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. 3

MEMORIE VAN TOELICHTING

A. Algemeen

1. Inleiding

Dit wetsvoorstel regelt de taken en bevoegdheden van de Minister van Economische Zaken en Klimaat (hierna: Minister van EZK) op het gebied van de verbetering van de digitale weerbaarheid van het niet-vitale bedrijfsleven in Nederland. Binnen het Ministerie van Economische Zaken en Klimaat (hierna: het Ministerie van EZK) is om dit doel te bewerkstelligen, in overeenstemming met de motie Hijink/Tellegen[1], in 2017 het Digital Trust Center (hierna: DTC) opgericht. Aanleiding voor deze motie was de kamerbrede behoefte aan een centrum dat «bedrijven en maatschappelijke organisaties kan informeren en adviseren over én concrete hulp en ondersteuning kan bieden bij het verbeteren van hun cybersecurity en bij het afslaan van aanvallen door hackers». Deze behoefte heeft zijn oorsprong onder meer in het besef dat de kansen van digitalisering alleen optimaal kunnen worden benut wanneer de digitale veiligheid op orde is. Zo niet dan kan zelfs het voortbestaan van een bedrijf in gevaar komen en de Nederlandse concurrentiepositie verzwakken. Het DTC heeft dan ook als missie bedrijven weerbaarder te maken tegen cyberdreigingen. Hiertoe zijn twee hoofdtaken voor de Minister van EZK geformuleerd die in de praktijk door het DTC worden uitgevoerd. Ten eerste informatie en advies geven. Ten tweede samenwerking tussen bedrijven op het gebied van digitale weerbaarheid bevorderen. Het DTC is onderdeel van de Directie Digitale Economie (DDE), vallend binnen het Directoraat Generaal Economie en Digitalisering (DGED) binnen het Ministerie van EZK.

Vanuit het DTC wordt nu voornamelijk algemene informatie over digitale dreigingen en incidenten aan het niet-vitale bedrijfsleven gegeven. Er is echter ook behoefte om het bedrijfsleven over specifieke digitale dreigingen en kwetsbaarheden te informeren. Verwacht mag worden dat bedrijven bij een voor hen concrete bedreiging eerder naar hun digitale

[1] Kamerstukken II 2016/17, 26 643, nr. 474.

kst-36270-3
ISSN 0921 - 7371
's-Gravenhage 2022

weerbaarheid zullen kijken waar dit nu nog uit blijft bij een meer generieke waarschuwing. Ook zal bij informatie over een specifieke dreiging door het DTC een zo praktisch mogelijk handelingsperspectief worden aangereikt zodat het bedrijf ook weet welke vervolgstap(pen) het kan nemen. Deze uitbreiding van de informatievoorziening vraagt een verdere inbedding van de taken en bevoegdheden van de Minister van EZK. Met dit wetsvoorstel worden de taken van de Minister van EZK alsook de daaraan gekoppelde bevoegdheid van een formele wettelijke grondslag voorzien. Naast de eerdergenoemde taken op het gebied van het verstrekken van algemene informatie en stimuleren van samenwerking die al op basis van de motie Hijink/Tellegen worden uitgevoerd, omvat dit ook de taak voor het delen van specifieke dreigingsinformatie. In het laatste geval kan het voorkomen dat de Minister van EZK bij het ontvangen, verwerken en delen van (dreigings)informatie, persoonsgegevens verwerkt. Door te voorzien in een formele wettelijke grondslag voor de taken en de daaraan gekoppelde bevoegdheden ontstaat tevens een expliciete wettelijke grondslag voor de Minister van EZK om in het kader van de taakuitvoering persoonsgegevens te verwerken.

Met dit wetsvoorstel ontstaat er, naast de reeds bestaande bevoegdheden op grond van de Wet beveiliging netwerk en informatiesystemen (Wbni), een nieuwe wettelijke taak voor de Minister van EZK.

2. Hoofdlijnen van het voorstel

2.1 Aanleiding

Uit jaarlijks onderzoek van het Centraal Bureau voor de Statistiek (CBS)[2] blijkt dat digitalisering ver is doorgedrongen in het Nederlandse bedrijfsleven. Echter, de digitale weerbaarheid van diezelfde bedrijven is nog geen vanzelfsprekendheid. De cijfers tonen aan dat digitalisering en de daaraan gekoppelde weerbaarheid niet alleen afhankelijk zijn van de omvang van een bedrijf. Zo zijn er voorbeelden in het grootbedrijf, bij het mkb en zzp'ers, waaruit blijkt dat zij de digitale weerbaarheid op orde hebben. Echter, uit onderzoek van het CBS blijkt dat bedrijven, ondanks hun omvang toch slachtoffer blijven van digitale verstoringen en aanvallen.[3] Met de verder doordringende digitalisering wordt de potentiële schade aan het bedrijfsleven, bij het achterblijven van digitale veiligheid en beveiliging, steeds groter. Digitalisering creëert ook nieuwe onderlinge afhankelijkheden bij bedrijven, niet alleen tussen digitale systemen, maar ook in de (digitale) (leveranciers)keten. Het belang van digitale veiligheid en beveiliging groeit omdat de (on)veiligheid van het ene bedrijf, via deze verbindingen invloed kan hebben op de (on)veiligheid eerder of verderop in de keten zo blijkt ook uit de waarschuwing in het Cyber Security Beeld Nederland 2021 (CSBN 2021).[4] Via het CIO-platform hebben bedrijven met een brief aan de Minister van Justitie en Veiligheid (hierna: de Minister van JenV)[5] gevraagd om te zorgen voor informatiedeling vanuit de overheid met bedrijven als de overheid beschikt over relevante informatie over dreigingen, kwetsbaarheden en incidenten. Op dit moment informeert de overheid door middel van de bestaande structuren, op basis van de Wbni, zowel de rijksoverheid als specifieke doelgroepen binnen het Nederlandse bedrijfsleven, zijnde de vitale bedrijven en digitale dienstverleners. Overige bedrijven kunnen op basis van dit wetsvoorstel informatie van de overheid ontvangen, in

---

[2] https://longreads.cbs.nl/ict-kennis-en-economie-2020/ict-gebruik-bij-bedrijven/.
[3] https://www.cbs.nl/nl-nl/publicatie/2019/37/cybersecuritymonitor-2019.
[4] https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021.
[5] https://www.cio-platform.nl/k/nl/n626/news/view/10130/6631/brief-aan-minister-grapperhaus-versterking-van-de-nederlandse-cyberweerbaarheid.html.

enkele gevallen zal dit in aanvulling zijn op de informatie die zij al via een schakelorganisatie ontvangen als bedoeld in artikel 3, tweede lid, Wbni. Door de (acute) dreigingsinformatie waar de overheid beschikt te verstrekken aan het niet-vitale bedrijfsleven stelt de overheid deze bedrijven in staat om op basis van deze objectieve informatie zelf te beoordelen of en in welke mate zij maatregelen moeten treffen ter mitigatie van een kwetsbaarheid, ter afwering van een dreiging of ter oplossing van een daadwerkelijke inbreuk.

De digitale weerbaarheid van bedrijven heeft zowel een economisch effect als een breder maatschappelijk effect doordat bedrijven in verbinding staan met burgers en overheidsorganisaties. Het vergroten van de digitale weerbaarheid van bedrijven levert een belangrijke bijdrage aan de Nederlandse economie. Weerbare bedrijven, dat wil zeggen bedrijven die bewuste, op risico's gebaseerde, keuzes maken over te nemen maatregelen op het gebied van digitale beveiliging, zullen over het algemeen minder snel slachtoffer zijn van digitale verstoringen. Deze maatregelen zijn pluriform. Zo kunnen bedrijven maatregelen nemen op het gebied van voorlichting door bijvoorbeeld trainingen voor personeel, specifieke IT-beveiligingsmaatregelen, maar ook maatregelen ten behoeve van de bedrijfscontinuïteit of de inhuur van gespecialiseerde diensten. Afgewogen maatregelen zullen enerzijds een bescherming bieden tegen onbewuste verstoringen anderzijds tegen moedwillige aanvallen. Door afgewogen maatregelen te nemen zullen bedrijven en ondernemers bij een digitaal incident sneller terug kunnen keren naar hun reguliere bedrijfsvoering wat direct bijdraagt aan het verdienvermogen van het bedrijf.

