Bezoekadres
Turfmarkt 147
2511 DP Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

I www.cybersecurityraad.nl
T 070 751 5333 (secretariaat)
E info@cybersecurityraad.nl

Directie Wetgeving en Juridische Zaken
Sector Staats- en Bestuursrecht
T.a.v. Mw. mr.
Postbus 20301
2500 EH Den Haag

Datum
13 augustus 2021

Uw kenmerk

Onderwerp
CSR Reactie op voorgestelde wijziging Wbni

Geachte mevrouw ,

Naar aanleiding van uw schrijven van 21 juni 2021 betreffende het conceptvoorstel tot wijziging van de Wet beveiliging netwerk- en informatiesystemen (Wbni) ontvangt u hierbij de reactie en adviezen hiertoe van de Cyber Security Raad (hierna de raad).

Cyberweerbaarheid steeds urgenter

Het midden- en kleinbedrijf (mkb) vormt de ruggengraat van onze economie en is in toenemende mate doelwit van cyberaanvallen met direct dan wel indirect schade tot gevolg. Het onlangs verschenen Cybersecuritybeeld Nederland (CSBN) 2021[1] en AIVD-rapport[2] rapporteren dat de cyberdreigingen permanent zijn en blijven groeien in omvang en de daarmee gepaard gaande schade. Een van de belangrijkste instrumenten om de cyberweerbaarheid van organisaties en burgers te verhogen, is hen snel te informeren wanneer hun IT-systemen kwetsbaarheden vertonen of gehackt zijn. Vooralsnog is het Nationaal Cyber Security Centrum (NCSC) niet in staat gesteld de bij hen bekende incidentinformatie te delen met niet-vitale organisaties en de daartoe opgerichte schakelorganisaties. Hierdoor bereikt deze essentiële incidentinformatie niet de getroffen bedrijven en burgers en zijn zij als gevolg hiervan niet in staat om tijdig beschermingsmaatregelen te nemen. Een zeer ongewenste situatie, daar zijn alle betrokkenen het over eens. De raad omarmt daarom het feit dat de demissionair minister van Justitie en Veiligheid (JenV) de wijziging van de Wbni met voorrang in gang heeft gezet, zodat de bevoegdheid van het NCSC om namens de minister van JenV dreigings- en incidentinformatie te verstrekken wordt uitgebreid. Het wetsvoorstel geeft daarmee gehoor aan de CSR Adviesbrief inzake een versnelde vorming van een volwassen Landelijk Dekkend Stelsel van informatie-uitwisseling (LDS) van 22 februari jl.[3]

[1] Cybersecuritybeeld Nederland 2021, Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), in samenwerking met het Nationaal Cyber Security Centrum (NCSC), juni 2021
https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2021/06/28/tk-bijlage-csbn2021/tk-bijlage-csbn2021.pdf
[2] Dreigingsbeeld Statelijke Actoren, Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), februari 2021
https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2021/06/28/cyberaanvallen-door-statelijke-actoren---zeven-momenten-om-een-aanval-te-stoppen/Publicatie+AIVD-MIVD+-+Cyberaanvallen+door+statelijke+actoren.pdf
[3] CSR Adviesbrief 'Inzake het versneld delen van incidentinformatie', CSR-advies 2021, nr. 1, februari 2021
https://www.cybersecurityraad.nl/documenten/adviezen/2021/02/22/csr-adviesbrief-inzake-het-versneld-delen-van-incidentinformatie

Naast het ingediende wetsvoorstel tot wijziging van de Wbni, heeft de demissionair staatssecretaris van Economische Zaken en Klimaat (EZK) het wetsvoorstel Bevordering digitale weerbaarheid bedrijven (Wbdwb) ingebracht voor de internetconsultatie. Het doel hiervan is om voor het Digital Trust Center (DTC) een expliciete wettelijke grondslag te creëren om dreigingsinformatie te kunnen ontvangen, te verwerken en te delen met het bedrijfsleven.[4]

De raad is van mening dat beide wetsvoorstellen een grote en belangrijke stap vormen in het verwezenlijken van het LDS om meer dreigingsinformatie die bij de overheid aanwezig is te delen met alle bedrijven en organisaties in Nederland.

