebben. Ze vertrouwen erop dat deze leveranciers passende maatregelen hebben genomen en dat in geval van calamiteiten, deze leveranciers ze effectief kunnen helpen.
- Grotere bedrijven, die zelf hun IT-beveiliging regelen, juist wel weer behoefte aan informatie hebben, en nog onvoldoende bediend worden. Het gaat dan wel om heel specifieke informatie, zoals gerichte dreigingsinformatie, en informatie over softwarelekken. De informatie moet zodanig van aard zijn dat ze bedrijven in staat stelt om er concreet naar te handelen.
- Gespecialiseerde IT-bedrijven, waaronder IT-leveranciers, netwerkbeheerders, internet service providers (ISP's), managed service providers (MSP's) ook een duidelijke informatiebehoefte hebben. Hoewel deze behoefte al deels wordt ingevuld door publieke en private bronnen (door de markt opgezette meldpunten, de Amerikaanse Common Vulnerabilities and Exposures (CVE)-databank,[10] etc.), is er nog steeds duidelijke behoefte naar (additionele) dreigingsinformatie in de Nederlandse context, zoals die momenteel beschikbaar is binnen het NCSC.



Figuur 1. Benaderingswijze doelgroepen onderzoek

In aanvulling op het bovenstaande bleek tijdens ons onderzoek dat er een heel specifiek thema is waarop kennis tekortschiet, namelijk dat van Operational Technology (OT). Dit betreft het gebruik van hardware en software om fysieke processen, apparaten en infrastructuur aan te sturen, en omvat onder meer industriële Internet of Things (IoT) en kritieke infrastructuren. Dit is een gebied waarin beveiliging, om historische redenen, vaak nog tekortschiet maar waarin de dreiging sterk is toegenomen. Dit levert een vooralsnog slecht ingevulde kennisvraag op.

[10] De CVE-databank wordt onderhouden door het bedrijf MITRE Corporation en wordt gefinancierd door de nationale divisie voor informatiebeveiliging van het Amerikaanse Departement van Binnenlandse Veiligheid.

Mogelijkheden om doelgroepen beter te bereiken en informatiebehoeften beter te vervullen

Op basis van ons onderzoek onderscheiden we een aantal verschillende routes die, apart of in combinatie met elkaar, het Nederlandse stelsel voor cybersecurity zouden kunnen versterken en informatie-uitwisseling zouden bevorderen, en op die manier zouden helpen in het bereiken van de doelstellingen van het Nederlands beleid. Deze routes zijn de volgende:

1. *Richting één (bekend) loket voor Mkb's en ZZP'ers*
2. *Verspreiden restinformatie[11] van NCSC via DTC naar de samenwerkingsverbanden;*
3. *Verspreiden restinformatie NCSC door andere partijen;*
4. *Uitbreiding aantal computercrisisteams[12] onder niet-vitale cybermature bedrijven;*
5. *Meer bedrijven als vitaal aanwijzen, of opsplitsing vitaal/niet-vitaal heroverwegen;*
6. *Een enkele backoffice voor zowel NCSC als DTC.*

Hoe de oplossingsrichtingen zich verhouden tot de Wet Markt en Overheid en de Wet beveiliging netwerk- en informatiesystemen

De enige oplossingsrichting waar concurrentievervalsing mogelijk een rol zou kunnen spelen, is oplossingsrichting 2, waarin restinformatie van het NCSC via het DTC naar de samenwerkingsverbanden en niet-vitale bedrijven wordt doorgezet. De Wet Markt en Overheid komt dan in beeld, omdat gratis informatie aan partijen wordt aangeboden die vergelijkbaar is met informatie die de partijen wellicht bij commerciële partijen zouden kunnen inkopen. De informatie zal echter bestaan uit gegevens die het DTC heeft verkregen in het kader van de uitoefening van zijn publiekrechtelijke bevoegdheden (voortkomend uit het wetsvoorstel dat in de oplossingsrichting wordt besproken). Voor dergelijke gegevens kent de Wet Markt en Overheid een uitzondering op de gedragsregel dat kosten van goederen en diensten integraal moeten worden doorberekend. Deze oplossingsrichting zal daardoor niet botsen met de Wet Markt en Overheid.

