Informatie-uitwisseling landelijk dekkend stelsel cybersecurity

Eindrapport

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.

Inhoudsopgave

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 Figuur 5 in paragraaf 3.1.1. 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.

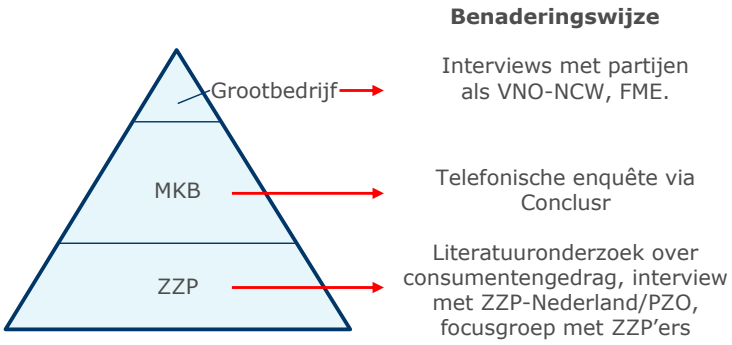
Informatiebehoeften van doelgroepen van niet-vitale bedrijven, en de mate waarin het huidige Nederlandse stelsel deze doelgroepen bereikt

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.

[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.

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 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 5.1.3), 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.

1 Inleiding

In dit hoofdstuk beschrijven we in paragraaf 1.1 de aanleiding voor dit onderzoek naar informatie-uitwisseling binnen een landelijk dekkend cybersecuritystelsel. Vervolgens worden de onderzoeksvragen genoemd (paragraaf 1.2) en presenteren we de onderzoeksaanpak (paragraaf 1.3). Afsluitend is er een leeswijzer voor dit rapport toegevoegd (paragraaf 1.4).

1.1 Achtergrond en aanleiding voor het onderzoek

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.[13] 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.[14] 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'.[15] 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*."[16] 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*."[17]

De benodigde kennis en capaciteiten zijn bij vele organisaties echter nog volop in ontwikkeling en er is dringend behoefte aan meer en beter toegesneden informatie over digitale dreigingen. Hoewel de informatie-uitwisseling tussen organisaties de afgelopen jaren sterk is verbeterd, is de volgende stap deze samenwerking structureel te borgen en tegelijkertijd breder in te richten.

In dit kader stelt de NCSA een aantal maatregelen voor:[18]

- Het landelijk situationeel beeld wordt versterkt met de inrichting van een samenwerkingsplatform met het oogmerk om binnen de wettelijke kaders meer en sneller handelingsperspectief met belanghebbende organisaties te kunnen delen.
- Onder coördinatie van de NCTV worden rondetafelgesprekken georganiseerd waarmee het landelijk dekkend stelsel van cybersecuritysamenwerkingsverbanden vorm kan krijgen.
- Het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Center (DTC) zullen de oprichting en doorontwikkeling van cybersecuritysamenwerkingsverbanden voor overheden, het bedrijfsleven en maatschappelijke organisaties stimuleren, en

[13] Cybersecuritybeeld Nederland CSBN 2019.

[14] Idem.

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

[16] Idem, p. 19.

[17] Idem, p. 19.

[18] Idem, p. 20.

– waar nodig – ondersteuning bieden. Ook wordt hierbij aandacht gegeven aan het opstellen van een set van basisbeveiligingsmaatregelen voor bedrijfsleven en maatschappelijke organisaties.
- Bezien wordt of de wetgeving gericht op het beschermen van nationale veiligheid voldoende handvatten biedt om deze veiligheid ook in het digitale domein te bevorderen, met behoud van fundamentele waarden en privacy.

Uit het bovenstaande blijkt al dat cybersecurity niet wordt gezien als een zaak van enkel de overheid, maar van alle betrokken partijen. Dit is ook goed herkenbaar in de zevende ambitie van NSCA, *"Nederland beschikt over een integrale, publiek-private aanpak van cybersecurity"*, Hierin staat: *"Voor een veilig klimaat in het digitale domein mag en moet van alle partijen verwacht worden dat zij hun verantwoordelijkheid nemen en hun bijdrage leveren om Nederland samen digitaal veilig te maken en te houden. De aanpak kan alleen succesvol zijn als zij in nauwe publiek-private samenwerking wordt vormgegeven, doorontwikkeld en geëvalueerd. De toenemende complexiteit en breedte van het cyberdomein vragen om continue verheldering van die rolverdeling en de verantwoordelijkheden. Het is daarbij zaak om de succesvolle marktinitiatieven ook in beeld te krijgen en aan deze agenda te verbinden. […] Ook aan de private kant moet er meer in samenhang gewerkt (gaan) worden aan de integrale Nederlandse cybersecurity aanpak."*[19] In het kader van deze ambitie zijn onder andere als doelstellingen geformuleerd dat de regierol van de overheid op de integrale aanpak wordt versterkt, maar ook dat bedrijven, burgers en overheidsorganisaties invulling geven aan hun verantwoordelijkheden, rechten en plichten op het gebied van cybersecurity.

Er zijn de afgelopen jaren diverse stappen genomen om het bestaande stelsel van samenwerkingsverbanden te versterken en uit te breiden, onder meer door de oprichting van het DTC onder aanvoering van het Ministerie van Economische Zaken en Klimaat (EZK). Deze is opgericht in 2018 en richt zich op niet-vitale private partijen.[20] Ook is er eind 2018 gestart met de publiek-private Cybersecurity Alliantie waarbinnen concrete (kortlopende) projecten worden uitgevoerd omtrent cybersecurity.

Vergeleken met andere landen wordt het Nederlandse cybersecuritystelsel gekenmerkt door een enigszins unieke, decentrale vormgeving, ondanks de roep van sommigen om een 'minister van Cybersecurity' en een 'deltacommissaris voor digitale veiligheid' aan te stellen.[21] Daarmee ligt het risico op de loer dat de overheid onvoldoende inzicht heeft als het gaat om het *bereik* van informatie over digitale veiligheid. Vanuit deze achtergrond heeft het WODC, op verzoek van de NCTV, opdracht gegeven tot dit onderzoek.

1.2 Probleemstelling en onderzoeksvragen

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[22] en effectiever kan worden gedeeld tussen publieke en

[19] Nederlandse Cyber Security Agenda (NCSA), p. 43.

[20] Voortgang Nederlandse Cybersecurity Agenda, 12 juni 2019.

[21] Geert Munnichs, Matthijs Kouw & Linda Kool, Een nooit gelopen race, Over cyberdreigingen en versterking van weerbaarheid. Den Haag, Rathenau Instituut 2017

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

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.

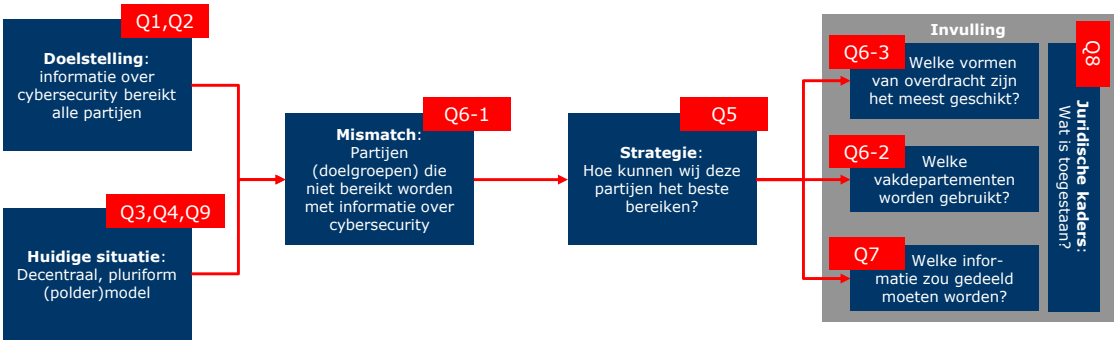
Het onderliggend onderzoek beoogt inzichten op te leveren voor het zojuist gestelde probleem, en heeft de volgende overkoepelende onderzoeksvraag:

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?

Voor het beantwoorden van de bovenstaande onderzoeksvraag heeft de opdrachtgever een aantal deelvragen opgesteld:

1. Uit welke aspecten bestaat cybersecurity volgens de definitie uit de CSBN 2019? En is deze anders voor en/of volgens de verschillende partijen (overheid, private vitale en niet vitale partijen)?
2. Welke doelen wil het kabinet voor deze partijen met cybersecurity bereiken?
3. Hoe is de huidige situatie van samenwerkingsverbanden en mogelijkheden van informatie-uitwisseling tussen overheid (NCSC, politie, DTC, e.a.) en private, niet vitale partijen op het gebied van cybersecurity ingericht? Hoe ziet een visuele weergave van het cybersecurity ecosysteem (in Nederland) eruit?
4. Wat houdt informatie-uitwisseling en samenwerking over cybersecurity in, wat betekent dit in de huidige situatie en welke aspecten van cybersecurity bevat deze wel en welke nog niet?
5. Wat zou aan informatie-uitwisseling en samenwerking nog nodig zijn in de huidige situatie om deze structureel te borgen en breder in te richten en de diverse aspecten van cybersecurity te borgen?
6. Welke doelgroepen worden nu nog niet bereikt (wie nog niet?) en op welke wijze en via welke vakdepartementen zouden voor hen nog nieuwe wijzen van informatie-uitwisseling (wat is er nog niet) kunnen worden gecreëerd?
7. Over welke aspecten van cybersecurity zou welke informatie-uitwisseling en samenwerking met deze doelgroepen dienen plaats te vinden?
8. Hoe verhouden de gevonden (on)mogelijkheden zich tot de vigerende regelgeving over concurrentievervalsing, bijv. de Wet Markt en Overheid alsmede Wet beveiliging netwerk- en informatiesystemen (Wbni)?
9. Hoe is in enkele andere landen het stelsel van cybersecurity tussen publieke en private partijen ingericht, en wat kan Nederland daarvan leren?

Figuur 2 geeft de onderlinge samenhang tussen de deelvragen weer.



Figuur 2. Samenhang tussen de deelvragen

1.3 Onderzoeksaanpak

Om de onderzoeksvragen te beantwoorden zijn een aantal verschillende onderzoeksmethoden ingezet: documenten- en data-analyse, gesprekken met experts en andere betrokkenen, dataverzameling bij doelgroepen (interviews, survey), en een landenvergelijking. Daarna is middels een integrale analyse alle opgehaalde informatie bij elkaar gebracht en antwoord gegeven op de onderzoeksvragen. De gebruikte methoden worden hieronder kort samengevat.

Documenten- en data-analyse

We zijn het onderzoek gestart met het uitvoeren van een documentenanalyse. Het doel hiervan was om een goed en zo volledig mogelijk beeld te krijgen van het huidige stelsel van cybersecurity en de rationale achter dat stelsel. De documenten zijn verzameld en –in samenhang– geanalyseerd. In aanvulling daarop hebben wij twee specifieke databronnen geraadpleegd: (1) CBS-data over het uitvoeren door bedrijven van ICT-beveiliging en databescherming, door eigen personeel of extern uitbesteed, en over ICT-veiligheid (gebruik van maatregelen, optreden risico's, oorzaak incidenten, kosten incidenten en uitvoeren updates); (2) CBS-data over cyberweerbaarheid onder ZZP'ers.[23]

Gesprekken met deskundigen en betrokkenen partijen

Parallel aan de hierboven genoemde documenten- en data-analyse zijn (groeps)interviews gehouden met professionals binnen het bestaande stelsel van cybersecurity, zowel bij publieke als bij private partijen. Ook hebben wij op verschillende momenten gesproken met een juridisch expert om de regelgeving omtrent informatie-uitwisseling – in relatie tot de onderzoeksvragen en voorlopige resultaten – goed in beeld te houden. In totaal hebben we 20 interviews gehouden;[24] een overzicht van de gesprekspartners is opgenomen in Bijlage 1.

[23] Hierbij is gebruik gemaakt van de volgende enquêtes en databestanden: (1.) Digitale Veiligheid & Criminaliteit (enquête DV&C); (2.) ICT-gebruik huishoudens en personen (ICT-enquête); (3.) Veiligheidsmonitor; (4.) Zelfstandigen Enquête Arbeid (ZEA); (5.) Politiestatistiek – Basisvoorziening Handhaving (BVH).

[24] Dit aantal is inclusief de gesprekken bedoelt onder het volgende kopje ('dataverzameling bij doelgroepen').

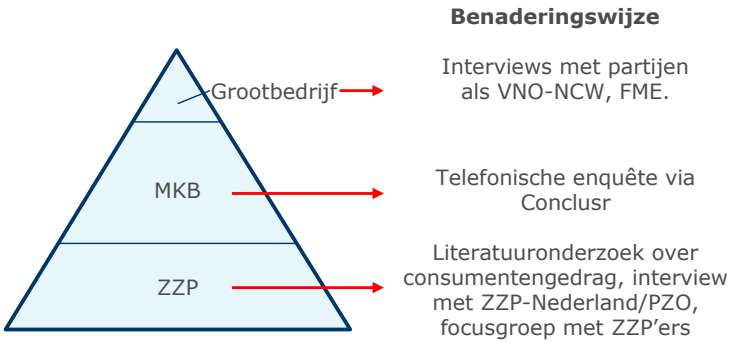
Dataverzameling bij doelgroepen

Om de onderzoeksvragen over het bereik van het netwerk goed te beantwoorden is het essentieel om direct data te verzamelen bij de doelgroepen zelf. Alleen zo kan een goed beeld verkregen worden welke private, niet-vitale partijen nog niet goed bereikt worden door de huidige initiatieven. Omdat de relevante doelgroepen divers van karakter zijn hebben we verschillende onderzoekmethoden ingezet om voor de verschillende doelgroepen op optimale wijze data te verzamelen. Met deze aanpak kunnen we precies aangeven waar lacunes in de informatie-uitwisseling liggen en welke eigenschappen de betreffende doelgroepen hebben.

De private, niet-vitale partijen zoals van belang voor ons onderzoek kunnen onderverdeeld worden in grootbedrijf, MKB en ZZP.

- Het grootbedrijf is een relatief kleine groep en is traditioneel goed vertegenwoordigd in werkgeversverenigingen. Voor deze groep hebben wij interviews ingezet; een overzicht van alle gesprekspartners is opgenomen in Bijlage 1.
- Het MKB is een grote, zeer heterogene groep die weinig betrokken is bij werkgeversverenigingen of andere overkoepelende organisaties. Daarom hebben wij ingezet op een grootschalige telefonische enquête (n=800). In opdracht van ons (en onder begeleiding van ons) heeft marktonderzoekbureau Conclusr 800 bedrijven geselecteerd volgens een gestratificeerde steekproef van de niet-vitale sector op basis van het aantal werknemers. Deze bedrijven zijn vervolgens gebeld[25] en gevraagd of ze weten met wie contact op te nemen in het geval dat ze slachtoffer worden van een cybercrime, aan wat voor informatie over cyberveiligheid ze behoeften hebben, hoe ze deze informatie willen ontvangen en of een hack een negatieve impact heeft op de bedrijfsvoering.
- ZZP'ers, tenslotte, vormen de grootste groep als wij kijken naar het aantal bedrijven. Zij zijn echter nauwelijks georganiseerd en hun gedrag vertoont veel gelijkenis met dat van particulieren. Voor deze groep hebben wij literatuur bekeken over hoe consumenten en ZZP'ers omgaan met cybersecurity, hebben wij ZZP-Nederland en PZO geïnterviewd, en een focusgroep met ZZP'ers georganiseerd.

Figuur 3 geeft een overzicht van de benadering van de verschillende doelgroepen.



Figuur 3. Benaderingswijze doelgroepen onderzoek

[25] De telefonisten vroegen steeds naar de IT-verantwoordelijke (kleine bedrijven) of securityspecialisten (grote bedrijven).

Landenvergelijking

Nederland kan ook leren van landen die reeds ver zijn in de ontwikkeling van een landelijk dekkend cybersecuritystelsel. Op basis van een quickscan zijn drie landen geselecteerd en middels *desk research* in detail bekeken: het Verenigd Koninkrijk, Frankrijk en Duitsland.

Voor ieder van deze drie landen beschrijven we de globale inrichting van het stelsel, maturity, de mate waarin bedrijven zichzelf organiseren, internationale samenwerkingsverbanden en ingezette methoden om (private, niet-vitale) bedrijven te bereiken. Geconstateerde best practices zijn opgenomen in het rapport.

Juridische toets

Gedurende het onderzoek bleek dat de huidige beperkingen omtrent informatie-uitwisseling grotendeels juridisch van aard zijn. In plaats van enkel een juridische toets van de geïdentificeerde oplossingsrichtingen uit te voeren, is er daarom voor gekozen om de juridische context en beperkingen al voorafgaand aan de oplossingsrichtingen te beschrijven. Het gaat met name over de Wet beveiliging netwerk- en informatiesystemen (Wbni) en de Algemene Verordening Gegevensbescherming (AVG). Per oplossingsrichting zijn vervolgens de juridische belemmeringen en mogelijkheden beschreven.

1.4 Leeswijzer

In hoofdstuk 2 gaan we in op het concept cybersecurity. In hoofdstuk 3 beschrijven we het Nederlandse stelsel, de juridische context rondom cybersecurity en drie stelsels van andere landen. In hoofdstuk 4 presenteren we een analyse van de doelgroepen die momenteel nog niet of onvoldoende bereikt worden en bespreken we hun informatiebehoeften. In hoofdstuk 5 bespreken we de mogelijkheden om informatie over cybersecurity breder, efficiënter en effectiever te delen tussen publieke en private partijen, om zo een landelijk dekkend stelsel van cybersecurity te bereiken. Hoofdstuk 6 bevat de conclusies van dit onderzoek. In Bijlage 1 zijn de interviewpartners opgenomen en in Bijlage 2 worden de landenstudies in meer detail beschreven.

2 Betekenis van cybersecurity, en de kaders en doelen van het Nederlands cybersecuritystelsel

In dit hoofdstuk beschrijven het concept cybersecurity, inclusief verschillende definities en de aspecten waaruit cybersecurity bestaat. We sluiten het hoofdstuk af met de doelen die het kabinet wil bereiken voor de verschillende partijen (overheid, vitale private en niet-vitale private partijen). Deelvragen die in dit hoofdstuk worden beantwoord:

Deelvraag 1: Uit welke aspecten bestaat cybersecurity volgens de definitie uit de CSBN 2019? En is deze anders voor en/of volgens de verschillende partijen (overheid, private vitale en niet vitale partijen)?

Deelvraag 2: Welke doelen wil het kabinet voor deze partijen met cybersecurity bereiken?

2.1 De definitie van cybersecurity zoals gebruikt door de Nederlandse overheid

De betekenis die de Nederlandse overheid aan het begrip cybersecurity toekent is mogelijk het best omschreven in de definitie die gegeven is in het Cybersecuritybeeld Nederland (CSBN)[26], dat jaarlijks door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) wordt vastgesteld. Deze definitie 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."*[27,28]

Het vrij zijn van genoemde schade en gevaren wordt beschouwd als *cyber* secure (een ideaal om na te streven). Deze definitie wordt ook gehanteerd in de Nederlandse Cybersecurity Agenda, en is tevens overgenomen door CBS en door VNO-NCW.

Om inzicht te krijgen in de betekenis van deze definitie, en de belangrijkste elementen/aspecten, bespreken we het CSBN nu in meer detail. Het CSBN biedt inzicht in dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de *nationale veiligheid*. Deze factoren bepalen in samenhang het risico. Cybersecurity grijpt vooral in op de weerbaarheid. Eén van de pijlers is het op orde krijgen van de digitale weerbaarheid van organisaties. Veel incidenten hadden voorkomen kunnen worden met behulp van basismaatregelen (vooral eenvoudige aanvalsmiddelen zoals phishing en misbruik van gebruikersnamen en wachtwoorden), maar de weerbaarheid staat ook onder druk door een

[26] 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.

[27] CSBN 2020, p. 48.

[28] In de CBS Cybersecuritymonitor 2019 wordt verwezen naar de uitgebreidere definitie in de 2018-versie.

toenemende complexiteit en connectiviteit in het ICT-landschap. De kern blijft dat digitaal onveilige producten en diensten een fundamentele katalysator zijn van incidenten. Ze kunnen onveilig zijn doordat leveranciers standaard onveilige configuraties leveren of geen updates (meer) beschikbaar stellen, doordat updates moeilijk te installeren zijn of doordat updatemechanismen veranderen of uitgeschakeld worden (bijvoorbeeld door het gebruik van verouderde software). Ook kan het zo zijn dat updates wel beschikbaar zijn, maar organisaties nalatig zijn bij de installatie daarvan. Daarnaast wordt de digitale infrastructuur steeds ingewikkelder, onder meer door fenomenen als gedeelde voorzieningen en doordat bedrijven hun inkoop en uitvoer door externen laten doen.

Methoden om de weerbaarheid daadwerkelijk te meten ontbreken nog volgens de CSBN 2019, maar het is duidelijk dat de digitale weerbaarheid nog niet op orde is. Het versterken van die weerbaarheid is nodig om de kansen van digitalisering verder te benutten. Ook constateert het CSBN 2019 dat hard- en softwarekwetsbaarheden een blijvend probleem zijn. Vanuit consumenten en toezichthouders ontstaan wel meer prikkels om cybersecurity, en als onderdeel daarvan privacy, serieuzer te nemen. In aanvulling daarop zou strengere overheidsregulering, bijvoorbeeld vanuit de Wbni[29] en Roadmap Digitaal Veilige Hard- en Software[30], voor meer prikkels kunnen zorgen.[31]

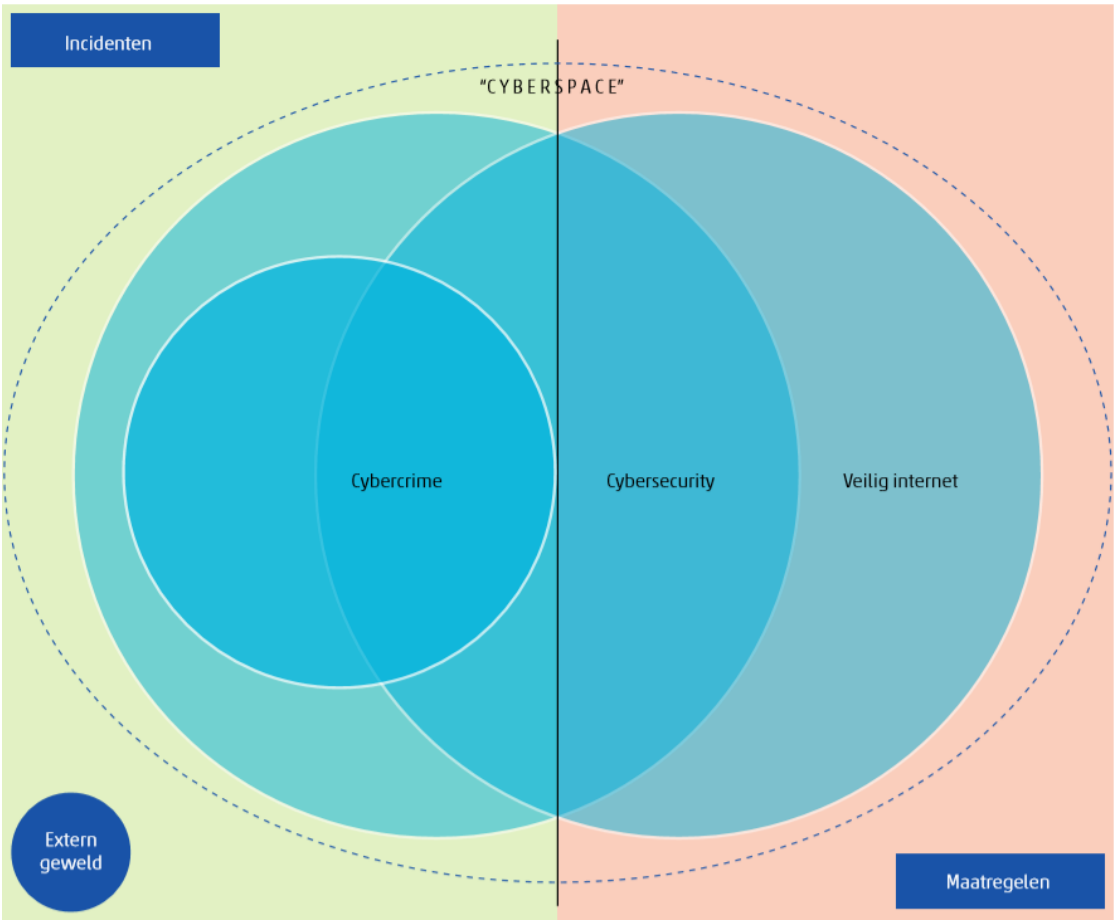
Ook het CBS schetst sinds 2017 een beeld van de situatie op het gebied van cybersecurity in Nederland met de jaarlijkse Cybersecuritymonitor.[32] Het doel van deze monitor is het rapporteren over de meest actuele stand van zaken over de cyberweerbaarheid van *bedrijven en huishoudens* in Nederland, waarin incidenten en maatregelen worden beschreven. Zoals al aangegeven houdt CBS dezelfde definitie aan als het CSBN. De uitleg van CBS van deze definitie geeft wel extra context: met name in de Cybersecuritymonitor 2018 wordt uitgebreid stilgestaan bij de definitiekwestie. Zij gebruiken het volgende 'contextdiagram', zie Figuur 4.

[29] Deze wet regelt een meldplicht van incidenten en een zorgplicht (treffen van beveiligingsmaatregelen).

[30] Hierin zijn maatregelen bijeengebracht die moeten leiden tot een aanzienlijke verbetering van de digitale veiligheid van hard- en software.

[31] Cybersecurity predictions for 2019, CSO Online, https://www.csoonline.com/article/3322221/security/9-cyber-security-predictions-for-2019.html; Prospects for cybersecurity in 2019, Oxford Analytica.

[32] De Cybersecuritymonitor wordt uitgebracht op verzoek van het Ministerie van Economische Zaken en Klimaat. Cijfers zijn afkomstig uit de CBS enquête 'ICT-gebruik bedrijven 2018'.



Figuur 4. Contextdiagram cybersecurity. Bron: CBS Cybersecuritymonitor 2018.

Cybercrime betreft alle moedwillige en strafbare gepleegde cyberdelicten en kent daarmee overlap met de definitie van cybersecurity. *Cybersecurity* is echter breder. Er vinden immers ook incidenten plaats die onbedoeld zijn of niet strafbaar zijn, zoals het tijdelijk uitvallen van een systeem door een verkeerde software-installatie of het onbedoeld lekken van vertrouwelijke gegevens door slordig omgaan met usb-sticks. Daarnaast omvat cybersecurity volgens het CBS ook nadrukkelijk alle preventieve maatregelen van burgers, bedrijven en organisaties om hun ICT-systemen minder kwetsbaar te maken. Die kunnen ICT-technische maatregelen nemen, maar ook organisatorische, procedurele en personele maatregelen. De focus bij cybersecurity ligt echter wel bij de ICT-systemen zelf: het beschermen van de ICT-systemen en de daarin opgeslagen informatie tegen misbruik. Het begrip *cyberspace* geeft vooral aan dat het speelveld van cybercrime en cybersecurity meer is dan het 'zichtbare' internet. Men kan hier bijvoorbeeld ook aan bedrijfsnetwerken denken. Dreigingen kunnen ook van buiten cyberspace komen, bijvoorbeeld elektriciteitsuitval of het wegvallen of in brand steken van zendmasten. De gevolgen zijn hetzelfde als bij een DDoS-aanval, namelijk dat de dienst tijdelijk niet beschikbaar is. Tot slot is er *veilig internet*. Het betreft vooral het sentiment rondom het internet dat ervoor zorgt dat burgers, bedrijven en organisaties bepaald internetgebruik bewust beperken, bijvoorbeeld ouders die maatregelen nemen om hun kinderen te vrijwaren van onwelgevallige content of privacy-zorgen met betrekking tot bepaalde bedrijven.

De eerdergenoemde CSBN definitie ("*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*") spreekt verder ook over *maatregelen*, en we kunnen deze definitie alleen goed begrijpen als we een concreet beeld hebben van deze maatregelen.