Reactie van de raad op de voorgestelde wijziging van de Wbni

De voorgestelde wetswijziging zorgt voor een uitbreiding van de bevoegdheid van het NCSC. Het maakt het mogelijk om, namens de minister van JenV, informatie over dreigingen en incidenten betreffende de netwerk- en informatiesystemen van aanbieders, die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid (zgn. andere aanbieders), te verstrekken aan deze andere aanbieders. Tevens biedt deze wetswijziging de mogelijkheid voor het NCSC om deze informatie te delen met organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten voor hun netwerk- en informatiesystemen (OKTT's).

Het wetsvoorstel strekt tot de volgende aanpassingen van de Wbni:

a. **het in bijzondere gevallen delen van dreigings- en incidentinformatie met aanbieders die geen vitale aanbieder of onderdeel van de rijksoverheid zijn ("andere aanbieders");**
b. **het zonder instemming van aanbieders delen van vertrouwelijke herleidbare gegevens met betrekking tot die aanbieders aan OKTT's en;**
c. **de aanwijzing van OKTT's bij ministeriële regeling.**

Hieronder volgt per voorgestelde aanpassing een reactie op deze aanpassing en de adviezen van de raad.

Het in bijzondere gevallen delen van dreigings- en incidentinformatie met aanbieders die geen vitale aanbieder of onderdeel van de Rijksoverheid zijn ("andere aanbieders")

In het wetsvoorstel wordt de kanttekening geplaatst dat de voorgestelde bevoegdheid van het NCSC tot het verstrekken van dreigings- en incident informatie aan andere aanbieders is beperkt tot bijzondere gevallen. De bevoegdheid laat deze verstrekking alleen toe wanneer een dreiging of incident aanzienlijke gevolgen heeft of kan hebben voor de continuïteit van hun dienstverlening (1) en er voor de verstrekking van deze gegevens geen schakelorganisatie is die de aanbieder van die informatie kan voorzien (2). Het laatste onderdeel (2) van deze uitzondering is helder en past in de huidige aanpak van de uitrol van het LDS. Wat betreft het eerste onderdeel van de uitzondering (1), stelt de raad zich de vraag of deze toets niet onnodig zwaar is. In de praktijk zal het niet altijd mogelijk zijn om vooraf een juiste inschatting te maken van de mogelijke impact van een dreiging of incident op een organisatie, laat staan of die mogelijk tot 'aanzienlijke gevolgen voor de continuïteit van de dienstverlening' zal kunnen leiden (wel melden) of tot andere vormen van schade (niet melden). De mogelijkheid dat de dreiging of het incident tot substantiële schade kan leiden, zou voldoende moeten zijn voor melding.

[4] Internetconsultatie Wet bevordering digitale weerbaarheid bedrijven (Wbdwb): https://internetconsultatie.nl/wbdwb

Advies van de raad:

- De raad adviseert om de drempel voor melding niet hoger te maken dan noodzakelijk. Op deze wijze kunnen niet-vitale organisaties erop rekenen dat het NCSC hen waarschuwt in geval er een risico op substantiële schade is (in welke vorm dan ook). Een situatie waarin er wel relevante dreigings- en incidentinformatie voorhanden is, maar niet wordt gedeeld, kan organisaties op het verkeerde been zetten. De raad is van mening dat een dergelijke situatie altijd moet worden vermeden.

Het zonder instemming van aanbieders delen van vertrouwelijke herleidbare gegevens met betrekking tot die aanbieders aan OKTT's

Deze wijziging stelt OKTT's in staat hun achterban te informeren ter bescherming van (potentiële) slachtoffers. Daarvoor is herleidbare informatie nodig, zodat organisaties na het verkrijgen van deze informatie ook daadwerkelijk maatregelen kunnen treffen.