De Wet beveiliging netwerk- en informatiesystemen (Wbni) geeft aan met wie het NCSC dreigingsinformatie met persoonsgegevens mag delen, door wettelijke taken te formuleren die als grondslag in de zin van de AVG dienen, en geeft aan met wie het NCSC herleidbare vertrouwelijke gegevens mag delen. Een aantal keer is aangegeven dat een wijziging van de Wbni bepaalde barrières weg zou nemen, maar voor geen enkele oplossingsrichting is dit echt vereist. De voornaamste stap die gezet moet worden die voortkomt uit de Wbni, is de aanwijzing van het DTC als OKTT, in het kader van oplossingsrichting 2. Een OKTT is een organisatie die 'Objectief Kenbaar Tot Taak' heeft om andere organisaties of het publiek te voorzien van dreigingsinformatie. Het NCSC kan, in samenwerking met de NCTV, een organisatie aanwijzen als OKTT. De aanwijzing is een belangrijke stap om het delen van dreigingsinformatie mogelijk te maken. De aanwijzing van het DTC kan echter pas plaatsvinden wanneer het DTC een wettelijke grondslag heeft om persoonsgegevens te verwerken.

Stelsels van cybersecurity in andere landen, en leermomenten voor Nederland

In dit onderzoek is gekeken naar het cybersecuritystelsel in Engeland, Frankrijk en Duitsland. Gegeven de specifieke context waarin verschillende landen zich bevinden, (denk aan juridisch

---

[11] Het NCSC heeft niet de taak om informatie te zoeken buiten zijn primaire doelgroep: Rijksoverheid en vitaal. Met 'restinformatie' wordt gedoeld op informatie die het NCSC uit hoofde van onderzoek ten behoeve van die doelgroep in zijn bezit heeft, maar die relevant is voor niet-vitale partijen.

[12] Een computercrisisteam is een gespecialiseerd team van professionals dat snel kan handelen bij beveiligingsincidenten met computers of netwerken. Als een computercrisisteam als zodanig is aangewezen, bij ministeriële regeling, mag het dreigingsinformatie met persoonsgegevens en herleidbare vertrouwelijke informatie ontvangen van het NCSC.

kader, omvang van de economie, bestuurlijke indeling, et cetera) is het lastig om een harde vergelijking te maken. Evaluaties van het centralistische Engelse systeem zijn positief, maar met een budget van (omgerekend) meer dan € 2 miljard gaat het dan ook om een inspanning die niet goed vergelijkbaar is met die in Nederland. Over het eveneens centralistische Franse systeem kregen we niet altijd consistente input. Hoewel Frankrijk bijvoorbeeld hoog scoort in de Global Cybersecurity Index, is het oordeel dat gesprekspartners over Frankrijk gaven toch veel kritischer. Het Franse GIP ACYMA (tot op zekere hoogte vergelijkbaar met het Nederlandse DTC) lijkt wel erg succesvol in het bereiken van kleine bedrijven, mede door het koppelen van deze bedrijven aan (private) ICT experts. Het Duitse cybersecurity systeem is deels decentraal, maar dat is vooral ingegeven door het federale bestuurssysteem. Bronnen geven aan dat er sprake is van versplintering en onduidelijke verdeling van de takenpakketten tussen de betrokken diensten, en dat deze situatie samenwerking in Duitsland bemoeilijkt.

Eindconclusie

Hoewel het streven van een landelijk dekkend stelsel steeds verder wordt verwezenlijkt, zijn er nog Mkb's en ZZP'ers die onvoldoende op de hoogte zijn van waar ze terecht kunnen met vragen over of problemen met cybersecurity. Zo is slechts een kleine groep op de hoogte van het bestaan van het DTC, terwijl veel bedrijven tegelijkertijd aangeven behoefte te hebben aan juist die zaken die het DTC aanbiedt, zoals een basisscan. Ook in meer algemene zin is een duidelijke behoefte uitgesproken voor een centrale en betrouwbare partij die bedrijven voorziet van informatie met betrekking tot cybersecurity.

Het delen van dreigingsinformatie is vaak problematisch vanwege de juridische beperkingen aan het delen van persoonsgegevens en herleidbare vertrouwelijke informatie. Dreigingsinformatie die relevant is voor de niet-vitale sector blijft daardoor 'hangen' bij het NCSC. Er zijn niet alleen juridische obstakels voor het delen van dreigingsinformatie, ook praktische en organisatorische problemen spelen een rol. Sommige samenwerkingsverbanden die in de toekomst mogelijk als OKTT aangewezen kunnen worden, kunnen de informatie die zij zouden willen ontvangen nu namelijk nog niet nuttig gebruiken, bijvoorbeeld doordat zij met hun huidige systemen en capaciteit niet in staat zijn om de juiste gegevens naar de juiste partijen in hun achterban te sturen, of kunnen niet aannemelijk maken dat zij dit veilig en AVG-compliant kunnen doen. Uiteindelijk wordt met name de groep niet-vitale cybermature bedrijven op het moment niet goed bediend wat betreft de gewenste informatievoorziening, deze groep heeft beperkt toegang tot de informatie die zij nodig achten om cyberweerbaar te kunnen functioneren. Het NCSC heeft bijvoorbeeld relevante dreigingsinformatie die de bedrijven niet uit andere bronnen kunnen halen.

