Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

35 257 Voorstel van wet van het lid Verhoeven houdende een regeling voor een afwegingsproces voor het gebruik van kwetsbaarheden in geautomatiseerde werken door de overheid (Wet Zerodays Afwegingsproces)

Nr. 14

BRIEF VAN DE MINISTERS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES EN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 3 februari 2021

Inleiding

Hierbij bieden wij u, mede namens de Minister van Defensie, het kabinetsstandpunt inzake het initiatiefwetsvoorstel «zerodays afwegingsproces» (Kamerstuk 35 257)aan. Het kabinet reageert met dit standpunt op het verzoek van de vaste commissie voor Binnenlandse Zaken in te gaan op het gewijzigde initiatiefwetsvoorstel van het Kamerlid Verhoeven (D66) (Kamerstuk 35 257, nr. 5).

Om te beginnen hecht het kabinet eraan nogmaals te benadrukken dat de aandacht die de Kamer, en in het bijzonder de initiatiefnemer, voor dit onderwerp heeft wordt gewaardeerd. Het kabinet onderschrijft de ernst van de betrokken belangen. Net als de initiatiefnemer beoogt het kabinet een zorgvuldige afweging, waarin het belang van cybersecurity vanzelfsprekend een prominente plaats heeft.

Het debat over dit onderwerp kent een voorgeschiedenis. Op 8 november 2016 stuurde de toenmalige Staatssecretaris van Veiligheid en Justitie – op verzoek van de initiatiefnemer – een brief over het gebruik van onbekende kwetsbaarheden door de overheid[1]. Daarna is dit onderwerp bij de behandeling van het wetsvoorstel dat tot de Wet op de Inlichtingen- en Veiligheidsdiensten 2017 (Wiv 2017) heeft geleid en het voorstel van wet Computercriminaliteit III in het parlement uitvoerig aan de orde geweest, hetgeen tot passende waarborgen heeft geleid. Van de wet Computercriminaliteit III worden de bevoegdheid tot binnendringen in geautomatiseerd werk en de omgang met onbekende wetsbaarheden momenteel geëvalueerd. Het rapport wordt in het najaar van 2021 verwacht.

[1] Kamerstuk 26 643, nr. 428

kst-35257-14
ISSN 0921 - 7371
's-Gravenhage 2021

Op 23 september 2020 (Handelingen II 2020/21, nr. 5, item 14) is het initiatiefwetsvoorstel in uw Kamer plenair behandeld.
Bij die gelegenheid hebben de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Justitie en Veiligheid namens het kabinet aangegeven dat het wetsvoorstel op een aantal punten op fundamentele bezwaren stuitte. Na de plenaire behandeling op 23 september is het wetsvoorstel aanzienlijk gewijzigd bij tweede nota van wijziging (Kamerstuk 35 257, nr. 13). Het kabinet verwelkomt de beslissing van de initiatiefnemer om het oprichten van een beoordelingsorgaan en het toezicht door de CTIVD uit het initiatiefwetsvoorstel te halen. Daarmee zijn belangrijke bezwaren van het kabinet weggenomen.
Hierna zal worden ingegaan op de bezwaren die het kabinet nog heeft over de operationele risico's, de relatie met de bestaande regelgeving en de uitvoerbaarheid van het initiatiefwetsvoorstel.

Kern van het wetsvoorstel

Het wetsvoorstel draagt bestuursorganen die gebruik maken van onbekende kwetsbaarheden op tot het inrichten van een aanvullend afwegingskader voor de bekendmaking van onbekende wetsbaarheden. Het uitgangspunt voor het beoogde afwegingskader is dat, indien een bestuursorgaan voor het binnendringen van een geautomatiseerd werk gebruik zal maken van een onbekende kwetsbaarheid, deze kwetsbaarheid bekend wordt gemaakt aan de desbetreffende producent of leverancier. Het initiatiefwetsvoorstel draagt daarnaast de regering op het aankopen van binnendringsoftware bij algemene maatregel van bestuur te regelen.

Het bestuursorgaan kan besluiten dat de kwetsbaarheid niet bekend wordt gemaakt met het oog op onder meer de veiligheid van de Staat, de economische en financiële belangen van de Staat, de opsporing en vervolging van strafbare feiten, de betrekkingen van Nederland met andere staten en met internationale organisaties, of een ernstige inbreuk van de persoonlijke levenssfeer. Bij de afweging wordt het bestuursorgaan geadviseerd door vertegenwoordigers van betrokkenen die vitale infrastructuur beheren.