Dit beeld wordt ondersteund door het rapport van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) «Voorbereiden op digitale ontwrichting»[6] en is tevens benoemd door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in het CSBN 2020 en CSBN 2021.[7, 8] In beide rapporten wordt de verregaande digitalisering en de daaraan gerelateerde risico's voor de Nederlandse samenleving benoemd. Door het informeren en adviseren van bedrijven in zijn algemeenheid en specifiek over kwetsbaarheden en dreigingen wordt gewerkt aan een weerbaar bedrijfsleven. Ook de Cyber Security Raad (CSR) adviseert de overheid om, indien zij beschikt over acute dreigingsinformatie die relevant is voor organisaties in Nederland, deze informatie actief te delen met potentiële en daadwerkelijke slachtoffers[9]. Dit wordt ook nog eens bevestigd door het onderzoeksrapport «Informatie-uitwisseling landelijk dekkend stelsel cybersecurity» uitgevoerd door Dialogic in opdracht van het WODC.[10]Volgens dit WODC-rapport heeft de Minister van EZK een centrale rol in de informatievoorziening over de digitale weerbaarheid van ondernemend Nederland. Het WODC-advies is overgenomen in het coalitieakkoord «Omzien naar elkaar, vooruitkijken naar de toekomst»[11] en zegt over het DTC het volgende: *«We beschermen onze bedrijven, vitale infrastructuur en economisch kapitaal beter door centraal gecoördineerde structurele samenwerking tussen o.a. het NCSC, het DTC, overheden, bedrijven en wetenschappen. Zij kunnen sneller en makkelijker informatie delen over digitale kwetsbaarheden en hacks»*. Hierin wordt expliciet het

---

[6] WRR-rapport nr. 101, 2019: https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting.

[7] https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020.

[8] https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021.

[9] https://cybersecurityraad.nl/010_Actueel/aanscherping-en-uitbreiding-van-maatregelen-noodzakelijk-voor-een-cyberweerbare-samenleving.aspx.

[10] https://wodc.nl/wodc-nieuws-2020/cybersecurity-stelsel.aspx.

[11] https://www.kabinetsformatie2021.nl/documenten/publicaties/2021/12/15/coalitieakkoord-omzien-naar-elkaar-vooruitkijken-naar-de-toekomst.

bestaan van het DTC en de intensieve samenwerking met het Nationaal Cyber Security Center (NCSC) en andere partijen aangehaald.

2.2 Wettelijke grondslag voor taken en gegevensverwerking Minister van EZK

De Minister van EZK is beleidsverantwoordelijke voor de bevordering van de digitalisering van ondernemers en heeft al stappen ondernomen om de digitale weerbaarheid van het niet-vitale bedrijfsleven te vergroten. Ten behoeve van de versteviging van deze rol voorziet dit wetsvoorstel in een vastlegging van de taken van de Minister van EZK op het terrein van digitale weerbaarheid van het niet-vitale bedrijfsleven, zoals het verwerken en verspreiden van informatie over kwetsbaarheden, dreigingen en incidenten en het samenwerken met andere bestuursorganen en organisaties (artikel 2). In het kader van deze taakuitoefening mogen persoonsgegevens worden verwerkt.

Voorts voorziet dit wetsvoorstel in een wettelijke grondslag om bijvoorbeeld bij andere (publiekrechtelijke) organisaties de voor bovengenoemde taakuitoefening noodzakelijke gegevens te vragen en in de mogelijkheid van die derden om in reactie daarop zo nodig ook persoonsgegevens te verstrekken aan de Minister van EZK (artikel 3). Ook voorziet dit wetsvoorstel in de voorwaarden waaronder vertrouwelijke gegevens die bij de Minister van EZK bekend zijn, verstrekt mogen worden aan derden (artikel 4). Ten slotte regelt dit wetsvoorstel een rechtstreekse informatie-uitwisseling tussen de Minister van EZK en onder meer andere overheidsorganisaties die zich met digitale beveiliging bezighouden (artikel 2, 4 en 5).

Het belangrijkste doel is de versterking van de digitale weerbaarheid van bedrijven (zie de aanhef van artikel 2, eerste lid). Ten behoeve van dat doel heeft de Minister van EZK verschillende taken. Het gaat hierbij allereerst om het analyseren en het onderzoeken van gegevens over kwetsbaarheden, dreigingen en incidenten met betrekking tot netwerk- en informatiesystemen van bedrijven, het informeren en adviseren van bedrijven over voor hun bedrijven relevante kwetsbaarheden, dreigingen en incidenten, én om het verstrekken van informatie over kwetsbaarheden, dreigingen en incidenten gerelateerd aan individuele bedrijven. Deze taken zijn vastgelegd in artikel 2, eerste lid. Op deze manier wordt het mogelijk om specifieke informatie en advies te verwerken en te delen binnen en buiten de overheid. Deze informatie wordt kosteloos aangeboden. De verantwoordelijkheid van de overheid voor de digitale weerbaarheid van niet-vitale bedrijven is hierin begrensd door de eigen verantwoordelijkheid van niet-vitale bedrijven. Hierbij dient in acht te worden genomen dat de informatie en adviezen van de Minister van EZK een niet volledige aanvulling zijn op de digitale weerbaarheid van een bedrijf. Zo heeft een specifieke individuele notificatie door de Minister van EZK betrekking op die concrete dreiging of kwetsbaarheid. Maar er kunnen meer kwetsbaarheden, dreigingen en incidenten zijn in de netwerk- en informatiesystemen van dat bedrijf waar de Minister van EZK géén weet van heeft. Een bedrijf is en blijft zelf verantwoordelijk voor het actief beheren en versterken van haar digitale veiligheid. De overheid speelt hierin een rol maar neemt uitdrukkelijk niet de verantwoordelijkheid van bedrijven over.

De taken van de Minister van EZK bestaan enerzijds uit het verstrekken van informatie en advies, direct of via samenwerkingsverbanden, en anderzijds uit het verstrekken van actuele dreigingsinformatie en vertrouwelijke informatie aan bedrijven en intermediaire organisaties. In deze zijn intermediaire organisaties vertegenwoordigers van een bepaalde

groep aan bedrijven. Denk hierbij aan sector en brancheorganisaties, regionale samenwerkingsverbanden, maar ook sector overstijgende belangenbehartigers van ondernemend Nederland.

Daarnaast heeft de Minister van EZK als taak om de ontwikkeling van samenwerkingsverbanden tussen bedrijven op het gebied van digitale weerbaarheid te stimuleren, samen te werken met bestuursorganen en rechtspersonen, én om indien relevant de in het kader van analyses en onderzoeken verkregen gegevens aan de Minister van JenV, ten behoeve van de taken van de laatstgenoemde Minister, bedoeld in artikel 3, eerste lid, van de Wbni, en aan het CSIRT voor digitale diensten te verstrekken (artikel 2, tweede lid).

De Wbni bevat de taken en bevoegdheden van de Minister van JenV op het terrein van cybersecurity, die in de praktijk worden uitgevoerd door het NCSC. Artikel 3, eerste lid, van die wet regelt als primaire taak van de Minister van JenV de verlening van bijstand bij digitale dreigingen en incidenten aan vitale aanbieders en andere aanbieders die onderdeel zijn van de rijksoverheid. Ook is de Minister van JenV belast met de taak van CSIRT voor een categorie vitale aanbieders (aanbieders van essentiële diensten). Daarnaast regelt artikel 3, tweede lid, van de Wbni dat dreigings- en incidentinformatie met betrekking tot netwerk- en informatiesystemen van andere aanbieders, die in het kader van de primaire taakuitoefening is verkregen, door de Minister van JenV kan worden verstrekt aan de in dat lid bedoelde schakelorganisaties (zoals CSIRT's, computercrisisteams, en organisaties die «objectief kenbaar tot taak» hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten (OKTT's). Daarnaast voorziet de Wbni ook in de regeling van een CSIRT voor digitale diensten. Deze laatste taak is reeds toegekend aan de Minister van EZK.