Reactie van de raad:

- De raad is van mening dat deze aanpassing overeenkomstig de bedoeling van de Wbni is en hiermee een einde komt aan de ongewenste situatie. Dit komt ten goede aan de bescherming van de belangen van de duizenden bedrijven, organisaties en burgers en daarmee aan de cyberweerbaarheid van ons land.

De aanwijzing van OKTT's bij ministeriële regeling en de verwezenlijking van het LDS

Door de aanwijzing van organisaties als OKTT nu ook bij ministeriële regeling te laten plaatsvinden, zoals reeds het geval is bij de aanwijzing van computercrisisteams, wordt transparantie, structuur en duidelijkheid geboden. Dat is een goede ontwikkeling. Wel wijst de raad erop dat uit deze wetswijziging onvoldoende blijkt welk toekomstbeeld wordt nagestreefd, bijvoorbeeld ten aanzien van het gewenste aantal OKTT's en de monitoring van de stand van zaken van het LDS op dit vlak. Een goed werkend LDS is essentieel voor het snel en betrouwbaar delen van dreigingsinformatie en daarmee voor onze cyberweerbaarheid. De raad is van mening dat binnen het LDS regie op samenwerking noodzakelijk is en dat de informatie makkelijk toegankelijk moet zijn voor organisaties. Daarom moet de rol van het DTC ten aanzien van andere OKTT's nader worden geëxpliciteerd. Tevens wordt veel onduidelijkheid voor de verschillende doelgroepen weggenomen als er één loket komt waar men terecht kan. Er bestaat momenteel immers overlap tussen de doelgroepen van het NCSC, het DTC en schakelorganisaties. Meer helderheid over wat bedrijven en maatschappelijke organisaties van de verschillende partijen in het LDS kunnen verwachten zal richting hen meer duidelijkheid scheppen. Gezien de urgentie van de vorming van het LDS is de raad verder van oordeel dat niet kan worden gewacht met het delen van de incidentinformatie met de OKTT's totdat de gehele wetswijzigingsprocedure doorlopen is.[5]

Adviezen van de raad:

- De raad roept de demissionair minister van JenV op om direct over te gaan tot het aanwijzen van het DTC als OKTT, opdat het DTC dreigingsinformatie van het NCSC kan ontvangen en delen met bedrijven.[6]

[5] CSR Adviesbrief 'Inzake het versneld delen van incidentinformatie', CSR-advies 2021, nr. 1, februari 2021
https://www.cybersecurityraad.nl/documenten/adviezen/2021/02/22/csr-adviesbrief-inzake-het-versneld-delen-van-incidentinformatie
[6] Brief van de staatssecretaris van Economische Zaken en Klimaat inzake voortgang Digital Trust Center, juni 2021
https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z09619&did=2021D21232

Met het wetsvoorstel Wbdwb wordt immers voldaan aan de randvoorwaarde van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) voor de toewijzing van de OKTT-status

- De raad adviseert het ministerie van JenV, in samenwerking met alle departementen, in het bijzonder het ministerie van EZK en in samenwerking met de private sectoren, de uitrol van het LDS verder te stimuleren, met daarin een duidelijke positie voor het DTC. Tevens adviseert de raad u de mogelijkheid te onderzoeken tot de introductie van één loket voor de diverse doelgroepen, in ieder geval voor die organisaties die hun weg nog niet hebben gevonden in het LDS.
- De raad adviseert om meer helderheid te verschaffen richting bedrijven en maatschappelijke organisaties over wat zij van de verschillende partijen in het LDS kunnen verwachten.
- De raad herhaalt hierbij het advies om, in afwachting van de afwikkeling van de wijziging van de Wbni, nu al tot het delen van incidentinformatie met OKTT's over te gaan.

Namens de Cyber Security Raad,

Covoorzitter CSR