Incidenten en maatregelen omtrent cybersecurity worden in de jaarlijkse cybersecuritymonitor van het CBS beschreven. Deze zijn:[33]

- Antivirussoftware;
- Beleid voor sterke wachtwoorden;
- Authenticatie via soft- of hardware-token;
- Encryptie voor het opslaan van data;
- Encryptie voor het versturen van data;
- Gegevens op andere fysieke locatie;
- Network access control;
- Virtueel Particulier Netwerk of Virtueel Privénetwerk (VPN) bij internetgebruik buiten eigen bedrijf;
- Logbestanden voor analyse incidenten;
- Methodes voor beoordelen ICT-veiligheid;
- Risicoanalyses;
- Andere maatregelen.

Over het algemeen geldt dat het ICT-beveiligingsniveau van een bedrijf hoger is naarmate er meer maatregelen genomen worden. Het CBS concludeert dat grote bedrijven beter scoren dan kleine bedrijven.[34] Ook scoren bedrijven die meer met ICT bezig zijn (zoals de ICT-sector) of bedrijven die een groot belang hebben bij het veilig houden van hun data (zoals in de gezondheidszorg) beter dan sectoren waar cybersecurity een minder belangrijke rol speelt of waar men denkt dat het een minder belangrijke rol speelt (zoals in de horeca). Wel wordt geconstateerd dat middelgrote bedrijven een behoorlijke inhaalslag hebben gemaakt door het invoeren van *two factor* authenticatie (zoals authenticatie via een soft- of hardware-token). Ook het tijdig uitvoeren van security-updates is een goede indicator van het cybersecurityniveau van een bedrijf. De meeste grote en middelgrote bedrijven hebben een security-updatebeleid.

Het DTC, gericht op niet-vitale sectoren, heeft vijf basisprincipes opgesteld voor veilig digitaal ondernemen die gelden als gids om de basale digitale veiligheidsmaatregelen op orde te krijgen (‘Basisscan’). Deze principes zijn:[35]

1. *Inventariseer kwetsbaarheden. Inventariseer de ICT-onderdelen, kwetsbaarheden en maak een risicoanalyse. Bij risico's kijk je naar beschikbaarheid, integriteit en vertrouwelijkheid.*
2. *Kies veilige instellingen. Controleer de instellingen van apparatuur, software en netwerk- en internetverbindingen. Pas standaardinstellingen aan en kijk kritisch naar functies en diensten die automatisch 'aan' staan.*
3. *Voer updates uit. Controleer of apparaten en software up-to-date zijn. Installeer beveiligingsupdates direct. Schakel automatische updates in zodat je apparaten en software voortaan altijd draaien op de laatste versie.*
4. *Beperk toegang. Definieer per medewerker tot welke systemen en data toegang vereist is om te kunnen werken. Zorg dat toegangsrechten worden aangepast als iemand een nieuwe functie krijgt of bij de onderneming vertrekt.*
5. *Voorkom virussen en andere malware. Er zijn 4 manieren om malware te voorkomen: Stimuleer veilig gedrag van medewerkers, gebruik een antivirusprogramma, download apps veilig en beperk de installatiemogelijkheden van software.*

---

[33] CBS Cybersecuritymonitor 2019.

[34] CBS Cybersecuritymonitor 2019.

[35] Website DTC

Deze basisprincipes en de achterliggende informatie zijn vooral gericht op het MKB en ZZP'ers. De grotere, meer *cybermature* bedrijven hebben andere behoeften op het gebied van cybersecurity (zie paragraaf 4.4).

2.2 Andere definities van cybersecurity

Het domein van cybersecurity is relatief jong en kent veel dynamiek, en de in de vorige paragraaf besproken definitie van CSBN is zeker niet de enige van het begrip cybersecurity. De definities zijn doorgaans ook afhankelijk van de context, organisatie of land.[36,37,38] Het CBS concludeert eveneens 'dat er geen eensluidende definitie van cybersecurity en aanverwante begrippen bestaat'.

Niet alleen het begrip 'cybersecurity', maar ook soortgelijke begrippen of beschrijvingen komen voor. Zo kiest VNG voor: *"Veiligheid met een digitaal component is de verbinding tussen de digitale en fysieke wereld waarin de digitale wereld zich op een dergelijke manier organiseert of manifesteert wat impact kan hebben op de openbare orde en veiligheid in de fysieke wereld."* Het Britse National Cyber Security Centre (Britse NCSC[39]) gebruikt een meer uitgeklede definitie; *"Cybersecurity is de manier waarop individuen en organisaties het risico op een cyberaanval verminderen".* De Bundesamt für Sicherheit in der Informationstechnik (BSI), de partij die grotendeels verantwoordelijk is voor cybersecurity in Duitsland (zie ook Bijlage 2), handelt aan de hand van *security of information technology*. Dit zien zij als *het nemen van bepaalde veiligheidsnormen voor de beschikbaarheid, integriteit of vertrouwelijkheid van informatie door middel van veiligheidsmaatregelen in of voor het gebruik van informatietechnologiesystemen, -componenten of -processen*.

Vele andere partijen laten zich überhaupt niet uit over de definitie van cybersecurity of een soortgelijke term. Op websites en bijvoorbeeld in rapporten geven ze aan wat je kunt doen (of wat zij voor je kunnen doen) om cyber secure te zijn, maar er wordt niet aangegeven wat zij daaronder verstaan. Het gebrek aan een gedeelde definitie van cybersecurity zorgt voor een relatief langzaam samenwerkingsproces tussen verschillende partijen en landen en maakt het lastiger om tot (internationale) afspraken te komen.

2.3 Doelen die het kabinet wil bereiken met cybersecurity-beleid

In de Nederlandse Cyber Security Agenda (NCSA) uit 2018 worden de kaders gesteld voor de volgende, noodzakelijk geachte stap in cybersecurity. De NCSA bouwt voort op de effecten die gerealiseerd zijn bij de eerdere Nationale Cybersecurity strategieën uit 2011 en 2013, en valt uiteen in zeven ambities die bijdragen aan de volgende doelstelling: "*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*." De ambities zijn als volgt:[40]

1. Nederland heeft zijn digitale slagkracht op orde.
2. Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein.

---

[36] PWC (2017) Cybersecurity Industry Market Analysis. VR 2017 Methodology Excerpt – Taxonomy. ECSO.

[37] Meulen, N van der (2015) Investeren in Cybersecurity. RAND Europe, in opdracht van WODC.

[38] CBS (2018) Cybersecuritymonitor 2018. Een verkenning van dreigingen, incidenten en maatregelen. CBS: Den Haag, p. 13.

[39] Omdat deze organisatie dezelfde korting heeft als de Nederlandse NCSC, korten we deze organisatie in dit rapport af tot 'Britse NCSC'.

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

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.

In deze Agenda heeft de minister van Justitie en Veiligheid deze ambities gepresenteerd voor Nederland als geheel, waarbij publiek-private samenwerking als uitgangspunt geldt. In een kamerbrief van 12 juni 2019[41] benadrukt de minister nogmaals dat voor alle vitale sectoren wordt ingezet op structurele en adaptieve risicobeheersing. Hiermee wordt invulling gegeven aan ambitie 7 van de NCSA om de regie op de kabinetsbrede aanpak te versterken. Het betekent:

1. Awareness – bewustwording van de risico's en het noodzakelijke niveau van de digitale weerbaarheid worden vergroot;
2. Beheersmaatregelen en toezicht – de digitale weerbaarheid wordt structureel verhoogd en het toezicht wordt versterkt;
3. Oefenen en testen – inzicht in de effectiviteit van genomen maatregelen;
4. Regie en interventie – partijen nemen hun verantwoordelijkheid en waar nodig wordt ingegrepen.

De overheid en vitale bedrijven hebben hier een gedeeld belang vanuit de continuïteit van de dienstverlening. De niet-vitale sectoren zijn geen directe doelgroep van het Ministerie van Justitie en Veiligheid (JenV), maar vallen onder de hoede van het Ministerie van Economische Zaken en Klimaat (EZK). Om te zorgen dat ondernemers in de niet-vitale sector digitaal weerbaar zijn en hun digitale veiligheid op orde hebben heeft het ministerie van EZK het Digital Trust Center (DTC) opgericht. Het kabinet als geheel werkt toe naar een landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden (ambitie 1 uit de NCSA). Met de oprichting van het DTC, in begin 2018, is een informatieknooppunt ingericht voor het niet-vitale bedrijfsleven. Het DTC en het NCSC werken (in theorie) nauw samen om zo veel als mogelijk informatie te ontsluiten ter verhoging van de cyberweerbaarheid van de onderscheidenlijke doelgroepen. Het DTC helpt daarnaast bij de oprichting van cybersecurity samenwerkingsverbanden tussen bedrijven. Voor alle partijen geldt dus het doel: digitale slagkracht verbeteren.[42]

2.4 Samenvattende conclusie

We sluiten dit hoofdstuk af met een korte samenvatting, gestructureerd langs de deelvragen die in dit hoofdstuk centraal staan.

Deelvraag 1: Uit welke aspecten bestaat cybersecurity volgens de definitie uit de CSBN 2019? En is deze anders voor en/of volgens de verschillende partijen (overheid, private vitale en niet vitale partijen)?

> 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

[41] Kamerbrief Beleidsreactie CSBN2019 en voortgangsrapportage NCSA (12 juni 2019).

[42] Voortgang Nederlandse Cybersecurity Agenda. Bijlage bij kamerbrief (18 juni 2019).

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 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.*"[43]

Deelvraag 2: Welke doelen wil het kabinet voor deze partijen met cybersecurity bereiken?

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:[44]

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.

[43] CSBN 2020, p. 48.

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

3 Het Nederlandse stelsel en de (on)mogelijkheden bij informatie-uitwisseling

In dit hoofdstuk bespreken we de partijen en informatiestromen in het Nederlandse cybersecuritystelsel, gevolgd door de juridische context en beperkingen bij informatie-uitwisseling tussen deze partijen. Het hoofdstuk sluit af met een vergelijking van Nederland met de cybersecuritystelsels in de geselecteerde andere landen en een conceptuele vergelijking tussen het centralistische model en een netwerkbenadering. Deelvragen die in dit hoofdstuk worden beantwoord:

Deelvraag 3: Hoe is de huidige situatie van samenwerkingsverbanden en mogelijkheden van informatie-uitwisseling tussen overheid (NCSC, politie, DTC, e.a.) en private, niet vitale partijen op het gebied van cybersecurity ingericht? Hoe ziet een visuele weergave van het cybersecurity ecosysteem (in Nederland) eruit?

Deelvraag 4: Wat houdt informatie-uitwisseling en samenwerking over cybersecurity in, in de huidige situatie en welke aspecten van cybersecurity bevat deze en welke nog niet?

Deelvraag 9: Hoe is in enkele andere landen het stelsel van cybersecurity tussen publieke en private partijen ingericht, en wat kan Nederland daarvan leren?

3.1 Het Nederlandse stelsel

3.1.1 Een dynamisch ecosysteem

Het Nederlandse cybersecuritystelsel is een ecosysteem met vele partijen die in contact staan met enkele meer centrale partijen. Op hoofdlijnen is er de splitsing vitaal/niet-vitaal, met respectievelijk het NCSC en het DTC als centrale partijen. Via vele andere organisaties breidt het netwerk zich uit tot aan individuele bedrijven en burgers.[45] Hieronder lichten wij dit toe.

De NCTV staat *beleidsmatig* aan de wieg van het landelijk dekkend stelsel.[46] Onder diens coördinatie zijn o.a. rondetafelgesprekken georganiseerd en is verder uitgedacht hoe het landelijk dekkend stelsel van cybersecurity-samenwerkingsverbanden vorm kan krijgen. Het Ministerie van Justitie en Veiligheid is de coördinerende entiteit binnen dit stelsel. De NCTV voert deze coördinerende taak namens het ministerie uit.

De *uitvoering* van het landelijk dekkend stelsel is binnen de Rijksoverheid verder opgedeeld. Daarmee heeft Nederland een unieke decentrale vormgeving van politiek-bestuurlijke krachten. Op hoofdniveau is er (a) het NCSC voor de Rijksoverheid en private, vitale partijen[47] en

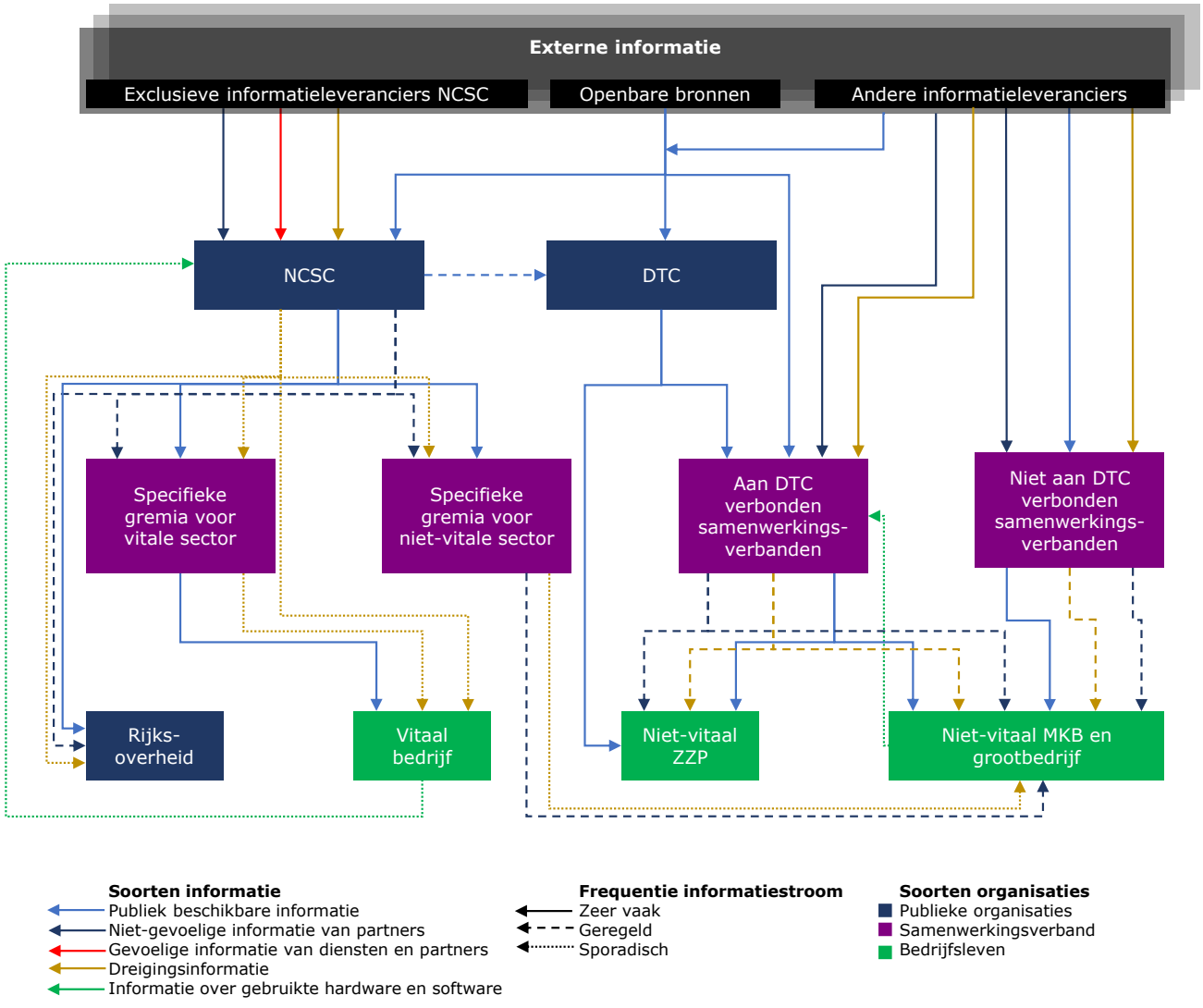
[45] Zie ook de NCSA, p. 19: "Zo werken we toe naar een cyber-ecosysteem waarin alle partijen capaciteiten opbouwen en informatie delen; van bedrijfsleven tot overheid en van burger tot informatiebeveiliger."

[46] NCSA, p. 19.

[47] Vitale sectoren zijn energie, telecommunicatie/ICT, drinkwater, voedsel, gezondheid, financieel, keren en beheren oppervlaktewater, openbare orde en veiligheid, rechtsorde, openbaar bestuur, transport en chemische en nucleaire industrie (bron: BZK, via IFV.nl).

(b) het DTC voor private, niet-vitale partijen. Daarnaast zijn er tal van andere relevante spelers, initiatieven en samenwerkingsverbanden. Er wordt op een veelheid aan onderwerpen geïnnoveerd en per onderwerp ontstaan specifieke samenwerkingsverbanden. Daardoor zijn er meerdere samenwerkingsverbanden ontstaan en komen er steeds nieuwe bij. Zo ontstaan er natuurlijke hubs rondom bedrijven en universiteiten en zijn er 'kunstmatige' hubs waar bepaalde kennisdeling wordt gestimuleerd. Een werkend regionaal of sectoraal stelsel ontstaat alleen als er voldoende initiatief is in de regio of sector. Zodoende betreft de huidige situatie van samenwerkingsverbanden en mogelijkheden van informatie-uitwisseling een dynamisch ecosysteem dat nog volop in ontwikkeling is.

Figuur 5 presenteert een schets van dit ecosysteem. In de niet-vitale kant van het stelsel zijn enkel private partijen opgenomen. Publieke, niet-vitale partijen (overheidsorganisaties die geen onderdeel uitmaken van de Rijksoverheid) zijn in dit onderzoek niet meegenomen en daarom niet opgenomen in de figuur. In de volgende paragrafen gaan we nader in op de in de figuur genoemde partijen en informatiestromen.



Figuur 5. Nederlandse cybersecurity ecosysteem en de belangrijkste informatiestromen daarbinnen

3.1.2 Typen informatie

Om de (on)mogelijkheden van informatie-uitwisseling in het stelsel te kunnen bespreken onderscheiden we verschillende typen informatie. Dit onderscheid kan op twee dimensies gemaakt worden: inhoudelijk en juridisch.

Inhoudelijk onderscheid

De eerste dimensie is inhoudelijk, en betreft het onderscheid tussen voorlichtingsinformatie en dreigingsinformatie.

Voorlichtingsinformatie betreft algemene informatie die organisaties kunnen gebruiken om hun cyberweerbaarheid te vergroten. Men kan hierbij denken aan algemene beveiligingsadviezen, factsheets en whitepapers. De informatie komt vaak uit openbare bronnen en wordt veelal verspreid door het DTC en brancheverenigingen die dergelijke onderwerpen onder de aandacht brengen van hun leden. Vanuit het DTC wordt informatie met name in de vorm van nieuwsberichten gedeeld. Daarnaast biedt het DTC ook een Basisscan Cyberweerbaarheid aan voor bedrijven waarin bedrijven bewust worden gemaakt van hun eigen cyberweerbaarheid. De focus van deze scan ligt vooral op het kleinbedrijf/ZZP.

Dreigingsinformatie is een term die veel gebruikt wordt, maar waar geen standaarddefinitie van is. Hetzelfde geldt voor verwante termen als risico-informatie of slachtofferinformatie. In dit rapport hanteren wij de volgende definitie en categorieën:

Met *dreigingsinformatie* wordt gedoeld op concrete informatie over dreigingen die zeer specifiek worden gericht op bepaalde partijen, of waar bepaalde partijen of systemen kwetsbaar voor zijn. Hierin worden de gegevens van (potentiële) slachtoffers (*slachtofferinformatie*), daders (*daderinformatie*) of systemen vermeld, bijvoorbeeld in de vorm van IP-adressen.[48] Dit soort informatie komt in de meeste gevallen uit niet-openbare bronnen. ICT-platformen als het Dutch Institute for Vulnerability Disclosure (DIVD) zijn bijvoorbeeld opgezet door vrijwilligers en zetten zelf onderzoekers in om het internet te scannen op kwetsbaarheden. Die informatie wordt onder andere beschikbaar gesteld aan netwerkbeheerders.

Juridisch onderscheid

De tweede dimensie waarop onderscheid tussen typen informatie kan worden gemaakt is op basis van de juridische beperkingen aan het delen van de informatie. Ten eerste is er informatie die vrijelijk te delen is; ten tweede zijn er persoonsgegevens, die vanwege de AVG[49] niet zomaar gedeeld mogen worden; ten derde is er, specifiek voor het verstrekken van informatie door het NCSC, herleidbare[50] vertrouwelijke informatie. Informatie in deze laatste categorie mag vanwege de Wbni[51] slechts zeer beperkt door het NCSC aan andere partijen worden verstrekt. De tweede en derde categorie kennen een overlap: persoonsgegevens kunnen ook vertrouwelijk herleidbaar in de zin van de Wbni zijn en vice versa.

Discussies over het delen van informatie worden bemoeilijkt doordat ook de twee genoemde dimensies overlappen. Voorlichtingsinformatie is altijd vrijelijk te delen, maar dreigingsinformatie valt meestal in de tweede of derde categorie, en mag daardoor meestal niet zomaar

---

[48] De IP in IP-adres staat voor Internet Protocol. Het is een techniek die gebruikt wordt om computers in een netwerk (zoals het internet) met elkaar te laten communiceren.

[49] Algemene Verordening Gegevensbescherming, de belangrijkste Europese privacywet.

[50] Herleidbaar in deze context wil zeggen dat de identiteit van het bedrijf kan worden vastgesteld.

[51] Wet beveiliging netwerk- en informatiesystemen.

gedeeld worden.[52] Onderstaande tabel geeft weer welke combinaties van typen informatie gebruikelijk zijn. In paragraaf 3.2 wordt de juridische context van informatie-uitwisseling uitgebreid behandeld.

Tabel 1. Overzicht van typen informatie, onderscheiden op de twee dimensies.

	Informatie die persoonsgegevens noch herleidbare vertrouwelijke informatie bevat	**Persoonsgegevens**	**Herleidbare vertrouwelijke informatie**
Voorlichtingsinformatie	Zeer gebruikelijk	Komt niet voor	Komt niet voor
Dreigingsinformatie	Minder gebruikelijk	Gebruikelijk	Gebruikelijk

3.1.3 Het NCSC voor de Rijksoverheid en de vitale sector

Zoals eerder al benoemd is het NCSC de centrale partij voor de informatie-uitwisseling voor zover het de cybersecurity van de rijksoverheid en de vitale sector betreft. Dreigingsinformatie die persoonsgegevens of herleidbare vertrouwelijke gegevens bevat wordt door het NCSC zelf doorgezet naar de organisaties op wie de dreiging betrekking heeft, voor zover zij binnen de vitale sector of de rijksoverheid vallen. Het NCSC heeft een database met IP-adressen van al deze partijen, zodat het weet op welke partij(en) bepaalde dreigingsinformatie betrekking heeft (dreigingsinformatie bevat vaak immers IP-adressen). Het is onmogelijk deze database continu 100% compleet en correct te houden; bedrijven kunnen immers nieuwe IP adressen in gebruik nemen en nalaten dat te melden bij het NCSC. Toch is deze kant van het stelsel, juist vanwege deze database, over het algemeen goed dekkend.

Daarnaast verwerkt het NCSC ook voorlichtingsinformatie en dreigingsinformatie die voor iedereen raadpleegbaar is. NCSC publiceert deze informatie op zijn website en verspreidt het via mailings. Vaak is deze informatie ook te vinden op de databank Common Vulnerabilities and Exposures (CVE).[53]

3.1.4 Het DTC voor de niet-vitale sector

Het DTC bedient alle niet-vitale bedrijven. Deze kant van het stelsel heeft meer spelers en de informatie-uitwisseling is hier over het algemeen minder ver ontwikkeld dan aan de vitale kant van het stelsel. Het DTC is een relatief jonge organisatie en is recent geëvalueerd.[54] In deze evaluatie wordt geconcludeerd: *"Het DTC heeft in korte tijd een organisatie opgezet die zich met een klein team richt op de doelgroep van 1,8 miljoen niet-vitale bedrijven in Nederland. Het DTC heeft een bijdrage geleverd aan de cyberweerbaarheid van ondernemend Nederland door informatie en advies te geven (hoofdtaak 1) en door samenwerkingsverbanden te stimuleren (hoofdtaak 2)."*

[52] Ook bestaat er herleidbare vertrouwelijke informatie die geen dreigingsinformatie is, maar in de context van informatie-uitwisseling binnen het geschetste ecosysteem is deze subset minder relevant.

[53] 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.

[54] Kwink groep (2020). Evaluatie programma Digital Trust Center.

Het DTC neemt een belangrijke plaats in binnen het cybersecuritystelsel en is het aanspreekpunt voor de overgrote meerderheid van de Nederlandse bedrijven. Daarbij moet wel een kanttekening worden gemaakt, namelijk dat het DTC zich nog hoofdzakelijk bezighoudt met voorlichtingsinformatie en dat de ontwikkelde producten vooral gericht zijn op ZZP'ers en MKB's. Grotere niet-vitale bedrijven hebben echter vooral behoefte aan andere informatie, zoals actuele dreigingsinformatie.[55,56] Het DTC kan dreigingsinformatie momenteel echter slechts zeer beperkt verstrekken, doordat het DTC nog geen wettelijke grondslag heeft om persoonsgegevens te verwerken. In paragraaf 3.2 gaan we hier verder op in.

Zolang geen persoonsgegevens verwerkt mogen worden zet het DTC vooral in op voorlichtingsinformatie (zoals de basisscan op de website ter voorlichting voor bedrijven) en op het stimuleren van samenwerkingsverbanden voor de niet-vitale sector. Dit laatste gebeurt onder andere door samenwerking met brancheorganisaties, platforms en kennisinstituten. In deze samenwerkingsverbanden werken ondernemers samen met andere organisaties aan het vergroten van de cyberweerbaarheid, binnen en tussen de niet-vitale branches, sectoren en regio's. Dit zijn de 'aan DTC verboden samenwerkingsverbanden' in Figuur 5. Alle samenwerkingsverbanden die momenteel (2020) zijn aangesloten bij het DTC, zijn weergegeven in Tabel 2.[57]

[55] Kwink groep (2020). Evaluatie programma Digital Trust Center.

[56] Het DTC stuurt incidenteel wel (openbare) dreigingsinformatie door naar samenwerkingsverbanden, in aanvulling op de wekelijkse nieuwsbrief.

[57] https://www.digitaltrustcenter.nl/samenwerkingsverbanden

Tabel 2. Overzicht van bij DTC aangesloten samenwerkingsverbanden (is met subsidie, de subsidies van 2020 zijn nog niet bekend). Bron: DTC (september 2020).*

Samenwerkingsverband/brancheorganisatie	Sector	Regio
NIDV Cyberweerbaarheid DVI*	Defensie	Heel Nederland
Thuiswinkel.org	E-commerce	Heel Nederland
Adfiz (branchevereniging van onafhankelijk financieel adviseurs)	Financieel	Heel Nederland
Cyber Security Programma Noordzeekanaalgebied* FERM Rotterdam Port Cyber Resilience*	Haven	West-Nederland
NPAL	(Hightech) Industrie	Noord-Nederland
Cybersecurity Centrum voor de Maakindustrie*		Oost-Nederland
Cyber Weerbaarheidscentrum Brainport (CWB)*		Zuid-Nederland
HI Cybersecurity Network		Heel Nederland
Nationale Beheersorganisatie Internet Providers (NBIP)	IT	Heel Nederland
Vergroting cyberweerbaarheid groentezaadveredelingsbedrijven*	Landbouw	Heel Nederland
CYSSEC (Cybersecurity Synergie Schiphol Ecosysteem)*	Luchtvaart	Heel Nederland
Groep Educatieve Uitgeverijen (GEU)*	Onderwijs	Heel Nederland
Federatie van technologiebranches (FHI) Verhogen cyberweerbaarheid Beveiligingsinstallaties	Techniek	Heel Nederland
NuBNO - De 8e disbalans	Zorg	Zuid-Nederland
Z-Cert	Zorg	Heel-Nederland
Noord Holland Samen Veilig Stichting Cyberweerbaarheid Noord-Nederland*	n.v.t.	Noord-Nederland
Cyberweerbaarheid in Limburg* Cyber Netwerk Drechtsteden*	n.v.t.	Zuid-Nederland
Agrifood cyberweerbaarheid Connect2trust Cyberchain Cybernetwerk Zuid-Hollandse Eilanden Cyberweerbaarheid in de agrarische sector Havenbedrijf Rotterdam (FERM) MKB Cyber Heroes Platform Zelfstandige Ondernemers (PZO) Transport en Logistiek Nederland	n.v.t.	Heel Nederland

Het DTC maakt onderscheid tussen drie soorten samenwerkingsverbanden:[58]

- Samenwerkingsverbanden met een DTC-subsidie;
- Samenwerkingsverbanden zonder DTC-subsidie;
- Information Sharing and Analysis Centers (niet-vitale ISAC's). Een ISAC is een vrijwillige samenwerking tussen partijen in een bepaalde sector met als doel het vertrouwelijk delen van informatie en analyses over dreigingen, incidenten, kwetsbaarheden, maatregelen en leerpunten.[59] In het Jaarwerkplan 2019 van

[58] DTC (2019). Jaarwerkplan 2019, p. 12.

[59] Kamerstukken 26643, nr. 560.

het DTC staat dat een aantal niet-vitale ISAC's worden overgedragen vanuit het NCSC aan het DTC, namelijk de ISAC Pensioenen, ISAC Verzekeraars, ISAC Media en ISAC Legal.[60] De overdracht is nog in ontwikkeling.

De meeste samenwerkingsverbanden (brancheorganisaties uitgezonderd) hebben tussen de 2 en 15 deelnemers.[61] Het DTC faciliteert deze verbanden door het verstrekken van informatie en adviezen, door het faciliteren van productontwikkeling en kennisdeling, en door middel van subsidieverstrekking. Uit de eerdergenoemde evaluatie bleek dat de ondersteuning van het DTC grotendeels aansluit bij de behoefte van de samenwerkingsverbanden.[62] Het DTC monitort of evalueert echter niet de *effecten* van de activiteiten van de samenwerkingsverbanden. Uit cijfers van het CBS [63] blijkt wel dat bedrijven die zich hebben aangesloten bij een samenwerkingsverband van het DTC, bewuster met ICT-veiligheid om lijken te gaan dan vergelijkbare bedrijven. In hoeverre dat toe te schrijven is aan het DTC is echter niet duidelijk.

3.1.5 Uitwisseling tussen vitaal en niet-vitaal

Informatie-uitwisseling tussen de beide kanten van het landelijke stelsel is een belangrijke stap in de richting van een landelijk dekkend stelsel. Momenteel is het vooral de niet-vitale kant die behoefte heeft aan (dreigings)informatie waar het NCSC over beschikt, maar ook de vitale sector kan baat hebben bij informatie die van de niet-vitale kant van het stelsel vandaan komt, zeker wanneer informatie-uitwisseling binnen de niet-vitale kant in de toekomst verder is ontwikkeld. Uitwisseling van voorlichtingsinformatie tussen het NCSC en het DTC gebeurt al, en ook niet-vitale bedrijven zelf kunnen voorlichtingsinformatie van het NCSC bekijken, maar uitwisseling van dreigingsinformatie is tot nu toe problematisch.

Het NCSC beschikt regelmatig over dreigingsinformatie die betrekking heeft op niet-vitale bedrijven, zogenaamde restinformatie.[64] Het NCSC mag deze partijen in principe echter niet direct benaderen (zie paragraaf 3.2) en kan dit meestal ook niet eens. Het NCSC kan zelf namelijk de IP-adressen niet koppelen aan partijen in de niet-vitale sector. In plaats daarvan zou deze dreigingsinformatie van het NCSC via bepaalde organisaties, namelijk de zogenaamde OKTT's en aangewezen computercrisisteams, bij de betreffende niet-vitale partijen terecht moeten komen.[65] Dit zijn de 'specifieke gremia voor de niet-vitale sector' uit Figuur 5. Hieronder staan deze toegelicht.

---

[60] Zie ook de Kamerbrief van 17 juni 2019.

[61] Uitschieters: Cyber Weerbaarheidscentrum Brainport staat open voor alle organisaties in de Hightech Industrie in Nederland en aan Noord Holland Samen Veilig nemen 34 gemeenten, politie en het OM deel.

[62] Kwink groep (2020). Evaluatie programma Digital Trust Center.

[63] Statistiek ICT-gebruik bedrijven 2019.

[64] 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.

[65] Dat dit de bedoeling is, is niet enkel een opvatting van gesprekspartners en van de onderzoekers, maar blijkt ook uit art. 3(2) Wbni.

OKTT's en computercrisisteams

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. Over het algemeen zijn OKTT's samenwerkingsverbanden. Er wordt ook wel gesproken van organisaties met 'OKTT-status'. OKTT's mogen dreigingsinformatie met persoonsgegevens ontvangen van het NCSC. Er zijn momenteel drie OKTT's:

- De NBIP (Nationale Beheersorganisatie Internet Providers)
- Het Cyberweerbaarheidscentrum Brainport
- De Abuse Information Exchange (ook wel AbuseHub)

Een **computercrisisteam** is een gespecialiseerd team van professionals dat snel kan handelen bij beveiligingsincidenten met computers of netwerken. Sommige computercrisisteams zijn ontstaan uit samenwerkingsverbanden, andere zijn opgezet voor een enkel (groot) bedrijf. Vaak kent een computercrisisteam een sectorspecifieke focus. Als een computercrisisteam als zodanig is aangewezen, bij ministeriële regeling, mag het dreigingsinformatie met persoonsgegevens en herleidbare vertrouwelijke informatie ontvangen van het NCSC. Er zijn momenteel vier aangewezen computercrisisteams:[66]

- De IBD (Informatiebeveiligingsdienst van de VNG)
- Het Z-CERT (voor de zorg)
- Het SURFcert (voor onderwijs- en onderzoeksinstellingen)
- Het CERT Watermanagement

Box 1. Toelichting OKTT's en computercrisisteams.

De beoogde informatiestroom van NCSC naar niet-vitale partijen via OKTT's is in de praktijk nog vrij beperkt, al wordt er wel informatie doorgezet. Op hoofdlijnen heeft dit twee oorzaken:

- Er zijn pas drie OKTT's. Uit onze interviews blijkt dat dit komt doordat veel samenwerkingsverbanden geen AVG-compliance kunnen bewijzen of onvoldoende handelingsperspectief aan de te ontvangen informatie kunnen bieden.
- Ook na het verkrijgen van een OKTT-status zijn er soms nog juridische barrières. Deze hebben zowel te maken met de AVG als met het verbod op het delen van herleidbare vertrouwelijke gegevens uit de Wbni. In paragraaf 3.2 komt dit verder aan de orde.

Dat veel samenwerkingsverbanden geen dreigingsinformatie van het NCSC kunnen ontvangen, leidt ertoe dat zij soms buiten het Nederlandse cybersecuritystelsel gaan kijken voor de noodzakelijke informatie. Voor een deel zouden zij dit toch al doen, maar een van de gesproken samenwerkingsverbanden noemt het gebrek aan informatie van het NCSC als specifieke reden om buitenlandse partijen op te zoeken. Uit onze interviews bleek dat samenwerkingsverbanden eigen meldpunten voor cybersecurity-incidenten opzetten (vaak opgezet door vrijwilligers)[67], zelf publieke informatie ophaalden, of samenwerking aangingen

[66] Staatscourant 2020 nr. 4410 24 januari 2020.

[67] Zoals het Nederlands Security Meldpunt, DIVD en het Abuse platform.

met buitenlandse instellingen die vergelijkbaar zijn met NCSC. Deze stappen lossen de informatietekorten deels op, maar zorgen ook voor verdere fragmentatie van het cybersecuritylandschap.

Het DTC mag momenteel enkel dreigingsinformatie zonder persoonsgegevens van het NCSC ontvangen. Er wordt echter gewerkt aan een sterkere wettelijke grondslag voor het DTC, waarmee het DTC onder andere dreigingsinformatie met persoonsgegevens zou kunnen verwerken, en aan het aanwijzen van het DTC als OKTT. Als dit rond is, zijn de belangrijkste obstakels weggenomen om dreigingsinformatie van het NCSC door te zetten naar het DTC (zie paragraaf 3.2.). Het is daarom goed denkbaar dat het DTC in de toekomst deze dreigingsinformatie wel zal ontvangen, om deze vervolgens zowel direct als via de vele samenwerkingsverbanden door te zetten naar de betreffende niet-vitale bedrijven. Op dit moment heeft het DTC daar nog niet de faciliteiten of capaciteit voor, maar er wordt ondertussen ook gewerkt aan de praktische kant van het doorzetten van deze informatie, zoals het opzetten van een informatiedienst die gefaseerd zal worden ingezet en uitgebreid.

3.2 Juridische context en beperkingen bij informatie-uitwisseling

De beperkingen met betrekking tot informatie-uitwisseling in het Nederlandse stelsel zijn in grote mate juridisch van aard. In deze paragraaf gaan wij daarom dieper in op de juridische context en de huidige en potentiële juridische obstakels bij informatie-uitwisseling. De focus ligt daarbij op het verwerken[68] van informatie door de twee centrale partijen in het stelsel: het NCSC en het DTC.

3.2.1 Dreigingsinformatie

Wanneer het gaat om het uitwisselen van dreigingsinformatie is meestal sprake van grote datasets. Het gaat dan bijvoorbeeld om een dataset met alle IP-adressen die onderdeel zijn van een lek, of die kwetsbaar zijn omdat ze bepaalde diensten of software hebben gebruikt. Veelal bevatten deze datasets niet alleen IP-adressen die tot bedrijven zijn te herleiden, maar ook IP-adressen die tot individuen zijn te herleiden. Uit het Brever-arrest blijkt dat een IP-adres van een individu al snel als persoonsgegeven[69] moet worden beschouwd, waardoor deze aan juridische beperkingen onderhevig is.[70] Omdat niet op voorhand duidelijk is welke gegevens in een dataset persoonsgegevens zijn en welke niet (men weet op voorhand niet welke IP-adressen naar individuen leiden), moet bijgevolg de hele dataset behandeld worden alsof deze persoonsgegevens bevat. Dit is de voornaamste reden dat het delen van dreigingsinformatie aan juridische beperkingen onderhevig is. De AVG bepaalt namelijk dat persoonsgegevens niet worden verwerkt zonder grondslag, ook niet door overheidsorganisaties.

Zowel voor het NCSC als voor het DTC betekent dit dat in principe een wettelijke basis nodig is om persoonsgegevens te mogen verwerken: zij mogen enkel persoonsgegevens verwerken voor zover dat noodzakelijk is om de taken van algemeen belang of openbaar gezag uit

---

[68] Wij gebruiken het begrip 'verwerken' met betrekking tot gegevens zoals het in de AVG wordt gebruikt met betrekking tot persoonsgegevens. Verwerken omvat dus alles wat iemand met gegevens kan doen, inclusief het verzamelen, opslaan, analyseren, bewerken en delen van gegevens, zie art. 4(2) AVG.

[69] Persoonsgegevens zijn alle gegevens over geïdentificeerde of identificeerbare natuurlijke personen (art. 4(1) AVG).

[70] Ook als de hulp van een ISP nodig is om een IP-adres te herleiden tot een persoon, wordt dit over het algemeen als persoonsgegeven beschouwd (zie het Breyer-arrest, ECLI:EU:C:2016:779).

te voeren die zij volgens de wet hebben.[71] Wat betreft die wettelijke taken zitten het NCSC en het DTC in verschillende situaties. Hieronder bespreken we dat in meer detail.

Juridische context bij het NCSC

De taken van het NCSC staan beschreven in de Wet beveiliging netwerk- en informatiesystemen (Wbni). De bepalingen in de Wbni vormen daarmee de wettelijke basis voor bepaalde specifieke verwerkingen van persoonsgegevens. Zo heeft het NCSC op grond van de Wbni onder meer de taak en bevoegdheid om vitale dienstenaanbieders, en dienstenaanbieders die onderdeel zijn van de rijksoverheid, te informeren en adviseren over dreigingen en incidenten met betrekking tot hun netwerksystemen.[72] Om deze taak uit te voeren mag het NCSC persoonsgegevens verwerken, voor zover dit noodzakelijk is. Deze bepaling zorgt er dus voor dat het NCSC inderdaad datasets met persoonsgegevens mag verwerken om vitale partijen en Rijksoverheidsorganisaties te voorzien van dreigingsinformatie. Concreet betekent dit bijvoorbeeld dat het NCSC IP-adressen en andere persoonsgegevens (soms bijvoorbeeld e-mailadressen) mag verzamelen en analyseren om te kijken welke vitale bedrijven en Rijksoverheidsorganisaties mogelijk kwetsbaar zijn voor een cyberaanval of een lek, om vervolgens de betreffende partijen op de hoogte te stellen.

Wanneer het echter gaat om dreigingen en incidenten met betrekking tot netwerksystemen van andere dienstenaanbieders (ie. niet-vitaal en geen onderdeel van de rijksoverheid), heeft het NCSC niet de taak en bevoegdheid om de betreffende dienstenaanbieders zelf te informeren of adviseren. Wel heeft het de taak om andere partijen te informeren, die op hun beurt de individuele niet-vitale aanbieders kunnen ondersteunen. De Wbni geeft een opsomming van typen partijen die wel geïnformeerd mogen en moeten worden, voor zover dat nodig is ter voorkoming van nadelige maatschappelijke gevolgen in en buiten Nederland:[73]

a. organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek daarover te informeren;
b. CSIRT's;
c. andere computercrisisteams, aangewezen bij regeling van Onze Minister of behorend tot een bij die regeling aangewezen categorie;
d. aanbieders van internettoegangs- en internetcommunicatiediensten ten behoeve van het informeren van gebruikers van die diensten.

CSIRT's

Een **CSIRT** is een Computer Security Incident Response Team. CSIRT's zijn een subset van computercrisisteams. CSIRT's zijn landelijk en werken samen met de CSIRT's van andere EU-lidstaten. De meeste landen hebben één CSIRT, Nederland heeft er twee:

- het NCSC (Nationaal Cyber Security Centrum)
- het CSIRT-DSP (CSIRT voor Digital Service Providers)

Box 2. CSIRT's

[71] Art. 6(1)(e) AVG. In theorie zijn ook andere grondslagen mogelijk, zoals toestemming, maar in het geval van het NCSC en het DTC ligt deze grondslag het meest voor de hand. Andere grondslagen zijn niet goed werkbaar; (potentiële) daders zullen bijvoorbeeld geen toestemming geven om hun persoonsgegevens te verwerken en de overheid kan geen gebruik maken van de grondslag van gerechtvaardigd belang.

[72] Art. 3(1)(e) Wbni.

[73] Art. 3(2) Wbni.

Om dreigingsinformatie met persoonsgegevens met deze partijen te delen moet het NCSC nog steeds voldoen aan het noodzakelijkheidsvereiste uit de AVG: persoonsgegevens mogen alleen verwerkt worden voor zover dat nodig is om de taak uit te voeren. Dit betekent ook dat de ontvangende partij wel iets met de gegevens moet kunnen. Gegevens waarvan niet aannemelijk is dat de ontvangende partij er iets mee kan, worden niet gedeeld. Daarom vereist het NCSC van OKTT's over het algemeen een lijst met IP-adressen van de achterban (van de OKTT), waarna het NCSC enkel dreigingsinformatie met betrekking tot die IP-adressen met de OKTT deelt. In Box 3 lichten we de uitwerking van de besproken wetgeving toe met een voorbeeld.

Voorbeeld gegevensverstrekking door NCSC

Stel het NCSC heeft een dataset met 5.000 IP-adressen waarvan bekend is dat zij (mogelijk) kwetsbaar zijn voor een specifieke aanval. Het NCSC, dat de IP-adressen van alle vitale bedrijven kent, ziet dat 200 van die 5.000 IP-adressen behoren tot vitale bedrijven. Deze bedrijven worden door het NCSC zelf op de hoogte gesteld.

Van de overige 4.800 IP-adressen weet het NCSC niet van welke bedrijven of personen ze zijn. Een deel van de IP-adressen is waarschijnlijk te herleiden tot individuele personen, daarom zijn de regels van de AVG van toepassing. Het NCSC mag deze 4.800 IP-adressen dus niet zomaar aan iedereen verstrekken.

Nu is er een samenwerkingsverband met OKTT-status met een achterban van 10.000 niet-vitale bedrijven. Deze OKTT heeft een lijst met IP-adressen van die bedrijven aan het NCSC aangeleverd. Het NCSC ziet dat 1.000 van de 4.800 testerende IP-adressen op deze lijst voorkomen en weet dus dat de OKTT de bedrijven kan bereiken die bij die 1.000 IP-adressen horen. Het NCSC verstrekt nu de informatie over die 1.000 IP-adressen aan de OKTT. De OKTT informeert en adviseert op zijn beurt de niet-vitale bedrijven die bij die 1.000 IP-adressen horen.

De overige 3.800 IP-adressen worden door het NCSC niet met de OKTT gedeeld, omdat niet voldoende aannemelijk is dat de OKTT hier daadwerkelijk iets mee kan. Doordat de OKTT niet voldoende handelingsperspectief aan deze gegevens kan bieden draagt het delen hiervan niet bij aan het voorkomen van nadelige maatschappelijke gevolgen. Voor het NCSC is het delen van deze gegevens dus niet noodzakelijk om de wettelijke taak uit te voeren.

Box 3. Voorbeeld gegevensverstrekking door het NCSC.

Juridische context bij het DTC

Tot nu is het DTC sterk beperkt in zijn bevoegdheden om dreigingsinformatie met persoonsgegevens te verwerken. Het is namelijk niet duidelijk dat het DTC de wettelijke taak heeft om dreigingsinformatie aan partijen te verstrekken (zoals het NCSC dat wel heeft), waardoor er geen sterke grondslag is om met dit doel persoonsgegevens te verwerken. Momenteel wordt gewerkt aan een wetsvoorstel waarin de wettelijke taak van het DTC wordt vastgelegd, waarmee een grondslag voor de verwerking van persoonsgegevens wordt gecreëerd. Dat maakt het onder meer mogelijk voor het DTC om dreigingsinformatie met persoonsgegevens te verwerken. Ook maakt dit het voor het NCSC mogelijk om het DTC aan te wijzen als OKTT en dreigingsinformatie over de niet-vitale sector met het DTC te delen. Uit de interviews met betrokken partijen blijkt echter dat het best nog even zou kunnen duren voordat deze beoogde wet in werking treedt. Op zijn vroegst zou dit begin 2021 zijn, maar het zou ook zo nog een jaar langer kunnen duren.

Het zou wellicht mogelijk kunnen zijn voor het DTC om al eerder te beginnen met het verwerken van dreigingsinformatie met persoonsgegevens, in plaats van de zojuist genoemde beoogde wet af te wachten. Het argument zou namelijk kunnen worden gemaakt dat de wettelijke taak van het DTC, en daarmee de verwerkingsgrondslag, kan worden afgeleid uit de Begrotingswet. Daarin staat het volgende:

"Structureel is € 2,5 mln. per jaar beschikbaar voor de activiteiten van het Digital Trust Center (DTC) om via voorlichting, tools en advisering bedrijven – van zzp-er tot grootbedrijf – beter in staat te stellen hun eigen cyberweerbaarheid te organiseren. Deze middelen zijn voor opdrachten zoals de ontwikkeling van een website en een online platform, kennisopbouw over cyberrisico's en kennisdeling met de doelgroep niet-vitale bedrijfsleven."[74]

Als 'voorlichting', 'advisering' en 'kennisdeling' ruim worden uitgelegd kan hier ook onder vallen dat het DTC bedrijven op de hoogte moet stellen van dreigingen en incidenten. De taakbeschrijving is echter niet heel duidelijk en nauwkeurig, iets wat de AVG wel vereist.[75] Vergelijk de beschrijving bijvoorbeeld met deze formulering in de Wbni, over een van de taken van het NCSC: *het informeren en adviseren van deze aanbieders en anderen in en buiten Nederland over dreigingen en incidenten met betrekking tot de in de aanhef bedoelde netwerk- en informatiesystemen*.[76] De taak van het DTC zoals deze is vastgelegd in de begrotingswet lijkt dus ongeschikt om als wettelijke grondslag te dienen om dreigingsinformatie met persoonsgegevens te mogen verwerken.

In combinatie met een concreet wetsvoorstel waarin de taakbeschrijving van het DTC nauwkeurig staat uitgewerkt, namelijk het wetsvoorstel waaraan momenteel wordt gewerkt, zou de grondslag al iets sterker worden. Een aantal gesproken partijen geeft aan dat het waarschijnlijk mogelijk (lees: politiek haalbaar) zou zijn om op basis van de Begrotingswet in combinatie met het concrete wetsvoorstel, al te spreken van een wettelijke taak op grond waarvan het DTC persoonsgegevens mag verwerken en de OKTT-status zou kunnen krijgen. Daardoor zou men al kunnen beginnen met informatie-uitwisseling voordat de wet in werking is getreden. Het is echter de vraag of een dergelijke, zwakkere, grondslag stand zou houden bij een rechter. Gelet op het structurele karakter van de beoogde gegevensverwerking is het namelijk denkbaar dat een rechter enkel genoegen zou nemen met een wet in formele zin waarin de specifieke wettelijke taak is vastgelegd.[77] De Begrotingswet zou dan dus niet afdoende zijn, ook niet in combinatie met het wetsvoorstel. In dat geval zou het DTC pas persoonsgegevens mogen verwerken wanneer de nieuwe wet in werking treedt.[78]

---

[74] Tweede Kamer, 2019–2020, 35 300 XIII, nr. 1, p. 44.

[75] Overweging 41 AVG stelt onder meer dat de rechtsgrond duidelijk en nauwkeurig moet zijn, en dat de toepassing voorspelbaar moet zijn.

[76] Art. 1(d) Wbni.

[77] In de MvT bij de uAVG, en in de jurisprudentie, is te vinden dat voor een beroep op een publieke taak, die taak wel in een wet moet zijn vastgelegd, maar niet in alle gevallen in een wet in formele zin. Helaas is nergens te vinden in welke gevallen een specifieke wet in formele zin nodig is, en in welke gevallen kan worden volstaan met algemene wetgeving. Een mogelijke interpretatie is dat voor structurele verwerkingen een specifieke formele wet nodig is.

[78] Men zou zich kunnen afvragen wie naar de rechter zou stappen om het gebruik van de zwakkere grondslag aan te vechten, omdat iedereen behalve cybercriminelen er in dit geval toch zeker belang bij heeft dat de informatie gedeeld wordt? Het is echter goed denkbaar dat er bijvoorbeeld privacyorganisaties zijn die hier een probleem van zouden maken, omdat de privacy van burgers in algemene zin niet genoeg gewaarborgd is wanneer de overheid zwakke, niet-specifieke grondslagen gaat gebruiken voor structurele gegevensverwerking, hoe goed de bedoelingen in dit specifieke geval ook zijn.

3.2.2 Vertrouwelijke gegevens

Zoals eerder kort aangegeven, stelt de Wbni strenge beperkingen aan het delen van vertrouwelijke gegevens. In de wet zelf is niet vastgelegd welke informatie vertrouwelijk is. Het NCSC moet dit zelf beoordelen. In de Memorie van Toelichting bij de Wbni is echter wel het volgende opgenomen:

"Bij het begrip vertrouwelijke gegevens kan worden gedacht aan informatie over netwerk- en informatiesystemen die een bedrijf gebruikt bij zijn dienstverlening. Het kan ook zien op kwetsbaarheden in die systemen (ongeacht of er sprake is van een concrete dreiging), of op specifieke informatie over dreigingen of incidenten met betrekking tot die systemen. Ook kan worden gedacht aan concrete informatie over de aanbieder die door een dreiging of incident is getroffen waarbij openbaarmaking tot gevolg heeft dat die aanbieder daarvan nadeel ondervindt (bijvoorbeeld omdat klanten weglopen, of omdat gegevens bekend worden waar concurrenten hun voordeel mee kunnen doen)."[79]

Binnen de categorie vertrouwelijke gegevens kan verder nog onderscheid gemaakt tussen gegevens die herleid kunnen worden tot de aanbieder waar zij betrekking op hebben (wat wil zeggen dat de identiteit van de aanbieder kan worden vastgesteld), en gegevens die niet herleidbaar zijn. Niet-herleidbare vertrouwelijke gegevens zijn in het kader van informatie-uitwisseling met betrekking tot cybersecurity minder van belang. Informatie over cybersecurity is over het algemeen namelijk pas vertrouwelijk wanneer bekend is om welk bedrijf het gaat.[80]

Om zijn taken uit te voeren mag het NCSC herleidbare vertrouwelijke gegevens (zonder instemming van de aanbieder) enkel delen met de volgende typen partijen:[81]

a. *CSIRT's;*
b. *andere computercrisisteams, aangewezen bij regeling van Onze Minister of behorend tot een bij die regeling aangewezen categorie;*
c. *de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2017.*

In tegenstelling tot (andere) dreigingsinformatie mag het NCSC herleidbare vertrouwelijke informatie dus niet verstrekken aan OKTT's of aanbieders van internettoegangs- en internetcommunicatiediensten. De categorie herleidbare vertrouwelijke informatie heeft echter vaak overlap met dreigingsinformatie. Dit leidt ertoe dat de bevoegdheid om bepaalde dreigingsinformatie met OKTT's te delen niet uitgevoerd mag worden omdat die informatie ook als herleidbare vertrouwelijke informatie wordt aangemerkt. De volgende tabel geeft enkele voorbeelden van dreigingsinformatie en herleidbare vertrouwelijke informatie, en geeft de overlap weer.

---

[79] Tweede Kamer, 2017–2018, 34 883, nr. 3, p. 46.

[80] Niet-herleidbare vertrouwelijke gegevens zijn over het algemeen bijvoorbeeld bedrijfsgeheimen als een formule of marketingconcept, waar concurrenten hun voordeel mee kunnen doen ongeacht of bekend is van welk bedrijf het afkomstig is. In het kader van het werk van het NCSC kan soms ook worden gedacht aan het feit er een grote kwetsbaarheid was in een systeem van een aanbieder uit een bepaalde sector. Het feit is vertrouwelijk, maar het is niet bekend bij welke aanbieder het heeft plaatsgevonden.

[81] Art. 20(2) Wbni. De gegevens mogen ook enkel verstrekt worden "voor zover dat dienstig is aan het bevorderen van maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer."

Tabel 3. Overlap tussen dreigingsinformatie en herleidbare vertrouwelijke informatie (kwadrant rechts-onder).

	Geen dreigingsinformatie	Dreigingsinformatie
Niet-vertrouwelijk	• Voorlichtingsinformatie	• IP-adres van (potentiële) dader • Kwetsbaarheden in bepaalde systemen
Vertrouwelijk, herleidbaar	• Informatie over systemen van een specifiek bedrijf	• Kwetsbaarheden in systemen van een specifiek bedrijf • Getroffen bedrijven

Het vierde kwadrant, rechtsonder in de tabel, is waar problemen ontstaan voor het delen van informatie met OKTT's. Het waarschuwen van bedrijven die kwetsbaar zijn is een belangrijke doelstelling van verschillende partijen die in de vorige hoofdstukken genoemd zijn, waaronder het DTC. Zoals toegelicht in het voorbeeld in Box 3 kan het NCSC OKTT's waarschuwen, die op hun beurt de bedrijven kunnen waarschuwen. Zoals beschreven in de vorige paragraaf bepaalt de Wbni ook dat het NCSC die informatie inderdaad mag doorzetten naar OKTT's en aanbieders van internetdiensten. Tegelijkertijd kan het echter, afhankelijk van de situatie, de wetsinterpretatie en het oordeel van het NCSC, ook juist *niet* toegestaan zijn om deze informatie naar die partijen door te zetten. Deze informatie kan namelijk ook onder herleidbare vertrouwelijke informatie vallen:

"… Het kan ook zien op kwetsbaarheden in die systemen (ongeacht of er sprake is van een concrete dreiging), of op specifieke informatie over dreigingen of incidenten met betrekking tot die systemen. Ook kan worden gedacht aan concrete informatie over de aanbieder die door een dreiging of incident is getroffen waarbij openbaarmaking tot gevolg heeft dat die aanbieder daarvan nadeel ondervindt…"[82]

De reden voor de extra beperking met betrekking tot het delen van herleidbare vertrouwelijke informatie, zo blijkt uit de parlementaire geschiedenis, is dat bedrijven bezorgd waren dat hun naam en kwetsbaarheden zonder hun toestemming aan allerlei samenwerkingsverbanden en internetaanbieders kon worden gegeven. De beperking zorgt er nu echter ook voor dat bedrijven zelf soms niet op de hoogte kunnen worden gesteld van het feit dat zij kwetsbaar zijn, omdat het NCSC deze informatie niet mag delen met OKTT's.

Volgens een gesprekspartner lijkt deze beperkende werking bij het opstellen van de wet over het hoofd te zijn gezien, of wellicht te zijn onderschat. Uit de gevoerde gesprekken blijkt dat in de praktijk dergelijke slachtofferinformatie door het NCSC in sommige gevallen toch via OKTT's wordt doorgezet, namelijk wanneer uit een zeer betrouwbare bron blijkt dat er ernstige kwetsbaarheden zijn, met een hoog risico en een grote impact. Ondertussen wordt er ook gekeken of de Wbni op dit punt kan worden aangepast, zo blijkt uit de interviews, al kunnen dezelfde zorgen van bedrijven nog steeds spelen en is er dus geen garantie dat een wijziging wordt aangenomen. Een andere oplossing zou wellicht zijn om de achterban van een OKTT, via de OKTT, toestemming te laten geven aan het NCSC om in de toekomst herleidbare vertrouwelijke informatie met de OKTT te delen. In Box 4 lichten we deze mogelijkheid en de rest van deze paragraaf toe met een voorbeeld. We gebruiken daarvoor een variant op het vorige voorbeeld (zie Box 3), waarin de informatie als herleidbaar vertrouwelijk wordt beschouwd.

[82] Tweede Kamer, 2017–2018, 34 883, nr. 3, p. 46.

Voorbeeld verstrekking herleidbare vertrouwelijke gegevens door het NCSC

Stel het NCSC heeft een dataset met 5.000 IP-adressen waarvan bekend is dat zij kwetsbaar zijn voor een specifieke aanval. Het NCSC is van oordeel dat bedrijven nadeel zullen ondervinden indien openbaar wordt dat zij deze kwetsbaarheid hebben, en beschouwt de informatie daarom als **vertrouwelijk** (in tegenstelling tot in het vorige voorbeeld, zie Box 3).

Het NCSC, dat de IP-adressen van alle vitale bedrijven kent, ziet dat 200 van die 5.000 IP-adressen behoren tot vitale bedrijven. Net als in het vorige voorbeeld worden deze bedrijven door het NCSC zelf op de hoogte gesteld.

Van de overige 4.800 IP-adressen weet het NCSC niet van welke bedrijven of personen ze zijn. Een deel van de IP-adressen is waarschijnlijk te herleiden tot individuele personen, daarom zijn de regels van de AVG van toepassing. Het NCSC mag deze 4.800 IP-adressen dus niet zomaar aan iedereen verstrekken.

Nu is er een samenwerkingsverband met OKTT-status met een achterban van 10.000 niet-vitale bedrijven. Deze OKTT heeft een lijst met IP-adressen van die bedrijven aan het NCSC aangeleverd. Het NCSC ziet dat 1.000 van de 4.800 testerende IP-adressen op deze lijst voorkomen en weet dus dat de OKTT de bedrijven kan bereiken die bij die 1.000 IP-adressen horen. Het NCSC zou nu de informatie over die 1.000 IP-adressen aan de OKTT kunnen verstrekken zonder dat dit in strijd is met de AVG, maar mag dit niet omdat het herleidbare vertrouwelijke informatie betreft.

Een mogelijke oplossing, waarvan onderzocht moet worden of het juridisch stand zou houden, is als volgt:

Stel dat van die laatste 1000 IP-adressen, er 600 behoren tot bedrijven die het NCSC toestemming hebben gegeven om herleidbare vertrouwelijke gegevens die op hen betrekking hebben, te delen met de OKTT. Dan zou het NCSC de gegevens over deze 600 IP-adressen wel met de OKTT mogen delen.

Omdat de bedrijven en het NCSC geen direct contact met elkaar hebben, zal deze toestemming via de OKTT moeten verlopen. In de praktijk zou dit er dus op neer komen dat de OKTT de eerdergenoemde lijst met IP-adressen van 10.000 bedrijven aan het NCSC aanlevert, en daarbij ook vermeldt welke van die 10.000 IP-adressen behoren tot bedrijven die het NCSC toestemming geven om herleidbare vertrouwelijke gegevens met de OKTT te delen.

Box 4. Voorbeeld verstrekking herleidbare vertrouwelijke informatie door het NCSC.

3.3 Het Nederlandse stelsel vergeleken met de stelsels in andere geselecteerde landen

Nederland kan ongetwijfeld leren van landen die ver zijn in de ontwikkeling van een landelijk dekkend cybersecuritystelsel. Met deze gedachte hebben we, zoals reeds benoemd, op basis van een quickscan drie landen geselecteerd: het Verenigd Koninkrijk, Frankrijk en Duitsland. Tijdens de *desk research* hebben we over alle landen relevante informatie kunnen vinden over de inrichting van hun stelsel. In de praktijk bleek dat de vergelijking van Nederland met de drie landen oppervlakkig bleef.

Dat komt ten eerste doordat het vergelijken van landen complex is. Elk land heeft zijn eigen, specifieke context. Juridische kaders verschillen, de bestuurlijke indeling is anders, de omvang van landen verschilt, er zijn culturele verschillen tussen landen, et cetera. Stelsels die

in een bepaald land gehanteerd worden, zijn deels een uitvloeisel van deze contextuele aspecten en deels keuzes die gemaakt zijn.

Ten tweede is het vaststellen van meetbare en betekenisvolle variabelen complex. Zo lijkt bijvoorbeeld het aantal cyberincidenten in eerste instantie informatief, maar is sterk afhankelijk van het aantal aanvallen dat een land te voorduren heeft en de kwaliteit van de metingen (hoe beter je meet, hoe meer incidenten er zijn). Wat tevens meespeelt is dat landen hun cybersecuritysterktes en -zwaktes logischerwijs maar beperkt vrijgeven. Openbare informatie over het systeem kan namelijk ook gebruikt worden om het systeem aan te vallen. De resultaten van onze *deskresearch* zullen dan ook voornamelijk kunnen worden gebruikt voor inspiratie, niet zo zeer om direct lessen te kunnen trekken uit bepaalde landen.

Onze resultaten op basis van *deskresearch* van materiaal over deze drie landen worden in de volgende paragrafen samengevat. Bijlage 2 bespreekt deze landen in groter detail.

3.3.1 Decentraal stelsel

Zoals al eerder aangegeven heeft Nederland gekozen voor een decentrale organisatie van het cybersecuritystelsel, ofwel een netwerkbenadering (zie ook paragraaf 3.4). Veel andere landen, en zo ook de twee van de drie door ons dieper bestudeerde landen, kennen een hoofdzakelijk centrale inrichting; doorgaans is er één partij verantwoordelijk voor alle cybersecurity gerelateerde zaken. Dat heeft bepaalde voordelen – zo is het voor iedereen duidelijk welke partij dient als loket. In het Verenigd Koninkrijk en Frankrijk zijn dit respectievelijk het Britse National Cyber Security Centre (Britse NCSC) en de Franse Agence nationale la sécurité des systèmes d'information (ANSSI). Beide landen scoren hoog op de Global Cybersecurity Index (GCI), respectievelijk 1e en 3e. Het derde bestudeerde land is Duitsland, waarbij het systeem zowel centraal als decentraal is ingericht. Duitsland heeft voor vitale bedrijven de Bundesamt für Sicherheit in der Informationstechnik (BSI) verantwoordelijk gesteld voor de cybersecurity en verkregen slechts een ontmoedigende 22e plaats op de GCI. Aangezien zowel Frankrijk als Duitsland één van de kleinere budgetten in Europa hebben voor cybersecurity, lijkt budget op zichzelf niet doorslaggevend te zijn voor succes op de GCI.

Uit de interviews blijkt dat Nederland heel bewust heeft gekozen voor een decentrale inrichting van het landelijk dekkend stelsel. Dat past beter bij de Nederlandse beleidscultuur, waarin uiteraard wel vaker een poldermodel (Nederlandse consensuspolitiek) wordt toegepast. Daarnaast is in landen met een centraal stelsel vaak een inlichtingendienst verantwoordelijk, iets wat erg gevoelig zou liggen in Nederland. Een inlichtingendienst levert vaak informatie die niet of moeilijk te verifiëren is, vaak zonder context en achtergrond. Nederland heeft geen inlichtingencultuur (zoals bijvoorbeeld het Verenigd Koninkrijk en de Verenigde Staten), waarbij een breed begrip voor kennis van de waarde en de betekenis van 'intelligence' bestaat.[83]

Het decentrale stelsel waar Nederland voor gekozen heeft komt soms versnipperd over en laat gaten in de dekking, maar heeft ook voordelen. Zo zit de kennis in deze vorm zo dicht mogelijk op de branche of sector waar het om gaat en wordt de verantwoordelijkheid (en de kosten voor de verantwoordelijke organisaties) gedeeld met private partijen. Wel is het NCSC als spil het nationale contactpunt (en centraal computercrisisteam).

[83] https://www.netkwesties.nl/1379/nederland-ontbeert-cultuur-van-begrip.htm

3.3.2 Lessen uit de specifieke landen

Verenigd Koninkrijk

Het Verenigd Koninkrijk (VK) is opvallend vanwege hun enorme budget voor cybersecurity (omgerekend ca. €2,2 miljard) en het behalen van de hoogste plek op de GCI (in 2018). Het Britse NCSC staat in nauw contact met de Britse inlichtingendienst en kan daarmee gebruikmaken van expertise op zeer hoog niveau.

Als er wordt gekeken naar de vijf pijlers waar de GCI uit is opgebouwd is zichtbaar dat er voor het VK wel nog wat te winnen is op samenwerkingsgebied.[84] Een kanttekening daarbij is dat vrijwel ieder land op deze pijler het laagst scoort, dus in het algemeen zou meer moeten worden ingezet op (inter)nationale samenwerkingen. Een van de voordelen van sterke (inter)nationale samenwerkingen is dat landen van elkaar kunnen leren, elkaar kunnen ondersteunen indien er sprake is van een grootschalige aanval, maar ook dat iedereen sneller op de hoogte is van wat er speelt op cybersecuritygebied. Een voorbeeld van een lonende samenwerking is dat in april 2018 Nederland in samenwerking met het VK met succes een internationale operatie geleidde die een website met een link naar 4 miljoen DDoS-aanvallen wereldwijd heeft afgesloten.

VK lijkt het belang van het samenwerken zelf ook te zien; (inter)nationale samenwerking is een belangrijk thema in de National Cyber Security Strategy.[85] Het Britse NCSC zet actief in op samenwerkingen tussen overheid, publieke sector, (vitale en niet-vitale) bedrijven en inwoners. Daarnaast heeft het VK zeer succesvolle awareness- en informatie-uitwisselingsinitiatieven, zoals voortgekomen uit het Active Cyber Defence programma[86], welke bewezen een significante waarde heeft gehad voor het verbeteren van de nationale cybersecurity in het VK.[87]

Frankrijk

Het cybersecuritystelsel van Frankrijk kenmerkt zicht net als het VK door een gecentraliseerde beleidsvoering en met een hoge score op de GCI (wereldwijd 3e plek in 2018). De ANSSI is verantwoordelijk voor de beveiliging van informatiesystemen van de staat en om advies en steun te verlenen aan overheden en bedrijven van vitaal belang.[88] Ze hadden in 2017 een jaarlijks budget van rond de €100 miljoen. Frankrijk maakt, net als Nederland, onderscheid tussen vitale en niet-vitale partijen en bepaalt aan de hand van deze indeling wie welke informatie ontvangt. Hiermee heeft Frankrijk dus, net als Nederland, de uitdaging om te bepalen welke bedrijven als vitaal moeten worden aangemerkt en dus onder de verantwoordelijkheid van de ANSSI (vergelijkbaar met het Nederlandse NCSC) vallen. De aangemerkte vitale bedrijven zijn, net als in Nederland, verplicht om bepaalde maatregelen te nemen met betrekking tot hun cybersecurity.

Frankrijk heeft een actieve ontwikkeling van beleidsvoering en methodieken voor cybercriminaliteitspreventie. Zo zijn er bijvoorbeeld voor zowel particulieren als professionals tools

---

[84] Global Cybersecurity Index (2018).

[85] Cabinet Office. National Cyber Security Strategy 2016 to 2021 (gepubliceerd op 1 november 2016 op www.gov.uk).

[86] NCSC (2019). Active Cyber Defence – The Second Year.

[87] Stevens, T. O'Brien, K., Overill, R., Wilkinson, B., Pildegovičs, T., Hill, S. (2019). UK Active Cyber Defence. A public good for the private sector. King's College London.

[88] Baumard, P. (2017). Cybersecurity in France. Springer International Publishing.

en handleidingen die gericht zijn op een preventieve of reactieve aanpak van cybercriminaliteit.

Frankrijk heeft net als Nederland een organisatie die zich richt op niet-vitale bedrijven. GIP ACYMA (vergelijkbaar met het Nederlandse DTC) is opgezet om cybersecuritymaatregelen toegankelijk te maken voor Franse private partijen. In de praktijk richt deze organisatie zich vooral op kleine bedrijven zonder IT-experts. GIP ACYMA claimt onder andere private ICT-experts in contact te brengen met organisaties die getroffen zijn door een cybersecurityincident en functioneert als informatiepunt. Wat duidelijk zal worden in paragraaf 4.3, is dat het DTC voor relevante partijen vaak nog onbekend is. Onduidelijk is of GIP ACYMA wel succesvol is in het bereiken van niet-vitale bedrijven.

Duitsland

Het cybersecuritystelsel van Duitsland is zowel centraal als decentraal van aard. Globaal gezien wordt de cybersecurity rondom vitale partijen centraal en de cybersecurity rondom niet-vitale partijen decentraal geregeld. Hier zijn echter veel uitzonderingen op. De versplintering en onduidelijke verdeling van de takenpakketten tussen de diensten in Duitsland maakt de samenwerking moeilijk[89,90], zeker in tijden van een grootschalige cyberaanval. Een nationaal initiatief genaamd UP KRITIS is opgezet om de samenwerking tussen de staat en de uitvoerders van kritieke infrastructuur te verbeteren en de complexiteit rondom cybersecurity weg te nemen. De samenwerking binnen UP KRITIS wordt grotendeels als positief ervaren door zowel publieke als private partijen.[91] Naast UP KRITIS zijn er vele andere samenwerkingsinitiatieven. Deze vinden vaak parallel plaats en zorgen voor verspreiding van verantwoordelijkheid, waardoor de effectiviteit van samenwerkingen buiten UP KRITIS beperkt is.[92]

Daarnaast zijn veranderingen in Duitsland lastig door te voeren, omdat de verdeling van de diensten diep verweven zit in het Duitse overheidsstelsel. Het Duitse politieke systeem is gebaseerd op een federaal stelsel, waarbij de macht verdeeld is tussen de centrale overheid en de deelstaten. Een van de voordelen die Nederland heeft ten opzichte van Duitsland is dat Nederland geen federaal systeem heeft. Hierdoor kan Nederland beleid direct landelijk doorvoeren en is het makkelijker om onderling af te stemmen. Aan de andere kant is het ook lastig om landen één-op-één te vergelijken. Een decentrale insteek betekent feitelijk dat de deelstaten grote autonomie hebben. Echter een deelstaat als Noordrijn-Westfalen heeft meer inwoners dan Nederland.

3.4 Conceptuele benadering

Vanuit een conceptuele benadering kan het huidige Nederlandse stelsel – of de bedachte structuur van het huidige stelsel – gezien worden als een groot netwerk. Dit in tegenstelling tot een meer centralistisch model zoals in het Verenigd Koninkrijk. Een stelsel volgens de netwerkbenadering past beter bij de Nederlandse beleidscultuur en kent verschillende voordelen, zoals kennis zo dicht mogelijk bij de sector laten, inzet en eigenaarschap niet beperken

---

[89] Schallbruch, M., & Skierka, I. (2018). Cybersecurity in Germany. Springer International Publishing. p. 35.

[90] Zedler D (2017) Zur strategischen Planung von cyber security in Deutschland. Zeitschrift für Außenund Sicherheitspolitik p100-101

[91] Zedler D (2017) Zur strategischen Planung von cyber security in Deutschland. Zeitschrift für Außenund Sicherheitspolitik p21

[92] Schallbruch, M., & Skierka, I. (2018). Cybersecurity in Germany. Springer International Publishing. P45

tot één partij binnen de overheid en het delen van verantwoordelijkheid en kosten met private partijen. Door de regie meer te verspreiden, is echter ook het overzicht moeilijker te houden. In onderstaand schema benoemen we de typische kenmerken van beide modellen.

Tabel 4. Centralistisch model vs. Netwerkbenadering, typische kenmerken.

Centralistisch model	Netwerkbenadering
Eén dominant belang (bijv. nationale veiligheid)	Grote variëteit aan (organisatie) belangen
Centrale regie gewenst	Vertrouwen en samenspel nodig
Formele afspraken noodzakelijk	Informele netwerken, energie en initiatieven vormen de basis
Eenrichtingsverkeer (topdown)	Meer-richtingsverkeer (brengen en halen)
Verplichtend/afdwingbaar door overheid	Vrijwillig/eigenaarschap bij organisaties
Stabiele omgeving	Dynamische omgeving

Uitgaande van het hulp bieden aan ieder met vragen over of problemen met cybersecurity, lijkt de netwerkbenadering het meest recht te doen aan de behoeftes en de situationele werkelijkheid. We hebben te maken met een dynamisch ecosysteem van vele kenniseilandjes: er zijn verschillende partijen voor het bereiken van de Rijksoverheid en private, vitale partijen (namelijk het NCSC) en voor het bereiken van niet-vitale partijen (namelijk het DTC), en er wordt gebruik gemaakt van tientallen samenwerkingsverbanden, die een grote rol spelen in de daadwerkelijke verspreiding van informatie en die sterk in beweging zijn (regelmatig komen er nieuwe bij of verandert hun samenstelling en bereik).

Deze benadering biedt ook het meeste perspectief op actieve kennisdeling tussen overheid en bedrijven, doordat partijen er belang bij hebben om kennis te delen binnen hun samenwerkingsverband, wat er op zijn beurt belang bij heeft om kennis te delen met andere samenwerkingsverbanden of de centralere partij. Gezien de relatief beperkte (brede) expertkennis op het gebied van cybersecurity is dit zeker gewenst. Dat neemt echter niet weg dat de bevraagde bedrijven wel degelijk behoefte hebben aan een duidelijk aanspreekpunt binnen de overheid (zie Hoofdstuk 4); een 'loket' dat ook de mogelijkheid heeft om door te verwijzen.

Mocht er sprake zijn van een nationale cybercrisis of een situatie waarin vitale processen gevaar lopen, dan biedt het centralistische model meer voordelen. In die situatie ligt opschaling naar één crisisorganisatie met een centrale regisseur voor de hand. Afspraken en draaiboeken moeten op voorhand zijn gemaakt, omdat hier in een crisis geen tijd voor is. In de huidige opzet in Nederland vervullen de NCTV en het NCSC een coördinerende rol binnen de nationale crisisstructuur wanneer een ICT-crisis zich voordoet.

3.5 Samenvattende conclusie

We sluiten dit hoofdstuk af met een korte samenvatting, gestructureerd langs de deelvragen die in dit hoofdstuk centraal staan.

Deelvraag 3: Hoe is de huidige situatie van samenwerkingsverbanden en mogelijkheden van informatie-uitwisseling tussen overheid (NCSC, politie, DTC, e.a.) en private, niet vitale partijen op het gebied van cybersecurity ingericht? Hoe ziet een visuele weergave van het cybersecurity ecosysteem (in Nederland) eruit?

> 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 (namelijk het NCSC) en voor het bereiken van niet-vitale partijen (namelijk 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 Figuur 5 in paragraaf 3.1.1. Het Nederlandse systeem is verder dynamisch omdat de samenwerkingsverbanden sterk in beweging zijn: regelmatig komen er nieuwe bij of verandert hun samenstelling en bereik.

Deelvraag 4: Wat houdt informatie-uitwisseling en samenwerking over cybersecurity in, in de huidige situatie en welke aspecten van cybersecurity bevat deze en welke nog niet?

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 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.

Deelvraag 9: Hoe is in enkele andere landen het stelsel van cybersecurity tussen publieke en private partijen ingericht, en wat kan Nederland daarvan leren?

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 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 cybersecuritysysteem 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.

4 Maatregelen, informatiebehoeften en het bereik van het Nederlandse stelsel

In dit hoofdstuk bespreken we recente cijfers over cybersecurityincidenten en -maatregelen, het bereik van het DTC en de informatiebehoeften van het MKB. Vervolgens specificeren we die informatiebehoeften van bedrijven aan de hand van vier categorieën. Tot slot bespreken we een specifiek thema waarop kennis tekortschiet. Deelvragen die in dit hoofdstuk worden beantwoord:

Deelvraag 6a: Welke doelgroepen worden nu nog niet bereikt (wie nog niet?)

Deelvraag 7: Over welke aspecten van cybersecurity zou welke informatie-uitwisseling en samenwerking met deze doelgroepen dienen plaats te vinden?

4.1 Inleiding

Voor de beantwoording van de relevante deelvragen maken we in dit hoofdstuk onderscheid tussen vier categorieën bedrijven, op basis van hun cybermaturity. De categorie met de minste cybermaturity bestaat vooral uit ZZP'ers en bedrijven met een beperkte IT-component. We zien dat een groot deel van de gesproken ZZP'ers aangeeft behoefte te hebben aan basisinformatie van een betrouwbare en neutrale partij. Feitelijk kan het DTC momenteel al in deze behoefte voorzien, maar de grote meerderheid van de bedrijven is hier niet van op de hoogte. Zo bleek niemand van de gesproken ZZP'ers het DTC te kennen.

De tweede categorie bedrijven zijn de bedrijven die beveiligingsdiensten afnemen van IT-leveranciers. Zij leggen de verantwoordelijkheid van hun cybersecurity grotendeels in handen van een externe partij, met wie ze bij een incident contact opnemen. Hierdoor is de noodzaak om deze bedrijven zelf te bereiken minder groot (evenals hun behoefte aan informatie). Deze categorie bestaat met name uit MKB's.

De laatste twee categorieën zijn cybermature bedrijven en gespecialiseerde IT-bedrijven. Zij hebben beide behoefte aan informatie waarover momenteel vooral het NCSC bezit, namelijk dreigingsinformatie. Deze bedrijven vallen echter onder niet-vitaal, waardoor zij het moeten doen met voorlichtingsinformatie en met dreigingsinformatie uit private initiatieven. De maatschappelijke en economische impact van een (succesvolle) cyberaanval zal bij deze twee categorieën over het algemeen het grootst zijn; cybermature bedrijven zijn vaak grote bedrijven en gespecialiseerde IT-bedrijven hebben ook de cybersecurity van andere bedrijven (de tweede categorie bedrijven) in handen.

In de volgende paragrafen bespreken we eerst incidenten, maatregelen en informatiebehoeften in brede zin, voornamelijk op basis van recente CBS-data. Vervolgens gaan we dieper in op de informatiebehoeften van de zojuist genoemde categorieën, voornamelijk gebaseerd op onze eigen data (interviews, telefonische enquête en focusgroep). Tot slot bespreken we nog een specifiek thema waarop kennis tekortschiet: Operational Technology.

4.2 Incidenten en huidige maatregelen

4.2.1 Recente cijfers en gevolgen van incidenten

Uit de meest recente cijfers van het CBS[93] blijkt dat bij 56% van de bedrijven in 2019 een veiligheidsincident is opgetreden. Interne fouten – zonder invloed van kwaadwillenden van buitenaf – zijn verantwoordelijk voor het grootste aandeel van veiligheidsincidenten, vaak met uitval van ICT-dienst tot gevolg. Als interne fouten (andere) gevolgen hadden, ging het in de meeste gevallen om onterechte toegang tot bepaalde systemen en gegevens voor hackers. In mindere mate zijn bestanden kwijtgeraakt of gegevens in verkeerde handen geraakt.

Bij 14% van de bedrijven was volgens het CBS[94] een incident opgetreden door een aanval van buitenaf. Voor de helft van de bedrijven heeft dit een negatieve impact op de bedrijfsvoering.[95] De meeste aanvallen (19%) waren gericht op bedrijven met meer dan 250 medewerkers en financiële instellingen waren het vaakst het doelwit van een aanval. Bij ongeveer de helft van alle incidenten is er sprake van financiële schade. Uit het Nationaal Cybersecurity Bewustzijnsonderzoek 2019 van Alert Online van de NCTV[96] blijkt dat één op de acht werkende Nederlanders zegt weleens op het werk daadwerkelijk op een foute link te hebben geklikt.

4.2.2 Gebruikte ICT-veiligheidsmaatregelen

Uit de meest recente cijfers van het CBS[97] blijkt dat er grote verschillen zijn in het toepassen van ICT-veiligheidsmaatregelen tussen verschillende bedrijfstakken.[98] Hoewel nagenoeg alle bedrijven gebruik maken van antivirussoftware en periodieke systeem updates, lijken verdere maatregelen vooral weggelegd voor bedrijven in de financiële dienstverlening en de ICT-sector (zie Figuur 6). Het gaat dan bijvoorbeeld om de encryptie van data, het maken van risicoanalyses en methodes voor het beoordelen ICT-veiligheid. Ca. 90% van de bedrijven in de financiële dienstverlening zet deze maatregelen in, tegenover slechts ongeveer 50% van de horecabedrijven. Ook lijkt de vuistregel te gelden dat hoe groter een bedrijf is, hoe meer maatregelen zij nemen (zie Figuur 7).

Ongeveer 66% van de Nederlandse bedrijven heeft eigen personeel in dienst dat zich bezighoudt met ICT-veiligheid. Dit zijn hoofdzakelijk bedrijven met meer dan 250 medewerkers. Niet verwonderlijk zijn de sectoren met het grootste aantal eigen personeel op dit thema de ICT- en informatie en communicatiesector (opdeling volgens CBS).

---

[93] Statline ICT-gebruik bij bedrijven – ICT-veiligheid 2019.

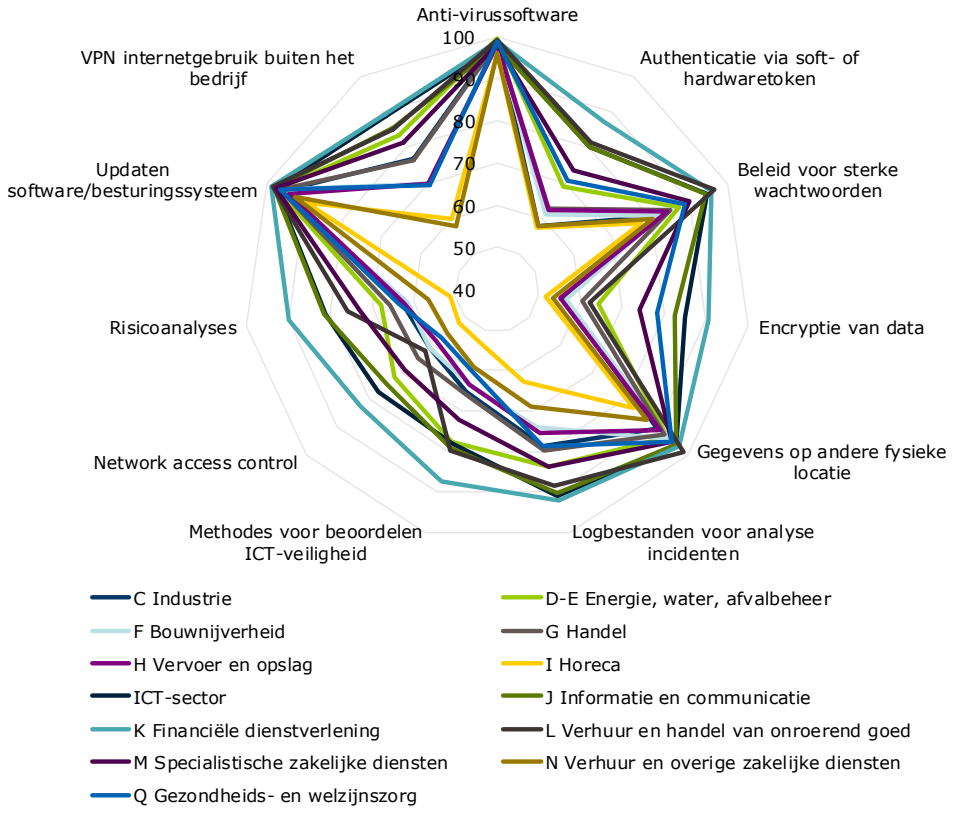
[94] Statline ICT-gebruik bij bedrijven – ICT-veiligheid 2019.

