Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

34 388 Regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity)

Nr. 7 **BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 4 oktober 2016

Tijdens het VAO Privacy op 27 september 2016 (Handelingen II 2016/17, nr. 4, Privacy) heb ik naar aanleiding van het indienen van een motie[1] door het lid Verhoeven (D66) toegezegd de Kamer nader te informeren over de rol van het Nationaal Cyber Security Centrum (NCSC) bij databeveiliging, dit mede in het licht van het feit dat het NCSC als onderwerp niet aan de orde is gekomen tijdens het AO Privacy op 18 mei 2016 (Kamerstuk 32 761, nr. 102).

Bij brief van 12 december 2013[2] heeft de toenmalige Minister van Veiligheid en Justitie uw Kamer al geschetst dat het NCSC, als onderdeel van het Ministerie van Veiligheid en Justitie, zijn taken vervult ter voorkoming en beperking van verstoringen in het digitale domein in het belang van de nationale veiligheid, en zich gelet daarop richt op de (rijks)overheid en vitale sectoren. Daarmee heeft het NCSC nu al een prominente rol op het gebied van informatiebeveiliging, waaronder de beveiliging van data, in de publieke sector, alsmede daarbuiten voor vitale private aanbieders. Ik hecht er daarbij aan te benadrukken dat informatiebeveiliging te allen tijde primair een eigen verantwoordelijkheid is van elke individuele organisatie.

In het bij uw Kamer aanhangige wetsvoorstel gegevensverwerking en meldplicht cybersecurity[3] worden de taken van het NCSC omschreven (als taken van de Minister (ingevolge de huidige taakverdeling: de Staatssecretaris) van Veiligheid en Justitie). Centraal hierin staat de rol van het NCSC als Computer Emergency Response Team, ofwel computercrisisteam, voor de rijksoverheid en vitale private aanbieders. Op grond hiervan heeft het NCSC tot taak om deze doelgroep bij te staan bij incidenten, te

[1] Kamerstuk 32 761, nr. 106.
[2] Kamerstuk 26 643, nr. 297.
[3] Kamerstuk 34 388, nr. 2.

kst-34388-7
ISSN 0921 - 7371
's-Gravenhage 2016

informeren en te adviseren inzake dreigingen en incidenten en om ten behoeve daarvan technisch onderzoek en analyses uit te voeren.

Het NCSC werkt intensief samen met andere organisaties zoals de Informatiebeveiligingsdienst voor gemeenten (IBD) van VNG/KING en andere computercrisisteams, met name ook om die samenwerkingspartners zo goed mogelijk in staat te stellen partijen buiten de primaire doelgroep van het NCSC te bedienen en om zo gezamenlijk een sluitend stelsel te creëren van organisaties die partijen bij kunnen staan om invulling te geven aan de genoemde eigen verantwoordelijkheid.

Tot slot heeft het NCSC een belangrijke rol als kenniscentrum en adviseur op het gebied van informatiebeveiliging. Het NCSC geeft zijn adviezen vanuit zijn centrale kennispositie die voortvloeit uit bovengenoemde taken. De kennisproducten van het NCSC, zoals bijvoorbeeld de ICT-beveiligingsrichtlijnen voor webapplicaties, worden gepubliceerd op www.ncsc.nl teneinde een ieder in staat te stellen kennis te nemen van deze producten en deze actief te gebruiken om de eigen verantwoordelijkheid voor informatiebeveiliging op actieve wijze in te vullen.

Daarmee is nu al sprake van een actieve rol op het gebied van informatiebeveiliging. Deze rol wordt zo ingevuld dat een ieder binnen de publieke en semi-publieke sector, alsmede ook in belangrijke mate daarbuiten toegang heeft tot de kennis van het NCSC. Ook wordt voortdurend bezien op welke wijze de expertise van het NCSC binnen bovenstaande kaders zo ingezet kan worden dat sprake is van maximale impact.

De Minister van Veiligheid en Justitie,
G.A. van der Steur