Alle geïdentificeerde oplossingsrichtingen kunnen bijdragen aan het doel om het Nederlandse cybersecuritystelsel landelijk dekkend te maken. Op basis van ons onderzoek ligt een combinatie van de eerste drie oplossingsrichtingen voor de hand, waarmee zowel verbetering op korte termijn als zo volledig mogelijke dekking op lange termijn gerealiseerd kan worden:

1. Voor het voorlichtingsaspect van het stelsel kan worden ingezet op grootschalige marketing van het DTC als centraal loket voor vragen over cybersecurity, om de herkenbaarheid en vindbaarheid van het DTC te verbeteren (oplossingsrichting 1). Op die wijze kan worden voorzien in de behoeften van bedrijven met een lage cybermaturity, met name ZZP'ers en kleine bedrijven.

2. Ook voor het doorzetten van dreigingsinformatie ligt het inzetten van het DTC voor de hand (oplossingsrichting 2). Het DTC kan op termijn de primaire actor voor dreigingsinformatie voor niet-vitaal worden. Deze oplossingsrichting biedt potentieel de meest volledige dekking, maar het zal naar verwachting nog even duren voor de

benodigde wettelijke grondslag van het DTC rond is en de informatie-uitwisseling echt kan starten (begin 2021 is mogelijk haalbaar, maar een jaar later is niet ondenkbaar).

3. In de tussentijd, en ook daarna, zou verspreiding van de dreigingsinformatie door bestaande en nieuwe OKTT's een oplossing kunnen zijn (oplossingsrichting 3). Met name het idee om OKTT's het NCSC te laten informeren over welke bedrijven in hun achterban toestemming hebben gegeven om herleidbare vertrouwelijke informatie met de OKTT te delen (zie paragraaf **Fout! Verwijzingsbron niet gevonden.**), zou de situatie op relatief korte termijn kunnen verbeteren, doordat informatie over kwetsbaarheden van specifieke bedrijven dan beter gedeeld kan worden. Deze mogelijkheid is inmiddels voorgelegd aan het NCSC, dat gaat kijken of dit juridisch mogelijk is.

Aanbevelingen

Op basis van de dit onderzoek komen we tot drie aanbevelingen:

1. Ontwikkel een communicatiestrategie om te voorzien in de geïdentificeerde informatiebehoefte van ZZP'ers en Mkb's (die geen beveiligingsdiensten afnemen bij ICT-leveranciers). Omdat uit dit onderzoek blijkt dat veel van de door deze partijen gewenste informatie al beschikbaar is via het DTC, maar niet bij hen terecht komt, is het belangrijk om te werken aan de bekendheid en vindbaarheid van het DTC.

2. Verken de voorgestelde oplossingsrichtingen 2 en 3, voor het beter verspreiden van dreigingsinformatie via het DTC en via samenwerkingsverbanden, en bespreek de haalbaarheid met de betrokken partijen. Doe indien nodig nader onderzoek naar de interpretaties van bepaalde juridische bepalingen, denk hierbij aan de vraag of toestemming om herleidbare vertrouwelijke gegevens te delen vooraf en via een andere partij kan worden gegeven, en de vraag in hoeverre kan worden begonnen met gegevensverwerking door het DTC voordat het aankomende wetsvoorstel geaccepteerd is.

3. Stimuleer samenwerking tussen de centrale partijen in het stelsel, met name tussen het NCSC en het DTC. Partijen hebben niet alleen de bevoegdheid nodig om informatie met elkaar te mogen delen, maar dienen ook elkaars doelgroepen, doelen en werkwijzen te begrijpen. Zij zouden daarvoor meer met elkaar in gesprek kunnen gaan, eventueel via periodieke meetings waarin problemen en ambities doorgesproken worden. Hier zouden ook andere informatieknooppunten, bijvoorbeeld computercrisisteams als Z-CERT (zorg) en SURFcert (onderwijs en onderzoeksinstellingen), bij betrokken kunnen worden.

Contact:
Dialogic innovatie & interactie
Hooghiemstraplein 33-36
3514 AX Utrecht
Tel. +31 (0)30 215 05 80
www.dialogic.nl