Ministerie van Justitie en Veiligheid

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
19 april 2022

Ons kenmerk
3973153

nota

Wet beveiliging netwerk- en informatiesystemen (Wbni): nader rapport en indiening TK

1. Aanleiding

De voorgelegde stukken zien op uw wetsvoorstel tot wijziging van de **Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni)**. Hierin wordt geregeld dat aanbieders die geen vitale aanbieder of rijksoverheidsorganisatie zijn (hierna: andere aanbieders) in ruimere mate van het Nationaal Cyber Security Centrum (hierna: 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.

2. Geadviseerd besluit

U wordt gevraagd om:
- in te stemmen met het nader rapport op het advies van de Afdeling advisering van de Raad van State op dit wetsvoorstel (hierna: Raad van State) en;
- in te stemmen met de verzending van het nader rapport, het wetsvoorstel en de memorie van toelichting aan het Kabinet van de Koning ten behoeve van de indiening van dit wetsvoorstel bij de Tweede Kamer der Staten-Generaal.

3. Kernpunten

Dit is een urgent wetsvoorstel. Het NCSC beschikt over dreigings- en incidentinformatie die relevant is voor andere aanbieders, maar kan deze informatie niet altijd met hen of hun schakelorganisatie delen omdat hiervoor een wettelijke grondslag ontbreekt. In paragraaf 4.1 wordt nader toegelicht wat een schakelorganisatie is. Zonder die informatie weten deze aanbieders niet dat hun netwerk- en informatiesystemen kwetsbaar zijn en kunnen zij hier geen maatregelen tegen nemen. Dit wetsvoorstel zorgt ervoor dat die informatie in ruimere mate bij hen terecht kan komen.

Gelet op de urgentie van dit wetsvoorstel heeft u de Raad van State verzocht om spoedadvies. Hierover heeft u op 8 februari jl. gebeld met de vice-president van de Raad van State. De Raad van State heeft inmiddels geadviseerd. Het betreft een licht dictum (dictum B). In het bijgevoegde nader rapport reageert u op dit advies. De hoofdpunten zijn:
1. een nadere toelichting op de verhouding van het NCSC tot het Digital Trust Center (DTC, vallende onder het ministerie van EZK) en;
2. een toelichting op het niveau van privacybescherming bij organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten (OKTT's).

Directie Wetgeving en Juridische Zaken
Sector Staats- en bestuursrecht

Datum
19 april 2022

Ons kenmerk
3973153

4. Toelichting

4.1 Kern van het wetsvoorstel

- Zie de bijgevoegde factsheet voor meer informatie over de Wbni.
- De Wbni regelt (onder meer) de taken en bevoegdheden van de minister van JenV op het terrein van cybersecurity. Deze taken en bevoegdheden worden in de praktijk uitgevoerd door het NCSC.
- De minister van JenV (in de praktijk: het NCSC) heeft op grond van de Wbni primair de taak om vitale aanbieders en aanbieders die deel uitmaken van de rijksoverheid te informeren en te adviseren over digitale dreigingen en incidenten. Ook heeft het NCSC de taak om ten behoeve van deze taken analyses en technisch onderzoek te verrichten. Tot de doelgroep van het NCSC behoren dus vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid.
- Het NCSC kan bij de uitoefening van die primaire taken de beschikking krijgen over dreigings- en incidentinformatie over de netwerk- en informatiesystemen van aanbieders die niet behoren tot de doelgroep van het NCSC. Deze informatie wordt ook wel "restdata" genoemd en die laatstbedoelde aanbieders worden in de memorie van toelichting op dit wetsvoorstel en in deze nota "andere aanbieders" genoemd.
- De Wbni voorziet erin dat het NCSC restdata kan delen met de in die wet genoemde schakelorganisaties. Schakelorganisaties hebben de taak om aanbieders in hun achterban te informeren en te adviseren over de hen aangaande digitale dreigingen en incidenten. Zij zijn het meest bekend met de in hun achterban aanwezige netwerk- en informatiesystemen, bijbehorende belangen en risico's en informatiebehoeften. Onder schakelorganisaties vallen onder meer computercrisisteams en zogeheten organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten (OKTT).
- Op dit moment kan het NCSC deze restdata lang niet altijd delen met die andere aanbieders of met hun schakelorganisaties, omdat de Wbni nog niet voorziet in de bevoegdheid om restdata telkens aan die schakelorganisaties of direct aan de andere aanbieders te verstrekken. Zonder een wettelijke grondslag mag niet worden overgegaan tot het delen van informatie.
- Zonder deze informatie weten andere aanbieders bij digitale dreigingen of incidenten niet dat hun systemen kwetsbaar zijn en kunnen zij hier geen maatregelen tegen nemen. Als die systemen kwetsbaar blijven, kunnen aanvallers die kwetsbaarheden misbruiken en kan de dienstverlening van andere aanbieders in gevaar komen.
- Dit voorstel regelt daarom dat het NCSC 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. Dit laatste wordt in het wetsvoorstel expliciet geregeld, want lang niet elke andere aanbieder wordt bediend door een schakelorganisatie. Dit geldt bijvoorbeeld voor politieke partijen en provincies.
- Het doel van de verstrekking is dat deze aanbieders dankzij de verkregen informatie maatregelen kunnen nemen om digitale incidenten te voorkomen of de gevolgen daarvan te beperken.
- De Algemene verordening gegevensbescherming (AVG) vereist een wettelijke grondslag voor de verstrekking van persoonsgegevens. De dreigings- en incidentinformatie kan ook persoonsgegevens bevatten. Dit wetsvoorstel regelt met de ruimere bevoegdheid tot verstrekking ook die vereiste grondslag.