Kern van het standpunt van het kabinet

Het kabinet stelt vast dat de bestuursorganen die thans gebruik (mogen) maken van onbekende kwetsbaarheden om zo op afstand geautomatiseerde werken binnen te dringen, reeds een afwegingskader hebben. Hiermee komt de vraag in beeld wat het initiatiefwetsvoorstel hier nog aan kan toevoegen.
Tevens is als gevolg van de tweede nota van wijziging onduidelijkheid ontstaan over de betekenis van delen van de onderbouwing van het wetsvoorstel in de memorie van toelichting. Dat maakt de wet lastig uitvoerbaar.
Voorts heeft het kabinet tijdens de plenaire behandeling bezwaren geuit ten aanzien van deze wet die onverkort blijven staan. Het delen van zeer gevoelige informatie over onbekende kwetsbaarheden met vertegenwoordigers uit de vitale sectoren leidt tot een zeer onwenselijke (en in voorkomend geval onaanvaardbare) toename van operationele risico's en inzicht in de werkwijzen. Bovendien kan hierdoor de internationale samenwerking van de inlichtingen- en veiligheidsdiensten negatief worden beïnvloed, hetgeen extra risico's met zich meebrengt. Voor de opsporing geldt dat de invoering van de wet zal leiden tot een stapeling van goedkeurings- en toezichtsprocessen die de taakuitvoering minder efficiënt maakt en onduidelijkheid met zich mee brengt, terwijl de zorgvuldigheid niet toeneemt. Deze elementen hebben naar verwachting

een negatief effect op de nationale veiligheid en op de opsporing van strafbare feiten.

Nadere toelichting

In de volgende paragrafen worden de belangrijkste bevindingen van het kabinet nader toegelicht. Daarbij wordt tevens ingegaan op enkele punten uit de Nota naar aanleiding van het Verslag[2].

1. Besluitvormingsproces: adviserende rol vitale infrastructuur Het wetsvoorstel introduceert een termijn van vier weken met een verlenging tot twaalf weken voor de besluitvorming over onbekende kwetsbaarheden. Om een zorgvuldige afweging te maken zijn vier weken voor de inlichtingen- en veiligheidsdiensten echter onrealistisch en in voorkomende gevallen geldt dat ook voor twaalf weken.
   Voorts wordt voorzien in een adviserende rol voor vertegenwoordigers van de vitale infrastructuur. De rol van de vitale infrastructuur is volgens de memorie van toelichting informatie aan te leveren over het gebruik van bepaalde software of apparaten. Dit betreft vaak bedrijfsgevoelige informatie van en tussen private ondernemingen. Bedrijven zullen naar verwachting zeer terughoudend zijn met het delen van technische details in breder verband. Het kabinet merkt op dat zodra vanuit het bestuursorgaan een vraag over een specifiek product of software zal worden gesteld, het stellen van de vraag al informatie prijsgeeft over het bestaan van eventuele onbekende kwetsbaarheden en het nut daarvan voor de inlichtingen- en veiligheidsdiensten of de politie, en over de werkwijze van de diensten of de politie. Voor de inlichtingen- en veiligheidsdiensten geldt bovendien dat de samenwerking met buitenlandse partnerdiensten negatief kan worden beïnvloed, omdat bij het ontvangen van dergelijke informatie van partnerdiensten de geheimhouding ervan niet meer kan worden gegarandeerd. Dit is vanuit operationeel oogpunt zeer onwenselijk.
   Bovendien verschillen de digitale omgevingen van bedrijven in de vitale infrastructuur onderling sterk. Dit geldt zowel binnen een vitale sector als tussen verschillende vitale sectoren. Hoewel de overheid een beeld heeft van de netwerken informatiesystemen van de partijen in de vitale sectoren ten behoeve van de weerbaarheid en de nationale veiligheid, is de overheid niet tot in detail op de hoogte van alle in gebruik zijnde hard- en software van deze private partijen. Dit maakt dat mogelijk een relatief grote groep private partijen bevraagd moet worden, hetgeen de noodzakelijke vertrouwelijkheid kan schaden. Indien informatie alleen op een hoger abstractieniveau wordt gedeeld, dan heeft het advies van deze private partijen navenant minder toegevoegde waarde. Overigens is het nu al mogelijk gericht informatie te delen over de veiligheid van systemen met partijen in de vitale sectoren indien dat nodig is.
2. Dubbel kader en proces voor de opsporing, met mogelijk divergerende besluiten In het kader van de wet Computercriminaliteit III heeft het proces voor het melden van onbekende kwetsbaarheden bij de inzet van de bevoegdheid van art. 126nba Sv een stevige wettelijke verankering gekregen in art. 126ffa Sv. Er wordt in beginsel gemeld. Voor het tijdelijk uitstellen van een melding is een beslissing van de officier van justitie vereist nadat hij daartoe is gemachtigd door de rechtercommissaris. Dit artikel 126ffa Sv is op basis van een amendement van de Tweede Kamer in het wetboek opgenomen en het afwegingskader is nader toegelicht in de Nadere Memorie van Antwoord aan de Eerste Kamer[3]. De initiatiefnemer heeft in de Nota naar aanleiding van het Verslag gemeld dat hij van mening is dat de

[2] Kamerstuk 35 257, nr. 8
[3] Kamerstuk 34 372, G.