Met de vorming van de in dit wetsvoorstel opgenomen grondslag ontstaat er de taak en de bevoegdheid voor de Minister van EZK om de voormelde (vertrouwelijke) informatie en adviezen, kwetsbaarheden en dreigingen te verwerken en te delen. Daarmee wordt, naast het bestaande regime van de Wbni, voorzien in taken en bevoegdheden voor de Minister van EZK, die aldus een plaats krijgt naast de Minister van JenV, het CSIRT voor digitale diensten en krachtens de Wbni als zodanig aangewezen computercrisisteams en OKTT's, waarmee het stelsel van (overheids)organisaties met een rol in de digitale weerbaarheid van Nederland verder wordt bevorderd.

In de artikelen 3, tweede lid, en 20, tweede lid, van de Wbni zijn organisaties genoemd waarmee het NCSC de in deze artikelleden genoemde gegevens mag delen. In artikel 21, tweede lid, van de Wbni zijn organisaties genoemd waarmee het CSIRT voor digitale diensten de in dit artikellid genoemde gegevens mag delen. Met de in artikel 5 voorgestelde wijziging van de Wbni wordt de Minister van EZK hieraan toegevoegd, waardoor een rechtstreekse informatie-uitwisseling door genoemde overheidsorganisaties aan de Minister van EZK mogelijk wordt gemaakt. In samenhang hiermee wordt in de voorgestelde artikelen 2, tweede lid, en 4 geregeld dat ook informatie-uitwisseling mogelijk is tussen de Minister van EZK enerzijds en het NCSC en het CSIRT voor digitale diensten anderzijds.

Op dit moment is er ook een wetsvoorstel bij de Eerste Kamer aanhangig aangaande de wijziging van de Wbni[12] welke een uitbereiding van bevoegdheden van de Minister van JenV bevat. Deze bevoegdheid houdt in dat het onder bepaalde voorwaarden mogelijk wordt voor het NCSC om in ruimere zin dreigings- en incidentinformatie te delen met andere aanbieders (niet zijnde rijksoverheid en vitale aanbieders). Een van die voorwaarden is dat er voor die aanbieders géén schakelorganisatie beschikbaar is die deze aanbieder als doelgroep heeft. De Minister van EZK vervult de rol van schakelorganisatie met als doelgroep niet-vitale bedrijven. Daardoor zal het NCSC informatie over deze doelgroep direct met de Minister van EZK kunnen delen, welke op haar beurt haar doelgroep zal kunnen informeren en adviseren. Hiermee wordt eventueel dubbel informeren van een niet-vitaal bedrijf voorkomen.

Met deze wettelijke bepalingen worden de onderscheidenlijke rollen en verantwoordelijkheden van de Minister van EZK en de Minister van JenV uitdrukkelijk in beide wetten benoemd. Daarnaast wordt hiermee voorzien in een wettelijke grondslag om elkaar ten behoeve van de onderscheidenlijke taken te voorzien van voor de uitoefening van die taken relevante informatie over digitale dreigingen, kwetsbaarheden en incidenten. Voor zover daar onduidelijkheid over zou bestaan, beide Ministers bedienen hiermee gescheiden doelgroepen. Het NCSC staat voor haar doelgroep de rijksoverheid en vitale organisaties, het CSIRT voor digitale diensten voor digitale dienstverleners en het DTC voor de overige bedrijven die niet onder de voorgaande categorieën vallen.

Naast de samenwerking binnen de overheid en met formele partners zoals benoemd in de Wbni, zal de Minister van EZK ook samenwerkingen aangaan met andere organisaties binnen en buiten de rijksoverheid. Denk hierbij aan andere vakdepartementen, decentrale overheden, maatschappelijke organisaties, onderzoeksinstituten, onderwijsinstellingen, cybersecurity bedrijven of onafhankelijke cybersecurity onderzoekers.

Het onderwerp digitalisering van ondernemers is ook belegd bij de Minister van EZK. In het verlengde hiervan en in combinatie met de huidige taak van de Minister van EZK om ondernemerschap te versterken, innovatievermogen te vergroten en randvoorwaarden voor economische groei te borgen is ervoor gekozen om de bredere taak en bevoegdheden van de Minister van EZK vast te leggen in een zelfstandige wet.

2.3 Motivering instrumentkeuze

Het verwerken en verspreiden van informatie (waaronder persoonsgegevens) door de overheid ten behoeve van de verbetering van de digitale weerbaarheid van niet-vitale bedrijven kan, conform het legaliteitsbeginsel, alleen als er een wettelijke taak aan ten grondslag ligt. Er is gekozen om de bevoegdheid van de Minister van EZK in deze vast te leggen in een formele wet. Hiermee wordt het bestaande stelsel van taken en bevoegdheden van de rijksoverheid uitgebreid. Dit nieuwe wetsvoorstel staat naast de Wbni. Waar de Wbni, zoals eerder gezegd, zich richt op de rijksoverheid, vitale bedrijven en digitale dienstverleners

[12] Voorstel van wet tot wijziging van de Wet beveiliging netwerk- en informatiesystemen in verband met de uitbreiding van de bevoegdheid van de Minister van Justitie en Veiligheid om dreigings- en incidentinformatie over de netwerk- en informatiesystemen van niet-vitale aanbieders te verstrekken aan deze aanbieders en aan organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten ten behoeve van deze aanbieders (Kamerstukken II 2021/22, 36 084, nr. 2).

zoals bedoeld volgens de Europese NIB-richtlijn[13], en schakelorganisaties, richt dit wetsvoorstel zich op het niet-vitale bedrijfsleven. De Wbni bevat daarmee verplichtingen voor haar doelgroep en voor naleving daarvan.[14] Op grond van het onderhavige voorstel geldt er geen zorg- of meldplicht voor haar doelgroep, niet-vitale bedrijven. Tevens is er geen sprake van toezicht en handhaving.

In de Wbni zijn de taken van de Minister van JenV vastgelegd ten aanzien van organisatie die deel uitmaken van de rijksoverheid en vitale aanbieders en zijn de vakministers primair verantwoordelijk gemaakt voor het toezicht op de naleving van verplichtingen in de Wbni ten aanzien van onder hen vallende specifieke sectoren. Voor de Minister van EZK zijn deze taken naast het genoemde toezicht op de naleving van de Wbni, ook het voorzien in de CSIRT-functie voor digitale dienstverleners. Op basis van dit wetsvoorstel verschillen de rol en de taken van de Minister van EZK, met die van de Minister van EZK op basis van de Wbni. 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, die als aanbieders van een essentiële dienst zijn aangewezen, en voor digitale dienstverleners. Het onderhavige wetsvoorstel ziet daarentegen op het informeren en adviseren van de niet-vitale bedrijven, ongeveer 2 miljoen bedrijven, die niet vallen onder het toepassingsbereik van de Wbni én waarvoor de Minister van EZK dus krachtens die wet ook géén toezichthoudende taken heeft. Dit laat onverlet dat de vakministers (in navolging van de Wbni) verantwoordelijk blijven voor het stellen van eisen aan en het toezicht op de naleving daarvan door niet-vitale aanbieders in onder hen vallende branches en sectoren.

Daarnaast is de doelgroep van onderhavig voorstel anders is dan de doelgroep van de Wbni. De Wbni is in hoofdzaak gericht op de digitale veiligheid van organisaties die deel uitmaken van de rijksoverheid, vitale private aanbieders en digitale dienstverleners. Hierin wordt bijvoorbeeld geregeld dat de Minister van JenV (en in de praktijk het 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. De Minister van JenV heeft krachtens de Wbni als primaire taak het informeren en het adviseren van vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid over digitale dreigingen en incidenten. Naast het informeren en het adviseren 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 aan de aanbieder uit de doelgroep ter plekke ondersteuning wordt geboden bij het duiden van het probleem en de maatregelen om dat probleem aan te pakken. De Minister van EZK 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 de Minister

[13] 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).

[14] Zorg- en meldplicht en daarbij behorend toezicht vindt plaats op vitale aanbieders welke ook aanbieders van essentiële diensten en digitaledienstverleners zijn. Voor andere vitale aanbieders geldt een meldplicht maar geen toezicht.

van EZK bij incidenten geen overige bijstand, ofwel incident response, aan de aanbieders in zijn doelgroep.

Tot slot bevat de Wbni primair de bevoegdheden van de Minister van Justitie en Veiligheid. Vanuit het wetgevingsstelsel is dit wetsvoorstel daarmee minder geschikt om daarin deze, naar aard, rol en doelgroep andere bevoegdheden van de Minister van EZK te verwerken. Door de bevoegdheden te scheiden is er duidelijkheid over de taken van beide Ministers en kunnen beide zich richten op het verbeteren van de digitale veiligheid van de onder hun verantwoordelijkheid vallende doelgroep(en). In de praktijk zal hierbij uiteraard nauw worden samengewerkt door beide ministeries en uitvoerende organisatieonderdelen te weten het NCSC en het DTC.

Deze belangen worden het beste worden gediend door deze onder te brengen in deze twee te onderscheiden wetten.

2.4 Verhouding DTC – NCSC

Zoals ook eerder toegelicht, hebben het DTC en het NCSC beiden duidelijk onderscheidende doelgroepen. Het NCSC richt zich op vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid. De doelgroep van dit wetsvoorstel is het niet-vitale bedrijfsleven. Beide organisaties zullen de analyses, onderzoeken en adviezen die zij uitvoeren en geven afstemmen op de taak die zij hebben voor hun doelgroep. Hierbij wordt met name in de formulering van het advies rekening gehouden met de aard en de relevantie van het advies voor de respectievelijke doelgroepen. Daarnaast zullen het DTC en het NCSC in dergelijke gevallen met elkaar samenwerken en informatie uitwisselen om te voorkomen dat sterk uiteenlopende analyses, onderzoeken en adviezen worden gegeven. Het NCSC en het DTC werken waar mogelijk samen. Voor wat betreft analyse en onderzoek zijn zoals hierboven aangegeven beide organisaties verantwoordelijk voor de eigen doelgroepen. Vanwege deze verschillende doelgroepen kan het zijn dat andere bronnen 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 maar eigenlijk gekocht zijn als consument. Dit laat onverlet dat als één van deze organisaties in de uitoefening van haar taken over informatie beschikt, die ook relevant is voor de doelgroep van de ander, deze informatie onderling uitgewisseld zal gaan worden.

Daarnaast wordt de samenwerking in de komende jaren verder vormgegeven door de voorgenomen vorming van één nieuwe organisatie waarin verschillende cybersecurity expertise van de overheid samen zal komen.[15]

2.5 Toepassing in Caribisch Nederland

De taken en bevoegdheden van de Minister van EZK zoals omschreven in het onderhavige wetsvoorstel gelden voor Nederland inclusief Caribisch Nederland (zijnde Bonaire, Saba en Sint-Eustatius). Ook bij het bedrijfsleven in deze drie bijzondere gemeentes is er een behoefte aan informatiedeling over digitale dreigingen (artikel 7).

[15] Kamerstukken II 2022/23, 26 643 nr. 915.

2.6 Monitoring en evaluatie

Het effect van het beleid wordt jaarlijks gemeten door het CBS als onderdeel van de meting «ICT-gebruik bedrijven».[16] Ook wordt er door het CBS-onderzoek gedaan naar de stand van cybersecurity in Nederland via de Cybersecuritymonitor.[17]

3. Verhouding tot andere nationale wetgeving

Dit wetsvoorstel regelt de informatiedeling door de rijksoverheid met het Nederlandse bedrijfsleven dat niet valt onder de werking van de Wbni. Daarmee richt het zich op bedrijven die vallen in de categorie niet-vitaal en geen digitale dienstverleners zijn. Deze groep bedrijven strekt zich uit van éénmansbedrijven (zzp) tot het grootbedrijf. Het wetsvoorstel heeft een directe relatie met de Wbni. Deze relatie zit in het feit dat het enerzijds de Minister van EZK de taak geeft de digitale weerbaarheid van niet-vitale bedrijven te verhogen door het informeren en adviseren over digitale dreigingen en incidenten en ten behoeve daarvan informatie te verwerken én daarnaast informatie die relevant is voor aanbieders in de doelgroepen van twee overheidsorganisaties genoemd in de Wbni, namelijk de Minister van JenV (uitgevoerd door het NCSC) en de Minister van EZK (als CSIRT voor digitale diensten), met die organisaties te delen. Anderzijds zorgt dit wetsvoorstel ervoor dat voornoemde organisaties, het NCSC en het CSIRT voor digitale diensten, informatie over digitale dreigingen en incidenten, die relevant is voor aanbieders in de doelgroep van dit wetsvoorstel, met inbegrip van vertrouwelijke informatie (persoonsgegevens, etc.), mogen delen met de Minister van EZK. In dit wetsvoorstel is derhalve ook een wijziging van de Wbni opgenomen (artikel 5).

De benodigde maatregelen die bedrijven kunnen treffen ter bescherming van de gegevens, zoals geformuleerd in artikel 32 van de AVG, schrijven voor dat de verwerker en verwerkingsverantwoordelijke passende technische en organisatorische maatregelen dienen te treffen ter bescherming van persoonsgegevens. Als gevolg van dit wetsvoorstel zal de Minister van EZK het bedrijfsleven beter kunnen voorzien van praktische handvatten waarmee deels invulling kan worden gegeven door bedrijven aan de hiervoor genoemde technische en/of organisatorische maatregelen. Bedrijven zijn uiteraard zelf primair verantwoordelijk als het gaat om het treffen van maatregelen aangaande de beveiliging van hun systemen.

4. Gevolgen (m.u.v. financiële gevolgen)

Dit wetsvoorstel regelt de taak van de Minister van EZK om vertrouwelijke informatie, kwetsbaarheden en dreigingen (inclusief persoonsgegevens) te verwerken ten behoeve van het niet-vitale bedrijfsleven in Nederland. In dit hoofdstuk worden de verschillende gevolgen van het wetsvoorstel behandeld per onderwerp.

4.1 Regeldruk

Er is geen regeldruk voorzien voor het Nederlandse bedrijfsleven. Er ontstaat geen verplichting voor bedrijven in Nederland om gebruik te maken van de informatie van het Ministerie van EZK.

[16] https://www.cbs.nl/nl-nl/publicatie/2019/42/ict-kennis-en-economie-2019.
[17] https://www.cbs.nl/nl-nl/publicatie/2019/37/cybersecuritymonitor-2019.

In het voorstel heeft de Minister van EZK de mogelijkheid om bedrijven te vragen om informatie te delen. Het delen van informatie op basis van een dergelijk verzoek is volledig vrijwillig. Mocht een bedrijf hier toch aan mee willen werken dan wordt de regeldruk die hiermee in potentie ontstaat verwaarloosbaar geacht, aangezien er op een dergelijk verzoek geen vormvereiste geldt en omdat dit om een incidentele en vrijwillige activiteit gaat.

Het Adviescollege Toetsing Regeldruk (ATR) heeft geen aanleiding gezien om een formeel advies uit te brengen en heeft het voorstel ambtelijk afgedaan.

4.2 Markt en overheid

Met dit wetsvoorstel is er geen impact op de verhouding markt en overheid. In het kader van het met het oog op het bevorderen van de digitale weerbaarheid van bedrijven uitoefenen van de taken, opgenomen in dit wetsvoorstel, beperkt de Minister van EZK zich tot het informeren van bedrijven over digitale kwetsbaarheden en dreigingen voor zover zij beschikt over die informatie. Een belangrijke scheidslijn in deze wet is dat de taken en bevoegdheden niet verder gaan dan wat nodig is om deze publieke taak uit te voeren, namelijk het informeren van bedrijven. De Minister van EZK zal, zoals al eerder gememoreerd, niet optreden als een «digitale brandweer». Het oplossen van incidenten en het nemen van preventieve maatregelen is aan bedrijven zelf. Hierin is ook een belangrijke rol weggelegd voor marktpartijen die dit voor bedrijven kunnen faciliteren. Sterker nog, met het bewust worden van bedrijven over de kwetsbaarheden waarmee zij te maken hebben, is het de verwachting dat de markt voor ICT-dienstverlening ter bevordering van de digitale weerbaarheid zal groeien.