Directie Wetgeving en Juridische Zaken
Sector Staats- en bestuursrecht

Datum
19 april 2022

Ons kenmerk
3973153

Voorbeelden (niet uitputtend)

Vitale aanbieders:
- de netbeheerder van het landelijk hoogspanningsnet
- Luchtverkeersleiding Nederland
- drinkwaterbedrijven
- de Nederlandse Aardolie Maatschappij B.V.

Organisaties die deel uitmaken van de rijksoverheid:
- ministeries

Computercrisisteams (op grond van de Wbni bij ministeriële regeling aangewezen):
- de Stichting Z-CERT, een expertisecentrum voor cybersecurity in de zorg
- CERT Watermanagement, onderdeel van het openbaar lichaam Het Waterschapshuis, ondersteunt bij cyberincidenten in watermanagement

OKTT (een organisatie dat objectief kenbaar tot taak heeft om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten):
- Cyberweerbaarheidscentrum Brainport, een stichting opgericht t.b.v. ondernemingen die deel uitmaken van de Nederlandse kennisintensieve industrie, geïnitieerd door grote bedrijven in de Eindhovense hightech regio
- het Digital Trust Center (DTC)
- Cyberveilig Nederland, een belangenvereniging ten behoeve van de cybersecurity sector.
- FERM, opgericht ten behoeve van de bedrijven die onderdeel zijn van de Rotterdamse haven

Aanbieders die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid (in het wetsvoorstel aangeduid als "andere aanbieders"):
- veiligheidsregio's
- politieke partijen
- provincies
- semipublieke organisaties
- een beheerder van parkeervoorzieningen
- een distributeur van voedselwaren
- een containeroverslagbedrijf

Digitale dreigingen of aanvallen op andere aanbieders die hebben plaatsgevonden:
- de besmetting van een containeroverslagbedrijf met Petya-ransomware waardoor de dienstverlening van dit bedrijf in 2017 dagenlang stil kwam te liggen
- de in de e-mailsoftware van Microsoft Exchange aanwezige kwetsbaarheid, die gebruikt is om gijzelsoftware te installeren bij een logistiek bedrijf voor voedselwaren in 2021, deze aanval leidde ertoe dat de distributie van kaas aan diverse supermarkten circa een week stil kwam te liggen
- de digitale aanval in 2021 op een ICT-leverancier van bijna honderd notarissen, de aanval leidde er onder andere toe dat geen aktes gepasseerd konden worden

De door het NCSC te verstrekken gegevens:
- IP-adressen van gebruikers van kwetsbare systemen of van aanvallers
- domeinnamen van gebruikers van kwetsbare systemen of van aanvallers
- e-mailadressen van gebruikers van kwetsbare systemen of van aanvallers
- let op: het gaat niet om bijzondere persoonsgegevens; dat zijn persoonsgegevens die door hun aard bijzonder gevoelig zijn, bijvoorbeeld omdat daaruit ras, etniciteit, religie of seksuele geaardheid uit blijken
- de namen van de bedrijven waarop een dreiging of incident betrekking heeft

Voorbeeldcasus (fictief)
Een onderzoeker van een universiteit heeft een publicatie gedaan over een kwetsbaarheid in veelgebruikte kantoorautomatiseringssoftware. Zij heeft een scan gedraaid naar kwetsbare systemen in Nederland en een lijst met de IP-adressen van die kwetsbare systemen gedeeld met het NCSC.
Het NCSC heeft op grond van de Wbni de taak om vitale aanbieders en andere aanbieders die deel uitmaken van de Rijksoverheid te informeren en adviseren over dit soort digitale kwetsbaarheden. Ten behoeve van die taak verricht het NCSC analyses en technisch onderzoek. Bij het analyseren van de lijst stuit het NCSC op IP-adressen van andere dan voornoemde aanbieders die ook kwetsbaar zijn (dit wordt "restdata" of "bijvangst" genoemd). Deze aanbieders vallen niet onder de primaire doelgroep

(vitaal en Rijk) van het NCSC, denk bijvoorbeeld aan een provincie of een distributeur van voedselwaren.
Het NCSC kan op grond van de Wbni restdata delen met een aantal schakelorganisaties (artikel 3, tweede lid, Wbni). Zo'n schakelorganisatie kan vervolgens zijn achterban informeren over de dreiging. Maar er zijn ook verschillende aanbieders die niet worden bediend door dit soort schakelorganisaties, bijvoorbeeld politieke partijen en provincies. Hierdoor kan de informatie niet belanden bij de kwetsbare aanbieder. De aanbieder weet dan niet dat hij kwetsbaar is en kan geen maatregelen nemen om deze kwetsbaarheid te verhelpen.
Het wetsvoorstel zorgt ervoor dat de informatie in bovenstaande gevallen wel kan belanden bij die aanbieder.

4.2 Wetsvoorstel van EZK over het DTC

- EZK werkt aan een wetsvoorstel voor een nieuwe wet, genaamd Wet bevordering digitale weerbaarheid bedrijven. Hierin worden de taken en bevoegdheden van de minister van EZK geregeld ter verbetering van de digitale weerbaarheid van het niet-vitale Nederlandse bedrijfsleven. Deze taken en bevoegdheden worden in de praktijk uitgevoerd door het Digital Trust Center (DTC).
- De minister van JenV (in de praktijk: het NCSC) heeft op grond van de Wbni al vergelijkbare taken en bevoegdheden, maar dan ten behoeve van de rijksoverheid en vitale aanbieders. Het wetsvoorstel van EZK regelt taken en bevoegdheden die op dit moment in de Wbni ongeregeld zijn en dus daarop een aanvulling betreffen.
- In het EZK-voorstel wordt mede door een wijziging van de Wbni voorzien in de wettelijke grondslag voor beide ministers om elkaar in het kader van de uitoefening van hun taken over en weer te voorzien van voor de taakuitoefening van de ander relevante dreigings- en incidentinformatie.
- Het EZK-voorstel, samen met het nu voorliggende JenV-voorstel, beogen mede het probleem van een te beperkte informatievoorziening over digitale dreigingen en incidenten voor niet-vitale bedrijven op te lossen. Vanuit de coördinerende verantwoordelijkheid van JenV voor digitale veiligheid ondersteunt JenV dit voorstel.
- Het EZK-voorstel wordt op korte termijn voorgelegd aan de Raad van State voor advies. Het JenV-voorstel is al voorzien van dat advies. De voorstellen lopen dus niet parallel, maar dat is niet bezwaarlijk omdat zij inhoudelijk goed van elkaar te scheiden zijn. Tijdens de ambtelijke afstemming van beide voorstellen heeft EZK (ambtelijk) zo nu en dan het idee van het gelijk optrekken van beide voorstellen geopperd, waarop JenV (ambtelijk) heeft aangegeven geen reden hiertoe te zien. Samenloop kan immers ertoe leiden dat het voorstel dat verder in het wetgevingstraject is, wordt opgehouden door het voorstel dat in een eerder stadium bevindt.

4.3 Grondslagenkwestie NCTV

- De grondslagenkwestie NCTV betreft een andere kwestie dan die waarop dit wetsvoorstel betrekking heeft.
- De Wbni regelt de taken van de minister van JenV met betrekking tot de beveiliging van netwerk- en informatiesystemen, die in de praktijk door het NCSC worden uitgevoerd. De in de Wbni geregelde taken zien – kort samengevat – op het informeren en adviseren van aanbieders uit zijn doelgroep over digitale dreigingen en incidenten.
- Het wetsvoorstel over de grondslagenkwestie ziet op de analyse- en coördinatietaken van de minister van JenV op het terrein van de bestrijding van terrorisme en bescherming van de nationale veiligheid en de daarmee gepaard gaande verwerking van (bijzondere) persoonsgegevens.