rechter-commissaris niet de juiste persoon is voor een dergelijke afweging vanwege het gebrek aan zeer technische en specialistische kennis. De huidige wettelijke regeling voorziet echter in mogelijkheden de benodigde expertise ter beschikking te stellen om de rechter-commissaris te ondersteunen in zijn besluit. De rechtercommissaris kan zich daarbij laten adviseren door ieder wie hij wenselijk acht. Het inroepen van technische expertise is daarbij een bestaande mogelijkheid, zodat de rechter-commissaris zich geïnformeerd een oordeel kan vormen over de gevolgen van het melden dan wel het uitstellen van de melding. De beoordeling van de rechter-commissaris wordt bovendien voorafgegaan door een beoordeling binnen het Openbaar Ministerie. Tot slot weegt de rechter-commissaris ook het bredere onderzoeksbelang in een strafrechtelijk onderzoek. Gelet op de wettelijke regeling van artikel 126nba zal dit onderzoeken betreffen naar zware vormen van criminaliteit of specifieke vormen van computercriminaliteit. Overigens is tot nu toe geen gebruik gemaakt van de mogelijkheid met machtiging van de rechter-commissaris een melding van een onbekende kwetsbaarheid uit te stellen.
Volgens het gewijzigde initiatiefwetsvoorstel besluit de politie (het bestuursorgaan dat de zero day mogelijk gebruikt) straks over het uitstel van de melding. De toelichting van de nota van wijziging vermeldt dat de huidige regelingen, waaronder art. 126ffa Sv dat dit voor de opsporing regelt, ongewijzigd blijven. Dat levert twee verschillende kaders en twee verschillende besluitvormingsprocessen op. Volgens het kader van 126ffa Sv besluit het OM hierover, na machtiging van de rechter-commissaris, op basis van de criteria genoemd in de wet en de Nadere Memorie van Antwoord aan de Eerste Kamer bij de behandeling van de wet Computercriminaliteit III (Kamerstuk 35 732). Volgens het gewijzigde initiatiefwetsvoorstel besluit de politie erover op basis van de elementen zoals genoemd in het initiatiefwetsvoorstel.
Het kabinet constateert dat het wetsvoorstel geen aanpassing van de bestaande wettelijke regelingen bevat. Daarmee introduceert het wetsvoorstel een stapeling van besluitvormingsprocessen met mogelijk divergerende uitkomsten. Dat heeft een negatief effect op de operationele processen en vergroot daarnaast de administratieve lasten.

3. Het is onduidelijk wat de algemene maatregel van bestuur voor binnendringsoftware zou moeten bevatten.
Het initiatiefwetsvoorstel bevat de verplichting een AMvB op te stellen over het aankopen van technische hulpmiddelen, waarvan aannemelijk is dat deze zijn gebaseerd op onbekende kwetsbaarheden. Het concept van de AMvB dient vier weken voorafgaand aan de vaststelling aan het parlement te worden overlegd. Ten eerste kan deze term verwarrend zijn. In de Wet Computercriminaliteit III is onderscheid gemaakt tussen software voor het uitvoeren van onderzoekshandelingen (de technische hulpmiddelen) en software voor het binnendringen. Deze laatste worden in de Wet Computercriminaliteit III niet aangeduid met de term technische hulpmiddelen. De twee soorten software kunnenwel in een enkel softwarepakket worden gecombineerd. Het in het initiatiefwetsvoorstel genoemde technisch hulpmiddel betreft software voor het binnendringen, en niet het technisch hulpmiddel in de zin van de Wet Computercriminaliteit III. Ten tweede bevat de memorie van toelichting veel aanwijzingen wat in deze AMvB opgenomen zou moeten worden. Echter, door de nota van wijziging is het afwegingsorgaan vervallen, waardoor het onduidelijk is welke elementen terug dienen te komen in de AMvB. Op basis van de voorgestelde wijziging zou de AMvB in beginsel een verhelderde codificatie van huidige regelingen betreffen, met inachtneming van de resultaten uit de evaluatie van de Wet Computercriminaliteit III, conform de desbetreffende passage in het

Regeerakkoord. Indien het een codificatie van huidige regelingen van onderscheidenlijk de politie en inlichtingen en veiligheidsdiensten betreft, met inachtneming van de resultaten van de verwachte evaluatie, is dit voor het kabinet niet bezwaarlijk.
Indien echter aanvullende wijzigingen worden beoogd, dan is op dit moment onduidelijk wat deze wijzigingen behelzen en kunnen de gevolgen niet worden beoordeeld.

4. Financiën en efficiëntie
Het initiatiefwetsvoorstel maakt niet duidelijk hoe de advisering door vertegenwoordigers van betrokkenen die vitale infrastructuur beheren wordt ingericht en gefinancierd. Voorts is onduidelijk welke kosten voortvloeien uit de normering van het aankopen van technische hulpmiddelen in de op te stellen AMvB. Gezien de beperkte financiële ruimte bij de betrokken departementen en andere overheidsorganisaties in combinatie met de geringe noodzaak voor het voorstel is momenteel geen financiële dekking van het voorstel voorzien.
Daarnaast brengt het wetsvoorstel een toename van de administratieve last met zich mee.
De efficiëntie van de betrokken diensten zal daardoor negatief worden beïnvloed. Dat is des te klemmender gezien de schaarste van de benodigde expertise.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
K.H. Ollongren

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus