Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

36 270 Regels ter bevordering van de digitale weerbaarheid van bedrijven (Wet bevordering digitale weerbaarheid bedrijven)

Nr. 6

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 8 maart 2023

A. Algemeen

De leden van de VVD-fractie hebben met veel interesse en waardering kennisgenomen van het onderhavige wetsvoorstel en hebben hierover nog enkele vragen en opmerkingen. Deze leden willen hier graag de noodzaak van dit wetsvoorstel onderschrijven, gezien de digitale dreiging waar Nederlandse niet-vitale bedrijven in toenemende mate dagelijks mee te maken hebben. Voornoemde leden beschouwen hun digitale veiligheid en weerbaarheid als randvoorwaardelijk voor het behoud en de groei van de Nederlandse economische belangen.

De leden van de D66-fractie hebben met interesse kennisgenomen van het onderhavige wetsvoorstel, het advies van de Afdeling advisering van de Raad van State en de reacties van diverse partijen. De leden willen de regering nog enkele vragen voorleggen.

De leden van de CDA-fractie hebben met interesse kennisgenomen van het onderhavige wetsvoorstel. Deze leden zien, samen met de regering, de noodzaak om informatie over specifieke digitale dreigingen en kwetsbaarheden te kunnen delen met het bedrijfsleven. Deze leden steunen daarom een spoedige behandeling en inwerkingtreding van het wetsvoorstel. Deze leden hebben nog enkele vragen.

De leden van de SP-fractie hebben het onderhavige wetsvoorstel gelezen en hebben hierover nog enkele vragen.

De leden van de ChristenUnie-fractie hebben kennisgenomen van het onderhavige wetsvoorstel. Zij constateren dat de wet voortkomt uit de behoefte om bedrijven en maatschappelijke organisaties beter te informeren en adviseren over én concrete hulp en ondersteuning te bieden bij het verbeteren van hun cybersecurity en bij het afslaan van aanvallen door hackers. De leden constateren dat de taken van het in 2017 opgerichte DTC uitgebreid worden van algemene informatievoorziening naar informatievoorziening over specifieke digitale dreigingen en

kst-36270-6
ISSN 0921 - 7371
's-Gravenhage 2023

kwetsbaarheden. Tevens constateren ze dat het DTC de mogelijkheid krijgt om handelingsperspectief aan te reiken aan bedrijven over vervolgstappen bij digitale dreigingen en kwetsbaarheden. De leden van de ChristenUnie-fractie hebben behoefte aan het stellen van enkele nadere vragen.

Het lid van de BBB-fractie heeft met belangstelling kennis genomen van het onderhavige wetsvoorstel. Het wetsvoorstel beoogt een wettelijke grondslag te bieden voor taken en bevoegdheden van de Minister van Economische Zaken en Klimaat (EZK) op het gebied van de digitale weerbaarheid van het niet-vitale bedrijfsleven in Nederland.

Met belangstelling heb ik kennisgenomen van de vragen van de leden van de vaste commissie voor Economische Zaken en Klimaat over het voorstel van wet, houdende regels ter bevordering van de digitale weerbaarheid van bedrijven (Kamerstuk 36 270, hierna: het wetsvoorstel). Hieronder ga ik graag in op de vragen en opmerkingen van de leden van de fracties van de VVD, D66, het CDA, de SP, de ChristenUnie en BBB. Daarbij volg ik de inhoudsopgave van het verslag.

Het lid van de BBB-fractie onderschrijft het belang van de bevordering van digitale weerbaarheid van Nederlandse bedrijven. Hier is echter geen wet voor nodig, maar een effectief communicatie- en scholingsplan. Het lid van de BBB-fractie is het daarom ook eens met het advies van de Afdeling advisering van de Raad van State, die feitelijk aangeeft dat dit wetsvoorstel een overbodig instrument is.

Het lid van de BBB-fractie leest dat het wetsvoorstel de Minister van EZK een wettelijke grondslag geeft om de voor haar taakuitoefening noodzakelijke (persoons)gegevens op te vragen en te delen. Dit kan echter al via de Wet beveiliging netwerk- en informatiesystemen (Wbni). De Wbni kent de Minister van EZK al enkele bevoegdheden toe. Die hebben betrekking op aanbieders van essentiële diensten binnen de sectoren energie en digitale infrastructuur. Daarnaast voorziet een recent wetsvoorstel tot wijziging van de Wbni in een grondslag voor de verstrekking van (persoons)gegevens door het Nationaal Cyber Security Center (NCSC), ook aan niet-vitale aanbieders. De Wbni regelt dus niet alleen bevoegdheden voor de Minister van Justitie en Veiligheid (JenV), maar ook voor de Minister van EZK. Bovendien regelt het, indien het recente wetsvoorstel tot wet wordt verheven, bevoegdheden ten aanzien van het niet-vitale bedrijfsleven. Tegen die achtergrond en uit het oogpunt van harmonisatie van wetgeving ligt het in de rede om de nieuwe bevoegdheden van de Minister van EZK ten aanzien van de verwerking en verstrekking van persoonsgegevens op te nemen in de Wbni.

Het lid van de BBB-fractie verzoekt de regering dan ook met klem dit overbodige wetsvoorstel in te trekken en zo een bijdrage te leveren aan de zo gewenste vermindering van de regeldruk voor ondernemers en burgers, zoals ook in het Regeerakkoord en het Coalitieakkoord als voornemen is vastgelegd. Het lid van de BBB-fractie roept de regering op te doen wat zij zegt.

Het lid van de BBB-fractie verzoekt de regering het wetsvoorstel in te trekken en zo een bijdrage te leveren aan het verminderen van regeldruk voor burgers en bedrijven.
Zoals in de memorie van toelichting bij het wetsvoorstel (Kamerstuk 36 270, nr. 3) is aangegeven, is het voorliggende wetsvoorstel enkel van toepassing op het niet-vitale Nederlandse bedrijfsleven waarbij er geen regeldruk is voorzien. Uit dit voorstel vloeit namelijk geen enkele verplichting voor bedrijven voort. Een bedrijf is en blijft zelf verantwoor-

delijk voor het actief beheren en versterken van zijn digitale veiligheid. De overheid speelt hierin een rol maar neemt uitdrukkelijk niet de verantwoordelijkheid van bedrijven over.

Voor zover de vraag van het lid van de BBB-fractie ook het nut en de noodzaak van een eigenstandige wet betreft, is het van belang te vermelden dat de digitale weerbaarheid van het niet-vitale bedrijfsleven onder de beleidsverantwoordelijkheid van de Minister van Economische Zaken en Klimaat (hierna: de Minister van EZK) valt. In nauw overleg met de Minister van Justitie en Veiligheid (hierna: de Minister van JenV) als coördinerend bewindspersoon cybersecurity is besloten om deze verantwoordelijkheden in een eigenstandige wet op te nemen. Zoals in het nader rapport (Kamerstuk 36 270, nr. 4) is aangegeven, zijn er drie redenen voor: de aard van de wetgeving, de rol van de Minister van EZK in de wetgeving en de doelgroep van dit wetsvoorstel.
In de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni) worden grotendeels de bepalingen vanuit de Europese Netwerk- en informatiebeveiligingsrichtlijn[1] (hierna: NIB-richtlijn) vastgelegd. De Wbni bevat daarmee de omzetting van Europeesrechtelijke verplichtingen (zorgplicht en meldplicht) voor haar doelgroep en regelt de naleving daarvan. Op grond van het onderhavige voorstel dat geen Europeesrechtelijke oorsprong kent, geldt er geen zorg- of meldplicht voor de doelgroep van dit wetsvoorstel, te weten de niet-vitale bedrijven. Tevens is er in dit wetsvoorstel geen sprake van toezicht en handhaving.
Het ligt niet in de rede om beleidsverantwoordelijkheden van de Minister van EZK voor digitale weerbaarheid van niet-vitale bedrijven in de Wbni te regelen waar enkele andere bevoegdheden aan de Minister van EZK zijn toegekend. De rol van de Minister van EZK in de Wbni verschilt namelijk van de rol die de Minister van EZK heeft in onderhavig voorstel. De uit de Wbni voortvloeiende taken en bevoegdheden voor de Minister van EZK betreffen het toezicht op de naleving van de zorg- en meldplicht door vitale aanbieders in bijvoorbeeld de sector energie en voor digitale dienstverleners. Het onderhavige wetsvoorstel kent de Minister van EZK geen toezichthoudende bevoegdheden toe, maar ziet daarentegen op het informeren en adviseren van de niet-vitale bedrijven, ongeveer 2 miljoen. Deze taken worden in de praktijk door het Digital Trust Center (hierna: DTC) uitgevoerd.
Ten slotte zijn de doelgroepen van de Wbni en onderhavig wetsvoorstel verschillend. De Wbni is gericht op de digitale veiligheid van vitale aanbieders, organisaties die deel uitmaken van de rijksoverheid en digitale dienstverleners. Hierin wordt bijvoorbeeld geregeld dat de Minister van JenV (en in de praktijk het Nationaal Cyber Security Centrum (hierna: NCSC)) verantwoordelijk is voor het informeren en adviseren van vitale aanbieders en rijksoverheidsorganisaties bij digitale dreigingen en incidenten. Het onderhavige wetsvoorstel richt zich daarentegen op de doelgroep van het niet-vitale bedrijfsleven.
Hierdoor zijn ook de taken van de Minister van JenV en de Minister van EZK anders. Het NCSC heeft krachtens de Wbni als primaire taak het informeren en het adviseren van zijn eigen doelgroep over digitale dreigingen en incidenten. Daarnaast verleent het NCSC de aanbieders in zijn doelgroep ook overige bijstand bij het treffen van maatregelen om incidenten te voorkomen en te verhelpen. Overige bijstand kan bijvoorbeeld inhouden dat er ter plekke ondersteuning wordt geboden bij het duiden van het probleem en de maatregelen om dat probleem aan te pakken.

[1] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PbEU 2016, L 194).

Het DTC richt zich bij het informeren en het adviseren over digitale dreigingen en incidenten op de doelgroep van het niet-vitale bedrijfsleven. Hierbij gaat het om algemene informatie en handelingsperspectieven maar ook om specifieke dreigingsinformatie gericht op individuele bedrijven. In tegenstelling tot het NCSC verleent het DTC bij incidenten geen overige bijstand, ofwel incident response, aan de aanbieders in zijn doelgroep.

De recente Wbni-wijziging om onder meer rechtstreekse informatieverstrekking vanuit het NCSC aan andere aanbieders dan vitale aanbieders en rijksoverheidsorganisaties mogelijk te maken, betreft alleen andere aanbieders die géén schakelorganisaties hebben én indien een dreiging of incident aanzienlijke gevolgen heeft of kan hebben voor de continuïteit van hun dienstverlening. In onderhavig wetsvoorstel wordt de positie van het DTC als schakelorganisatie voor zijn doelgroep wettelijk vastgelegd. Daarmee is dit voorstel complementair aan de bestaande wetgeving en geeft het NCSC en het DTC meer ruimte voor samenwerking en informatiedeling. Daarnaast is dit wetsvoorstel randvoorwaardelijk voor het realiseren van de doelstelling uit het coalitieakkoord om sneller en makkelijker informatie te kunnen delen vanuit de overheid met bedrijven over digitale kwetsbaarheden en «hacks».

1. Hoofdlijnen van het voorstel

De leden van de VVD-fractie lezen dat het voorliggende wetsvoorstel het DTC in staat stelt om niet-vitale bedrijven te voorzien van specifieke (acute) dreigingsinformatie die relevant is voor organisaties in Nederland en om deze informatie dus actief te delen met potentiële en daadwerkelijke slachtoffers van digitale aanvallen. De leden van de VVD-fractie beschouwen dit als een zeer belangrijke en urgente taak van het DTC. Gegeven het feit dat het DTC beschikt over 23 fte en het een doelgroep behelst van 2 miljoen ondernemers maken deze leden zich zorgen over de haalbaarheid en effectieve uitvoering van voorliggende substantiële uitbreiding van informatievoorziening. In hoeverre voorziet dit wetsvoorstel ook in de additionele (personele) capaciteit die nodig is om te voldoen aan de nieuwe volwaardige taakvoorziening van het DTC en om uiteindelijk het hoofddoel van het DTC daadwerkelijk te kunnen bewerkstelligen? Wordt deze capaciteit ook gemeten en tussentijds geëvalueerd, zodat aan de eventuele toegenomen vraag tegemoet kan worden gekomen door het DTC? Zo nee, waarom niet?

Het DTC zal in de uitvoering van de in het voorliggende wetvoorstel voorgestelde taken zoveel als mogelijk efficiëntie en effectiviteit nastreven en gebruik maken van digitale processen. Er wordt ingezet op een geleidelijke doorgroei van het DTC waarin periodiek zal worden geëvalueerd of de inzet van mensen en budgetten gelijklopen met de ambities van het kabinet en de vraag vanuit het bedrijfsleven.
Op de EZK-begroting is reeds € 3,5 miljoen structureel beschikbaar voor het DTC. Met de extra middelen van het Coalitieakkoord loopt dit bedrag op naar € 5,6 miljoen in 2023, € 8,1 miljoen per jaar in de periode 2024–2026 en vanaf 2027 structureel € 9,0 miljoen per jaar. Hiermee is het totaal structureel beschikbare bedrag voor het DTC momenteel voldoende voor de uitvoering van dit wetsvoorstel en is er in de basis financiële dekking voor zowel de personeelsuitgaven als de materiële uitgaven voor wat betreft het verstrekken van algemene en specifieke dreigingsinformatie aan de doelgroep en het stimuleren van samenwerking en samenwerkingsverbanden.

De leden van de VVD-fractie willen voorts aandacht vragen voor de verscheidenheid aan ondernemers en bedrijven die onder de doelgroep van het DTC vallen. Deze leden zijn van mening dat deze verscheidenheid zorgt voor verschillende behoeftes en hulpvragen en derhalve een veelzijdige aanpak behoeft van het DTC in de uitvoering van hun taken. Zo bestaan er grote verschillen tussen de ondernemingen over het volwassenheidsniveau van cybersecurity, als tevens de aanwezigheid en beschikbaarheid van geschikt cybersecurity personeel. Op welke wijze borgt voorliggend wetsvoorstel een veelzijdige en flexibele aanpak en werkwijze van het DTC om tegemoet te komen aan de uiteenlopende behoeftes van de doelgroep? Worden er plannen gemaakt om de verschillende doelgroepen en bedrijven zo goed mogelijk te bereiken en de bekendheid van het DTC te vergroten?

Het wetsvoorstel biedt de ruimte om de voor de doelgroep meest geschikte vorm van informatie te kiezen. Daarbij houdt het DTC met een flexibele aanpak rekening met de uiteenlopende behoeftes van de doelgroep, bedrijfsgrootte en risicoclassificatie. Zo staat het DTC in nauw contact met zijn doelgroep en zijn vertegenwoordigers over de verschillende behoeftes en zal zijn dienstverlening daarop afstemmen.
Het DTC maakt plannen om de verschillende doelgroepen en bedrijven zo goed mogelijk te bereiken en de bekendheid van het DTC te vergroten. Daarbij wordt ook de manier van dienstverlening op de doelgroep afgestemd. De Kamer wordt jaarlijks geïnformeerd over de voortgang van het DTC, waaronder aspecten als het vergroten van de naamsbekendheid en het bereik van het DTC.

De leden van de VVD-fractie willen daarnaast nader ingaan op de belangrijke taak van de Minister van EZK om de ontwikkeling van samenwerkingsverbanden tussen bedrijven op het gebied van digitale weerbaarheid te stimuleren en het aantal samenwerkingsverbanden dat momenteel is aangesloten op het DTC. Hoeveel samenwerkingsverbanden telt het DTC momenteel en om welke samenwerkingsverbanden gaat het? Klopt het dat het streven voor 2023 een uitbreiding van het aantal samenwerkingsverbanden betreft? Zo ja, om hoeveel extra samenwerkingsverbanden gaat het? In hoeverre en op welke wijze voorziet dit wetsvoorstel in de capaciteit en vereisten die deze uitbreiding behoeft? Op welke wijze worden samenwerkingsverbanden geïnventariseerd en geïnitieerd? In hoeverre wordt dit gedaan in samenwerking met bedrijven en brancheorganisaties?

Op 13 februari 2023 telde het DTC 52 samenwerkingsverbanden. Een actueel overzicht is terug te vinden op: www.digitaltrustcenter.nl/overzicht-van-samenwerkingsverbanden.
In 2023 zal meer worden ingezet op de synergie tussen de bestaande samenwerkingsverbanden, in plaats van enkel uitbreiding van het netwerk. Dat laatste zal uiteraard nog steeds plaatsvinden, maar de focus zal meer komen te liggen op kennisdeling binnen het huidige netwerk van samenwerkingsverbanden.
Het stimuleren van de ontwikkeling van samenwerkingsverbanden is één van de taken volgend uit voorliggend wetsvoorstel. Deze taak kan binnen de reeds beschikbare EZK middelen worden uitgevoerd.
Het DTC staat in nauw contact met de bestaande en potentieel nieuwe samenwerkingsverbanden en faciliteert en stimuleert de verdere ontwikkeling daarvan. Het DTC heeft geen initiërende rol, een samenwerkingsverband start doorgaans vanuit private initiatieven op.

De leden van de VVD-fractie willen tevens stilstaan bij de te vormen nieuwe organisatie waarin onder andere het DTC en het NCSC zullen worden samengebracht. Deze leden ondersteunen deze voorgenomen

samensmelting van harte, gezien het belang van het snel en zorgvuldig delen van dreigingsinformatie bij het adequaat omgaan met cyberaanvallen. Welke mogelijkheden voor het onderhavige wetsvoorstel ziet de regering om de voorgenomen eenwording te faciliteren en waar mogelijk te kunnen versnellen? Welke stappen is de regering hiervoor bereid te zetten? Kan de regering deze stappen toelichten aan de hand van het voorliggende tijdspad behorend bij de voorgenomen integratie van het DTC, NCSC en het Computer Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP)?

Het voorliggende wetsvoorstel en de integratie van het DTC, het CSIRT[2] voor digitale diensten en het NCSC zijn twee verschillende trajecten. Met dit wetsvoorstel worden de taken en bevoegdheden van de Minister van EZK op het gebied van de digitale weerbaarheid van het niet-vitale bedrijfsleven in Nederland wettelijk geborgd en daardoor kan het DTC dreigingsinformatie die persoonsgegevens bevat, verwerken. Daarmee is dit wetsvoorstel voorwaardelijk voor de nieuwe organisatie om in de breedte informatie te kunnen delen.
Voor wat betreft de vraag over mogelijke versnelling van de integratie: in het debat met de vaste commissie van Digitale Zaken van 15 december jl. is door de Minister van JenV over het integratietraject kort aangegeven dat het gedegen doorlopen van de integratie van de verschillende onderdelen tijd kost. Waar mogelijk zullen activiteiten binnen het proces op basis van de huidige wetgeving eerder worden uitgevoerd. De einddatum is de datum dat de organisaties volledig geïntegreerd moeten zijn. In de periode ervoor zal in toenemende mate tussen het DTC en het NCSC worden samengewerkt. Zo werken er al medewerkers van het DTC samen met medewerkers van het NCSC om beter bekend te raken met elkaars werkwijzen. Ook wordt er al samengewerkt op de ontwikkeling van gezamenlijke (informatie-)producten die relevant zijn voor vitale en niet-vitale organisaties.
De Kamer wordt voor de zomer nader geïnformeerd over de integratie en het daarbij behorende tijdspad.

De leden van de CDA-fractie vragen of de regering wil reageren op de berichten dat één op de vijf bedrijven het risico loopt gehackt te worden en dat met name het midden- en kleinbedrijf (mkb) kwetsbaar is. Deze leden vragen of de regering de mening deelt dat het mkb in het algemeen minder goed voorbereid is op een digitale dreiging en dat er daarom extra aandacht voor het mkb moet zijn. Deze leden vragen welke stappen de regering zet om ervoor te zorgen dat het Digital Trust Center (DTC) voldoende toegerust is om het kwetsbare mkb te informeren en helpen bij digitale dreigingen.

Op basis van CBS-data blijkt dat er in 2021 bij 25% van de bedrijven met 10 of meer medewerkers een incident met een interne oorzaak zich heeft voorgedaan, zoals storingen van ICT-systemen, en bij 10% een incident met een externe oorzaak, zoals cybercrime. Tegelijkertijd laten CBS-data zien dat (basale) veiligheidsmaatregelen door veel bedrijven niet worden genomen.[3] Hier is nog een wereld te winnen. Door basismaatregelen te nemen wordt de weerbaarheid van ondernemers vergroot. Ongeacht of een verstoring een interne of externe oorzaak heeft helpen deze maatregelen. Daarmee wordt het ook cybercriminelen minder makkelijk gemaakt om netwerken binnen te komen en schade aan te richten, direct of indirect. Zoals in de Nederlandse Cybersecurity Strategie[4] ook is

---

[2] Computer security incident response team.
[3] https://opendata.cbs.nl/#/CBS/nl/dataset/85180NED/table?ts=1650540851138. Voor bedrijven tussen de 50 en 250 werknemers was dit 37% en 15% (respectievelijk intern en extern incident).
[4] Brief van de Minister van Justitie en Veiligheid, Kamerstuk 26 643, nr. 925.

opgenomen bestaat volledige veiligheid niet maar kunnen basismaatregelen veel cyberincidenten voorkomen. Het is daarbij van belang te constateren dat het mkb een heterogene groep is. Er bestaan grote verschillen in omvang (klein, midden en groot mkb), sectoren, risicoprofiel en de mate van cyberweerbaarheid. Het doel van de inspanningen van het DTC is daarom de cyberweerbaarheid te verhogen, effecten van incidenten te minimaliseren en cyberrisico's inzichtelijk te maken.[5] Hiertoe biedt het DTC een breed pallet van informatieproducten en diensten aan. Voorliggend wetsvoorstel voorziet in de mogelijkheden om de mkb-er zover mogelijk te informeren en adviseren, zowel met algemene als specifieke (dreigings-)informatie. Het DTC verstrekt tevens handelingsperspectieven, zoals het doen van back ups of het installeren van een patch. Het is aan de bedrijven zelf om de nodige maatregelen te nemen, zo nodig met ondersteuning van hun ICT-dienstverleners en commerciële cybersecuritydienstverleners. Daarmee is het DTC geen «digitale brandweer». Zoals eerder aangegeven, is op de EZK-begroting € 3,5 miljoen structureel beschikbaar voor het DTC. Met de extra middelen van het Coalitieakkoord loopt dit bedrag op naar € 5,6 miljoen in 2023, € 8,1 miljoen per jaar in de periode 2024–2026 en vanaf 2027 structureel € 9,0 miljoen per jaar. Met de extra middelen van het Coalitieakkoord is het totaal jaarlijks beschikbare bedrag voor het DTC voldoende voor de uitvoering van dit wetsvoorstel.

1.1 Wettelijke grondslag voor taken en gegevensverwerking Minister van EZK

De leden van de SP-fractie vragen waarom het volgens de regering noodzakelijk is dat de Minister van EZK ook een bevoegdheid krijgt ten aanzien van het verwerken van gegevens rondom digitale veiligheid van bedrijven, nu deze bevoegdheid ook door de wet bij de Minister van JenV is belegd. Hoewel deze leden begrijpen dat de regering hier een verschil in rollen ziet, vragen zij of het desondanks niet meer voor de hand ligt dat de taken die met dit voorstel bij de Minister van EZK komen te liggen ook worden belegd bij de Minister van JenV. Dit voorkomt immers dat er onnodig gegevens worden gedeeld tussen onderdelen van de verschillende ministeries en er onduidelijkheid optreedt welk ministerie waar precies verantwoordelijk voor is.

Zoals eerder is toegelicht, is in nauw overleg met de Minister van JenV besloten om de beleidsverantwoordelijkheden van de Minister van EZK op het gebied van digitale weerbaarheid van het niet-vitale bedrijfsleven in een eigenstandige wet op te nemen onder andere omdat de aard van de Wbni en onderhavig wetsvoorstel anders zijn. De Wbni bevat op dit moment grotendeels de bepalingen en verplichtingen vanuit Europese wetgeving, de NIB-richtlijn, en ziet op de rijksoverheid en vitale organisaties. Onderhavig wetsvoorstel ziet op de weerbaarheid van het niet-vitale bedrijfsleven en geeft daarmee nadere invulling aan het vergroten van de digitale weerbaarheid van de Nederlandse samenleving, in dit geval het niet-vitale bedrijfsleven. Uit dit voorstel vloeit geen enkele verplichting voor bedrijven voort. Met een eigenstandige wet wordt tevens de beleidsverantwoordelijkheid van EZK voor digitale weerbaarheid van het niet-vitale bedrijfsleven transparant gemaakt.

Voor zover de leden van de SP-fractie doelen op de recente wijziging van de Wbni om onder meer rechtstreekse informatieverstrekking door de Minister van JenV aan andere aanbieders dan vitale aanbieders en rijksoverheidsorganisaties mogelijk te maken, geldt het volgende. Deze bevoegdheid betreft alleen andere aanbieders die géén schakelorganisaties hebben én indien een dreiging of incident aanzienlijke gevolgen

[5] Brief van de Minister van Economische Zaken en Klimaat, Kamerstuk 26 643, nr. 907.

heeft of kan hebben voor de continuïteit van hun dienstverlening. In onderhavig wetsvoorstel wordt de positie van het DTC als schakelorganisatie voor zijn doelgroep wettelijk vastgelegd. Dit leidt ertoe dat het NCSC niet ook aan individuele aanbieders in de doelgroep van het DTC informatie kan verstrekken. Daarmee is dit voorstel complementair aan de bestaande wetgeving.

1.2 Motivering instrumentkeuze

De leden van de CDA-fractie lezen dat de Afdeling advisering van de Raad van State heeft geadviseerd om de nieuw voorgestelde grondslag niet vast te leggen in een zelfstandige wet, maar in de Wbni. Deze leden danken de regering voor de toelichting op de noodzaak van een zelfstandige wet en hebben hierover nog een vraag. Deze leden zijn van mening dat het in dit geval belangrijk is om vanuit de praktijk te bezien hoe de wettelijke grondslag het beste vormgegeven kan worden. Deze leden vragen daarom of en, zo ja, welke praktische problemen er kunnen ontstaan en of er bedrijven in de knel kunnen komen als onderhavige grondslag wordt opgenomen in de Wbni.

De Ministers van EZK en JenV hebben onderscheidenlijke doelgroepen van organisaties waaraan informatie en advies over concrete digitale dreigingen en incidenten worden verstrekt. Het kabinet is dan ook van mening dat deze doelgroepen het beste worden gediend door deze onder te brengen in deze twee te onderscheiden wetten. Zoals eerder gememoreerd bevat de Wbni op dit moment grotendeels de bepalingen en verplichtingen vanuit Europese wetgeving, de NIB-richtlijn. Onderhavig wetsvoorstel ziet op de weerbaarheid van het niet-vitale bedrijfsleven en geeft daarmee nadere invulling aan het vergroten van de digitale weerbaarheid van de Nederlandse samenleving, in dit geval het niet-vitale bedrijfsleven.
Er ontstaan niet direct praktische problemen of knelpunten voor bedrijven, maar met een eigenstandige wet is het voor niet-vitale bedrijven duidelijk dat voor hen geen cyber meld- en zorgplicht, met bijbehorende toezicht en regeldruk, gelden. Dat is anders dan voor partijen die onder de Wbni vallen.

1.3 Verhouding DTC – NCSC

De leden van de D66-fractie vinden digitalisering binnen het bedrijfsleven van groot belang. Er worden hierbij grote stappen gemaakt en het is belangrijk dat deze transitie gezond versneld kan worden, waarbij er extra oog is voor het mkb, dat nog niet voldoende kan meekomen. De veiligheid en digitale weerbaarheid van bedrijven in deze transitie is cruciaal. Deze leden merken op dat er binnen de overheid twee verschillende loketten zijn waar bedrijven terecht kunnen met hun veiligheidsvraagstukken omtrent digitalisering. Deze leden maken zich zorgen dat het niet duidelijk is wat de taakverdeling tussen het NCSC en het DTC is. Kan de regering verduidelijken wat de wisselwerking tussen deze loketten is en of hierbij overlap ontstaat? Is het voor ondernemers duidelijk tot welk contactpunt zij behoren? Bestaat er risico's dat bedrijven niet eenduidig geïnformeerd worden of dat er verzuimd wordt om een bedrijf te informeren, doordat er onduidelijkheden bestaan over de informatievoorziening?

Er is wisselwerking tussen beide organisaties. Het DTC en het NCSC hebben duidelijk te onderscheiden doelgroepen van organisaties waaraan informatie en advies over concrete digitale dreigingen en incidenten worden verstrekt en ten behoeve waarvan analyses en onderzoek naar aanleiding van (aanwijzingen voor) dergelijke dreigingen en incidenten worden gedaan. Tot de doelgroep van het NCSC behoren vitale

aanbieders en rijksoverheidsorganisaties. Alle andere bedrijven vallen onder de doelgroep van het DTC of het CSIRT voor digitale diensten. Daarmee is er geen overlap in de informatievoorziening vanuit de overheid aan bedrijven en is het duidelijk bij welk contactpunt zij horen. Immers, als een bedrijf niet op basis van de Wbni direct in contact staat met het NCSC of het CSIRT voor digitale diensten, dan behoort een bedrijf tot de doelgroep van het DTC. Op basis van deze werkwijze fungeert het DTC als contactpunt voor het niet-vitale bedrijfsleven. In de uitvoering is er door nauwe samenwerking tussen de drie organisaties sprake van de nodige wisselwerking.

Dit laat onverlet dat voor wat betreft analyse en onderzoek de organisaties verantwoordelijk zijn voor de eigen doelgroepen. Vanwege deze verschillende doelgroepen kan het zijn dat voor het DTC en het NCSC andere bronnen, die algemene of specifieke (dreigings-)informatie bevatten welke van publieke of private partijen afkomstig zijn, relevant zijn. Zo zijn niet alle kwetsbaarheden, dreigingen en incidenten relevant voor doelgroepen van het DTC. Dit geldt ook voor de door het NCSC bijgestane vitale aanbieders of overheidsorganisaties. Denk hierbij aan systemen die alleen bij de overheid worden gebruikt, of aan de andere kant van het spectrum, producten die door zzp'ers worden gebruikt. Daarnaast kunnen beide organisaties informatie meer toespitsen op de doelgroep.

Bij grote incidenten zoals de kwetsbaarheid in Log4j eind 2021 werken beide organisaties nauw samen om informatie en adviezen op elkaar af te stemmen. Daarbij trekken zij gezamenlijk op, bijvoorbeeld door gezamenlijk webinars te organiseren. Uiteraard zal het streven zijn om als één van deze organisaties in de uitoefening van diens taken over informatie beschikt, die ook relevant is voor de doelgroep van de ander, deze informatie onderling uitgewisseld zal gaan worden. Het onderhavige wetsvoorstel draagt daar aan bij.

De leden van de CDA-fractie vragen of de regering een toelichting wil geven op het onderscheid tussen het vitale en niet-vitale bedrijfsleven, dat in wet- en regelgeving op het gebied van digitale veiligheid vaak wordt gebruikt. Deze leden vragen of dit onderscheid niet achterhaald dreigt te raken, gezien de toenemende vervlechting van de digitale infrastructuur in Nederland. Deze leden vragen of door het NCSC en DTC ook een prioriteitsafweging wordt gemaakt die ziet op het meewegen van bijvoorbeeld ketenafhankelijkheid, kritische processen en het volwassenheidsniveau op het gebied van cybersecurity bij organisaties.