De Minister van EZK zal, op grond van artikel 2 van dit voorstel, gegevens over kwetsbaarheden, dreigingen en incidenten die betrekking hebben op netwerk- en informatiesystemen delen met bedrijven. Deze informatie, die bij de Minister van EZK bekend is, wordt omgezet in twee stromen. De Minister van EZK zal algemene dreigingsinformatie delen door middel van nieuwsberichten bij beveiligingslekken of kwetsbaarheden in netwerk- en informatiesystemen welke een grote bedreiging vormen voor ondernemend Nederland.

Vervolgens kan de Minister van EZK als zij informatie heeft dat een kwetsbaarheid, dreiging of incident te herleiden is op één of meerdere bedrijven, deze bedrijven hierover informeren. Het advies dat de Minister van EZK uitbrengt is in grote mate gebaseerd op de (publieke) informatie van cybersecurity onderzoekers, leveranciers van netwerk- en informatiesystemen en andere (publieke) informatie gerelateerd aan de kwetsbaarheid, dreiging of incident. Het advies is nadrukkelijk geen verplichting voor bedrijven. Ook zal het advies van de Minister van EZK in algemene bewoordingen worden opgesteld waarbij het aan bedrijven zelf is om te beoordelen (al dan niet met behulp van ICT-dienstverleners) welke concrete maatregelen noodzakelijk zijn en kunnen worden doorgevoerd. Daarbij verleent de Minister van EZK geen ondersteuning bij het doorvoeren van deze adviezen. De informatie over kwetsbaarheden, dreigingen en incidenten, waar de Minister van EZK over beschikt, zal vaak in de vorm van ruwe data zijn. Wanneer de Minister van EZK de ruwe data naar een bedrijf heeft kunnen herleiden, zal de Minister van EZK deze data verrijken met de contactgegevens van het getroffen bedrijf. Daarna zal notificatie plaatsvinden aan het individuele bedrijf. Er vindt geen verdere bewerking van de informatie plaats.

Het informeren van bedrijven (algemeen en individueel) over bij de Minister van EZK bekende kwetsbaarheden, dreigingen en incidenten in netwerk- en informatiesystemen vindt plaats in het algemeen belang. Het belang dat hier wordt gediend is enerzijds de digitale weerbaarheid van individuele ondernemingen in Nederland, anderzijds het voorkomen van nadelige maatschappelijke gevolgen voor burgers, klanten en bedrijven onderling. Een digitale verstoring bij een supermarkt heeft direct gevolgen voor het bedrijf, haar klanten, de omgeving en leveranciers en partners.

De Minister van EZK informeert en geeft algemeen handelingsperspectief en daarmee is er ook een grens aan wat de overheid doet. Bedrijven ontvangen informatie, het is aan hen om hierop te handelen. Het gegeven handelingsperspectief, bijvoorbeeld het updaten van een systeem, is niet op het individuele bedrijf afgestemd en wordt niet door de Minister van EZK uitgevoerd. Bedrijven zijn en blijven zelf verantwoordelijk voor het nemen van de nodige maatregelen. Bedrijven zullen juist dan, wanneer zij zelf onvoldoende mogelijkheid hebben om de juiste maatregelen te nemen, een beroep doen op marktpartijen om hen te ondersteunen. Bedrijven worden ongeacht hun branche of sector, regio of bedrijfsomvang op dezelfde wijze behandeld.

Vanwege het bovengenoemde, behoort het delen van, bij de Minister van EZK bekende algemene of specifieke informatie over kwetsbaarheden, dreigingen en incidenten aan de Nederlandse bedrijven tot de uitoefening van bevoegdheden van openbaar gezag. Het bevorderen van de digitale weerbaarheid van bedrijven en daarmee ook openbare (digitale) veiligheid behoort immers tot de taken van de overheid. Daar waar marktactiviteiten beginnen, houdt de advisering van de Minister van EZK op. De in dit wetsvoorstel voorgestelde taken van de Minister van EZK zijn derhalve geen economische activiteit en zijn de staatssteunregels daar niet op van toepassing. Uit het arrest van het Hof (Derde kamer) van 12 juli 2012, ECLI:EU:C:2012:449, volgt dat het publiek toegankelijk maken van informatie die verzameld is ten behoeve van een wettelijke taak geen economische activiteit vormt. Daar is bij de werkzaamheden van de Minister van EZK sprake van.

4.3 Privacy

De persoonlijke levenssfeer in algemene zin wordt beschermd door artikel 10, eerste lid, van de Grondwet, artikel 8 van de Europese verklaring voor de rechten van de mens (EVRM), artikel 17 van het Internationaal verdrag inzake burgerlijke en politieke rechten (IVBPR) en artikel 7 van het Handvest van de gronden van de EU (Handvest). Bescherming van persoonsgegevens wordt daarnaast in het bijzonder beschermd door artikel 16, eerste lid, van het Verdrag betreffende de werking van de Europese Unie (VWEU), artikel 8 van het Handvest en artikel 10, tweede en derde lid, van de Grondwet. Ook in de Algemene verordening gegevensbescherming (AVG) staat de bescherming van persoonsgegevens centraal. De AVG werkt als verordening rechtstreeks in de Nederlandse rechtsorde.

Voor een goede uitvoering van de taken en bevoegdheden van de Minister van EZK, die met dit wetsvoorstel worden vastgelegd ter bevordering van de digitale weerbaarheid van bedrijven, zal het in voorkomende gevallen noodzakelijk zijn om persoonsgegevens te verwerken. Daarvan kan sprake zijn bij het doen van analyses om met name specifieke dreigingen te kunnen achterhalen en bij het verstrekken van informatie daarover aan bedrijven. De bedrijfsgegevens die het hierbij betreft kunnen in sommige gevallen herleidbaar zijn tot een individu. Dat kan bijvoorbeeld het geval zijn bij een eenmansbedrijf of contactpersoon

van een bedrijf. Hierbij gaat het om «gewone» persoonsgegevens waarbij niet meer gegevens worden verwerkt dan strikt noodzakelijk, en deze niet voor andere doeleinden worden gebruikt dan waarvoor zij oorspronkelijk zijn verzameld.

De taken en bevoegdheden van de Minister van EZK uit dit wetsvoorstel gelden ook voor Caribisch Nederland. Caribisch Nederland, dat geen deel uitmaakt van de Europese Unie, is een zogeheten derde land in de zin van de AVG. Voor doorgifte geldt in aanvulling op de gebruikelijke eisen voor de verwerking van persoonsgegevens dat tevens aan de voorwaarden van Hoofdstuk V van de AVG dient te worden voldaan. Voor het voldoen aan een adequaat beschermingsniveau zijn verschillende mogelijkheden. Artikel 46 van de AVG staat doorgifte van persoonsgegevens naar een derde land toe wanneer er sprake is van passende waarborgen en betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken. In Caribisch Nederland geldt een wettelijke regeling inzake de bescherming van persoonsgegevens – de Wet bescherming persoonsgegevens BES (Wbp BES). Deze wet biedt waarborgen voor de bescherming van deze gegevens en de rechten van betrokkenen. In verhouding tot de AVG biedt de Wbp BES een vergelijkbaar beschermingsniveau van persoonsgegevens. Zo moet aan vergelijkbare vereisten van rechtmatigheid worden voldaan, en worden de rechten en rechtsbescherming van betrokkene gewaarborgd. Net als bij de AVG heeft de betrokkene o.m. het recht op inzage in zijn of haar persoonsgegevens. Voor zover het voor een goede uitvoering van de voorgestelde taken en bevoegdheden noodzakelijk zal zijn om persoonsgegevens in Caribisch Nederland te verwerken biedt de Wbp BES aldus een passend beschermingsniveau.

Op 25 oktober 2021 heeft de Autoriteit Persoonsgegevens (AP), per brief met kenmerk z2021-13945[18], aangegeven geen opmerkingen te hebben over dit wetsvoorstel.

5. Uitvoering

Ter uitvoering van de in dit wetsvoorstel genoemde algemene taken van informatiedeling en stimulering van samenwerking, zijn andere middelen en processen nodig dan voor de specifieke taak van het individueel notificeren van bedrijven. Voor deze laatste taak is een zogenaamde informatiedienst ingericht. Deze informatiedienst zal ingericht worden om informatie van binnen en buiten de overheid te ontvangen, beoordelen, verwerken en verspreiden voor zover relevant voor de doelgroep van dit wetsvoorstel. De informatiedienst zal hierbij zoveel mogelijk gebruik gaan maken van digitale systemen en processen. Voor de uitvoering van alle taken zullen de binnen de rijksoverheid geldende richtlijnen en kaders zoals de Baseline Informatiebeveiliging Overheid (BIO) worden gehanteerd.

6. Toezicht en handhaving

Er is geen direct toezicht en handhaving op basis van dit wetsvoorstel voorzien. Ondernemen is risico's afwegen en risico's nemen, bedrijven zijn dan ook, behoudens wettelijke kaders, autonoom om beslissingen te nemen over hun bedrijfsvoering.

[18] https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_wet_bevordering_digitale_weerbaarheid_bedrijven.pdf.

7. Financiële gevolgen

Voor de in dit wetsvoorstel beschreven taken en bevoegdheden van de Minister van EZK is structureel € 1 mln aanvullende financiering nodig voor het DTC. Kosten uiten zich voornamelijk in het werven van nieuw personeel. Bij het Regeerakkoord is er aanvullende financiering geleverd vanuit de EZK-begroting. In 2023 is er een extra bedrag van € 2,1 mln en in de jaren 2024–2026 is er een extra bedrag van € 4,6 mln beschikbaar gesteld. Op de EZK-begroting is reeds € 2,5 mln structureel beschikbaar voor het DTC. Met de extra middelen van het Regeerakkoord is het totaal structureel beschikbare bedrag voor het DTC 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 de samenwerking en samenwerkingsverbanden.

8. (Internet) consultatie

Het wetsvoorstel is van 28 juni tot en met 23 augustus 2021 geconsulteerd.[19] Gedurende de periode van acht weken hebben een negental organisaties gereageerd en deze zijn publiekelijk beschikbaar via de website: www.internetconsultatie.nl/wbdwb[20].

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

8.1 Algemeen beeld

Veel organisaties onderschrijven het belang van digitale weerbaarheid van ondernemend Nederland ten behoeve van het verdienvermogen van het Nederlandse bedrijfsleven. Tevens wordt door enkele organisaties het belang benadrukt van de rol die de overheid heeft op het domein van veiligheid. De reacties van respondenten zijn ingedeeld naar de volgende thema's: afbakening doelgroep, relatie met het voorstel van de Europese Commissie voor de herziening van de Richtlijn inzake de beveiliging van netwerk- en informatiesystemen[21] (hierna: NIB 2-richtlijn), samenhang van overheidsinitiatieven en reacties over de AVG en vertrouwelijkheid. Naast deze thema's zijn er ook specifieke punten die door slechts één organisatie zijn genoemd. Dit zijn: de relatie van het wetsvoorstel met de Wet markt en overheid, het delen van Indicators of Compromise (IOC's) en mogelijke gevolgen voor digitale zorgplicht. Deze punten komen aan de orde in de laatste paragraaf.

8.2 Afbakening doelgroep van het wetsvoorstel

Een aantal respondenten vraagt in hoeverre de taken van de Minister van EZK samenhangen met de vorming van het landelijk dekkend stelsel (LDS) en hoe die zich verhouden tot de taken van het NCSC.

Het Ministerie van EZK maakt met het DTC onderdeel uit van het LDS en draagt actief bij aan de vorming van het LDS, ten aanzien waarvan de coördinerende verantwoordelijkheid bij de Minister van JenV ligt. De Minister van EZK draagt bij door de stimulering van samenwerkingsverbanden en door het verstrekken van subsidie aan initiatieven ten behoeve

[19] https://www.internetconsultatie.nl/wbdwb.
[20] Tevens ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.
[21] COM(2020) 823 final.

van de digitale weerbaarheid van bedrijven. Het actuele overzicht van samenwerkingsverbanden is terug te vinden op de samenwerkingspagina van het DTC.[22]

Enkele respondenten vragen aandacht voor de onwenselijkheid van het dubbel verstrekken van dezelfde informatie door de overheid waarbij expliciet is gerefereerd aan de rolverdeling tussen het NCSC en de Minister van EZK. De verdeling van de taken is wat betreft het Ministerie van EZK helder: het NCSC heeft het primair als taak om vitale aanbieders en (andere) aanbieders die deel uitmaken van de rijksoverheid te informeren en adviseren over hen aangaande digitale dreigingen en incidenten. De Minister van EZK bedient het niet-vitale bedrijfsleven, voor zover zij ook niet onder de verantwoordelijkheid van het CSIRT voor digitale diensten vallen. Het NCSC en DTC hebben dus duidelijk onderscheidenlijke doelgroepen, maar werken daarnaast desalniettemin samen om het risico van onder meer dubbele informatieverstrekking te vermijden. De Memorie van Toelichting is hier in paragraaf 2.2 op aangescherpt.

Sommige respondenten stellen vragen over de omvang van de doelgroep ten opzichte van de beschikbare capaciteit op het Ministerie van EZK om deze taken en bevoegdheden uit te voeren. In de financiële paragraaf van deze memorie worden de minimale eisen voor wat betreft de financiering en bezetting benoemd. Het DTC zal in de uitvoering van de taken en bevoegdheden zoveel als mogelijk efficiëntie en effectiviteit nastreven en gebruik maken van digitale processen. Er wordt ingezet op een geleidelijk groeimodel waarin periodiek zal worden geëvalueerd of de inzet van mensen en budgetten gelijklopen met de vraag en de taken van de Minister van EZK.

8.3 Verhouding met NIB 2-richtlijn

Respondenten vragen aandacht voor het verband tussen de toekomstige Europese regelgeving (NIB-2-richtlijn) en eventuele consequenties voor het onderhavige wetsvoorstel. Het Europese voorstel staat een verdere behandeling van dit wetsvoorstel en de eerstgenoemde taak, om het niet-vitale bedrijven vanuit de overheid te voorzien van informatie en advies over relevante digitale dreigingen en incidenten, niet in de weg. Zonder vooruit te lopen op de inhoud of de implementatie van de NIB 2-richtlijn, is het de verwachting dat de inhoud van de richtlijn aanleiding kan geven tot aanpassingen van de nationale wetgeving in het kader van het implementatietraject. Voor nu geldt dat op basis van de uitkomsten van de onderhandelingen op dit moment wordt bezien wat en hoe aangepast moet worden aan de nationale wetgeving.

8.4 Samenhang van overheidsinitiatieven

Op meerdere plekken wordt er binnen de overheid gewerkt aan digitale weerbaarheid. Enkele respondenten vragen ook om een één-loket benadering door de overheid. Dit wetsvoorstel is een logische aanvulling op het huidige stelsel, waarin het NCSC primair verantwoordelijk is voor het informeren en adviseren van organisaties die deel uitmaken van de rijksoverheid en vitale aanbieders en het CSIRT voor digitale diensten bijstand verleend aan digitale dienstverleners. Binnen dit stelsel werken het NCSC en DTC nauw samen om ervoor te zorgen dat zij in het kader van hun onderscheidenlijke taken hun doelgroepen zo goed mogelijk van informatie en advies voorzien. Zoals al eerder aan gerefereerd, is ook in het coalitieakkoord hier aandacht voor gevraagd en wordt de samen-

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

werking, zoals gemeld in paragraaf 2.4, in de komende tijd verder vormgegeven.

Daarnaast zal actief de samenwerking worden gezocht met andere organisaties binnen en buiten de overheid zoeken ter bevordering van de digitale weerbaarheid van bedrijven. Voor wat betreft de systeemverantwoordelijkheid van andere (vak)ministers is er geen twijfel over bevoegdheid. Vakministers zijn volgens eigen beleid en wetgeving verantwoordelijk voor bijvoorbeeld het stellen van veiligheidseisen aan bedrijven binnen onder hen vallende sectoren. Als de Minister van EZK relevante informatie heeft voor of over de niet-vitale sectoren van andere vakdepartementen, zal dit actief worden gedeeld. Op deze en andere manieren wordt binnen de overheid samengewerkt om het Nederlandse niet-vitale bedrijfsleven digitaal weerbaarder te maken. Op dit moment werkt het DTC daartoe al samen met onder andere het NCSC en het CSIRT voor digitale diensten.

8.5 AVG en vertrouwelijkheid van informatie

Binnen dit thema vallen diverse onderwerpen die nader worden toegelicht. Het gaat hier om reacties over de AVG, over de informatiebeveiliging van informatie(deling) bij en door de Minister van EZK en reacties die gaan over de Wet openbaarheid van bestuur (Wob) / Wet open overheid (Woo).

Respondenten hebben zorgen over de mogelijke invloed van de AVG op de informatiedeling via de Minister van EZK. De zorg is dat voorafgaand aan de deling van informatie het noodzakelijk is om een verwerkersovereenkomst te sluiten. Deze zorg is ongegrond. Met dit wetsvoorstel ontstaat voor de Minister van EZK een wettelijke grondslag voor de verwerking en meer in het bijzonder ook verstrekking van informatie, waaronder persoonsgegevens. Daarom is het niet noodzakelijk om met de ontvanger van de informatie een verwerkersovereenkomst te sluiten. Daarnaast worden er waarborgen getroffen over de zekerheid en zorgvuldigheid waarmee persoonsgegevens door de Minister van EZK worden verwerkt. Het wetsvoorstel is voorgelegd aan de AP. Het advies van de AP is terug te vinden in paragraaf 4.3.

Ook zijn er reacties over het risico van informatiedeling door de Minister van EZK. De zorgen zien op enerzijds de feitelijke verwerking van informatie door de Minister van EZK en anderzijds het ontvangen daarvan door individuele bedrijven. Bij de uitvoering van de taken uit dit wetsvoorstel volgt de Minister van EZK de in het algemeen voor de overheid geldende voorschriften voor informatiebeveiliging. Daarnaast zal de Minister van EZK waar nodig aanvullende maatregelen nemen ter bescherming van informatie en gegevens en processen inrichten 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.

Tevens vragen enkele respondenten naar de definitie van vertrouwelijke gegevens. Voor het geval hier onduidelijkheid over bestaat gaat het dan om gegevens die of naar hun aard of inhoud vertrouwelijk zijn. Dit wetsvoorstel sluit in dit verband aan bij de terminologie zoals gebruikt in de Wbni.[23]

[23] Zie memorie van toelichting bij de Wbni (Kamerstukken II 2017/18, 34 883, nr. 3).

Respondenten hebben zorgen geuit over de openbaarmaking van informatie door de overheid op basis van de Wob en haar opvolger, de Woo, die op 1 mei 2022 in werking is getreden. 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, om te waarborgen dat dezelfde gegevens, ongeacht of deze door het NCSC, het CSIRT voor digitale diensten of de Minister van EZK worden verwerkt, op dezelfde wijze worden behandeld, wordt in dit wetsvoorstel aansluiting gezocht op het reeds bestaande stelsel van de Wbni. In de Wbni worden vertrouwelijke tot een aanbieder herleidbare gegevens, vanwege een bijzondere openbaarmakingsregeling, uitgezonderd van de toepasselijkheid van de Woo. Op grond van de in dit wetsvoorstel voorgestelde uitzondering worden dezelfde gegevens ook uitgezonderd van de werking van de Woo, indien deze aanwezig zijn bij de Minister van EZK. Door de toevoeging in dit wetsvoorstel van de bepaling in artikel 4, vierde lid, inhoudende dat vertrouwelijke tot bedrijven of andere aanbieders herleidbare informatie buiten de toepasselijkheid van de Woo vallen, is er sprake van een uitzondering op de Woo voor soorten gegevens die vergelijkbaar zijn met die waarvoor in de Wbni een dergelijke uitzondering reeds geldt. Doordat in die zin is aangesloten op bovenbedoelde regeling in de Wbni blijft het doel en de werking van de Woo onverminderd in stand. Door de toevoeging van de uitzonderingsgrond voor dit wetsvoorstel aan de Woo vindt er 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.

8.6 Diverse punten

Een van de respondenten vraagt naar de relatie tussen de regelgeving inzake markt en overheid en dit wetsvoorstel. Zoals eerder in paragraaf 4.2 is toegelicht, heeft 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.

Sommige respondenten hebben gevraagd om IOC's[24] te delen omdat deze mede de digitale weerbaarheid van bedrijven vergroot. In voorkomende gevallen zullen, als IOC's bekend zijn en met inachtneming van de wettelijke kaders deelbaar zijn door de Minister van EZK, deze ook worden gedeeld bij het informeren van bedrijven over specifieke dreigingen. Daarnaast kan de Minister van EZK dergelijke informatie ook in generieke

[24] Bron: Cybersecurity Woordenboek: «Informatie die je kunt gebruiken om te kijken of iemand een aanval heeft uitgevoerd op één van je assets. De informatie bevat vaak kenmerken van een aanvaller, van een aanvalsmethode of van malware. Bijvoorbeeld, als men weet dat een bepaalde aanvaller zijn aanvallen vanuit een specifiek IP-adres uitvoert, dan kan je dat IP-adres gebruiken als indicator of compromise. Als je op je eigen digitale systemen sporen ziet van verbindingen met dat IP-adres, dan weet je dat die aanvaller misschien bij jou een aanval heeft geprobeerd uit te voeren.» https://www.cyberveilignederland.nl/woordenboek.

zin delen als deze informatie dit toelaat en bijdraagt aan de digitale weerbaarheid van bedrijven.

Eén respondent meent dat het wetsvoorstel gevolgen zou kunnen hebben met betrekking tot de digitale zorgplicht van bedrijven en eventuele strafrechtelijke consequenties. De vraag is of het delen van informatie door de Minister van EZK en het niet opvolgen door een individueel bedrijf kan leiden tot een strafbaar feit. De respondent zoekt hierin steun bij het concept van digitale zorgplicht. Dit wetsvoorstel legt geen directe of indirecte normen aan het Nederlandse bedrijfsleven op. Door het informeren van individuele bedrijven ontstaat er geen plicht tot het opvolgen van deze informatie. Zoals eerder aangegeven is het aan bedrijven zelf om te beoordelen of en op welke wijze zij opvolging geven aan deze informatie. In dit wetsvoorstel is daarnaast geen toezicht of sanctionering voorzien. Het is nadrukkelijk niet de bedoeling van dit wetsvoorstel om invulling te geven aan de strafrechtelijke bepalingen uit artikel 350b Sr.

B. Artikelen

Artikel 1 (Begripsbepalingen)

Het begrip «bedrijf» slaat zowel op natuurlijke personen als op privaatrechtelijke rechtspersonen die in Nederland gevestigd zijn, bedrijfsmatige activiteiten uitvoeren en die niet onder de werkingssfeer van de Wet beveiliging netwerk- en informatiesystemen (Wbni) vallen. Vitale aanbieders en digitale dienstverleners behoren derhalve niet tot de doelgroep van dit wetsvoorstel.

De begrippen aanbieder, incident en netwerk- en informatiesysteem hebben dezelfde betekenis als in de NIB-richtlijn en in de Wbni. Dit om eenheid in terminologie te waarborgen.

Incident: elke gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen.

Netwerk- en informatiesysteem:
a) een elektronisch communicatienetwerk in de zin van artikel 2, onder a), van Richtlijn 2002/21/EG;
b) een apparaat of groep van geïnterconnecteerde of bij elkaar behorende apparaten, waarvan een of meer, overeenkomstig een programma, digitale gegevens automatisch verwerkt of verwerken, of
c) digitale gegevens die via in de punten a) en b) bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan.

Het begrip CSIRT voor digitale diensten heeft dezelfde betekenis als in de Wbni. Dit om eenheid in terminologie te waarborgen.

Artikel 2 (Taken van de Minister van EZK)

Het artikel bevat een opsomming van de taken van de Minister van EZK op het terrein van digitale weerbaarheid van bedrijven, ten behoeve waarvan verwerking van gegevens, waaronder persoonsgegevens, aangewezen is, en omschrijft de doeleinden van die taken. Zie voor een nadere toelichting hierop paragraaf 2.2 van het algemeen deel van deze memorie.

Artikel 3 (Verstrekking gegevens aan de Minister van EZK)

Het eerste lid voorziet in een wettelijke bevoegdheid voor de Minister van EZK om rechtspersonen (overheden of private partijen) of organen daarvan om gegevens te vragen die noodzakelijk zijn voor de uitoefening van de in artikel 2, eerste lid, genoemde taken. Het gaat hierbij niet om een bevoegdheid tot het vorderen van gegevens; de rechtspersoon of het orgaan daarvan waaraan het verzoek is gericht is niet verplicht tot medewerking.

Ingevolge het doelbindingsbeginsel van artikel 5, eerste lid, onder b, AVG moeten persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen zij vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt. De AVG biedt echter de mogelijkheid om onder voorwaarden door middel van nationale bepalingen de verdere verwerking van persoonsgegevens mogelijk te maken, ook als dat geschiedt voor een doel dat niet verenigbaar is met het doel waarvoor de persoonsgegevens zijn verkregen. Het tweede lid van artikel 3 geeft toepassing aan die bevoegdheid. Dat is een noodzakelijke en evenredige maatregel ter waarborging van meerdere in artikel 23, eerste lid, AVG, genoemde belangen, waaronder onder meer de openbare veiligheid.

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

Artikel 4, eerste lid, regelt de verstrekking door de Minister van EZK, ter uitvoering van de in artikel 2, eerste en tweede lid, onder c en d, bedoelde taken, aan derden, waaronder de Minister van JenV en het CSIRT voor digitale diensten, van vertrouwelijke gegevens met betrekking tot digitale dienstverlenersbedrijven, zoals gegevens over de identiteit van een bij een incident betrokken bedrijf of specifieke gegevens over de beveiliging van een elektronisch informatiesysteem van een bedrijf. Artikel 4, eerste lid, staat uiteraard niet in de weg aan verstrekking door de Minister van EZK aan derden van gegevens die niet vertrouwelijk zijn.

Het eerste lid bepaalt dat bij de Minister van EZK berustende vertrouwelijke gegevens met betrekking tot bedrijven slechts ter uitvoering van de in artikel 2, eerste lid en tweede lid, onder c en d, genoemde taken aan derden worden verstrekt, indien aldaar de geheimhouding van de gegevens voldoende is gewaarborgd en voldoende is gewaarborgd dat de gegevens uitsluitend worden gebruikt voor het doel waarvoor zij worden verstrekt. Het eerste lid ziet op vertrouwelijke gegevens met betrekking tot bedrijven, dus niet op andere vertrouwelijke gegevens, zoals persoonsgegevens die niet tevens vertrouwelijke informatie betreffende een bedrijf betreffen. Voor de verwerking van persoonsgegevens door de Minister van EZK geldt de AVG.

Ter uitvoering van de in artikel 2, tweede lid, onder c, bedoelde taak regelt artikel 4, tweede lid, de mogelijkheid van verstrekking door de Minister van EZK aan de Minister van JenV, ten behoeve van de uitoefening van de taken als bedoeld in artikel 3, eerste lid, van de Wbni, van vertrouwelijke gegevens met betrekking tot vitale aanbieders en andere aanbieders die onderdeel zijn van de rijksoverheid.

Ter uitvoering van de in artikel 2, tweede lid, onder d, bedoelde taak regelt artikel 4, derde lid, de mogelijkheid van verstrekking door de Minister van EZK aan het CSIRT voor digitale diensten, ten behoeve van de uitoefening van de taken als bedoeld in artikel 4, vierde lid, Wbni, van vertrouwelijke gegevens met betrekking tot digitale dienstverleners.

Deze laatste twee bevoegdheden maken het voor de Minister van EZK mogelijk om vertrouwelijke gegevens over andere partijen dan die in de eigen doelgroep (bedrijven) met de relevante overheidsorganisaties te delen.

Bij het begrip vertrouwelijke gegevens kan worden gedacht aan informatie over netwerk- en informatiesystemen die een bedrijf of een andere aanbieder gebruikt bij zijn dienstverlening. Ook vertrouwelijke gegevens die herleid kunnen worden tot een bedrijf of een andere aanbieder of digitale dienstverlener vallen hieronder.

Het is voor de toepassing van artikel 4 niet relevant of de Minister van EZK de gegevens heeft verkregen van de partij zelf of anderszins, zoals door analyse van de Minister van EZK of ontvangst van een andere organisatie.

Zoals uiteengezet in het algemeen deel van deze memorie bevat artikel 4 in het vierde lid, in samenhang met de drie voorafgaande leden, een bijzondere openbaarheidsregeling voor vertrouwelijke tot bedrijven of de in het tweede en derde lid bedoelde aanbieders herleidbare gegevens die afwijkt van de Woo. Deze afwijking geldt niet alleen zolang die gegevens bij de Minister van EZK berusten, maar ook nadat zij, na verstrekking door de Minister van EZK op grond van artikel 4, bij een ander overheidsorgaan berusten. Een en ander geldt echter niet voor milieu-informatie. Ter uitvoering van het Verdrag van Aarhus[25] en EU-richtlijn 2003/4/EG[26] bevat de Woo voor het verstrekken van milieu-informatie diverse afwijkende bepalingen.

Artikel 5 (wijziging Wet beveiliging netwerk- en informatiesystemen)

In de artikelen 3, tweede lid, en 20, tweede lid, van de Wbni worden partijen genoemd waarmee het NCSC in voorkomende gevallen gegevens in een beperkte kring van derden mag delen. Hierbij kan het ook gaan om persoonsgegevens en (andere) vertrouwelijke gegevens die herleid kunnen worden tot een aanbieder.

In artikel 21, tweede lid, van de Wbni worden partijen genoemd waarmee het CSIRT voor digitale diensten in voorkomende gevallen vertrouwelijke gegevens die herleid kunnen worden tot een digitale dienstverlener, zonder diens instemming, in een beperkte kring van derden mag delen.

Ten behoeve van de taakuitoefening door de Minister van EZK op grond van dit wetsvoorstel wordt met de voorgestelde wijziging van de Wbni de Minister van EZK toegevoegd aan de kring van derden waarmee het NCSC en het CSIRT voor digitale diensten in voorkomende gevallen persoonsgegevens en vertrouwelijke herleidbare gegevens mogen delen.

In dit voorstel wordt, net als in het voorstel tot wijziging van de Wet beveiliging netwerk- en informatiesystemen in verband met de uitbreiding van de bevoegdheid van de Minister van Justitie en Veiligheid om dreigings- en incidentinformatie over de netwerk- en informatiesystemen van niet-vitale aanbieders te verstrekken aan deze aanbieders en aan organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten ten behoeve

[25] Verdrag betreffende toegang tot informatie, inspraak bij besluitvorming en toegang tot de rechter inzake milieuaangelegenheden, Trb. 2001, 73.

[26] Richtlijn 2003/4/EG van het Europees Parlement en de Raad van 28 januari 2003 inzake de toegang van het publiek tot milieu-informatie en tot intrekking van Richtlijn 90/313/EEG van de Raad, PbEU 2003, L 41).

van deze aanbieders, voorzien in wijzigingen van artikel 3, tweede lid, en artikel 20, tweede lid, van de Wbni. De samenloopbepaling waarmee geregeld wordt dat beide wetten op elkaar zijn afgestemd, is in het laatstgenoemde wetsvoorstel opgenomen.

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