Ministerie van Justitie en Veiligheid

Aan de Minister van Justitie en Veiligheid

Directie Wetgeving en Juridische Zaken
Sector Staats- en Bestuursrecht

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Datum
30 juni 2022

Ons kenmerk
4082121

nota

Nota naar aanleiding van het verslag Wet beveiliging netwerk- en informatiesystemen

1. Aanleiding

Deze nota gaat over uw wetsvoorstel tot wijziging van de **Wet beveiliging netwerk- en informatiesystemen** (Wbni). Met dit wetsvoorstel wordt geregeld dat aanbieders die geen vitale aanbieder of rijksoverheidsorganisatie zijn (hierna: **andere aanbieders**) in ruimere mate van het Nationaal Cyber Security Centrum (NCSC) dreigings- en incidentinformatie over hun eigen netwerk- en informatiesystemen kunnen krijgen. Met die informatie kunnen zij maatregelen nemen om digitale incidenten te voorkomen of de gevolgen daarvan te beperken.

Het wetsvoorstel is op 20 april 2022 ingediend bij de Tweede Kamer. Op 2 juni 2022 heeft de vaste commissie voor Digitale Zaken verslag uitgebracht over dit wetsvoorstel. In het verslag stellen diverse fracties vragen over dit wetsvoorstel. In de bijgevoegde **nota naar aanleiding van het verslag** beantwoordt u die vragen.

2. Geadviseerd besluit

U wordt gevraagd om in te stemmen met de nota naar aanleiding van het verslag en de verzending daarvan aan de Tweede Kamer.

3. Kernpunten

De leden van de fracties van VVD, PVV, SP, GroenLinks en Volt hebben inbreng geleverd voor het verslag. Uit die inbreng volgen geen grote principiële bezwaren tegen dit wetsvoorstel. De leden van de CDA-fractie hebben met instemming kennisgenomen van dit wetsvoorstel en hebben naar aanleiding daarvan geen vragen. De leden van de D66-fractie hebben geen inbreng geleverd.

De belangrijkste punten uit het verslag (zie voorts paragraaf 4.2):

- De **afbakening van de groep "andere aanbieders"** waaraan rechtstreeks dreigings- en incidentinformatie kan worden verstrekt. Volt merkt op dat het begrip "andere aanbieders" erg ruim is. GroenLinks geeft aan dat deze groep voornamelijk is gedefinieerd op kenmerken die het niet heeft en vraagt waarom de groep niet is gedefinieerd op kenmerken die het wel heeft. In reactie hierop geeft u aan dat deze groep voldoende specifiek is. Zie paragraaf 4.2.1.
- **Beveiligingsverplichtingen voor OKTT's** (organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten). PVV, GroenLinks en VVD vragen waarom er in de Wet beveiliging netwerk- en informatiesystemen geen beveiligingsverplichtingen worden opgenomen voor OKTT's. OKTT's zijn

schakelorganisaties van "andere aanbieders", door tussenkomst waarvan die aanbieders met dit wetsvoorstel in ruimere zin dreigings- en incidentinformatie van het NCSC kunnen verkrijgen. U geeft aan hiervoor geen reden te zien omdat het uitvallen van OKTT's niet maatschappelijk ontwrichtend is en er voldoende waarborgen zijn voor bijvoorbeeld een vertrouwelijke omgang met gegevens door een OKTT. Zie paragraaf 4.2.2 voor een nadere toelichting en voorbeelden.
- De **verhouding tussen het Nationaal Cyber Security Centrum en het Digital Trust Center (DTC)**. VVD en PVV vragen naar de verhouding tussen deze organisaties. De SP wijst erop dat er mogelijk dubbel werk wordt gedaan, werk blijft liggen of dat deze organisaties elkaar zelfs tegenwerken. In reactie hierop licht u toe wat hun onderscheidenlijke taken en doelgroepen zijn en geeft u aan dat door die taakverdeling er geen overlap of verwarring kan zijn. Zie paragraaf 4.2.3 voor een nadere toelichting.