4.4 Advies Afdeling advisering van de Raad van State

De Raad van State heeft advies uitgebracht over dit wetsvoorstel en dit advies voorzien van een zogeheten dictum B. Dit is een licht dictum en houdt in dat de Raad van State een aantal opmerkingen heeft bij het voorstel en adviseert

daarmee rekening te houden voor de indiening van het voorstel bij de Tweede Kamer.[1] In het nader rapport reageert u op dit advies en geeft u aan wat u naar aanleiding daarvan heeft aangepast of aangevuld in het wetsvoorstel en de memorie van toelichting. Hieronder volgt een samenvatting hiervan:

4.4.1 Taakafbakening tussen het NCSC en het DTC

Advies Raad van State
De Raad van State vraagt naar de verhouding tussen de taakstelling van het NCSC en het DTC. Het DTC ondersteunt en informeert het niet-vitale bedrijfsleven. Het voorliggende wetsvoorstel regelt dat het NCSC zich meer kan bezighouden met het informeren van niet-vitale aanbieders, waaronder aanbieders waar ook het DTC contacten mee onderhoudt. Doordat er mogelijk een overlap is tussen het NCSC en het DTC kan het voor bedrijven onduidelijk zijn bij welk loket zij moeten zijn en met wie zij in tijden van crisis in verbinding kunnen staan, aldus de Afdeling.

Reactie in nader rapport en opvolging van het advies
- In het nader rapport geeft u aan dat het NCSC en het DTC duidelijk onderscheidenlijke primaire doelgroepen van organisaties hebben waaraan informatie en advies wordt gegeven over concrete dreigingen en incidenten:
  - De doelgroep van het NCSC zijn vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid.
  - De doelgroep van het DTC is het niet-vitale bedrijfsleven, behalve digitaledienstverleners.
  - Digitaledienstverleners (bijvoorbeeld cloudcomputerdiensten) zijn geen vitale aanbieder, maar behoren ook niet tot de doelgroep van het DTC. Zij vallen namelijk op grond van de Wbni onder het zogeheten *Computer security incident response team* (CSIRT) voor digitale diensten.
- Door deze duidelijke afbakening in doelgroepen kan er geen verwarring ontstaan over van welke overheidsinstantie een aanbieder op informatie en advies bij digitale dreigingen en incidenten kan rekenen. Met het wetsvoorstel van de minister van EZK, waarin de taken van het DTC worden vastgelegd, wordt de afbakening nog verder verduidelijkt.
- Naar aanleiding van dit advies van de Raad van State is de memorie van toelichting aangevuld met een hoofdstuk waarin de voorgaande punten worden besproken.

4.4.2 Niveau van beveiliging en privacybescherming bij OKTT's

Advies Raad van State
De Raad van State geeft aan dat OKTT's dreigingsinformatie ontvangen en de taak hebben om die door te geven aan de aanbieders die bij hen zijn aangesloten. Ook kunnen zij informatie doorgeven aan het publiek. In de Wbni zoals die nu luidt kan het alleen gaan om algemene informatie, maar het wetsvoorstel regelt dat zij ook vertrouwelijke (tot een specifieke organisatie) herleidbare gegevens aan het publiek kunnen doorgeven, aldus de Raad van State. De Raad van State wijst hierbij op het belang dat schakelorganisaties zoals OKTT's voldoen aan beveiligingseisen en privacynormen. Bij de aanwijzing van deze organisaties als schakelorganisaties toetst de minister hieraan, maar OKTT's hoeven niet te voldoen aan de veel concretere en specifiekere eisen die bij en krachtens hoofdstuk 4 van de Wbni gelden voor aanbieders van essentiële diensten en

[1] Dictum A betreft het lichtste dictum (de Afdeling heeft geen opmerkingen bij het voorstel en adviseert het voorstel bij de Tweede Kamer in te dienen). Dictum D betreft het zwaarste dictum (de Afdeling heeft ernstige bezwaren tegen het voorstel en adviseert het niet bij de Tweede Kamer in te dienen).

digitaledienstverleners, aldus de Raad van State. Volgens de Raad van State is hiermee onvoldoende wettelijk gewaarborgd dat schakelorganisaties het vereiste niveau van beveiliging en privacybescherming hebben op het moment dat zij worden aangewezen, en dat zij aan dat niveau blijven voldoen.

