Reactie op internet consultatie voorstel wet bevordering digitale weerbaarheid bedrijven

1. (Internet) consultatie

Het wetsvoorstel heeft van 28 juni 2021 tot en met 23 augustus 2021 opengestaan voor consultatie[1]. Gedurende de periode van acht weken hebben diverse organisaties gereageerd en deze zijn publiekelijk beschikbaar via de website: www.internetconsultatie.nl/wbdwb.

In dit verslag wordt in zijn algemeenheid ingegaan op de reacties en zullen specifieke onderdelen en suggesties alsmede de eventuele opvolging worden behandeld.

1.1 Algemeen beeld

In veel reacties is het belang van digitale weerbaarheid van ondernemend Nederland ten behoeve van het verdienvermogen van het Nederlandse bedrijfsleven onderschreven. Tevens wordt in enkele reacties het belang benadrukt van de rol die de overheid heeft op het domein van digitale veiligheid.

Naast deze unaniem positieve grondhouding zijn er zeker ook verbeterpunten benoemd in de verschillende reacties. Er is op een aantal onderwerpen en van diverse partijen een reactie ontvangen. Deze zijn gebundeld naar onderwerp. De volgende thema's worden hierna nader toegelicht: afbakening doelgroep, relatie met NIS-2, samenhang van overheidsinitiatieven en stelsel o.a. de 1-loket gedachte, gegevensbescherming en vertrouwelijkheid van informatie.

Naast deze thema's zijn er ook specifieke punten die door slechts één organisatie zijn genoemd, dit zijn: verhouding met de Wet markt en overheid (Stichting Connect2Trust), het delen van IOC's (Cyberveilig Nederland), gevolgen voor digitale zorgplicht (Simmons+Simmons). Deze punten komen aan de orde in de laatste paragraaf.

1.2 Afbakening doelgroep

Zowel Cyberveilig Nederland, Stichting Connect2Trust als Deloitte stellen vragen over de afbakening van de doelgroep van het wetsvoorstel. De zorgen die geuit worden bevatten:

- in hoeverre de beoogde taken van de minister van EZK afbreuk doen aan het Landelijk Dekkend Stelsel (LDS),
- in hoeverre de beoogde taken samenvallen met taken van het Nationaal Cyber Security Center (NCSC)

[1] https://www.internetconsultatie.nl/wbdwb

- de omvang van de doelgroep van het wetsvoorstel ten opzichte van de capaciteit beschikbaar op het ministerie van EZK om deze taken en bevoegdheden uit te voeren.

Het ministerie van EZK maakt met het Digital Trust Center (DTC) onderdeel uit van het LDS en draagt actief bij aan de vorming van het LDS, waarvan de regie bij de Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV) ligt. Dit doet het DTC door de stimulering van samenwerkingsverbanden onder andere door het verstrekken van subsidie aan initiatieven ten behoeve van de digitale weerbaarheid van bedrijven. Deze samenwerkingsverbanden vertegenwoordigen vaak een sector, branche of bepaalde regio, waarin bedrijven samenwerken op digitale weerbaarheid. Ook biedt het DTC ruimte aan andere initiatieven op het gebied van digitale weerbaarheid welke geen subsidie ontvangen maar wel onderdeel uitmaken van het netwerk van het DTC. Denk hierbij aan de eerder genoemde Stichting Connect2Trust, maar ook de samenwerking met de Groep Educatieve Uitgevers (GEU) en de samenwerking in de Rotterdamse haven onder de regie van FERM. Meer voorbeelden zijn te vinden op de samenwerkingspagina van het DTC[2].

Een tweede element van de afbakening van de doelgroepen is de zorg voor dubbeling van informatie bij de overheid waarbij expliciet wordt gerefereerd aan de rolverdeling tussen het NCSC en het DTC. De rolverdeling is duidelijk: het NCSC heeft de centrale rol voor de digitale beveiliging van de Rijksoverheid en de onder de Wet beveiliging netwerk- en informatiesystemen (Wbni) aangewezen vitale sectoren en organisaties en daarnaast bestaat het CSIRT voor digitale diensten (CSIRT-DSP) Het DTC zal de bedrijven bedienen die niet onder de verantwoordelijkheid van het NCSC of onder de verantwoordelijkheid van het CSIRT-DSP vallen. Het NCSC, CSIRT-DSP en DTC werken nauw samen en hebben samenwerkingsafspraken vastgelegd om het risico van dubbele informatie of blinde vlekken te vermijden.

Het derde element van dit thema gaat over de uitvoerbaarheid van de voorziene taken en bevoegdheden door de minister van EZK. In de financiële paragraaf van de memorie van toelichting bij het wetsvoorstel worden de structurele financiering en bezetting benoemt. Het DTC zal in de uitvoering van de taken en bevoegdheden zoveel als mogelijk efficiëntie en effectiviteit nastreven en gebruik maken van digitale processen.

1.3 NIS2[3]

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

[3] Voorstel voor een richtlijn van het Europees Parlement en de Raad houdende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148, (COM(2020)0823)

Stichting Connect2Trust en Cyberveilig Nederland refereren in hun reactie aan het verband tussen de toekomstige Europese regelgeving (NIS-2) en de consequenties voor het wetsvoorstel.

Het is mogelijk dat er in de toekomst wijzigingen in het huidige stelsel van vitale en niet-vitale bedrijven kan ontstaan als gevolg van nieuwe Europese regelgeving, waaronder NIS-2. Het belang van samenwerking, de samenhang en de afhankelijk van bedrijven in diverse ketens welke ook kunnen bestaan uit een mix van vitale en niet vitale bedrijven wordt onderkend. Deze toekomstige Europese wetgeving is afgewogen tegen de urgentie van de problematiek in het hier en nu en de conclusie is dat de eerder genoemde maatschappelijke wens om specifieke informatie over digitale kwetsbaarheden, dreigingen en incidenten bij individuele bedrijven niet kan wachten op herziening van de huidige Europese richtlijnen. Stichting ONL refereert hier zelfs aan in haar reactie en vraagt vervolgens om verdergaande stappen door de overheid.

1.4 Samenhang van overheidsinitiatieven

Op basis van het huidige stelsel waarbij het NCSC verantwoordelijk is voor Rijksoverheid en de vitale partijen aangewezen op basis van de Wbni en de daarin ook genoemde verantwoordelijkheden van de vakministers is dit wetsvoorstel een logische aanvulling op het stelsel. De minister van EZK heeft een verantwoordelijkheid voor het niet-vitale bedrijfsleven en zoekt actief de samenwerking met andere organisaties binnen en buiten de overheid. Voor wat betreft de systeemverantwoordelijkheid van andere (vak)ministers is er geen twijfel over bevoegdheid. Vakministers zijn volgens eigen beleid en wetgeving verantwoordelijk voor eigen doelgroepen. Als het DTC relevante informatie heeft voor andere vakdepartementen zal dit actief worden gedeeld. Op deze wijze wordt er samengewerkt binnen en buiten departementen om samen Nederland digitaal weerbaarder te maken. Op dit moment doet het DTC dit al met NCSC, CSIRT-DSP, Z-Cert en vele andere organisaties. Ter verduidelijking is ook in paragraaf 2.3 van de memorie van toelichting dit nader toegelicht.

Zowel Cyberveilig Nederland als Stichting Connect2Trust vragen om een 1-loket benadering door de overheid om zoveel mogelijk helderheid voor ondernemend Nederland te creëren. In Nederland is er gekozen voor het wettelijk onderscheid tussen vitaal en niet-vitaal bedrijfsleven. Het DTC en NCSC werken uiteraard nauw samen, niet alleen onderling, maar ook met andere organisaties binnen en buiten de overheid om gezamenlijk de digitale weerbaarheid te vergroten. Deze samenwerking krijgt vorm via onder meer organisaties zoals de samenwerkingsverbanden, de organisaties met een rol in de Wbni en het LDS. De minister van EZK heeft hierin een rol voor het niet-vitale bedrijfsleven, NCSC is en blijft verantwoordelijk voor vitale aanbieders. Samen met andere vakministers staat de Nederlandse overheid in zijn totaliteit voor de opgaven om Nederland digitaal weerbaar te maken.

1.5 AVG en vertrouwelijkheid van informatie

Binnen dit thema vallen diverse onderwerpen welke nader worden toegelicht. Het gaat hier om reacties over de Algemene verordening gegevensbescherming (AVG) door VNO-NCW / MKB-Nederland en het CIO Platform NL, maar ook over de informatiebeveiliging van informatie(deling) bij en door het DTC door Simmons+Simmons, Stichting Connect2Trust en Deloitte, en over de Wob of diens opvolger de Woo door Cyberveilig Nederland en VNO-NCW / MKB Nederland.

Er worden zorgen geuit over de mogelijke invloed van de AVG op de informatiedeling via het ministerie van EZK. Op basis van dit wetsvoorstel zal het mogelijk zijn om informatie te verwerken waaronder persoonsgegevens. Het is deze wettelijke grondslag die het voor de minister van EZK een rechtmatige verwerking maakt. Het is dan niet nodig om met de ontvanger van de informatie een overeenkomst te sluiten omdat de verstrekking van informatie vanuit het ministerie van EZK op basis van een wettelijke taak gaat. Uiteraard worden er waarborgen getroffen over de zekerheid en zorgvuldigheid waarmee persoonsgegevens door het DTC worden verwerkt. Het wetsvoorstel is voorgelegd aan de AP. Het advies van de AP en de reactie daarop zijn terug te vinden in paragraaf 4.3 van de memorie van toelichting.

Deloitte en Stichting Connect2Trust stellen vragen over het risico van informatiedeling, enerzijds door de verwerking door het DTC en anderzijds bij het ontvangen door individuele bedrijven. Tevens wordt gevraagd naar de definitie van vertrouwelijke gegevens. Voor deze laatste sluit het wetsvoorstel in terminologie aan bij de Wbni.. Voor wat betreft het delen van informatie aan individuele bedrijven betracht het DTC uiteraard grote zorg en zal de meest gepaste communicatie methode worden gehanteerd.

Door zowel Cyberveilig Nederland en VNO-NCW / MKB-Nederland zijn zorgen geuit over de openbaarmaking van informatie door de overheid op basis van de Wob en haar opvolger de Woo. De vertrouwelijkheid van tot bedrijven herleidbare informatie (zoals IP-adressen, domeinnamen, AS-nummers, bedrijfsnamen en contactgegevens) dient voor een goede uitvoering van de taken genoemd in dit wetsvoorstel te worden beschermd. Respondenten zijn van mening dat een Woo uitzondering noodzakelijk is. De Woo bevat in artikel 5.1 verschillende gronden op basis waarvan dit soort informatie van openbaarmaking kan worden uitgezonderd. Echter, ondanks deze bestaande ruime bescherming onder de Wob en Woo is er, ten behoeve van de eenheid van stelsel voor gekozen om het bestaande regime van Woo uitzondering voor de Wbni op gelijke wijze in dit wetsvoorstel te implementeren om zo te waarborgen dat dezelfde gegevens op dezelfde wijze worden behandeld. Het wetsvoorstel is op dit punt aangevuld.

Door de toevoeging van de uitzonderingsgrond voor dit wetsvoorstel aan de Woo vindt er echter geen inhoudelijke uitbereiding plaats van het soort gegevens dat wordt uitgezonderd. In aanvulling hierop: de Woo is onverkort van toepassing op andere bij de Minister van EZK berustende informatie die wordt verwerkt in het kader van de uitoefening van de in dit wetsvoorstel bedoelde taken van de minister van EZK. Het belang van een eenduidige, transparante en open overheid wordt door de minister van EZK nadrukkelijk onderschreven.

1.6 Diverse punten

Stichting Connect2Trust stelt een verdiepende vraag over de relatie markt en overheid en het wetsvoorstel. Dit wetsvoorstel geen gevolgen voor de verhouding markt en overheid. De taken en bevoegdheden van de Minister van EZK in dit wetsvoorstel zijn beperkt tot het informeren van bedrijven over kwetsbaarheden en dreigingen voor zover zij beschikt over die informatie. Het oplossen van incidenten en het nemen van preventieve maatregelen is aan bedrijven zelf.

Cyberveilig Nederland vraagt in haar reactie of IOC's ook zullen worden gedeeld door het DTC omdat deze noodzakelijk zijn om de digitale weerbaarheid van bedrijven te vergroten en refereert dan expliciet aan dreigingen die nog niet gerelateerd zijn aan specifieke bedrijven. In voorkomende gevallen zal relevante informatie waarover het DTC beschikt, waaronder ook IOC's, met inachtneming van de wettelijke kaders worden gedeeld bij het informeren van bedrijven over specifieke dreigingen. Maar ook zal het DTC generieke informatie over digitale weerbaarheid en dreigingen verspreiden.

Als laatste is door Simmons+Simmons een vergezicht geschetst in het kader van de digitale zorgplicht van bedrijven en eventuele strafrechtelijke consequenties. Met dit wetsvoorstel worden geen directe of indirecte normen opgelegd aan het Nederlandse bedrijfsleven of wordt door dit wetsvoorstel invulling gegeven aan de strafrechtelijke bepalingen uit artikel 350b Sr. Door het informeren van bedrijven over kwetsbaarheden, dreigingen of incidenten ontstaat er geen verplichting om deze informatie op te volgen. Het is aan de ondernemers zelf om te bepalen of en op welke wijze zij opvolging geven aan deze informatie . Dat in de markt in bijvoorbeeld in de leveranciersketen afnemers of bedrijven in de keten over en weer eisen stellen aan elkaars digitale veiligheid valt onder de contractvrijheid van partijen.