4. Toelichting

4.1 Kern van het wetsvoorstel

- Zie ook de bijgevoegde factsheet over de Wet beveiliging netwerk- en informatiesystemen met diverse voorbeelden.
- De minister van JenV (in de praktijk: het Nationaal Cyber Security Centrum) heeft op grond van de Wet beveiliging netwerk- en informatiesystemen primair de taak om vitale aanbieders en Rijksoverheidsorganisaties te informeren en te adviseren over digitale dreigingen en incidenten. Het heeft ook de taak om ten behoeve van deze taken analyses en technisch onderzoek te verrichten. Het Nationaal Cyber Security Centrum kan daarbij de beschikking krijgen over dreigings- en incidentinformatie over de netwerk- en informatiesystemen van aanbieders die niet behoren tot zijn doelgroep, ook wel "andere aanbieders" genoemd. De Wet beveiliging netwerk- en informatiesystemen bevat een bevoegdheid voor het Nationaal Cyber Security Centrum om die data te delen met de in die wet genoemde schakelorganisaties van die andere aanbieders. Schakelorganisaties hebben de taak om aanbieders in hun achterban te informeren en te adviseren over de hen aangaande digitale dreigingen en incidenten.
- De Wet beveiliging netwerk- en informatiesystemen voorziet echter lang nog niet altijd in de bevoegdheid om die data aan die schakelorganisaties of direct aan de andere aanbieders te verstrekken. Dit voorstel regelt daarom dat het Nationaal Cyber Security Centrum in ruimere mate dreigings- en incidentinformatie over de systemen van andere aanbieders aan de schakelorganisaties van deze andere aanbieders, meer in het bijzonder OKTT's, kan verstrekken, of direct aan deze andere aanbieders als een schakelorganisatie niet aanwezig is. Dankzij die informatie kunnen deze aanbieders maatregelen treffen tegen digitale dreigingen of incidenten.

4.2 De belangrijkste punten in het verslag van de commissie voor Digitale Zaken en uw reactie daarop in de nota naar aanleiding van het verslag

4.2.1 Afbakening "andere aanbieders" (nieuw onderdeel e in artikel 3, tweede lid, Wbni)

Volt en GroenLinks hebben opmerkingen bij de afbakening van de groep "andere aanbieders" waaraan rechtstreeks dreigings- en incidentinformatie kan worden verstrekt. Volt meent dat het begrip "andere aanbieders" erg ruim is en GroenLinks geeft aan dat "andere aanbieders" voornamelijk zijn gedefinieerd op kenmerken die zij niet hebben en vraagt waarom niet is gedefinieerd op kenmerken die zij wel hebben.

In reactie hierop geeft u aan dat de groep voldoende concreet is omschreven door de volgende objectieve cumulatieve criteria:
1. de aanbieder is geen vitale aanbieder en evenmin een rijksoverheidsorganisatie;
2. er is geen schakelorganisatie die de aanbieder van dreigings- en incidentinformatie kan voorzien én;

3. er is sprake van informatie over een dreiging of incident met (potentiële) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de betrokken aanbieder.

De groep omvat aanbieders (zoals veiligheidsregio's en politieke partijen) met uiteenlopende kenmerken. Het niet hebben van de onder 1 en 2 genoemde kenmerken maakt de groep juist zo kenmerkend. Het benoemen van de kenmerken die deze aanbieders wel zouden hebben leidt bovendien tot het risico dat er onverhoopt aanbieders buiten de groep vallen en daardoor geen dreigings- en incidentinformatie kunnen ontvangen over hun eigen netwerk- en informatiesystemen.

4.2.2 Beveiligingsverplichtingen voor OKTT's

In het verslag vragen de leden van de fracties van PVV, GroenLinks en VVD waarom er in de Wet beveiliging netwerk- en informatiesystemen geen beveiligingsverplichtingen worden opgenomen voor OKTT's (organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten).

In reactie hierop geeft u aan hier geen reden voor te zien. De bedoelde verplichtingen uit de Wet beveiliging netwerk- en informatiesystemen hebben namelijk alleen betrekking op de krachtens die wet als "aanbieder van essentiële diensten" aangewezen vitale aanbieders Hierbij gaat het onder meer om drinkwaterbedrijven, de Nederlandse Aardolie Maatschappij B.V. en de netbeheerder van het landelijk hoogspanningsnet. Als hun dienstverlening uitvalt, dan is dat in grotere mate maatschappelijk ontwrichtend dan wanneer dat gebeurt met de dienstverlening van een niet-vitale aanbieder of diens schakelorganisatie.

U legt daarnaast uit dat er zowel vóór de aanwijzing als OKTT als na de aanwijzing voldoende waarborgen zijn dat een dergelijke schakelorganisaties bijvoorbeeld vertrouwelijk omgaat met de van het Nationaal Cyber Security Centrum verkregen informatie. Zo wordt er voordat een schakelorganisatie als OKTT wordt aangewezen een grondige beoordeling verricht om te bepalen of de informatieverstrekking door het Nationaal Cyber Security Centrum aan de schakelorganisatie verantwoord en gerechtvaardigd is. In het kader daarvan wordt onder meer getoetst of de organisatie voldoende technische en organisatorische beveiligingsmaatregelen heeft genomen. Ook geeft u aan dat het Nationaal Cyber Security Centrum de informatiedeling kan opschorten, indien op basis van een melding van de schakelorganisatie zelf of op basis van door het ministerie anderszins ontvangen informatie blijkt dat de schakelorganisatie niet meer voldoet aan de toetsingscriteria.

4.2.3 Verhouding Nationaal Cyber Security Centrum – Digital Trust Center

VVD en PVV vragen naar de verhouding tussen het Nationaal Cyber Security Centrum en het Digital Trust Center. De SP wijst erop dat er mogelijk dubbel werk wordt gedaan, werk blijft liggen omdat geen organisatie zich verantwoordelijk voelt of dat organisaties elkaar zelfs tegenwerken.

In reactie hierop geeft u in de nota naar aanleiding van het verslag aan dat het Nationaal Cyber Security Centrum en het Digital Trust Center nadrukkelijk onderscheidenlijke taken en doelgroepen. Het NCSC heeft krachtens de Wet beveiliging netwerk- en informatiesystemen 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 Nationaal Cyber Security Centrum deze aanbieders ook overige bijstand bij het treffen van maatregelen om incidenten te voorkomen en te verhelpen. Het Digital Trust Center heeft tot taak het niet-vitale bedrijfsleven te informeren en adviseren over digitale dreigingen en incidenten.[1] Door deze afbakening van doelgroepen en taken kan er geen verwarring en overlap ontstaan.

[1] Uitzondering op deze afbakening van doelgroepen zijn overigens digitaledienstverleners. Zij zijn geen vitale aanbieder, maar vallen ook niet in de doelgroep van het DTC. Zij vallen namelijk op grond van de Wet

4.3 Politiek-bestuurlijke context

Urgentie wetsvoorstel
Dit is een urgent wetsvoorstel. Dit wetsvoorstel zorgt ervoor dat het Nationaal Cyber Security Centrum dreigings- en incidentinformatie die relevant is voor andere aanbieders in ruimere mate bij hen terecht kan laten komen, zodat zij maatregelen in hun netwerk- en informatiesystemen kunnen treffen. Vanwege de urgentie van dit wetsvoorstel heeft u de Raad van State en de Autoriteit Persoonsgegevens verzocht om snel met hun adviezen te komen, hetgeen ook is gebeurd.

Kamerbrieven en commissiedebat over het anticiperen op dit wetsvoorstel
Op 13 mei 2022 heeft u de Tweede Kamer bij brief geïnformeerd over uw voornemen om te anticiperen op dit wetsvoorstel. Op 25 mei 2022 vond hierover een debat plaats met de commissie Digitale Zaken. Op 1 juni 2022 heeft u aan de Tweede Kamer een overzicht gestuurd van de gevallen waarin het Nationaal Cyber Security Centrum in ruimere zin dan wettelijk mogelijk was informatie heeft gedeeld. De Tweede Kamer heeft aangegeven gebruik te willen maken van uw aanbod van een technische briefing over de laatstgenoemde brief. De briefing vindt naar verwachting plaats in de week van 4 juli a.s.

Verzoeken om deling van informatie over digitale dreigingen
Na de uitbraak van de oorlog in Oekraïne hebben meerdere organisaties (die geen vitale aanbieders zijn en evenmin deel uitmaken van de Rijksoverheid) zich gemeld bij het Nationaal Cyber Security Centrum met het verzoek om informatie over digitale dreigingen te delen.

4.4 Afstemming

Deze nota en de bijgevoegde stukken zijn afgestemd met de NCTV.

4.5 Bijlagen

- Nota naar aanleiding van het verslag
- Wetsvoorstel tot wijziging van de Wet beveiliging netwerk- en informatiesystemen
- Memorie van toelichting
- Factsheet over de Wet beveiliging netwerk- en informatiesystemen

5. Informatie die zich niet leent voor openbaarmaking

Geen.

beveiliging netwerk- en informatiesystemen onder het computer security incident response team (CSIRT) voor digitale diensten, dat hen bijstaat bij het treffen van maatregelen om de continuïteit van de dienst te waarborgen of te herstellen (zie artikel 4, vierde lid, van de Wet beveiliging netwerk- en informatiesystemen).