In de visie van het kabinet worden bedrijven, overheden en maatschappelijke organisaties in staat gesteld om in principe zelfstandig, in samenspel met elkaar en met behulp van ICT- of cybersecuritydienstverleners te bepalen welke risico's zij lopen in de digitale ruimte en welke maatregelen zij kunnen nemen in de omgang met deze risico's. Vanwege het belang van de vitale infrastructuur voor het functioneren van onze maatschappij wordt aan deze vitale organisaties een hoog niveau van weerbaarheid gevraagd. De overheid stelt, mede gelet op Europese wet- en regelgeving extra eisen aan deze vitale organisaties om zodoende ook de digitale weerbaarheid van deze organisaties te verhogen.
In het huidige stelsel is de primaire taak van de Minister van JenV het verlenen van bijstand aan vitale aanbieders en rijksoverheidsorganisaties bij digitale dreigingen en incidenten. Dit om het uitvallen van de beschikbaarheid of het verlies van integriteit van netwerk- en informatiesystemen bij de wettelijke doelgroeporganisaties te voorkomen of te beperken. Vitale aanbieders of categorieën van zodanige aanbieders worden op basis van artikel 5 van de Wbni aangewezen. Het uitvallen van die netwerk- en informatiesystemen bij deze organisaties kan immers

potentieel tot maatschappelijke ontwrichting leiden. Denk bijvoorbeeld aan de gevolgen als de dienstverlening van een drinkwaterbedrijf uitvalt.

De onderscheidende doelgroepen van het NCSC en het DTC worden, ongeacht hun branche of sector, regio of bedrijfsomvang op dezelfde wijze behandeld door beide organisaties. Hierbij is er binnen de respectievelijke doelgroepen geen sprake van prioritering. Zover mogelijk wordt de dienstverlening wel aangepast aan de volwassenheid van de organisaties. Hierbij onderkent het kabinet ook het belang van ketenafhankelijkheden. Zowel het NCSC als het DTC verspreiden informatie over het belang van weerbare ketens. De inzet van het DTC op synergie tussen de samenwerkingsverbanden is ook een uitvloeisel van het toenemende belang hiervan.

De leden van de ChristenUnie-fractie vragen hoe voorliggend voorstel zich verhoudt tot de aanstaande samenvoeging van het NCSC en het DTC en de nieuwe Europese richtlijnen die de komende jaren zullen worden geïmplementeerd.

Zoals ook eerder aangegeven, zijn het voorliggende wetsvoorstel en de integratie van het DTC, het CSIRT voor digitale diensten en het NCSC twee verschillende trajecten. Met dit wetsvoorstel worden de taken en bevoegdheden van de Minister van EZK wettelijk geborgd en daardoor kan het DTC dreigingsinformatie die persoonsgegevens bevat, verwerken. Daarmee is dit wetsvoorstel voorwaardelijk voor de nieuwe organisatie om in de breedte informatie te kunnen delen.
Er zal in de toekomst, na afronding van de integratie, sprake zijn van één nieuwe organisatie die de taken van de Ministers van EZK en JenV zal uitvoeren waardoor voor de doelgroepen duidelijk is bij welk contactpunt ze moeten zijn.

Voor onderhavig wetsvoorstel is enkel de herziene Europese Netwerk- en informatiebeveiligingsrichtlijn (NIB2-richtlijn)[6] relevant. Op dit moment loopt het proces van de nationale implementatie. In dat proces wordt bezien welke aanpassingen van de nationale wetgeving noodzakelijk zijn. De Minister van JenV en ik zijn alert op relevante Europese ontwikkelingen.

De leden van de ChristenUnie-fractie maken zich zorgen of de extra taak voor het DTC, naast de taken die het NCSC en de organisaties die «objectief kenbaar tot taak» hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere netwerken informatiesystemen (OKTT's) reeds vervullen, het delen van dreigingsinformatie niet juist inefficiënter maakt. Zou het niet verstandiger zijn het delen van dreigingsinformatie meer te concentreren? Hoe weegt de regering hierbij ook de consultatie-inbreng van Cyberveilig Nederland? Genoemde leden maken zich zorgen dat voorliggend voorstel leidt tot versplintering van informatie en dat dit juist een averechts effect kan hebben.

Door het opbouwen en versterken van een Landelijk Dekkend Stelsel (hierna: LDS) van cybersecurity-samenwerkingsverbanden kan informatie steeds breder, efficiënter en effectiever worden gedeeld tussen schakelorganisaties ten behoeve van de informatievoorziening richting hun doelgroepen. Actuele kennis en informatie over cyberdreigingen,

---

[6] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PbEU 2022, L 333).

-incidenten, -trends, en -kwetsbaarheden moeten zo snel mogelijk beschikbaar zijn voor partners in het LDS zodat zij tot handeling kunnen overgaan. De overheid heeft hierbij het voortouw.
Om versnippering zoveel mogelijk tegen te gaan wordt als één van de speerpunten binnen het LDS toegewerkt naar één organisatie waar het NCSC, het DTC en het CSIRT voor digitale diensten in opgaan.

De leden van de ChristenUnie-fractie vragen de regering in elk geval in gesprek te gaan met het bedrijfsleven over hoe de informatievoorziening richting bedrijven zo kan worden gestroomlijnd dat voornoemde risico's zo veel als mogelijk worden voorkomen bijvoorbeeld middels een loketfunctie. Hierbij kunnen genoemde leden zich ook voorstellen dat richtlijnen worden opgesteld omtrent het delen van vertrouwelijke informatie.