Reactie in nader rapport en opvolging van het advies

- In het nader rapport geeft u aan dat er voldoende waarborgen zijn dat OKTT's vertrouwelijk omgaan met de van het NCSC verkregen informatie. U wijst onder meer op het volgende:
  - Voordat een schakelorganisatie als OKTT wordt aangewezen, wordt een grondige beoordeling verricht om te bepalen of de informatieverstrekking door het NCSC 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.
  - Een schakelorganisatie moet bij de aanwijzing als OKTT een verklaring ondertekenen waarin is opgenomen dat aan het NCSC melding wordt gemaakt van belangrijke wijzigingen van de beveiligingsmaatregelen of van de doelgroep en de taken die voor die doelgroep worden verricht.
  - Het NCSC kan de informatiedeling opschorten op basis van zo'n melding of op basis van door het ministerie anderszins ontvangen informatie.
  - De aanwijzing als OKTT kan worden ingetrokken als uit verdere navraag blijkt dat niet meer aan de toetsingscriteria wordt voldaan.
- U ziet geen aanleiding in het aan OKTT's opleggen van beveiligingsverplichtingen in wetgeving, zoals die in de Wbni voor bepaalde aanbieders zijn opgenomen. Deze Wbni-verplichtingen (zie hierover meer in de factsheet) betreffen alleen aanbieders die diensten leveren waarvan de continuïteit van essentieel belang is voor de Nederlandse samenleving (zoals drinkwater en luchtvervoer). Wanneer de beschikbaarheid van de dienstverlening van bijvoorbeeld een drinkwaterbedrijf of de Luchtverkeersleiding Nederland wordt aangetast, dan is dat in veel grotere mate maatschappelijk ontwrichtend dan wanneer dat gebeurt met de dienstverlening van een andere aanbieder of diens OKTT.
- Naar aanleiding van dit advies van de Raad van State is de memorie van toelichting aangevuld met enkele passages waarin de voorgaande punten worden besproken.

4.4.3 Redactioneel advies

De Raad van State heeft enkele adviezen van redactionele aard gegeven. Naar aanleiding hiervan is het wetsvoorstel (de tekst van de voorgestelde Wbni-bepalingen) op twee punten redactioneel (dus niet-inhoudelijk) aangepast.

4.5 Politiek-bestuurlijke context

Kamervragen
Begin 2021 heeft u Kamervragen gesteld over belemmeringen bij de informatiedeling door het NCSC. In antwoord hierop heeft uw ambtsvoorganger toegezegd met een wetsvoorstel te komen en dit voorstel rond de zomer te consulteren.[2] Na de consultatie van dit wetsvoorstel zijn opnieuw Kamervragen gesteld en beantwoord over dit onderwerp.[3]

Adviesbrief Cyber Security Raad

---

[2] Vragen van Yeşilgöz-Zegerius (VVD) over het bericht 'Justitie deelt kritieke informatie over hacks niet met bedrijven' van 8 maart 2021, https://zoek.officielebekendmakingen.nl/ah-tk-20202021-2173.html.
[3] Antwoorden op de vragen van de leden Amhaouch en Palland d.d. 18 november 2021.

De Cyber Security Raad (CSR) heeft u op 22 februari 2021 een advies gestuurd over het versneld delen van incidentinformatie.[4] Uw ambtsvoorganger heeft de CSR geïnformeerd dat het CSR-advies wordt meegenomen in dit wetsvoorstel en in overige initiatieven waarmee de informatiedeling over cybersecurity vanuit de overheid (met de "andere aanbieders") wordt verbeterd.

Aandacht in de media
Dit onderwerp heeft in 2020 en 2021 met enige regelmaat aandacht gekregen in diverse media, waarin onbegrip is getoond over het feit dat het NCSC beschikt over dreigings- en incidentinformatie die relevant is voor bedrijven, maar deze om juridische redenen niet met hen kan delen.[5]

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 NCSC met het verzoek om informatie over digitale dreigingen te delen.

4.6 Afstemming

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

4.7 Bijlagen

- Wetsvoorstel tot wijziging van de Wbni
- Memorie van toelichting
- Nader rapport
- Factsheet over de Wbni

4.8 Afkortingen

Wbni	Wet beveiliging netwerk- en informatiesystemen
NCSC	Nationaal Cyber Security Centrum
DTC	Digital Trust Center
OKTT	organisatie die objectief kenbaar tot taak heeft om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten

5. Informatie die zich niet leent voor openbaarmaking

Geen.

[4] https://www.cybersecurityraad.nl/adviezen/documenten/adviezen/2021/02/22/csr-adviesbrief-inzake-het-versneld-delen-van-incidentinformatie
Volkskrant van 12 december 2020: 'Informatie over lekken in computernetwerken wordt niet gedeeld' en in het Financieel Dagblad van 14 december 2020: 'Hackers manifesteren zich extra aan einde coronajaar'.
[5] FD 28 september 2021 ('Bedrijfsleven start eigen alarmsysteem tegen hackers: 'overheid te traag') en in Volkskrant 29 september 2021 ('Informatie over op handen zijnde hacks wordt grotendeels weggegooid').