[95] Dit is voornamelijk het geval bij bedrijven in de ICT-branche, financiële dienstverlening en industrie.

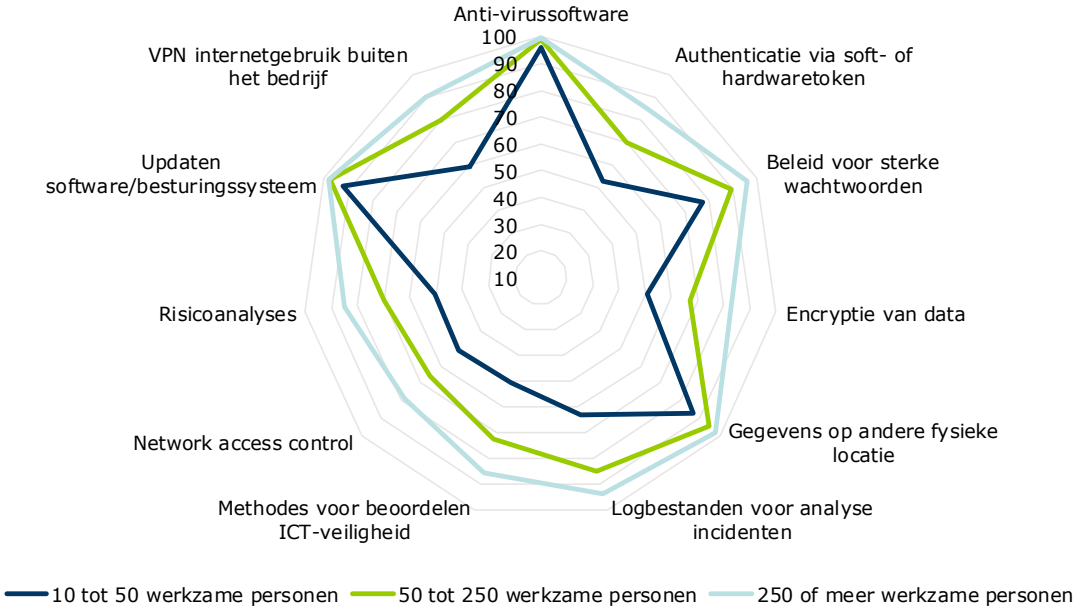
[96] Bevolkingsonderzoek uitgevoerd onder 1004 Nederlanders tussen de 16-80 jaar. In 2012 is de NCTV de campagne Alert Online gestart om de bewustwording op het gebied van cybersecurity te verhogen, zowel thuis als onderweg en op het werk.

[97] Statline ICT-gebruik bij bedrijven – ICT-veiligheid 2019.

[98] We nemen hier alle sectoren mee, dus ook de vitale sectoren.



Figuur 6. Gebruikte ICT-veiligheidsmaatregelen per bedrijfstak in 2019 (in % bedrijven). De cirkels geven het percentage aan. Bron: CBS ICT-gebruik bij bedrijven – ICT-veiligheid 2019.



Figuur 7. Gebruikte ICT-veiligheidsmaatregelen per bedrijfsgrootte in 2019 (in % bedrijven). De cirkels geven het percentage aan. Bron: CBS ICT-gebruik bij bedrijven – ICT-veiligheid 2019.

In vergelijking met de cijfers uit 2018 kunnen we spreken van een verbetering.[99] Zo geldt voor alle veiligheidsmaatregelen dat ze in 2019 door meer bedrijven zijn gebruikt dan in 2018. Gemiddeld werd per sector een stijging van ca. 3% geboekt, met encryptie van data als de grootste stijger met 15%.[100] Daarnaast blijkt uit het Nationaal Cybersecurity Bewustzijnsonderzoek 2019 van Alert Online van de NCTV dat werkend Nederland steeds vaker maatregelen neemt met betrekking tot cybersecurity.[101] Het grote publiek wordt bovendien steeds bekender met opties als een digitale wachtwoordkluis of wachtwoordmanager, VPN-verbindingen[102], opensource hard- en software[103] en web tracking blockers[104].

In maart 2020 heeft het CBS een rapportage gepubliceerd over cyberweerbaarheid onder ZZP'ers.[105] Kennis over internetveiligheid varieert sterk. Ruim 95% van de ZZP'ers heeft gehoord van 'back-ups maken' en 'antivirusprogramma', 31% heeft gehoord van cryptoware en 17% is bekend met pharming[106]. Wat betreft preventieve maatregelen worden vooral apparaten vergrendeld en sterke wachtwoorden gebruikt (door 2/3^{e} van de ZZP'ers). De helft van de ZZP'ers maakt regelmatig back-ups (of denkt dat dit gedaan wordt) en houdt programma's up-to-date. Het wijzigen van wachtwoorden, veiligheidsinstellingen aanpassen en zelf controleren op virussen wordt door minder dan een vijfde gedaan.

Uit onze focusgroep blijkt dat cybersecuritymaatregelen onder ZZP'ers sterk afhankelijk zijn van het kennisniveau en de digitale vaardigheden. De gesproken ZZP'ers maakten vooral regelmatig een back-up en veranderden regelmatig hun wachtwoorden. Wat hen tevens bezighoudt is dat ze enerzijds gevonden willen worden (website met contactgegevens) en anderzijds de behoefte hebben aan privacy en niet kwetsbaar willen zijn voor cybercrime.

---

[99] CBS Cybersecuritymonitor (2019).

[100] De cijfers zijn uitgerekend middels een gemiddelde zonder weging naar aantallen bedrijven. Hoewel er significant meer kleine en middelgrote bedrijven zijn, is de financiële en productiviteit impact significant groter per aanval bij een groter bedrijf.

[101] Dit is een bevolkingsonderzoek uitgevoerd onder 1004 Nederlanders tussen de 16-80 jaar. In 2012 is de NCTV de campagne Alert Online gestart om de bewustwording op het gebied van cybersecurity te verhogen, zowel thuis als onderweg en op het werk.

[102] Een Virtueel Particulier Netwerk (VPN) is een netwerk dat door een ander netwerk 'getunneld' wordt. Hierdoor kan er veiliger gebruik worden gemaakt van publieke wifi-netwerken. Daarnaast kan een internetprovider of netwerkbeheerder niet achterhalen welke website de gebruiker bezoekt. Een VPN geeft een gebruiker dus beveiligde en anonieme toegang tot een netwerk en beschermt daarmee iemands online gegevens.

[103] Van opensource software is de broncode vrijgegeven en aan te passen/te verbeteren door gebruikers.

[104] Tracking blockers maken het lastiger voor externe partijen om het online gedrag van de gebruiker te volgen.

[105] CBS Verkennend onderzoek cyberweerbaarheid onder zzp'ers (maart 2020). In opdracht van het DTC. ZZP'ers vormen qua aantal gezien de grootste groep van ondernemingen. In 2018 verdienden 1.538.000 personen inkomen als ZZP'er, voor 940.000 personen is dit de voornaamste inkomensbron (CBS Verkennend onderzoek cyberweerbaarheid onder zzp'ers, maart 2020). ZZP'ers gedragen zich voornamelijk als consumenten (Mede daarom pleitte ACM al voor het gelijktrekken van de rechten voor ZZP'ers en consumenten, ACM Signaal 2019), wat literatuur over consumentengedrag en cybersecurity relevant maakt. Maar er zijn ook een paar belangrijke verschillen; zo hebben ZZP'ers vaak documenten als klantenbestanden, contracten en facturen op hun computer staan, en zou men om die reden meer van hen mogen verwachten qua beveiligingsinspanningen dan van consumenten.

[106] Pharming is een oplichtingstechniek die erin bestaat internetgebruikers te misleiden door hun internetverkeer met een bepaalde website ongemerkt om te leiden naar een andere (malafide) website.

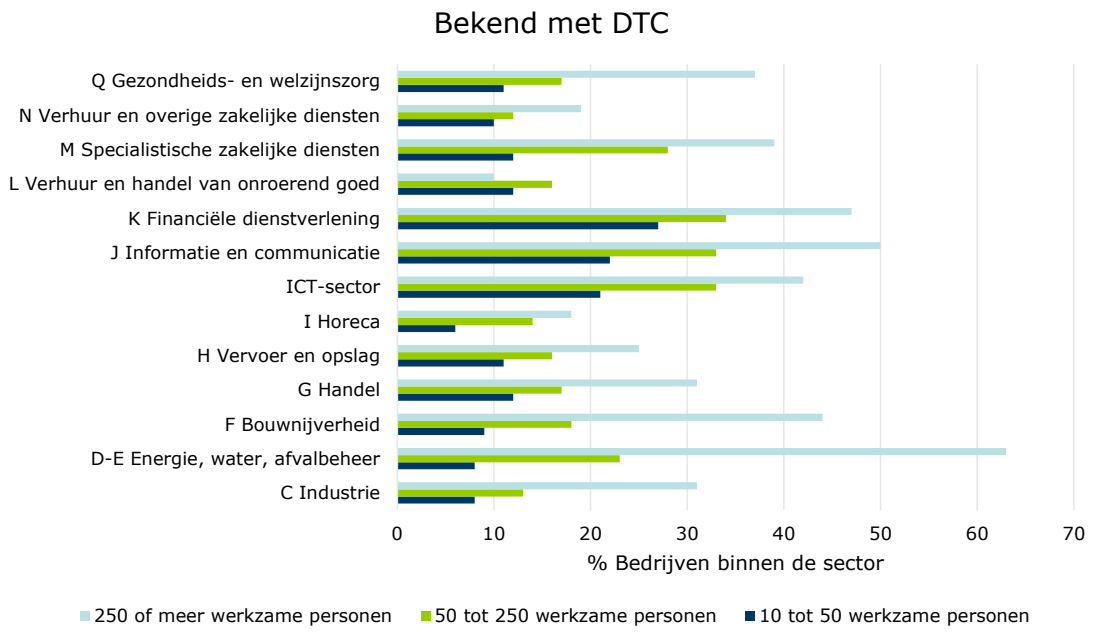
Onderzoek van het Centre of Expertise Cybersecurity van de Haagse Hogeschool en NSCR stelt dat – hoewel er tal van technische maatregelen (zoals virusscanners en firewalls) beschikbaar zijn – een groot deel van het slachtofferschap terug te voeren is op het gedrag van mensen.[107] Daarbij komt dat het daadwerkelijke onlinegedrag van mensen niet altijd overeenkomt met het gedrag dat ze denken online te vertonen. De onderzoekers hebben een experimentele survey uitgezet waaruit blijkt dat onveilig gedrag in hoge mate voorkomt. Bijna 60% gebruikt een zwak wachtwoord, 40% download onveilige software en 30% deelt persoonlijke gegevens. Ook klikt 20% op een hyperlink uit phishing emails of kopieert een URL genoemd in zo'n email naar de webbrowser.

4.3 Bereik DTC

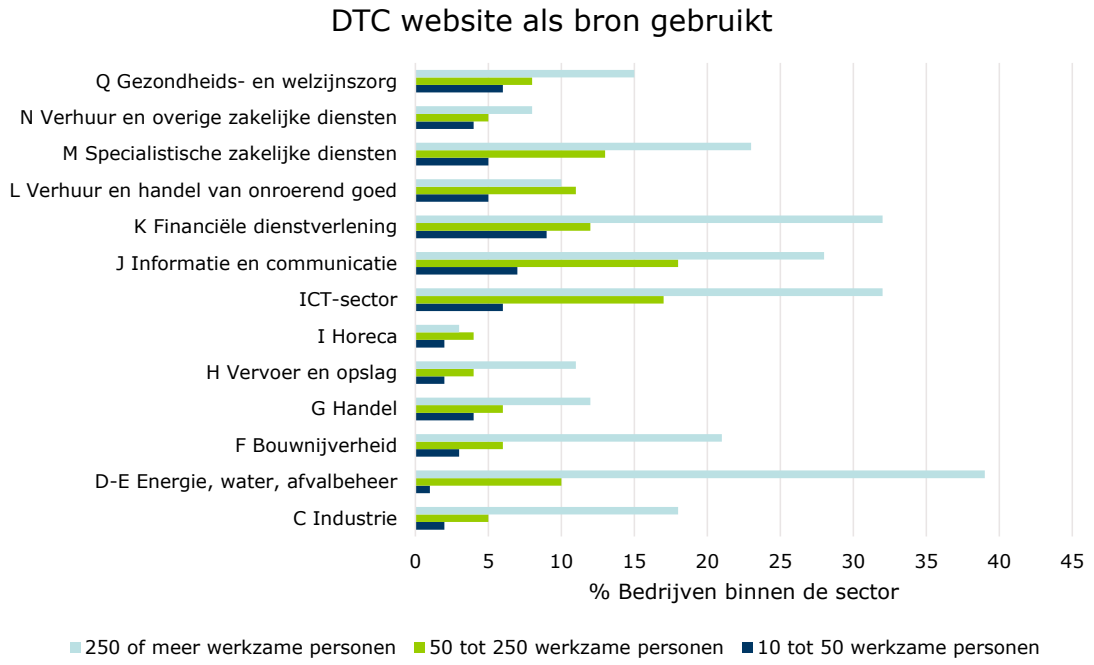
Zoals reeds aangegeven in hoofdstukken 2 en 3 helpt het Digital Trust Center (DTC) sinds 2018 Nederlandse bedrijven zich weerbaarder te maken tegen cyberdreigingen. Het DTC richt zich op 1,8 miljoen bedrijven, van ZZP'ers tot en met grootbedrijf behorend tot de niet-vitale sectoren. Het CBS heeft aan bedrijven gevraagd of ze bekend zijn met DTC en of ze de DTC-website als bron voor informatie over cybersecurity hebben gebruikt (zie Figuur 8 en Figuur 9). Er zijn grote verschillen tussen bedrijven.

- Als eerste valt op dat hoe groter het bedrijf, hoe beter men bekend is met DTC en hoe vaker men DTC als bron gebruikt. Bij kleine bedrijven (10-50 werkzame personen) ligt het ongewogen gemiddelde van de sectoren op circa 13%. Bij grotere bedrijven (250+ werkzame personen) ligt dit op ruim 30%.
- Ten tweede valt op dat bekendheid met DTC en het gebruik van DTC als bron sterk correleren. Dat is tot op zeker hoogte logisch. Alleen de groep die aangeeft DTC te kennen, kan aangeven ook gebruik te maken van DTC als bron. Echter, de mate waarin dit gebeurt is relatief hoog. Met andere woorden: een groot deel van de bedrijven die DTC kennen, maken ook gebruik van haar diensten.
- Ten derde valt op dat de sector veel sterker bepalend is voor de mate waarin met DTC kent en gebruikt als bron dan de omvang van bedrijven. Sectoren in de financiële dienstverlening, informatie en communicatie en uiteraard de ICT-sector scoren bovengemiddeld. Zwakke sectoren zijn de horeca, logistiek ("vervoer en opslag") en de bouw ("bouwnijverheid").

[107] Hoff - de Goede, S. van 't, Kleij, R. van der, Weijer, S. van de, Leukfeldt, R. (2019). Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders. Den Haag: De Haagse Hogeschool - Centre of Expertise Cybersecurity/WODC.



Figuur 8. Bedrijven die bekend zijn met DTC. Bron: CBS ICT-gebruik bij bedrijven – ICT-veiligheid 2019.



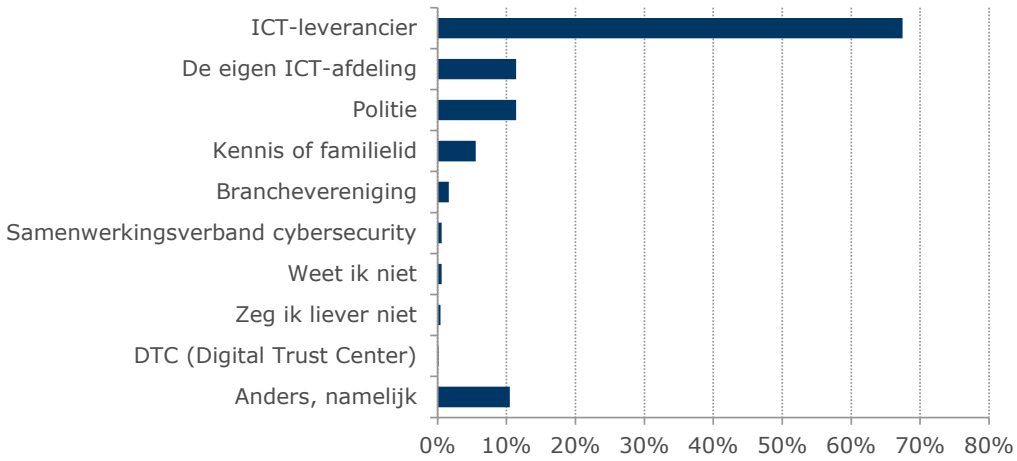
Figuur 9. Bedrijven die website DTC als bron gebruiken per sector. Bron: CBS ICT-gebruik bij bedrijven – ICT-veiligheid 2019.

Geen van de door ons in de focusgroep gesproken ZZP'ers was bekend met het DTC. Toch hadden ze allemaal behoefte aan precies hetgeen dat het DTC aanbiedt (zie paragraaf 4.5.1). Dit benadrukt dat er gewerkt dient te worden aan de naamsbekendheid en vindbaarheid van het DTC.

4.4 Informatiebehoefte MKB

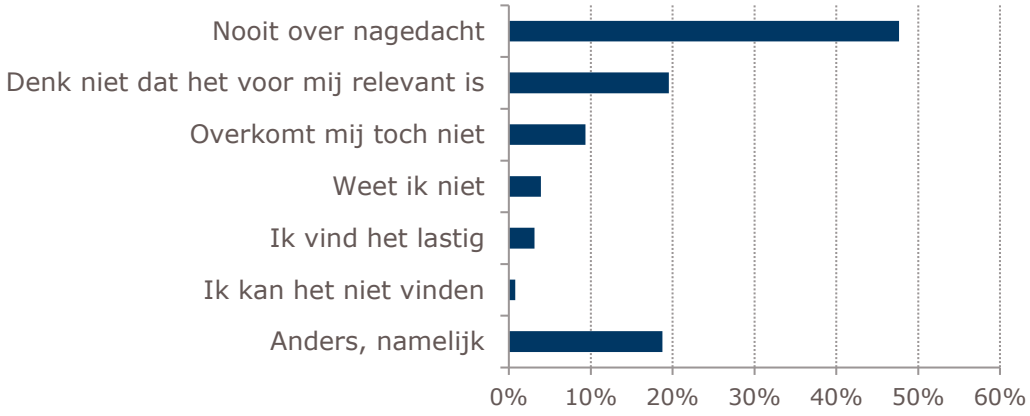
Zoals in het vorige hoofdstuk besproken richt het DTC zich momenteel in grote mate op het MKB. In Figuur 8 is echter te zien dat slechts 21% van de MKB's bekend is met het DTC en dat slechts 9% de DTC-website als bron heeft gebruikt. In deze paragraaf analyseren we de informatiebehoefte van deze diverse doelgroep.

In onze grootschalige telefonische enquête zijn 806 bedrijven bevraagd over cybersecurity. Het betreft een representatieve steekproef van het MKB in Nederland. Mocht hun bedrijf slachtoffer worden van cybercrime, dan zegt 83% te weten met wie contact op te nemen om het incident op te lossen. Slechts 16% geeft aan dit niet te weten. De branche, niet de grootte, van een bedrijf lijkt de bepalende factor te zijn in of ze weten wie te benaderen. Zo weten bedrijven in de financiële dienstverlening veel vaker met wie ze contact moeten opnemen dan landbouwbedrijven en bedrijven in de cultuursector. De bedrijven die aangaven te weten wie ze zouden moeten benaderen, zijn gevraagd wie dat dan zou zijn. Voor de meeste bedrijven was het antwoord op deze vraag 'mijn ICT-leverancier' (zie Figuur 10). Bijna 80% van de bedrijven maakt ook gebruik van externe leveranciers als het gaat om ICT-veiligheid. Zelfs bij het gebruik van externe leveranciers is het van belang enige (basis)kennis te hebben van cybersecurity, om zo hun diensten veilig te kunnen gebruiken. De categorie 'anders, namelijk' loopt zeer uiteen, maar vooral de bank, verzekeringsmaatschappij en Autoriteit Persoonsgegevens worden genoemd.



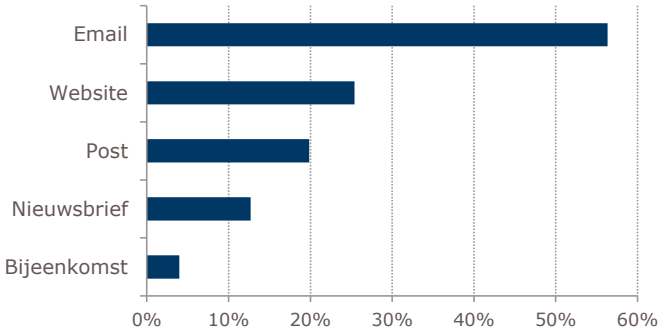
Figuur 10. Met wie neemt u dan contact op? (n=667: elk bedrijf dat aangaf te weten met wie het contact op moet nemen). Bron: eigen data – telefonische enquête (2020).

Respondenten die aangeven niet te weten wie te contacteren na een incident (16%) hebben daar vooral niet eerder over nagedacht of denken niet dat het relevant is voor hen (zie Figuur 11). Ook geven veel mensen aan dat ze het nog nooit hebben meegemaakt (onder: anders, namelijk).



Figuur 11. Kunt u toelichten waarom u niet weet met wie u contact moet opnemen na een incident? (n=128: elk bedrijf dat aangaf niet te weten met wie het contact op moet nemen). Bron: eigen data – telefonische enquête (2020).

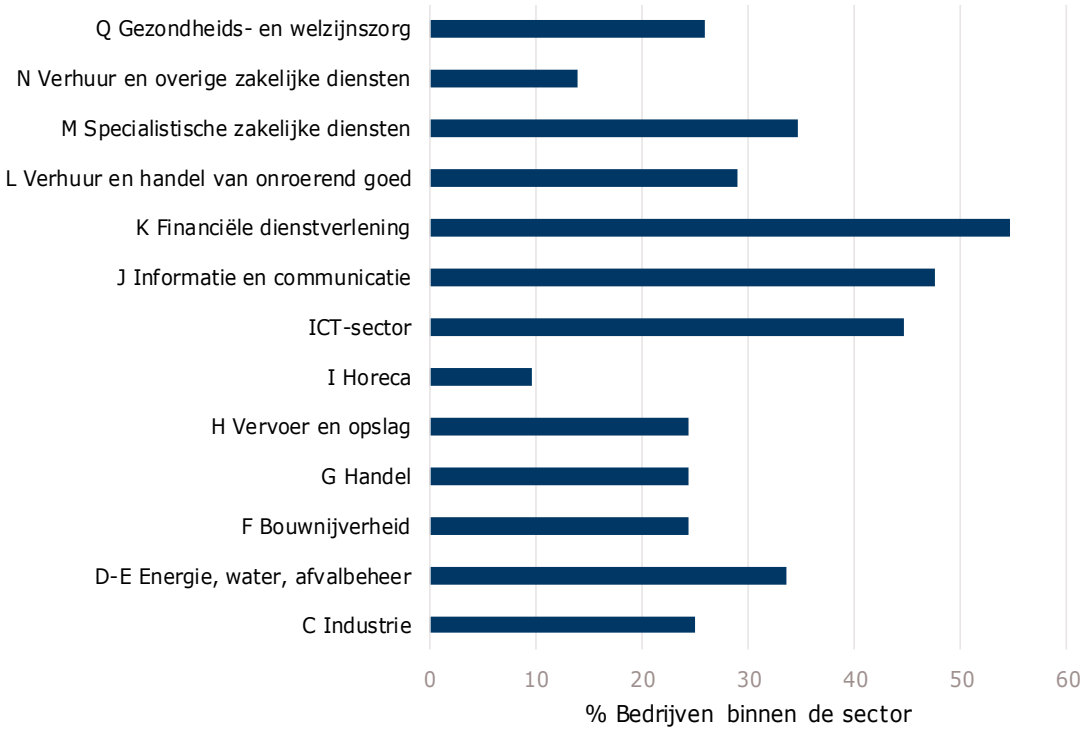
Uit onze telefonische enquête blijkt dat slechts 16%, 126 van de 806 MKB's, behoefte heeft aan meer informatie over cyberveiligheid. Zij hebben vooral behoefte aan algemene informatie over cyberveiligheid. Wat kun je doen om incidenten te voorkomen en, als er toch iets gebeurt, wat te doen in welke situatie? Eveneens is er de behoefte om te weten waar betrouwbare informatie te vinden is (voor velen nu onbekend – sommigen noemen zelfs specifiek dat de overheid een betrouwbaar centraal punt moet leveren), waar je jezelf kunt melden na gehackt te zijn en waar je kunt lezen over rechten en plichten. Ook geven een aantal respondenten aan dat ze graag een stress test willen doen om na te gaan of hun beveiliging voldoende is. Er is geen vraag naar specifieke informatie over een bepaalde vorm van cyberdreiging. Informatie ontvangen de bedrijven het liefst via email vanuit een centraal, betrouwbaar loket (zie Figuur 12).



Figuur 12. Hoe wilt u informatie tot u krijgen over cyberveiligheid? (n=126: elk bedrijf dat aangaf behoefte te hebben aan meer informatie over cyberveiligheid). Bron: eigen data – telefonische enquête (2020).

Uit de data van CBS[108] blijkt dat ongeveer de helft van alle bedrijven in de financiële, ICT- en informatie en communicatiesector in 2019 gezocht heeft naar meldingen over cyberdreigingen (zoals informatie over bekende kwetsbaarheden). Voor de andere sectoren ligt dit percentage veel lager (zie Figuur 13). Eveneens geldt dat grotere bedrijven veel vaker zoeken naar meldingen dan kleine bedrijven.

[108] Statline ICT-gebruik bij bedrijven – ICT-veiligheid 2019.



Figuur 13. Gezocht naar meldingen cyberdreigingen per bedrijfstak in 2019 (in % bedrijven). Bron: CBS ICT-gebruik bij bedrijven – ICT-veiligheid 2019.

4.5 Informatiebehoefte bedrijven naar cybermaturity

In de volgend paragrafen zoomen we in op behoeften van bedrijven naar informatie over cybersecurity. We onderscheiden vier categorieën, oplopend in cybermaturity.

4.5.1 Bedrijven met een lage cybermaturity

Deze categorie bestaat voornamelijk uit ZZP'ers en kleinbedrijven met een beperkte IT-component. Een typisch bedrijf dat in deze categorie valt is de lokale bakker. Bedrijven met een lage cybermaturity maken vooral gebruik van Google- en Microsoftdiensten. Het is een relatief moeilijk te bereiken doelgroep, maar de impact van een aanval is vermoedelijk ook minder groot dan bij andere typen bedrijven. Het zou niet correct zijn om te stellen dat alle ZZP'ers tot deze categorie behoren, de kennis van cybersecurity van ZZP'ers verschilt namelijk sterk (net als van kleinbedrijven), het is echter aannemelijk dat de meeste ZZP'ers tot deze categorie behoren (evenals een groot aantal kleinbedrijven).[109] Informatie over deze categorie komt daarom vooral uit de telefonische enquête (gefilterd op kleinbedrijven), de interviews met belangenbehartigers van ZZP'ers en de focusgroep met ZZP'ers.

Binnen het kleinbedrijf is de informatie en communicatiesector de sector die het meest behoefte heeft aan meer informatie over cyberveiligheid (hoewel deze sector in de regel al over meer kennis beschikt dan de andere branches), 24% van hen geeft aan deze behoefte te hebben. [110] Vlak daarna volgen bedrijven in de handel (21%), horeca (21%) en industrie

[109] CBS Verkennend onderzoek cyberweerbaarheid onder zzp'ers (maart 2020). In opdracht van het DTC.

[110] Eigen data – telefonische enquête (2020)

(20%). De gezondheids- en welzijnszorg (12%), het onderwijs (10%) en de financiële dienstverlening (9%) hebben het minst behoefte aan meer informatie. Qua type informatie dat ZZP'ers en kleinbedrijven nodig hebben gaat het vooral over bewustwording rondom cyberveiligheid en om algemene informatie. Informatie moet op een laagdrempelige manier worden gebracht, moet actiemogelijkheden bevatten en moet op verschillende manieren worden verspreid.

Uit de interviews met de belangenverenigingen blijkt dat ZZP'ers zeer divers zijn. Veel ZZP'ers hebben weinig of niets met computers/systemen/internet van doen; zij gebruiken bijvoorbeeld Word en Excel voor de administratie, maar verder niets. Veel van deze ZZP'ers zullen logischerwijs weinig behoefte hebben aan kennis over cybersecurity. Tussen de ZZP'ers die wel meer met cyber te maken hebben, verschilt het kennisniveau sterk. Dit kan ook invloed hebben op de behoefte aan informatie. Uit de focusgroep blijkt duidelijk dat er een groep ZZP'ers is die een behoefte heeft aan informatie over cybersecurity waarin momenteel niet goed wordt voorzien. Deze behoefte werken wij hieronder uit.[111]

Volgens de gesproken ZZP'ers in de focusgroep is er betreffende cybersecurity nauwelijks voorlichting. De voorlichting die er is, is volgens hen versnipperd en komt vaak niet van betrouwbare, neutrale partijen, maar van bedrijven die geld willen verdienen. Ze hebben het gevoel dat in geval van een hack, ze volledig toegewezen zijn op hun eigen kennis of iemand in hun persoonlijke netwerk. De gesproken ZZP'ers hadden zonder uitzondering behoefte om te checken of wat ze nu aan cybersecurity doen voldoende is en sommige suggereerde ook een benchmark met andere ZZP'ers. Onder de gesproken ZZP'ers was er een algemeen verlangen naar een betrouwbare en neutrale partij. Feitelijk kan het DTC deze rol vervullen, maar niemand van de gesproken ZZP'ers kende het DTC. Toch hadden ze allemaal behoefte aan precies hetgeen het DTC aanbiedt, namelijk een basisscan.[112] Daarnaast gaven de ZZP'ers aan dat de voorlichting waar ze behoefte aan hebben vooral én-én-én moet zijn. Een goede basiswebsite, nieuwsbrieven, papieren brieven, een stand op bijeenkomsten waar veel ZZP'ers komen, etc.

Over de rol van de overheid waren de ZZP'ers duidelijk: ze verwachten dat de overheid op zijn minst verantwoordelijkheid neemt voor goede opsporing en handhaving (en daarvoor moet ook een helder aanspeekpunt zijn). Daarnaast moet ze informeren over wat een ZZP'er zou kunnen doen om cybersecure te zijn. Met andere woorden, er moet betrouwbare basisinformatie beschikbaar zijn, op basis waarvan de ZZP'er zelf zijn of haar keuzes kan maken. Het is duidelijk dat het DTC voor een groot deel al in deze behoeften kan voorzien (opsporing en handhaving uitgezonderd). Het is op dit punt dus belangrijk om te werken aan naamsbekendheid en vindbaarheid van het DTC.

4.5.2 Bedrijven die beveiligingsdiensten afnemen van IT-leveranciers

De tweede categorie bedrijven zijn de bedrijven die beveiligingsdiensten afnemen van IT-leveranciers, deze groep hebben wij geïdentificeerd op basis van interviews met experts. Deze bedrijven leggen de verantwoordelijkheid van hun cybersecurity grotendeels in handen van een externe partij, met wie ze bij een incident contact opnemen. Bedrijven die hiervoor kiezen gaan ervan uit dat IT-leveranciers de expertise hebben om hun bedrijf te beschermen.

---

[111] De focusgroep is naar alle waarschijnlijkheid niet representatief is voor alle ZZP'ers in Nederland. Zoals besproken zijn ZZP'ers een diverse groep, en deelnemers aan een vrijwillige focusgroep zijn per definitie mensen die interesse hebben om over het onderwerp in gesprek te gaan.

[112] Het DTC biedt deze aan op: https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen/doe-de-basisscan-cyberweerbaarheid.

De leverancier wordt gezien als een partij die veilige diensten moet aanbieden en verantwoordelijk is voor het updaten van deze diensten.

Deze bedrijven weten met wie ze contact op moeten nemen bij een incident. Zij worden dus bereikt, volgens de hier gehanteerde definitie van bereiken. De behoefte aan informatie over cybersecurity lijkt voor deze groep bedrijven dan ook beperkt te zijn. Indien een partij als het DTC deze doelgroep actief van informatie zou willen voorzien, kan dit het beste door IT-leveranciers te benaderen (zie paragraaf 4.5.4 voor een toelichting bij deze categorie).

4.5.3 Cybermature bedrijven

De derde categorie zijn de zogenaamde cybermature bedrijven: de bedrijven die zelf goed hun IT-beveiliging regelen. Deze categorie bestaat voornamelijk uit grootbedrijven, die zelf experts in huis hebben om hun IT-beveiliging te regelen. Uit onze interviews met experts op het gebied van cybersecurity en vertegenwoordigers van grootbedrijven kan geconcludeerd worden dat vooral deze bedrijven niet goed bediend worden wat betreft (gewenste) informatievoorziening. Zij hebben, net als gespecialiseerde IT-bedrijven (zie paragraaf 4.5.4), behoefte aan gerichte dreigingsinformatie. Als er softwarelekken zijn, of andere dreigingen die potentieel betrekking op hen hebben, dan willen ze dat zelf weten omdat ze zelf ook in staat zijn om ernaar te handelen. Er zijn echter weinig mogelijkheden om aan deze informatie te komen. Zoals beschreven in het vorige hoofdstuk heeft (binnen de overheid) vooral het NCSC deze informatie, en kan en mag het NCSC deze informatie niet delen met niet-vitale bedrijven. Vanwege de omvang van deze bedrijven, en vanwege hun eventuele connecties met vitale bedrijven, ligt het voor de hand dat de maatschappelijke en economische gevolgen van een aanval of lek groot kunnen zijn, zelfs al zijn zij zelf niet vitaal. Het is dus belangrijk om, waar mogelijk, in de behoefte van deze bedrijven naar dreigingsinformatie te voorzien.

4.5.4 Gespecialiseerde IT-bedrijven

De laatste categorie bestaat uit IT-leveranciers, netwerkbeheerders, internet service providers (ISP's), managed service providers (MSP's)[113] en andere gespecialiseerde IT-bedrijven. Dit is de belangrijkste doelgroep van de door de markt zelf opgezette meldpunten, zoals het Nederlands Security Meldpunt, het DIVD en het Abuseplatform. en deze bedrijven zijn (doorgaans) op de hoogte van wat er in de Amerikaanse Common Vulnerabilities and Exposures (CVE) staat.[114] Het bereiken van deze doelgroep is dan ook relatief makkelijk.

Deze groep is momenteel aangewezen op publieke informatie en informatie die voortkomt uit private initiatieven, zoals de zojuist genoemde meldpunten. Ze zouden geholpen zijn met (meer) dreigingsinformatie van het NCSC, die ze nu slechts deels ontvangen. Zoals in het voorgaande hoofdstuk besproken is het op dit moment geen taak van het NCSC om deze informatie te delen met individuele bedrijven uit deze groep en is de informatieverstrekking via OKTT's nog redelijk beperkt.

In theorie zorgt het bedienen van deze groep ervoor dat ook de bedrijven die IT uit handen geven worden afgevangen, wat de urgentie voor het verkrijgen van dreigingsinformatie voor deze groep bedrijven alleen maar groter maakt.

---

[113] Aanbieders van bijvoorbeeld netwerkdiensten, digitale infrastructuur of beveiligingsdiensten.

[114] 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.

4.6 Operational Technology

Dat we in Nederland een tekort hebben aan cybersecurity experts is algemeen bekend. Een verdere uitvraag in interviews biedt meer inzicht in de thema's waarop kennis tekortschiet. Uit de interviews kwam één thema naar voren waar nog veel lacunes in kennis zijn: Operational Technology (OT). OT is het gebruik van hardware en software om fysieke processen, apparaten en infrastructuur aan te sturen. Systemen voor OT voeren een breed scala aan taken uit, variërend van het bewaken van kritieke infrastructuur tot het besturen van robots op een productievloer. OT wordt bijvoorbeeld ingezet bij industriële processen. OT-systemen zijn in het verleden vaak ontworpen met weinig aandacht voor cybersecurity. De reden hiervoor was simpel: ze waren volledig gescheiden van andere IT-systemen en internet, en uitgerold in een geïsoleerde omgeving met beperkte data-uitwisseling met een IT-omgeving. Door een groeiende behoefte aan data-uitwisseling (bijv. real-time data en industriële IoT) worden IT en OT steeds meer met elkaar verbonden. Dreigingen in het IT-domein verspreiden zich daarmee steeds meer naar het OT-domein.[115]

Een aantal OT cyberaanvallen heeft dan ook het nieuws gehaald. Ter illustratie geven we hier een paar voorbeelden: uitschakeling uraniumcentrifuges Iran (2010), uitval elektriciteitsnetwerk Oekraïne (2015 en 2016), ransomware aanval op containeroverslagbedrijf Nederland (2017), Triton-aanval[116] op de raffinaderij van Aramco (2017), aanval op elektriciteitsnetwerk VS (2018), malware aanval op TSMC (2018), WannaCry[117] aanval op fabriek van Boeing (2018).

In 2019 heeft onderzoeksbureau Pb7 Research een survey uitgezet onder bedrijven die gebruikmaken van OT.[118] Meer dan de helft van de ondervraagde organisaties geeft aan dat industriële controlesystemen met het kantoornetwerk zijn verbonden. Ook geeft 57% aan dat cybersecurity in productieomgevingen (OT-omgevingen) onvoldoende of helemaal niet wordt erkend als een risicofactor. Ontbreken van zicht op kwetsbaarheden en onvoldoende bewustzijn van risico's worden als grootste uitdagingen genoemd.

OT-security vraagt om een andere aanpak en de kennis bij overheidspartijen op dit gebied lijkt onvoldoende. Daarmee zijn bedrijven met problemen al snel toegewezen tot private IT-consultants zoals FOX-IT. Interessant is dat Cyberweerbaarheidscentrum Maakindustrie (Oost Nederland)[119] een scan of weerbaarheidsanalyse heeft ontwikkeld speciaal voor OT-security. Op die manier vullen zij een deel van de behoefte al in.

4.7 Samenvattende conclusie

We sluiten dit hoofdstuk af met een korte samenvatting, waarbij we in dit geval de volgende twee onderzoeksvragen gecombineerd beantwoorden:

Deelvraag 6a: Welke doelgroepen worden nu nog niet bereikt (wie nog niet?)

Deelvraag 7: Over welke aspecten van cybersecurity zou welke informatie-uitwisseling en samenwerking met deze doelgroepen dienen plaats te vinden?

---

[115] Zie bijv. PWC (2018). Cybersecurity van operationele technologie

[116] Triton is malware die ervoor kan zorgen dat er een fout ontstaat in bepaalde veiligheidssystemen.

[117] WannaCry is ransomware: malware die zorgt dat het slachtoffer niet meer bij zijn gegevens kan, tenzij de aanvaller dat weer toestaat, bijvoorbeeld na betaling.

[118] https://www.infosecuritymagazine.nl/artikelen/nationale-cybersecurity-monitor-2020-steeds-meer-incidenten-met-medewerkers

[119] Samenwerkingsverband gelinkt aan DTC.

Op basis van eigen dataverzameling 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.
- 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 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 CVE databank, etc.), is er nog steeds duidelijke behoefte naar (additionele) dreigingsinformatie in de Nederlandse context, zoals die momenteel beschikbaar is binnen de NCSC.

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 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.

5 Oplossingsrichtingen voor het bereiken van alle partijen

In dit hoofdstuk bespreken we verschillende oplossingsrichtingen om huidige problemen op te lossen en lacunes in het stelsel af te dekken. We staan daarbij ook stil bij hoe deze mogelijkheden zich verhouden tot de regelgeving. Deelvragen die in dit hoofdstuk worden beantwoord:

Deelvraag 5: Wat zou aan informatie-uitwisseling en samenwerking nog nodig zijn in de huidige situatie om deze structureel te borgen en breder in te richten en de diverse aspecten van cybersecurity te borgen?

Deelvraag 6b: Op welke wijze en via welke vakdepartementen zouden voor [deelgroepen die nog niet bereikt worden] nog nieuwe wijzen van informatie-uitwisseling (wat is er nog niet) kunnen worden gecreëerd?

Deelvraag 8: Hoe verhouden de gevonden (on)mogelijkheden zich tot de vigerende regelgeving over concurrentievervalsing, bijv. de Wet Markt en Overheid alsmede Wet beveiliging netwerk- en informatiesystemen (Wbni)?

5.1 Nieuwe wijzen van informatie-uitwisseling

Zoals in de vorige hoofdstukken al naar voren kwam, zijn er obstakels rondom het delen van informatie. Uitgesplitst naar voorlichtings- en dreigingsinformatie lijkt er bij het eerste vooral sprake te zijn van een probleem rondom het bereik van de informatie en de herkenbaarheid van spelers, terwijl er bij het tweede juist sprake is van juridische barrières rondom het delen. Zoals bekend, en bevestigd in de interviews, is de realisatie van het niet-vitale deel van het stelsel op dit moment nog niet voldoende uitgewerkt. Hierbij dient wel erkend te worden dat het huidige stelsel nog volop in ontwikkeling is. Zo zijn het DTC en NCSC opgezet en is het vitale deel van het stelsel grotendeels afgedekt. Nu het stelsel de Rijksoverheid en de vitale partijen dekt, wordt er gewerkt aan een uitbreiding van het stelsel richting het MKB via het DTC. Binnen deze ontwikkeling worden er ook nieuwe samenwerkingsverbanden opgezet die bedrijven per branche kunnen voorzien van informatie. Op deze manier breidt het stelsel zichzelf langzaamaan uit.

In dit onderzoek hebben wij vastgesteld welke gaten en problemen er op dit moment nog in het landelijk dekkend stelsel zitten; verschillende doelgroepen vallen deels buiten de boot (met name kleine bedrijven voor voorlichtingsinformatie en de niet-vitale cybermature bedrijven voor dreigingsinformatie) en niet alle thema's zijn even goed afgedekt door de huidige structuur (specifiek Operational Technology). In dit hoofdstuk bespreken we welke oplossingsrichtingen mogelijk zijn. Deze oplossingsrichtingen zijn voortgekomen uit een integrale analyse van de interviews, enquête en deskstudie, en zijn getoetst op juridische haalbaarheid. We behandelen ze hieronder. Oplossingsrichting 1 gaat over het breder delen van voorlichtingsinformatie. Oplossingsrichting 2 t/m 6 hebben vooral betrekking op het delen van dreigingsinformatie.

5.1.1 Oplossingsrichting 1: Richting één (bekend) loket voor MKB's en ZZP'ers

Een deel van het MKB en de ZZP'ers hebben behoefte aan één centraal loket voor alles wat met cybersecurity te maken heeft. Uit de telefonische enquête en focusgroep/interviews concluderen wij echter dat een aanzienlijke groep ondernemers geen idee heeft waar ze

terecht kunnen met vragen en waar betrouwbare informatie te vinden is. Het DTC is een voor de hand liggende optie en is in feite al een soort centraal loket, maar slechts weinig ondernemers zijn bekend met deze organisatie.[120] Het betekent echter niet dat het DTC alle informatie zelf in huis moet hebben, maar wel dat het door kan verwijzen naar partijen die wel over gespecialiseerde kennis beschikken. Kortom, de informatiedekking moet worden verbreed en de vindbaarheid van centrale partijen vergroot. Dat is voornamelijk een marketingkwestie, waarmee partijen veelvuldig en via verschillende routes moeten worden gewezen op het bestaan van het DTC (of een andere herkenbare organisatie).

5.1.2 Oplossingsrichting 2: Verspreiden restinformatie van NCSC via DTC naar de samenwerkingsverbanden

Het NCSC is bij uitstek de partij in Nederland met de meest complete en waardevolle (dreigings)informatie. Deze organisatie krijgt vanuit een grote variëteit aan bronnen (denk aan internationale overheidspartijen, bedrijven als Microsoft, etc.) dreigingsinformatie binnen. Het betreft grote hoeveelheden gegevens, waarvan het deel dat gaat over vitale partijen en organisaties binnen het Rijk door het NCSC naar de betreffende partijen wordt doorgezet. Informatie die over de niet-vitale sector gaat kan het NCSC echter niet direct naar de betreffende partijen doorzetten. Ook mag het NCSC deze 'restinformatie' slechts beperkt met andere organisaties delen, zoals besproken in paragraaf 3.2.

In de toekomst zou het NCSC deze informatie met het DTC kunnen delen, beide partijen zien het belang hiervan in. Het DTC kan dan zorgen dat de informatie bij de juiste samenwerkingsverbanden voor de niet-vitale sector terechtkomt. Deze samenwerkingsverbanden kunnen vervolgens hun achterban als geheel, of individuele partijen daarin, op de hoogte stellen van dreigingen. Ook kan het DTC een eigen directe achterban creëren, door bedrijven de mogelijkheid te bieden om zich aan te melden via het Digital Trust Platform. Deze bedrijven kunnen dan direct door het DTC worden geïnformeerd over relevante dreigingen.

Vereisten Wbni en AVG

Om het voor het NCSC juridisch mogelijk te maken om deze informatie aan het DTC te verstrekken zal het DTC OKTT-status moeten verkrijgen (zie paragraaf 3.2). Een andere mogelijkheid is uiteraard dat de Wbni wordt aangepast om het delen van dreigingsinformatie en/of vertrouwelijke informatie met het DTC mogelijk te maken zonder deze aan te wijzen als computercrisisteam of OKTT.

Een wet die echter niet snel zal worden aangepast is de AVG, wat betekent dat er twee belangrijke vereisten zijn waar in ieder geval aan moet worden voldaan in het kader van deze oplossingsrichting:

- Het DTC heeft een wettelijke grondslag nodig om dreigingsinformatie met persoonsgegevens te mogen verwerken.
- Het verstrekken van persoonsgegevens door het NCSC moet aan het noodzakelijkheidsvereiste uit de AVG voldoen.

Een (sterkere) wettelijke grondslag van het DTC is in ontwikkeling (zie paragraaf 3.2.1), deze zal naar verwachting de meeste juridische obstakels wegnemen. Het zou echter best nog even kunnen duren voordat deze wet rond is. Uit de gevoerde gesprekken blijkt dat het wellicht mogelijk zou zijn om op basis van de Begrotingswet, in combinatie met het concrete wetsvoorstel, al te spreken van een wettelijke taak op grond waarvan het DTC persoonsgegevens mag verwerken. Daardoor zou men al kunnen beginnen met informatie-uitwisseling

[120] Vergelijk met bijvoorbeeld het Britse NCSC in het Verenigd Koninkrijk, een herkenbare centrale partij.

voordat de wet in werking is getreden, wat veel tijd zou schelen. Het is echter de vraag of een dergelijke, zwakkere, grondslag stand zou houden bij een rechter.[121]

Ook wanneer de wettelijke grondslag rond is, blijft het noodzakelijkheidsvereiste aan de kant van het NCSC bestaan: het NCSC mag alleen persoonsgegevens delen indien dit noodzakelijk is voor de uitvoering van zijn publieke taak, wat in de praktijk betekent dat het alleen persoonsgegevens met het DTC mag delen indien aannemelijk is dat het DTC ook iets met die gegevens kan. Dit komt er kort gezegd op neer dat alleen dreigingsinformatie met persoonsgegevens mag worden gedeeld indien de betreffende IP-adressen bekend zijn bij het DTC (direct of via een ander samenwerkingsverband).

Dreigingsinformatie met betrekking tot IP-adressen die niet bij het DTC bekend zijn, zou gedeeld kunnen worden nadat de IP-adressen en andere identificerende gegevens zijn verwijderd. Het DTC kan deze gegevens dan nog gebruiken om bijvoorbeeld trends of zwakheden in software te signaleren.[122]

De noodzakelijkheidstoets is ook een belangrijk aandachtspunt wanneer het gaat om automatische verwerking. Een zekere mate van automatische verwerking zal nodig zijn om deze oplossingsrichting te laten slagen (en zelfs dan is het de vraag of het DTC over genoeg capaciteit beschikt). Bij automatische verwerking van persoonsgegevens moet goed gewaarborgd zijn dat er enkel gegevens worden verwerkt waaraan het DTC handelingsperspectief kan bieden.

Concurrentievervalsing

Een van de deelvragen in dit onderzoek betreft de vraag hoe de oplossingsrichtingen zich verhouden tot de regelgeving met betrekking tot concurrentievervalsing. In het kader van deze oplossingsrichting is deze vraag relevant.

Concurrentievervalsing komt in beeld wanneer de overheid nieuwe economische activiteiten gaat verrichten. Wanneer de overheid economische activiteiten verricht is namelijk de Wet Markt en Overheid van toepassing. Deze wet, onderdeel van de Mededingingswet (Mw), geeft vier gedragsregels voor het economisch handelen van overheden.[123] In grote lijnen houden deze het volgende in:

1. het verplicht doorberekenen van de integrale kosten aan afnemers;
2. een verbod op bevoordeling van overheidsbedrijven t.o.v. andere ondernemingen;
3. een verbod om gegevens die in verband met publiekrechtelijke werkzaamheden zijn verkregen, te gebruiken voor economische activiteiten die niet dienen ter uitvoering van publiekrechtelijke bevoegdheden; en
4. een functiescheiding tussen de bestuurlijke en uitvoerende rol van de overheid.

---

[121] In de MvT bij de uAVG, en in de jurisprudentie, is te vinden dat voor een beroep op een publieke taak, die taak wel in een wet moet zijn vastgelegd, maar niet in alle gevallen in een wet in formele zin. Helaas is nergens te vinden in welke gevallen een specifieke wet in formele zin nodig is, en in welke gevallen kan worden volstaan met algemene wetgeving. Gelet op het structurele karakter van de beoogde gegevensverwerking is het echter denkbaar dat een rechter enkel genoegen zou nemen met een wet in formele zin waarin de specifieke wettelijke taak is vastgelegd. De Begrotingswet zou dan dus niet afdoende zijn, ook niet in combinatie met het wetsvoorstel.

[122] Als het DTC aannemelijk kan maken dat het zelfs iets kan met de set IP-adressen wanneer de individuele adressen onbekend zijn, bijvoorbeeld door nuttige patronen te ontdekken, is het denkbaar dat het NCSC de informatie inclusief IP-adressen kan delen.

[123] Artikel 25i t/m 25l Mw.

De vraag is nu of de gedragsregels van toepassing zijn op het verstrekken van informatie door het DTC, en, indien zij van toepassing zijn, of het DTC informatie aan bedrijven en samenwerkingsverbanden kan verstrekken zonder de gedragsregels te schenden.

De gedragsregels zijn van toepassing indien economische activiteiten worden verricht. Dat wil zeggen dat goederen of diensten worden aangeboden in concurrentie met ondernemingen.[124] De vraag is dus of bedrijven het soort data dat het DTC gratis aan hen wil verstrekken, ook zouden kunnen inkopen bij private partijen. Dit is discutabel: hoewel sommige bedrijven vergelijkbare informatie tegen betaling aanbieden aan bepaalde sectoren of bedrijven, bleek in hoofdstuk 4 dat er een duidelijke behoefte is naar (additionele) dreigingsinformatie, waar momenteel niet in wordt voorzien. Zelf geeft het DTC ook aan dat de doelgroep momenteel niet door de markt wordt bediend.

Het maakt in de praktijk echter niet uit of de gedragsregels van toepassing zijn of niet. Het DTC kan namelijk dreigingsinformatie aan partijen verstrekken zonder de regels te schenden. De enige regel die op het eerste gezicht problematisch zou kunnen zijn is regel (1), het verplicht doorberekenen van de integrale kosten. Op deze regel zijn echter een aantal uitzonderingen. Eén daarvan is de uitzondering voor gegevensverstrekking:

"Van de verplichting tot het doorberekenen van de integrale kosten zijn de economische activiteiten van uw overheidsorganisatie uitgezonderd, indien die inhouden het verstrekken van gegevens die uw organisatie heeft verkregen in het kader van de uitoefening van haar publiekrechtelijke bevoegdheden of het verstrekken van gegevensbestanden die uit de genoemde gegevens zijn samengesteld."[125]

Volgens een geïnterviewde jurist valt de gegevensverstrekking door het NCSC aan vitale partijen onder deze uitzondering. Ook gegevensverstrekking door het DTC zal hieronder vallen, het gaat immers om gegevens die het DTC heeft verkregen in het kader van de uitoefening van zijn publiekrechtelijke bevoegdheden (die vastgelegd zullen worden in de eerder genoemde aankomende wet).[126] Deze oplossingsrichting zal daardoor niet botsen met de Wet Markt en Overheid.

5.1.3 Oplossingsrichting 3: Verspreiden restinformatie van NCSC via andere partijen

Restinformatie van het NCSC zou ook via andere (private) organisaties kunnen worden verspreid. Dit kan door hier een apart platform voor in te richten, maar het kan ook door organisaties in te zetten die al over de OKTT-status beschikken. Een samenwerking tussen het DIVD en Connect2Trust[127] dient bijvoorbeeld reeds als een meldpunt voor de niet-vitale bedrijven. Hierbinnen wordt dreigingsinformatie uitgewisseld. Dit is op dit moment nog geen officieel landelijk meldpunt, maar het zou daartoe eventueel wel kunnen worden uitgebreid. Daarnaast zijn er organisaties als de Stichting Nationale Beheersorganisatie Internet Providers (NBIP) die al over een OKTT-status beschikken. Die stichting levert ondersteunende

---

[124] Ministerie van Economische Zaken, Landbouw en Innovatie (2012), Handreiking Wet Markt en Overheid, p. 14.

[125] Ministerie van Economische Zaken, Landbouw en Innovatie (2012), Handreiking Wet Markt en Overheid, p. 36. Zie ook artikel 25i(2)(b) Mw.

[126] Overigens zal het ministerie van EZK voor deze wet waarschijnlijk een staatssteuntoets uitoefenen. Als sprake is van staatssteun, volgens gesprekspartners is dit vooraf niet met zekerheid te zeggen, valt de toepasselijkheid van de gedragsregels weg (art. 25h(4) Mw).

[127] De Stichting Connect2Trust is een cross-sectoraal samenwerkingsverband tussen (inter)nationale in Nederland actieve bedrijven waarbinnen vertrouwelijke informatie over cyberdreigingen en best practices wordt uitgewisseld.

diensten aan internetproviders en heeft dus een brede dekking. Aan de hand van de IP-adressen waar kwetsbaarheden zijn gevonden kan de NBIP bepalen welke ISP's gewaarschuwd moeten worden. Op deze manier kun je de meeste netwerken in Nederland bereiken, onafhankelijk van de sector, bedrijfsgrootte of regio. Het is dus zeker een effectieve route. Een kanttekening is wel dat niet alle ISP's en MSP's zijn aangesloten bij de NBIP.

Uit het onderzoek kwam ook naar voren dat de professionaliteit, het handelingsperspectief en de AVG-compliance van sommige samenwerkingsverbanden niet afdoende is om OKTT-status te verkrijgen. Hier ligt mogelijk een rol voor het DTC, dat samenwerkingsverbanden zou kunnen helpen om deze aspecten te verbeteren.

Juridisch spelen bij deze oplossingsrichting nog wel dezelfde obstakels als eerder genoemd. Voor zover de informatie niet als herleidbaar vertrouwelijk wordt gezien omdat het IP-adres niet bij de OKTT/ISP bekend is, is wederom de noodzakelijkheidstoets een obstakel. Als het IP-adres echter wel bij de partij bekend is, wordt slachtofferinformatie (informatie over [potentiële] slachtoffers) van het NCSC gekwalificeerd als herleidbare vertrouwelijke informatie. Ondanks de OKTT-status van de genoemde partijen mogen zij daarom informatie over kwetsbaarheden van specifieke partijen in hun achterban vaak niet ontvangen. Zoals eerder aangegeven wordt momenteel een wetswijziging verkend om te proberen dit probleem te verhelpen. Een andere oplossing hiervoor zou wellicht zijn om de achterban van een OKTT, via de OKTT toestemming te laten geven aan het NCSC om in de toekomst herleidbare vertrouwelijke informatie met de OKTT te delen. Dat zou als volgt werken:

De OKTT zou onder haar achterban kunnen uitvragen wie aan het NCSC toestemming wil geven om vertrouwelijke gegevens met de OKTT te delen. Vervolgens kan de OKTT als doorgeefluik richting NCSC optreden; er wordt een lijst IP-adressen aan het NCSC gestuurd van de organisaties die het NCSC toestemming willen geven om alle (toekomstige) vertrouwelijke gegevens die op hen betrekking hebben door te geven aan de OKTT. Wanneer het NCSC dan vertrouwelijke gegevens over een IP-adres heeft, weet het nog steeds niet welk bedrijf daarachter zit, maar heeft het wel toestemming om de informatie met de OKTT te delen.[128]

5.1.4 Oplossingsrichting 4: Uitbreiding aantal computercrisisteams onder niet-vitale cybermature bedrijven

Een groep die in de huidige situatie niet goed bediend wordt wat betreft (de gewenste) informatievoorziening is de groep niet-vitale cybermature bedrijven. Zij hebben behoefte aan dreigingsinformatie op hoog technisch niveau, maar kunnen hiervoor niet aankloppen bij het NCSC. Bovendien zijn de door het bedrijfsleven zelf opgezette constructies voor het delen van dit type informatie niet volledig. Het zou voor de hand liggen om relevante informatie van het NCSC door te zetten naar deze partijen.

Zoals eerder besproken kan het NCSC deze partijen niet direct van informatie voorzien. Via aangewezen computercrisisteams (en OKTT's, zie vorige oplossingsrichting) kan dit echter wel. In januari 2020 zijn vier sectorale computercrisisteams door de minister van JenV aangewezen, waaronder het Z-CERT en SURFcert.[129] Relevante gegevens van het NCSC kunnen daardoor intensiever en efficiënter worden verspreid binnen deze sectoren. Hetzelfde is wellicht mogelijk voor (andere) niet-vitale cybermature bedrijven. Het is echter wel de vraag in

[128] Deze route is ondertussen voorgelegd aan juristen van het NCSC, die zullen onderzoeken of het inderdaad juridisch mogelijk is om op deze manier vooraf toestemming te geven voor het doorzetten van herleidbare vertrouwelijke gegevens.

[129] https://www.ncsc.nl/actueel/nieuws/2020/januari/27/aanwijzing-certs

hoeverre grote commerciële instanties bereid zijn zich aan te sluiten bij een computercrisis-team. Het is denkbaar dat zij liever niet hun incidentrespons afstaan en delen met hun concurrenten. Een verkenning onder deze doelgroep zou hier meer zicht op kunnen bieden.

5.1.5 Oplossingsrichting 5: Meer bedrijven als vitaal aanwijzen, of opsplitsing vitaal/niet-vitaal heroverwegen

Meerdere gesprekspartners vragen zich af of de splitsing tussen vitaal en niet-vitaal wel de juiste is. De vitale bedrijven worden in het stelsel afgedekt door het NCSC en de niet-vitale bedrijven worden afgedekt door het DTC. Deze opsplitsing bemoeilijkt soms de samenwerking en heeft (tot nu toe) sterke invloed op welke bedrijven voorzien worden van hoogwaardige (dreigings)informatie. Het is echter niet altijd even voor de hand liggend dat bepaalde partijen wel of niet als vitaal worden aangemerkt en ook het opsplitsen zelf zorgt al voor problemen:

- Er zijn bedrijven die diensten leveren aan vitale bedrijven, maar zelf onder de huidige opsplitsing niet als vitaal worden aangemerkt. Aangezien de huidige tak van het landelijk dekkend stelsel voor de niet-vitale bedrijven nog niet geheel is gerealiseerd, kan het zich voordoen dat vitale bedrijven via deze toeleveranciers cyberkwetsbaarheden in hun organisatie introduceren.
- Er is veel meer essentieel dan enkel de vitale sectoren. Nederland zou volledig plat komen te liggen als alleen de vitale bedrijven blijven draaien. De huidige situatie rondom het coronavirus illustreert dit. Zo is de lijst met cruciale beroepen aanzienlijk breder dan de lijst met vitale bedrijven.
- Er zijn tal van grote niet-vitale bedrijven die met dezelfde problemen omtrent cybersecurity te maken hebben als de grote vitale bedrijven. Gezien de gelijkenis in problematiek voor deze groepen, zouden ze er beiden baat bij kunnen hebben om (via het NCSC) informatie uit te kunnen wisselen.
- De opsplitsing vitaal/niet-vitaal zorgt indirect ook voor een ‘opsplitsing’ van cybersecurity experts. Het is algemeen bekend dat er een tekort is aan cybersecurity experts en in de huidige situatie wordt de waardevolle kennis gefragmenteerd ingezet, namelijk deels voor de vitale sector en deels voor de niet-vitale sector. Bij een bredere informatiedeling kan deze fragmentatie beter overbrugd worden.

Op het eerste gezicht ligt de oplossing wellicht in het vitaal verklaren van specifieke groepen bedrijven (zoals grote bedrijven en hun toeleveranciers). Om een aantal redenen is het echter niet zo eenvoudig. Ten eerste zijn er harde eisen gedefinieerd om een sector of bedrijf als vitaal aan te merken. Deze hebben te maken met de verwachte gevolgen voor de maatschappij bij uitval van de sector, bijvoorbeeld in de vorm van de omvang van de financiële schade of het aantal doden. Uiteraard zouden deze eisen aangepast kunnen worden, maar zij zijn er niet voor niets. De stempel ‘vitaal’ brengt allerlei gevolgen en verplichtingen mee voor een bedrijf, ook buiten het gebied van cybersecurity. Deze verplichtingen zijn gerechtvaardigd vanwege de impact als er iets mis gaat, maar zouden niet onnodig aan bedrijven opgelegd moeten worden. Het is dus niet zo dat nieuw vitaal-verklaarde bedrijven steun zouden krijgen van het NCSC en er verder niets voor hen zou veranderen.

Ook los van het vorige argument moet voorzichtig worden omgegaan met het uitbreiden van de doelgroep van het NCSC. Het NCSC heeft niet voldoende capaciteit om de te bedienen doelgroep oneindig uit te breiden. Gelukkig is dit ook niet nodig, omdat er meer manieren zijn om cyberweerbaarheid in de keten te verhogen (bijv. groot helpt klein, stimuleren van certificering en gebruik van veiligheidsstandaarden). Voor een deel zullen bovenstaande punten ook opgelost worden wanneer de informatie-uitwisseling tussen het NCSC en het DTC op orde is.

Desalniettemin is een discussie over de volledigheid van de lijst met vitale bedrijven op zijn plaats, of in ieder geval een discussie over de volledigheid van de doelgroep van het NCSC. Zo zou het aan die doelgroep toevoegen van de groep grote cybermature bedrijven die behoefte heeft aan dreigingsinformatie van het NCSC een deel van de lacunes in het huidige stelsel oplossen. Daarna ligt de uitdaging nog vooral bij het breder verspreiden van voorlichtingsinformatie, wat in ieder geval veel minder juridische barrières kent.

5.1.6 Oplossingsrichting 6: Een enkele back-office voor zowel NCSC als DTC

Om de informatie-uitwisseling en samenwerking tussen het NCSC en het DTC te verbeteren zouden de partijen een gezamenlijk backoffice kunnen delen. Hier zijn verschillende varianten mogelijk. Om de betere informatie-uitwisseling te realiseren moeten de partijen in ieder geval de bevoegdheid hebben om informatie met elkaar te delen, maar dit is niet alles. Zij moeten ook oplettend zijn en bedenken voor wie bepaalde informatie relevant is, om deze vervolgens ook daadwerkelijk te delen.

Volledige toegang tot elkaars informatie is voor het NCSC en het DTC juridisch niet haalbaar, al zouden sommige partijen dit wellicht wel willen. De verschillende doelgroepen van beide organisaties maken namelijk dat niet alle informatie voor beide partijen relevant is. Vanwege het noodzakelijkheidsvereiste van de AVG mag daarom niet zomaar alle informatie gedeeld worden. Er zal dus altijd een noodzakelijkheidstoets uitgevoerd moeten worden voordat informatie gedeeld kan worden, hoe het gezamenlijk backoffice ook wordt ingericht.

Een gezamenlijke backoffice hoeft niet te betekenen dat beide organisaties samen op dezelfde afdeling in één pand werken. Hoewel dit wellicht zou helpen met de collegialiteit en de samenwerking, wordt het er juridisch en organisatorisch niet makkelijker op wanneer veel informatie niet gedeeld mag worden met mensen die fysiek aanwezig zijn. Wel kan bijvoorbeeld gedacht worden aan het delen van dezelfde informatiesystemen (met gescheiden rechten).

Een gezamenlijke backoffice kan ook meer conceptueel worden gezien: een situatie waarin het NCSC en het DTC de bevoegdheid en oplettendheid hebben om relevante informatie met elkaar te delen. Hiervoor is belangrijk dat de partijen elkaars doelgroep snappen. Zij zouden daarvoor meer met elkaar in gesprek moeten gaan, eventueel via periodieke meetings waarin problemen en ambities doorgesproken worden. Hier zouden ook andere informatieknooppunten, bijvoorbeeld computercrisisteams als Z-CERT en SURFcert, bij betrokken kunnen worden.

5.2 Samenvattende conclusie

We sluiten dit hoofdstuk af met een korte samenvatting, gestructureerd langs de deelvragen die in dit hoofdstuk centraal staan. De eerste twee deelvragen worden daarbij gecombineerd behandeld:

Deelvraag 5: Wat zou aan informatie-uitwisseling en samenwerking nog nodig zijn in de huidige situatie om deze structureel te borgen en breder in te richten en de diverse aspecten van cybersecurity te borgen?

Deelvraag 6b: Op welke wijze en via welke vakdepartementen zouden nieuwe wijzen van informatie-uitwisseling kunnen worden gecreëerd voor doelgroepen die niet bereikt worden?

> 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 van NCSC via DTC naar de samenwerkingsverbanden;*
3. *Verspreiden restinformatie NCSC door andere partijen;*
4. *Uitbreiding aantal computercrisisteams 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.*

Het bovenstaande hoofdstuk bespreekt de (implementatie)aspecten van ieder van deze routes in groter detail.

Deelvraag 8: Hoe verhouden de gevonden (on)mogelijkheden zich tot de vigerende regelgeving over concurrentievervalsing, bijv. de Wet Markt en Overheid alsmede Wet beveiliging netwerk- en informatiesystemen (Wbni)?

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 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. Die aanwijzing kan echter pas plaatsvinden wanneer het DTC een wettelijke grondslag heeft om persoonsgegevens te verwerken.

6 Conclusies

In Nederland is gekozen voor decentrale organisatie van het cybersecuritystelsel. Deze netwerkbenadering heeft belangrijke voordelen, maar gaat gepaard met het risico dat de overheid een minder goed inzicht heeft als het gaat om het *bereik* van informatie over digitale veiligheid (waarbij 'bereik' verwijst naar het aantal relevantie organisaties dat weet waar ze terecht kunnen in geval van vragen over of problemen met cybersecurity). Dat mindere inzicht speelt vooral voor de niet-vitale partijen. Bij het Ministerie van Justitie en Veiligheid (JenV) speelt dan ook de vraag of informatie over cybersecurity nog breder, efficiënter[130] en effectiever kan worden gedeeld tussen publieke en private partijen, en de vraag wat er nog gedaan kan worden om een landelijk dekkend stelsel van cybersecurity te bereiken.

Met dit onderzoek hebben wij beoogd om inzicht in de situatie te geven en de volgende overkoepelende onderzoeksvraag te beantwoorden:

> *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?*

In dit afsluitende hoofdstuk presenteren we in paragraaf 6.1 de conclusies van dit onderzoek, waarna we in paragraaf 6.3 afsluiten met onze aanbevelingen.

6.1 Conclusies per deelvraag

Bij de onderstaande conclusies gebruiken we de structuur die voortkomt uit de deelvragen die in Hoofdstuk 1 zijn geïntroduceerd.

Hoe de verschillende partijen cybersecurity, en de verschillende aspecten daarvan, definiëren (deelvraag 1)

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 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.*"[131]

---

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

[131] CSBN 2020, p. 48.

De doelstellingen van het Nederlandse kabinet ten aanzien van cybersecurity (deelvraag 2)

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:[132]

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.

De huidige inrichting van het Nederlandse cybersecurity-beleid (deelvraag 3)

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 (namelijk het NCSC) en voor het bereiken van niet-vitale partijen (namelijk 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 Figuur 5 in paragraaf 3.1.1. 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 (deelvraag 4)

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 moet worden uitgelegd en wat de bedoelingen van de wetgever waren bij de beperkingen aan het delen daarvan). Het valt buiten het bestek

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

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 (deelvragen 6a en 7)

Op basis van eigen dataverzameling concluderen we dat:

- ZZP'ers en een deel van de MKB's een zeer duidelijke behoefte hebben aan informatie over cybercriminaliteit (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.
- 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 overeenkomen met die van 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 CVE databank, etc.), is er nog steeds duidelijke behoefte naar (additionele) dreigingsinformatie in de Nederlandse context, zoals die momenteel beschikbaar is binnen de NCSC.

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 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.

Mogelijkheden om doelgroepen beter te bereiken en informatiebehoeften beter te vervullen (deelvragen 5 en 6b)

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 van NCSC via DTC naar de samenwerkingsverbanden;*
3. *Verspreiden restinformatie NCSC door andere partijen;*
4. *Uitbreiding aantal computercrisisteams 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.*

Hoofdstuk 5 bespreekt de (implementatie)aspecten van ieder van deze routes in groter detail.

Hoe de oplossingsrichtingen zich verhouden tot de Wet Markt en Overheid en de Wbni (deelvraag 8)

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 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. Die aanwijzing 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 (deelvraag 9)

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 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.

6.2 Eindconclusie

6.2.1 Breder, efficiënter en effectiever informatie delen

Met het NCSC, het DTC en het toenemende aantal samenwerkingsverbanden wordt het landelijk dekkend stelsel voor cybersecurity meer en meer de realiteit. In dit onderzoek hebben wij onderscheid gemaakt tussen twee typen informatie met betrekking tot cybersecurity: voorlichtingsinformatie (informatie en advies over cyberweerbaarheid) en dreigingsinformatie (informatie over dreigingen of kwetsbaarheden met betrekking tot bepaalde bedrijven of software). De doelgroepen van, behoeften naar en juridische beperkingen bij deze twee typen informatie zijn niet gelijk, waardoor ook de conclusies en mogelijke maatregelen verschillen. Voor beide typen informatie geldt wel dat de lacunes zich vooral in de niet-vitale sector bevinden. De vitale sector is door het NCSC over het algemeen goed afgedekt.

Voorlichtingsinformatie

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. De eerste oplossingsrichting betreft daarom het toewerken naar een centraal loket voor alle bedrijven. Het DTC zou hier een logische kandidaat voor zijn, omdat het deze rol deels al vervult. Om deze rol goed te vervullen moeten vooral nog flinke stappen gezet worden in het creëren van een groter bereik en grotere bekendheid van het DTC.

Dreigingsinformatie

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. De bedoeling van de wetgever was om deze informatie via OKTT's door te zetten naar de relevante bedrijven in de niet-vitale sector, maar de huidige regelgeving leidt tot een eigenlijk paradoxale situatie waarin OKTT's bepaalde dreigingsinformatie, namelijk slachtofferinformatie, bijna nooit van het NCSC mogen ontvangen: als zij geen IP-adressen van hun achterban hebben mogen zij veel dreigingsinformatie niet ontvangen omdat ze niet voldoende handelingsperspectief aan de persoonsgegevens kunnen bieden, maar als zij wel IP-adressen van hun achterban hebben mogen ze slachtofferinformatie vaak niet ontvangen vanwege het verbod op het delen van herleidbare vertrouwelijke informatie. Dit is niet het enige obstakel, 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.

We kunnen echter niet negeren dat de groep niet-vitale cybermature bedrijven op het moment niet goed wordt bediend wat betreft de gewenste informatievoorziening en beperkt toegang heeft tot de informatie die zij nodig achten om cyberweerbaar te kunnen functioneren. In tegenstelling tot het breder verspreiden van voorlichtingsinformatie en het herkenbaarder maken van het DTC – wat op termijn vermoedelijk ook vanzelf gebeurt als het op de huidige manier doorgaat – zal deze lacune in het huidige stelsel niet worden opgelost als er geen (juridische) stappen worden ondernomen. Met oplossingsrichtingen 2 t/m 5 hebben wij verschillende mogelijkheden besproken om dreigingsinformatie van het NCSC toch te kunnen laten neerslaan bij de niet-vitale bedrijven die daar behoefte aan hebben; via het DTC, via OKTT's, via een uitbreiding van het aantal computercrisisteams en via een uitbreiding van het aantal vitale bedrijven (dan wel van de doelgroep van het NCSC).

In de toekomst is het belangrijk dat dreigingsinformatie niet alleen van het NCSC via een of meer van de genoemde wegen naar de niet-vitale sector stroomt, maar dat informatie ook van niet-vitaal naar vitaal stroomt. De meest voor de hand liggende manier om dit te bereiken is via een goede informatie-uitwisseling tussen het NCSC en het DTC. Oplossingsrichting 6 richt zich hierop: via een (conceptueel) 'gezamenlijke backoffice' zou informatie in de toekomst makkelijker gedeeld kunnen worden met partijen voor wie dit relevant is.

6.2.2 Richting een landelijk dekkend cybersecuritystelsel

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). Door genoegen te nemen met een minder sterke wettelijke grondslag (gebaseerd op de begrotingswet en een concreet wetsvoorstel) zou sneller gestart kunnen worden, maar daarmee zou de overheid zich juridisch in een grijs gebied bevinden. Het is denkbaar dat deze grondslag geen stand zou houden bij toetsing door een rechter.

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 5.1.3), 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.

Het uitbreiden van het aantal computercrisisteams voor niet-vitaal (oplossingsrichting 4) is een interessante richting, maar vereist wel dat commerciële partijen bereid zijn om zich hierbij aan te sluiten en hun incidentrespons te delen. Over die bereidwilligheid kunnen wij op basis van dit onderzoek geen uitspraken doen. Een verdere verkenning van deze oplossingsrichting zou daarom kunnen beginnen met een uitvraag onder deze partijen.

Het uitbreiden van de lijst vitale bedrijven (oplossingsrichting 5) kent flinke haken en ogen, omdat de status 'vitaal' over meer gaat dan alleen cybersecurity en ook andere gevolgen en verplichtingen meebrengt. Toch lijkt het een goed idee om eens goed te kijken of de doelgroep van het NCSC niet beter zou kunnen worden uitgebreid, zodat (een deel van) de huidige niet-vitale cybermature bedrijven beter van dreigingsinformatie kan worden voorzien.

Zowel het aantal aangewezen computercrisisteams als de indeling vitaal/niet-vitaal zijn voortdurend in ontwikkeling, maar beide richtingen verdienen in onze ogen meer aandacht naarmate de zojuist besproken richtingen 2 en 3 minder voorspoedig verlopen. Als richtingen 2 en 3 goed verlopen kan het voldoende zijn om de computercrisisteams en de splitsing vitaal/niet-vitaal zich te laten ontwikkelen zoals ze dat nu al doen, maar het kan geen kwaad om hier extra aandacht aan te geven om het landelijk stelsel een impuls te geven.

Het gezamenlijk backoffice (oplossingsrichting 6) ligt enigszins in het verlengde van richting 2. Er wordt momenteel al gewerkt aan het verbeteren van de samenwerking tussen het NCSC en het DTC, maar wanneer de wettelijke grondslag van het DTC rond is kan dit naar het volgende niveau getild worden. Dan kunnen de twee organisaties elkaar namelijk daadwerkelijk helpen door dreigingsinformatie uit te wisselen.

6.3 Aanbevelingen

Op basis van de dit onderzoek komen we tot drie aanbevelingen die hieronder nader worden uitgewerkt.

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.

Bijlage 1. Overzicht gesprekspartners

Naam	Organisatie	Functie
Alex de Joode	NLDigital	Public policy officer
Alexis Barron	Cyber Weerbaarheidscentrum Brainport	Directeur
Andries Kuipers en Eelco van Vliet	CBS	Projectleider cybersecurity monitor en statistisch onderzoekers
Angela van der Putten	Inspectie Justitie en Veiligheid	Hoofdinspecteur Migratie, Cyber en Security
Erik Miedema	MKB Cyber Campus	Directeur
Frank Alfrink	ZZP-Nederland	Directeur
Frank Breedijk	Nederlands cybersecurity meldpunt en Schuberg Philis	Directeur/CISO
Hans de Vries en Charlotte Kroon-Koning	NCSC	Directeur, Coördinerend juridisch adviseur privacy en cybersecurity
Jaya Baloo	Avast	CISO
John Remmerswaal	NCTV	Programmamanager PNDV
Margreet Drijvers	PZO	Directeur
Marjolijn Bonthuis	ECP	Programmamanager Cybersecurity Alliantie
Michel Verhagen, Liesbeth Kruizinga en Kim van der Veen	DTC	Programmamanagers, relatiemanager
Nicole Mallens	VNO-NCW	Secretaris cybersecurity MKB
Octavia de Weerdt	Abuse platform en NBIP	Algemeen directeur
Petra Oldengarm	Cyberveilig Nederland	Directeur
Raymond Bierens	Connect2Trust, Cybery, C-CERT	Voorzitter, directeur
Stijn Bouwhuis en Leah Postma	FME	Belangenbehartiger Digitalisering & Cybersecurity, clustermanager security

Bijlage 2. Landenstudies

In deze bijlage beschrijven we de cybersecuritystelsels en best practices van de volgende landen: het Verenigd Koninkrijk, Frankrijk en Duitsland.[133] De nadruk ligt op de samenwerking en informatie-uitwisseling tussen publieke en private partijen.

Verenigd Koninkrijk

Inrichting cybersecuritystelsel op hoofdlijnen

De basis van het cybersecuritystelsel van het Verenigd Koninkrijk ligt in de National Cyber Security Strategy 2016-2021[134]. Deze strategie valt onder het National Cyber Security Programme en hierin worden de overheidsplannen om het land veilig en veerkrachtig in cyberspace te maken, uitgewerkt. Daar hangt een groot budget aan, namelijk £1,9 miljard (ca. €2,2 miljard). De vorige strategie (van 2011) had een budget van £860 miljoen (ca. €1 miljard).

Een belangrijke uitvoerende partij van de strategie is het Britse National Cyber Security Centre (Britse NCSC), opgericht op 1 oktober 2016. Het Britse NCSC is de centrale organisatie op het gebied van cybersecurity in het hele Verenigd Koninkrijk. Deze organisatie beheert nationale cyberincidenten, dient als expertisecentrum en levert ondersteuning aan departementen, decentrale overheden en bedrijven. Ook het stimuleren van innovatie en ontwikkeling van cybersecurity skills valt onder de taak van het Britse NCSC. Het Government Communications Headquarters (GCHQ)[135] is de moederorganisatie en daarmee kan het Britse NCSC gebruikmaken van expertise op zeer hoog niveau. Het Britse NCSC werkt actief aan samenwerkingen tussen overheid, publieke sector, (vitale en niet-vitale) bedrijven en inwoners.

Met de komst van het Britse NCSC werd het cybersecuritylandschap een stuk simpeler: kennis en vaardigheden vanuit Communications-Electronics Security Group (CESG; de informatiebeveiligingsafdeling van GCHQ), het Centre for the Protection of National Infrastructure, CERT-UK, en het Centre for Cyber Assessment worden samengevoegd in één organisatie. Eén verenigd advies- en meldpunt (voor incidenten) voor iedereen. Het Britse NCSC heeft een hoofdkantoor in Londen en heeft een team van ca. 700 werknemers.[136]

De National Crime Agency (NCA) is de belangrijkste partij wanneer het aankomt op het bestrijden van cybercrime (naast onderwerpen als georganiseerde misdaad). Zij werken nauw samen met (inter)nationale partijen. Het Verenigd Koninkrijk heeft daarnaast een uitgebreide wetgeving op het gebied van cybersecurity, waaronder de Computer Misuse Act.[137] Om de standaarden voor cybersecurity te verhogen, maakt de regering vooral gebruik van de beschikbare wetten (zoals de Europese General Data Protection Regulation (GDPR), ofwel

---

[133] De keuze voor deze landen is in samenspraak met de begeleidingscommissie gemaakt en berust op een quick scan.

[134] Cabinet Office. National Cyber Security Strategy 2016 to 2021 (gepubliceerd op 1 november 2016 op www.gov.uk).

[135] Britse inlichtingendienst

[136] Cabinet Office. National Cyber Security Strategy 2016 to 2021 (gepubliceerd op 1 november 2016 op www.gov.uk).

[137] Deze wet maakt de handeling van toegang tot of wijziging van gegevens die op een computersysteem zijn opgeslagen, strafbaar maakt zonder de juiste toestemming.

de AVG), wanneer nodig door aanvullende regelgeving.[138] Het Verenigd Koninkrijk heeft ook een stevig beleid voor certificatie van organisaties en (IT-) professionals. Alle bedrijven die meedingen naar overheidsopdrachten zijn verplicht om te voldoen aan bepaalde basisbeveiligingsmaatregelen. De maatregelen zijn vastgelegd in het Cyber Essentials Scheme.[139]

Maturity

De Global Cybersecurity Index (GCI) is een gewaardeerde meting van de inzet van landen op het gebied van cybersecurity. Uit de rapportage van 2018 blijkt dat het Verenigd Koninkrijk wereldwijd het beste scoort met een score van 0,931.

Tabel 5. Scores Global Cybersecurity Index – Verenigd Koninkrijk

Kenmerk	Toelichting	Score (max 0,200)
Legal	Wet- en regelgeving omtrent cybersecurity	0,200
Technical measures	CERT, standards implementation framework, etc.	0,191
Organizational measures	Nationale strategie, organisatie, maatstaven	0,200
Capacity building measures	Publieke awareness initiatieven, training voor professionals, certificering, etc.	0,189
Cooperation measures	Overeenkomsten, deelname in internationale verbanden, pps-en, best practices, etz.	0,151[140]

Internationale samenwerkingen

(Inter)nationale samenwerking is een belangrijk thema in de National Cyber Security Strategy. Er wordt vooral ingezet op multilaterale organisaties zoals de Verenigde Naties, G20, Europese Unie, NAVO, OVSE, Raad van Europa en het Gemenebest. Maar ook niet-overheidspartijen als industrie, burgers, academia en de technische gemeenschap worden als cruciaal beschouwd voor het beleid.

Bereik van bedrijven en best practices

Het Verenigd Koninkrijk staat bekend om haar succesvolle awareness- en informatie-uitwisselingsinitiatieven. Onderdeel van de opgestelde strategie was het Active Cyber Defence programma.[141] De missie van dat programma luidt als volgt: "Protect the majority of people in the United Kingdom from the majority of the harm caused by the majority of the cyberattacks the majority of the time." Het programma is geëvalueerd door King's College London en zij concludeerden dat het een significante waarde heeft voor het verbeteren van de nationale cybersecurity in het VK.[142] Duizenden aanvallen zijn inmiddels voorkomen en de gemiddelde tijd dat een phishing site online is, is verminderd van 27 naar 1 uur.[143]

---

[138] Cabinet Office. National Cyber Security Strategy 2016 to 2021 (gepubliceerd op 1 november 2016 op www.gov.uk).

[139] Geert Munnichs, Matthijs Kouw & Linda Kool, Een nooit gelopen race - Over cyberdreigingen en versterking van weerbaarheid. Den Haag, Rathenau Instituut 2017; Gov.uk

[140] Weinig landen scoren hoger op dit kenmerk. Litouwen als hoogst 0,155.

[141] NCSC (2019). Active Cyber Defence – The Second Year.

[142] Stevens, T. O'Brien, K., Overill, R., Wilkinson, B., Pildegovičs, T., Hill, S. (2019). UK Active Cyber Defence. A public good for the private sector. King's College London.

[143] Global Cybersecurity Index 2018.

Er wordt ook hard gewerkt aan cybersecurity communities. Het Cyber Security Information Sharing Partnership heeft een publiek private samenwerkingsconstructie opgericht om cyberdreigingsinformatie real time te delen. Momenteel zijn er 15,571 geregistreerde leden. Het Britse NCSC schat dat het 5.500 organisaties van 22 sectoren beslaat.[144] Het doel is om toe te werken naar een systeem waarin cybersecuritysystemen elkaar automatisch op de hoogte stellen van een incident. Daarnaast is er nog Industry 100, een programma waarin talenten van buiten de organisatie nadenken over cybersecurity en innovatieve ideeën testen. Tot slot werken de nationale politie en de verschillende regionale crime units van de politie samen in een Cyber PROTECT-netwerk waarin zij het advies van Britse NCSC zo toegankelijk mogelijk maken voor de diverse gemeenschappen, bijvoorbeeld door het beschikbaar stellen van materiaal of het organiseren van workshops. [145]

De Cyber Essentials regeling is ontwikkeld om organisaties te leren zichzelf te beschermen tegen de meest voorkomende cyberdreigingen. Het is beschikbaar voor alle organisaties en bevat zowel zelfhulptips als certificeringsmogelijkheden. Om zoveel mogelijk bedrijven actief te bereiken is opgenomen in de National Cyber Security Strategie dat de Britse National Cyber Security Centre (Britse NCSC[146]) via organisaties als verzekeraars, toezichthouders en investeerders invloed uitoefent op bedrijven om ervoor te zorgen dat zij hun cyberrisico beheren. Dit zijn bij uitstek partijen die voorwaarden kunnen stellen aan hun klanten of bedrijven waarop zij toezicht houden. Het gaat voorbij bewustwording genereren en betreft vooral het aanzetten tot actie. Ook wordt er gezorgd voor een streng regelgevingskader om cyberrisico's te beheren die de markt niet aanpakt, gebruikmakend van o.a. de AVG. Deze initiatieven hebben als doel de standaarden van cybersecurity binnen de bedrijven te verhogen.

Voor individuen en kleine organisaties is er de overheidscampagne Cyber Aware. Het doel van de campagne is deze doelgroepen zichzelf te helpen beschermen online. Het initiatief is er eveneens één uit de koker van Britse NCSC, in samenwerking met het Cabinet Office, Home Office en het Ministerie voor Digital, Cultuur, Media en Sport. De doelgroepen worden bereikt door gerichte berichtenservice via social media en advertenties, en in samenwerking met bedrijven.[147]

Ook zijn er diverse programma's om jongeren te interesseren een carrière in cybersecurity na te streven. Naast voorlichting wordt er zwaar ingezet op innovatie. Er zijn bijvoorbeeld cyberinnovatiecentra opgezet die startups en de ontwikkeling van innovatieve cybersecurityproducten stimuleren.

---

[144] NCSC (2019). Annual review 2019. ncsc.gov.uk/annual-review-2019

[145] NCSC (2019). Annual review 2019. ncsc.gov.uk/annual-review-2019

[146] Omdat deze organisatie dezelfde korting heeft als de Nederlandse NCSC, korten we deze organisatie in dit rapport af tot 'Britse NCSC'.

[147] NCSC (2019). Annual review 2019. ncsc.gov.uk/annual-review-2019

Frankrijk

Inrichting cybersecuritystelsel op hoofdlijnen

Het cybersecuritystelsel van Frankrijk kenmerkt zicht tevens door een gecentraliseerde beleidsvoering en is daarmee vergelijkbaar met die van het Verenigd Koninkrijk. Veiligheid in Frankrijk (inclusief cybersecurity) valt onder verantwoordelijkheid van het Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), wat onder het gezag staat van de Franse premier.[148] Binnen de SGDNS is een aparte instantie specifiek belast met cybersecurity; Agence nationale la sécurité des systèmes d'information (ANSSI). Dit vormt de basis van het cybersecuritystelsel binnen Frankrijk en had in 2017 een jaarlijks budget van rond €100 miljoen met 600 vaste werknemers.[149]

De ANSSI is opgezet in 2009 als antwoord op opkomende cyberdreigingen en voorzettende digitalisatie.[150] Sindsdien is ANSSI verantwoordelijk voor de beveiliging van informatiesystemen voor de staat en om advies en steun te verlenen aan overheden en bedrijven van vitaal belang. Zo is bijvoorbeeld in 2013 is er een wet aangenomen die bedrijven van vitaal belang verplicht stelt om bepaalde maatregelen te nemen met betrekking tot hun cybersecurity, afhankelijk van hun mate van vitaal belang. Dit laatste blijft een punt van discussie, omdat het onduidelijk blijft wat een vitale functie is en welke sector.

Eén van de belangrijkste taken van ANSSI is het meetbaar maken van cybercriminaliteit. Goede cijfers zijn cruciaal om inzicht te krijgen in een probleem en daarnaast helpt het in het strategisch verdelen van middelen die nodig zijn om cybercriminaliteit te bestrijden. Dit doet ANSSI samen met het Nationale criminaliteit monitoringsagentschap (Observatoire national de la délinquance; ONDRP).[151] Daarnaast zorgt ANSSI voor het opstellen van veiligheidsregels, het uitgeven van cyberweerbaarheid certificaten, en het uitvoeren van inspecties bij bedrijven. Ze zijn verantwoordelijk voor registratie en afhandeling van incidenten en het verbinden van partijen die een incident hebben gehad.[152]

Om de cybersecuritymaatregelen toegankelijk te maken voor een groot deel van de private organisaties werd in 2017 de organisatie Groupement d'intérêt public Actions contre la cybermalveillance (GIP ACYMA) opgezet. Deze organisatie – gefinancierd door ANSSI en partnerpartijen – biedt hulp aan het overgrote deel van de Franse private bedrijven.[153] In 2018 had de organisatie een budget van €1,3 miljoen.[154] In Frankrijk is de groep middelgrote bedrijven relatief klein. Er zijn vooral veel zeer grote bedrijven met nationale impact of kleine bedrijven die geen ICT-cybersecurity experts in dienst hebben. GIP ACYMA richt zich vooral op de laatste groep. Ze brengen private ICT-experts in contact met organisaties die getroffen zijn door een cybersecurityincident, informeren burgers over algemene maatregelen die ze preventief kunnen nemen en functioneren als informatie punt. De informatie die ze in huis hebben wordt aangeleverd door ANSSI en hun samenwerkingspartners en wordt verwerkt tot toolkits, informatielijsten, artikelen, actiepunten, kennisdagen en trainingen die gericht zijn op preventieve en reactieve maatregelen voor de meest voorkomende cyberrisico's.

---

[148] IA Overview Netwerk (2015). Rijksdienst voor Ondernemend Nederland

[149] Baumard, P. (2017). Cybersecurity in France. Springer International Publishing.

[150] Idem.

[151] Nationale strategie voor digitale beveiliging - ANSSI (2015) Bron: ssi.gouv.fr

[152] Baumard, P. (2017). Cybersecurity in France. Springer International Publishing.

[153] Toelichting GIP ACYMA (2019) Bron: cybermalveillance.gouv.fr

[154] Analyse van de GIP ACYMA cybersecurity platform (2018) Bron: Zdnet.fr

Maturity

Uit de Global Cybersecurity Index (GCI) van 2018 blijkt dat Frankrijk het goed doet. Met een score van 0,918 neemt Frankrijk de 3de plek in op de globale schaal en de 2e plaats op de Europese schaal.[155] Alleen de Verenigde Staten en het Verenigd Koninkrijk scoren beter.

Kenmerk	Toelichting	Score (max 0,200)
Legal	Wet- en regelgeving omtrent cybersecurity	0,200
Technical measures	CERT, standards implementation framework, etc.	0,193
Organizational measures	Nationale strategie, organisatie, maatstaven	0,200
Capacity building measures	Publieke awareness initiatieven, training voor professionals, certificering, etc.	0,186
Cooperation measures	Overeenkomsten, deelname in internationale verbanden, pps-en, best practices, etc.	0,139

Internationale samenwerkingen

Frankrijk zet actief in op internationale samenwerking binnen Europa. Ze nemen een actieve rol op zich het vormen van beleid op Europees niveau op het gebied van cybersecurity. Dit wordt onderstreept met de volgende quote:" In order to contribute to a reliable and sustainable roll-out of digital technologies in all countries, and in particular the developing ones, France owes it to itself to assist in reinforcing the capabilities of countries that would like to increase the resilience and security of their information systems, notably in terms of the protection of critical infrastructures and the combat against cybercrime."[156] Daarnaast heeft Frankrijk de ambitie om zich in te zetten voor het opzetten van samenwerkingsverbanden tussen internationale Europese private en publieke partijen.

Best practices

De huidige awareness- en informatie-uitwisselingsinitiatieven ontwikkeld door ANSSI in samenwerking met publieke en private partners bevat een breed scala aan tools en handleidingen. Voor particulieren en professionals is een kennis toolkit ontwikkeld genaamd Etalab 2.0.[157] Hierin worden door middel van video's, artikelen, actiepunten en memo's de belangrijkste cybersecurity risico's behandeld. Dit is gericht op zowel een preventieve als reactieve aanpak. Daarnaast worden er ook professionals met slachtoffers op het platform met elkaar in contact gebracht, waar ze hulp kunnen krijgen na een cybersecurity incident.[158] Daarnaast worden er workshops en kennisdagen georganiseerd, en worden toolkits verder uitgebreid.

Hoewel er actieve ontwikkeling is van beleidsvoering en ontwikkeling van methodieken voor cybercriminaliteitspreventie, is de actieve benadering richting bedrijven en particulieren beperkt binnen Frankrijk. Actieve informatiespreiding richt zich vooral tot het ontwikkelen van publiciteit via reclame over basale te nemen maatregelen en het verwerven van bewustwording. Daarnaast werft de organisatie vooral actief IT-partners voor IT-expertise via hun platform.[159]

---

[155] Global Cybersecurity Index 2018.

[156] French national Digital Security Strategy. SGDSN.

[157] Introductie van de cyberawareness toolbox (2018) Bron: interieur.gouv.fr

[158] Toelichting GIP ACYMA (2019) Bron: cybermalveillance.gouv.fr

[159] Baumard, P. (2017). Cybersecurity in France. Springer International Publishing.

Duitsland

Duitsland is waarschijnlijk een van de meest interessante landen als het gaat om het nationale cyberbeleid. [160] Zij waren een van de eerste die zich bezig hielden met data privacy en informatiebeveiliging en nog steeds zijn ze actief in dit onderwerp.

Inrichting cybersecuritystelsel op hoofdlijnen

In 2011 werd in Duitsland de Nationale Cyber Security Strategie gelanceerd, die onder andere gericht is op de bescherming van kritieke infrastructuren, de beveiliging van IT-systemen, de versterking van IT-Veiligheid in het openbaar bestuur, effectieve controle van cybercriminaliteit en coördinatie van cyberveiligheid in Europa en wereldwijd, het gebruik van betrouwbare en betrouwbare IT, de ontwikkeling van personeelsontwikkeling bij federale overheden en de ontwikkeling van instrumenten om te kunnen reageren op cyberaanvallen.[161] Een groot gedeelte van het document focust zich op het probleem van grootschalige aanvallen op kritieke infrastructuur.

Duitsland heeft verschillende cybersecurity beveiligings- en incident-response teams verdeelt over verschillende sectoren. Het bedrijf dat voornamelijk betrokken is, is de Bundesamt für Sicherheit in der Informationstechnik (BSI). Zij hebben toezicht op vitale sectoren en industrieën, onder meer de infrastructuur, telecom en de overheidsinstanties. BSI heeft geen politie- of inlichtingenbevoegdheden, maar vervult wel die functie op het gebied van cybersecurity. Daarnaast spelen de federale staten (Länder) een rol in de opsporing en vervolging van cybercriminaliteit binnen hun eigen staat. Iedere staat heeft een eigen divisie die hiervoor verantwoordelijk is.[162] Hoewel het takenpakket van BSI breed is, is BSI met €120 miljoen een agentschap met één van de kleinere budgetten in Europa.[163] Dit heeft vooral te maken met de verspreiding van verantwoordelijkheden van cybersecurity binnen Duitsland. Iedere betrokken partij heeft budget nodig en dit zorgt ervoor dat BSI niet al te veel te besteden heeft.

BSI wordt vanaf 2009 gezien als Duitslands centrale autoriteit voor cybersecurity.[164] Er werken momenteel ongeveer 1100 medewerkers en het maakt deel uit van het federale ministerie van Binnenlandse Zaken.[165] Het is een onafhankelijk en neutraal orgaan voor vragen over IT-beveiliging. Hun werkzaamheden zijn samen te vatten in: het opzetten en beoordelen van product- en systeembeveiliging, het toezicht houden op de implementatie van cybersecuritymaatregelen en operationele cyberdefensie. In de volgende alinea wordt kort uitgelegd wat dit ongeveer inhoud.

BSI heeft zeggenschap over wat kan worden gezien als veilige informatietechnologie en wat niet. BSI is binnen Duitsland de partij die het meest af weet van cybersecurity en zal dus als eerst worden benaderd voor advies hierover. Daarnaast houdt BIS ook actief in de gaten of iedereen de verplichte cybersecurity maatregelen toepast en mag het openbaar maken en boetes opleggen indien bedrijven zich er niet aan houden. BSI is zelfs wettelijk verplicht om

---

[160] Cybersecurity in Germany. Springer International Publishing

[161] The Governance of Cybersecurity (2015). Universiteit Tilburg

[162] Schallbruch, M., & Skierka, I. (2018). Cybersecurity in Germany. Springer International Publishing. p33

[163] M. Shulze (2018) Germany develops office cyber capabilities without coherent strategy what to do with them Bron: Cfr.org

[164] Graulich K (2016) Elemente der sogenannten Neuen Sicherheitsarchitektur der Bundesrepublik. In: Festgabe für Rosemarie Will 'Worüber reden wir eigentlich?', Berlin, pp 738–779

[165] www.bsi.bund.de

te waarschuwen indien ze relevante informatie omtrent IT-veiligheid opmerken. Als laatste is BSI verantwoordelijk voor het ondersteunen van de federale overheidsorganisaties in het afweren van cyberaanvallen. Ze monitoren de netwerken van de federale overheid, onderzoeken beveiligingsincidenten en nemen defensieve maatregelen.

Naast het opereren in federale netwerken werkt BSI ook regelmatig samen met openbare aanklagers en politie-eenheden en ondersteunen ze op aanvraag ook kritieke infrastructuurbeheerders. Dit laatste zijn bedrijven die andere bedrijven informeren over hoe ze zichzelf kunnen beveiligen.

Een van de andere partijen die betrokken is, is de Bundeskriminalamt (BKA), de federale recherche van Duitsland. Zij komen in actie als de vitale infrastructuur of een overheidsinstantie aangevallen wordt. Ze proberen erachter te komen wie er achter de aanval zit. Hun rechten gelden voornamelijk voor hele specifieke misdrijven, zoals spionage uit het buitenland.

Bij een grootschalige cyberaanval, is het mogelijk dat verschillende partijen verantwoordelijk zijn voor een deel van de aanval. In zulke gevallen moeten de diensten op individuele basis met elkaar overleggen en de verantwoordelijkheden verdelen. Deze samenwerking wordt sinds 2011 gecoördineerd door een speciaal daarvoor opgezette afdeling binnen de BSI; Cyber-Abwehrzentrum (Cyber-AZ). De 10 man sterke afdeling op zichzelf heeft geen aparte rechten of verantwoordelijkheden, en de effectiviteit van deze opstelling is meerdere keren in twijfel gesteld.[166] Nog steeds is de verdeling tussen de verschillende federale en provinciale diensten is niet altijd even helder.[167]

Maturity

Uit de Global Cybersecurity index (GCI) van 2018 blijkt dat Duitsland met een score van 0.849 de 22e plaats inneemt op de globale schaal en de 13e plaats op de Europese schaal.[168] Een uitsplitsing van de score zoals gedaan is bij het Verenigd Koninkrijk en Frankrijk kan niet weergegeven worden, omdat deze informatie niet openbaar lijkt te zijn. Wat wel duidelijk is, is dat Duitsland een perfecte score heeft gekregen op wetgeving en beleidsvoering, en lager dan gemiddeld heeft gescoord op samenwerking en organisatorische indicatoren.[169] Mogelijk de lage score op samenwerking te verklaren door de Duitsland cultuur met betrekking tot fouten. Een gezegde onder Duitse ministeries luidt: "Het ministerie maakt nooit een fout".[170] Als er toch een fout gemaakt is, wat feitelijk onvermijdelijk is in een complex gebied als cybersecurity, proberen ze het zo om te vormen dat het een succes lijkt. Dit maakt het leren van fouten lastig, maar het zou ook invloed kunnen uitoefenen in hun samenwerking met andere landen. Wie niet kritisch naar zichzelf kan kijken, kan dit ook niet naar andere doen. En daarnaast zou het kunnen zijn dat andere landen de waarde niet inzien van het samenwerken met Duitsland; ze willen niet van hun fouten leren en kunnen zich daardoor minder snel ontwikkelen op cybersecurity gebied.

---

[166] Zedler D (2017) Zur strategischen Planung von cyber security in Deutschland. Zeitschrift für Außenund Sicherheitspolitik p75

[167] Schallbruch, M., & Skierka, I. (2018). Cybersecurity in Germany. Springer International Publishing. p35

[168] Global Cybersecurity Index 2018.

[169] Khare, A. (2020) Rising to the Digital Challenge. Springer Nature. p 25-26

[170] Cybersecurity in Germany. Springer International Publishing

Internationale samenwerkingen

Duitsland beschouwd internationale samenwerking op het gebied van cybersecurity als een zeer belangrijk thema.[171] Duitsland zet vooral in op UN-onderhandelingen op het gebied van cybersecurity, evenals andere bilaterale en multilaterale samenwerking. Denk hierbij aan het uitwisselen van technische kennis. In respons op de openbaringen van Edward Snowden over de spionageactiviteiten van de NSA, specifiek het afluisteren van bondskanselier Angela Merkel nam Duitsland een veel prominentere rol in de UN-cybersecurity onderhandelingen. Dit resulteerde in het doorvoeren van meerdere UN-resoluties op het gebied van privacy en cyberactiviteiten.[172]

(De)centraal systeem

De samenstelling van het Duitse cybersecuritystelsel is zowel organisatorisch als historisch van aard. Globaal gezien wordt de cybersecurity rondom vitale partijen en de nationale veiligheid van Duitsland geregeld met een centraal systeem. De verantwoordelijkheid van cybersecurity rondom niet-vitale partijen wordt opgesplitst over verschillende partijen en wordt decentraal geregeld. De uitzonderingen op deze indeling zijn eerder regel dan uitzondering. De versplintering en onduidelijke verdeling van de takenpakken tussen de diensten maakt de samenwerking moeilijk[173] en ook het aanstellen van de Cyber-AZ, een speciale eenheid om de samenwerking te coördineren, lijkt niet te helpen. Tegelijkertijd zijn veranderingen lastig door te voeren, omdat de verdeling van de diensten diep verweven zit in het Duitse overheidsstelsel. Het Duitse politieke systeem is gebaseerd op een federaal stelsel, waarbij de macht verdeeld is tussen de centrale overheid en de deelstaten.

Bereik van bedrijven en best practices

Net als in veel landen zijn in Duitsland grote delen van de (IT) infrastructuur in private handen. Hierdoor wordt er nadruk gelegd op samenwerkingsverbanden tussen de publieke cybersecurity instellingen en private partijen om de cyberweerbaarheid te waarborgen.[174] De verschillende benaderingen van de publiek-private samenwerking kunnen in grote lijnen worden verdeeld in vier gebieden van samenwerking tussen de overheid en het bedrijfsleven[175], afhankelijk van de mate van betrokkenheid:

- de gezamenlijke organisatie van de verantwoordelijkheid voor cybersecurity in een sector
- platformen en voor de uitwisseling van operationele cybersecurity informatie
- samenwerkingsverbanden voor preventieve cyberweerbaarheid
- vormen van samenwerking voor de verspreiding van cybersecurity vakkennis aan het grote publiek

Het *eerste samenwerkingsgebied* omschrijft de meest intensieve en oudste samenwerking tussen publieke en private partijen. Het nationaal initiatief tussen de staat en uitvoerders van de kritieke infrastructuur voor de bescherming van kritieke informatie-infrastructuur in Duitsland, genaamd UP KRITIS, speelt hierin een belangrijke rol. Naar aanleiding van dit

---

[171] The State of IT Security in Germany 2018 - BSI

[172] Schallbruch, M., & Skierka, I. (2018). Cybersecurity in Germany. Springer International Publishing. p61

[173] Zedler D (2017) Zur strategischen Planung von cyber security in Deutschland. Zeitschrift für Außenund Sicherheitspolitik p100-101

[174] Bundesministerium des Innern (2016b) Referentenentwurf des BMI - Entwurf einer Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz, 13 01 2016. Bron: www.bmi.bund.de

[175] Cybersecurity in Germany. Springer International Publishing. P41.

initiatief ontstond er een platform voor de uitwisseling van informatie en coördinatie van cybersecurity. Aanvankelijk waren hier 40 belangrijke publieke en private partijen actief met als BSI als voorzitter, maar intussen zijn er 540 partijen aangesloten en heeft BSI de volledige verantwoordelijkheid over de coördinatie en administratief van het platform. [176] Voor publieke en private partijen begon dit initiatief als een manier om de complexiteit rondom cybersecurity weg te nemen; een plek voor betrouwbare informatie voor iedereen. Naast het platform komen er ook verschillende groepen samen die zorgen voor het creëren van overzicht van afhankelijkheden binnen de infrastructuur, opzetten van crisis management processen in het geval van een cyberaanval, het voorbereiden van gezamenlijke oefeningen en het uitwisselen van standpunten over de activiteiten van EU en EU-wetgeving.

De exponentiële groei van de UP KRITIS is grotendeels te wijten aan de verplichte deelname voor alle publieke partijen binnen de kritieke infrastructuur vanaf 2012. Zo is de UP KRITIS zich ontwikkeld van een vrijwillige publiek-private samenwerkingsverband naar een samenwerkingsplatform van staats- en kritieke infrastructuren welke opereert binnen een raamwerk van wettelijke voorschriften. Hieruit zijn er 14 industriële en negen thematische werkgroepen gevormd welke zich bezighouden met de verbetering van cybersecurity. De samenwerking binnen UP KRITIS wordt grotendeels als positief ervaren door zowel publieke als private partijen.[177]

Het tweede samenwerkingsgebied richt zich op de samenwerking tussen publieke partijen en grotere private bedrijven. De doelstelling hiervan is het vergaren en uitwisselen van cyberweerbaarheid informatie. Met de introductie van IT Security Act werden alle bedrijven in Duitsland formeel verplicht gesteld om cyberaanvallen te melden.[178] Naast het functioneren als meldpunt zorgen een tal van platformen voor het verspreiden van cyberweerbaarheid informatie en worden er formele fysieke samenwerkingen opgezet met een team bestaande uit publieke en private partijen om oplossingen te bedenken voor cyberaanvallen. Op dit moment zijn er werkzaamheden gaande om een uniform platform op te zetten welke het meldpunt samenvoegt met andere platformen tot één platform voor alle Duitse bedrijven.[179]

Het derde samenwerkingsgebied is toegespitst op preventieve maatregelen, voornamelijk op het gebied van assistentie en advies. Onder leiding van BSI en BMI werd de Alliance voor Cybersecurity opgezet, die inmiddels meer dan 2600 individuele partijen telt. Binnen de Alliance voor Cybersecurity, wat voornamelijk de functie heeft van een financieringsprogramma, zijn er verschillende vormen van samenwerkingen, platformen en verbanden opgezet.[180] Het hoofddoel hiervan is kennis over cyberweerbaarheid te verspreiden tussen de Duitse midden- en kleinbedrijven. Daarnaast worden er cyberweerbaarheidstrainingen, toolkits en wekelijkse updates verspreid in vorm van een

---

[176] UP KRITIS-Geschäftsstelle (2017) "UP KRITIS-Jahresbericht 2017," 29 01 2018.

[177] Zedler D (2017) Zur strategischen Planung von cyber security in Deutschland. Zeitschrift für Außenund Sicherheitspolitik p21

[178] Schallbruch, M., & Skierka, I. (2018). Cybersecurity in Germany. Springer International Publishing. p43

[179] Bundesministerium des Innern (2016b) Referentenentwurf des BMI - Entwurf einer Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz, 13 01 2016. Bron: www.bmi.bund.de

[180] Federal Office for Information Security, "Alliance for Cybersicherheit. General Information.," 01 08 2014. Bron: allianz-fuer-cybersicherheit.de

email. Tegenover de bovengenoemde verbanden is de participatie voor de bedrijven vrijblijvend en is de informatie die uitgewisseld wordt van beperkte mate.[181]

Het vierde samenwerkingsgebied legt focus gezamenlijke informatie, advies en ondersteuning voor burgers met betrekking tot cyberspace bedreigingen. [182] Om deze verspreiding van cyberweerbaarheidsinformatie voor de Duitse burgers te verspreiden is de non-profit organisatie Deutschland sicher im Netz e. V. (DsiN) opgezet. DsiN staat onder leiding van de het Ministerie van Binnenlandse zaken (BMI) en haar leden zijn voornamelijk grotere bedrijven uit de ICT-industrie. Het biedt een breed scala aan informatie over cybersecurity en voert projecten uit om bepaalde doelgroepen bij IT-beveiliging te betrekken, bijvoorbeeld senioren. Er zijn verschillende soortgelijke initiatieven op zowel nationaal als staatsniveau.

In totaal werken duizenden publieke en private instellingen in Duitsland samen om de cyberweerbaarheid op peil te houden. Veel van de initiatieven vinden parallel plaats, en zorgen voor een spreiding van de verantwoordelijkheid op dit gebied. Desniettemin is de effectiviteit van deze samenwerkingen buiten UP KRITIS beperkt.[183] Vooral de samenwerkingsverbanden gericht op grote bedrijven en MKB schieten tekort in het voorzien van bedrijven met informatie die noodzakelijk is om zich goed te beschermen tegen cyberaanvallen. Er is veel ruimte voor verbetering, zeker met de toenemende hoeveelheid van informatie die BSI binnenkrijgt door het verplicht stellen van het melden van cyberaanvallen en het hanteren van een bepaald niveau van bescherming van de IT-producten bij Duitse bedrijven.

[181] Schallbruch, M., & Skierka, I. (2018). Cybersecurity in Germany. Springer International Publishing. p44

[182] Deutschland sicher im Netz e.V. (2016) "Jahresbericht 2016," 03 2017.

[183] Schallbruch, M., & Skierka, I. (2018). Cybersecurity in Germany. Springer International Publishing. P45

Bijlage 3. Begeleidingscommissie

Naam	Functie
prof. dr. Marleen Huysman (Voorzitter)	Directeur van KIN Center for Digital Innovation op Vrije Universiteit Amsterdam en hoofd van de afdeling Knowledge, Information and Innovation.
mr. Anne Beckers	Senior beleidsmedewerker Ministerie van Justitie en Veiligheid
mr. Corine van Ginkel	Projectbegeleider WODC
mr. Pieter Wolters	Universitair hoofddocent burgerlijk recht en onderzoeker bij het Onderzoekcentrum Onderneming & Recht en de Interdisciplinary Hub for Security, Privacy and Data Governance van de Radboud Universiteit.
drs. Michel Verhagen	Programmamanager DTC

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