Het DTC en het NCSC hebben reguliere contacten met vertegenwoordigers van ondernemend Nederland over onder andere efficiënte informatiedeling.
Op termijn zal de samenvoeging van het DTC, het CSIRT voor digitale diensten en het NCSC vanuit de synergie-gedachte tot één uitvoerende organisatie en loket leiden voor alle doelgroepen waardoor de informatievoorziening verder kan worden gestroomlijnd. Het onderhavige wetsvoorstel en de Wbni voorzien in het onderling uitwisselen van vertrouwelijke informatie.

De leden van de SP-fractie vrezen dat er in praktijk straks veel onduidelijkheid zal bestaan over welk ministerie voor welke taak verantwoordelijk is. Daarbij is er een risico dat de twee instanties, de DTC en de NCSC, taken dubbel of niet uitvoeren, omdat het onduidelijk is welke instantie waar verantwoordelijk voor is. Kan de regering daarbij ook nader ingaan op de kritiek van de Afdeling advisering van de Raad van State?

Zoals in het nader rapport is toegelicht, hebben het DTC en het NCSC duidelijk te onderscheiden doelgroepen. Het NCSC richt zich op vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid. De doelgroep van het DTC is het niet-vitale bedrijfsleven.
Het NCSC en het DTC werken waar mogelijk samen. Voor wat betreft analyse en onderzoek zijn beide organisaties verantwoordelijk voor de eigen doelgroepen. Vanwege deze verschillende doelgroepen kan het zijn dat voor het DTC en het NCSC andere bronnen, die algemene of specifieke (dreigings-) informatie bevatten welke van publieke of private partijen afkomstig zijn, relevant zijn. Zo zijn niet alle kwetsbaarheden, dreigingen en incidenten relevant voor doelgroepen van het DTC. Dit geldt ook voor de door het NCSC bijgestane vitale aanbieders of overheidsorganisaties. Denk hierbij aan systemen die alleen bij de overheid worden gebruikt, of aan de andere kant van het spectrum, producten die door zzp'ers worden gebruikt. Dit laat onverlet dat als één van deze organisaties in de uitoefening van diens taken over informatie beschikt, die ook relevant is voor de doelgroep van de ander, deze informatie onderling uitgewisseld zal gaan worden.
Hiermee worden de door de leden van de SP-fractie genoemde risico's gemitigeerd.

2. Uitvoering

De leden van de D66-fractie vinden het van groot belang dat bedrijven zich digitaal weerbaar kunnen maken. Laagdrempeligheid staat hierbij centraal. Deze leden vragen in hoeverre het DTC niet-vitale bedrijven van informatie voorziet omtrent de overgang naar digitale middelen in bedrijfsvoering en de risico's die hierbij ontstaan. Bestaat hierbij een

verschil in de grote van bedrijven? Kunnen bedrijven hiervoor bij het DTC terecht? Zijn hieruit al best-practices gekomen die actief naar ondernemers kunnen worden gecommuniceerd?

Spelen ondernemersorganisaties een rol bij het verbeteren van digitale informatievoorziening? Zo niet, ziet de regering voor deze organisaties een rol, zodat kennis laagdrempelig en toegankelijk naar bedrijven die in de digitale transitie zitten kan worden gecommuniceerd?

Het DTC is niet het loket voor ondernemers voor vragen hoe de transitie van analoog naar digitaal wordt gemaakt, maar helpt ondernemers met informatie over digitale weerbaarheid. Op dit moment zet het DTC twee instrumenten in: de zelfscan-tool op basis van de vijf basisprincipes van online veiligheid (de basisscan) en de risicoanalyse-tool.[7] Deze helpen ondernemers kwetsbaarheden te vinden en de juiste (basis)maatregelen te nemen. Het DTC zal dit aanvullen met een tool die kleine bedrijven op weg helpt, waaronder ZZP-ers, die geen tot weinig kennis hebben van, of interesse hebben in, cybersecurity. De tool wordt zo praktisch mogelijk, in voor de ondernemer begrijpelijke taal en activerend. Centraal bij alle voorlichting van het DTC staan de concrete handelingsperspectieven voor ondernemers. Het is namelijk cruciaal dat de stap van weten naar doen wordt gemaakt.[8] Hierbij staat het DTC in nauw contact met vertegenwoordigers van verschillende ondernemersorganisaties.

B. Artikelen

Artikel 4 (Verstrekking van vertrouwelijke gegevens door de Minister van EZK)

De leden van de D66-fractie nemen kennis van het delen van dreigingsinformatie en de kans die daarbij bestaat om juist gevoelige informatie te lekken, wanneer de digitale beveiliging van een bedrijf onvoldoende op orde is. De leden verzoeken de regering toe te lichten hoe dit voorkomen kan worden. Zet de regering hier instrumenten voor in en, zo ja, welke?

Zoals in de memorie van toelichting is aangegeven, volgt de Minister van EZK bij de uitvoering van de taken uit dit wetsvoorstel de in het algemeen voor de overheid geldende voorschriften voor informatiebeveiliging. Daarnaast worden waar nodig aanvullende maatregelen genomen ter bescherming van informatie en gegevens en worden processen ingericht om vertrouwelijkheid te waarborgen.

Voor wat betreft het delen van informatie met individuele bedrijven betracht de Minister van EZK uiteraard grote zorg en zal bij twijfel extra onderzoek worden gedaan en zal in geval van twijfel de meest gepaste communicatiemethode worden gehanteerd.

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens

---

[7] Deze twee instrumenten zijn reeds functioneel en toegankelijk op www.digitaltrustcenter.nl/tools.

[8] Brief van de Minister van Economische Zaken en Klimaat, Kamerstuk 26 643, nr. 907.