Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 536

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 april 2018

Hierbij bied ik uw Kamer, vanuit mijn coördinerende verantwoordelijkheid voor cybersecurity, namens het kabinet de Nederlandse Cybersecurity Agenda (NCSA) aan[1]. Hiermee geeft het kabinet invulling aan het voornemen uit het Regeerakkoord 2017–2021 «Vertrouwen in de toekomst» (bijlage bij Kamerstuk 34 700, nr. 34) om een ambitieuze cybersecurityagenda tot stand te brengen.

Nederland beschikt over een uitstekende uitgangspositie om de economische en maatschappelijke kansen van digitalisering te verzilveren. Tegelijkertijd nemen kwetsbaarheden en dreigingen in het digitale domein toe: de dreiging vanuit beroepscriminelen is gegroeid en blijft zich verder ontwikkelen. Statelijke actoren richten zich op digitale economische en politieke spionage, en treffen voorbereidingen voor digitale sabotage. Niet alleen het aantal landen dat digitale aanvalscapaciteiten ontwikkelt neemt toe, de aanvallen worden ook steeds complexer. Daarom is veiligheid in het digitale domein voor het kabinet een topprioriteit.

Deze directe dreigingen voor de nationale veiligheid vragen om extra inspanningen om de gecoördineerde cybersecurityaanpak te versterken en zo de vitale belangen van Nederland te beschermen. In deze agenda worden de kaders gesteld voor de volgende noodzakelijke stap in cybersecurity. De gezamenlijke koers wordt aangegeven, en diverse publieke, private, nationale en internationale maatregelen worden in samenhang beschouwd.

Hierbij geldt evenzeer dat we ons rekenschap geven van de aanwezige waarden-spanning in de ontwikkeling van cybersecurity. De verregaande digitalisering zet regelmatig de balans tussen de kernwaarden veiligheid, vrijheid en economische groei onder druk. Nederland zet in op een heldere afweging van die belangen bij het maken van (beleids)keuzes en hierover transparantie te betrachten. Het beschermen van waarden en

[1] Raadpleegbaar via www.tweedekamer.nl

kst-26643-536
ISSN 0921 - 7371
's-Gravenhage 2018

grondrechten in het digitale domein is eveneens een belangrijk onderdeel van cybersecurity. Burgers moeten er op kunnen rekenen dat hun grondrechten zowel online als offline gewaarborgd zijn, en dat hun privacy ook in het digitale domein gegarandeerd is.

Totstandkoming en samenhang

Aan de totstandkoming van NCSA heeft een groot aantal partijen actief bijgedragen (waaronder publieke en private partijen, kennisinstellingen, maatschappelijke organisaties en vertegenwoordigers van de cybersecurity *community*). De rijksoverheid en het bedrijfsleven zijn samen opgetrokken om deze agenda tot stand te brengen. Daarnaast is de Cyber Security Raad (CSR) geconsulteerd. Bovendien is bij de totstandkoming van de NCSA dankbaar gebruik gemaakt van diverse onderzoeks- en adviesrapporten.

Het beleidsterrein cybersecurity richt zich op het voorkomen van schade door verstoring, uitval en misbruik van ICT. Hieraan zijn verschillende beleidsthema's verwant die onder verantwoordelijkheid van andere bewindspersonen worden vormgegeven. In het bijzonder betreft het de Minister en Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties vanwege de verantwoordelijkheid voor de digitale overheid en de Algemene Inlichtingen- en Veiligheidsdienst, de Minister en Staatssecretaris van Economische Zaken en Klimaat in verband met digitalisering, de Minister van Buitenlandse Zaken vanwege de coördinerende rol voor internationale vrede en veiligheid en tot slot de Minister van Defensie aangaande de taken van de krijgsmacht in het digitale domein. In deze context kent de NCSA nauwe samenhang met de volgende deels nog in voorbereiding zijnde strategische documenten: de Digitaliseringsstrategie, de Brede Agenda Digitale Overheid, de Defensienota en de Geïntegreerde Buitenland- en Veiligheidsstrategie, de Internationale Cyberstrategie, de integrale aanpak cybercrime en de Defensie Cyber Strategie.

Met de NCSA wordt tevens uitvoering gegeven aan een van de verplichtingen in de Europese Netwerk- en Informatiesystemenbeveiligingsrichtlijn voor de lidstaten die momenteel wordt geïmplementeerd, namelijk het beschikken over een actuele cybersecuritystrategie. Aan diezelfde richtlijn wordt ook uitvoering gegeven door het onlangs aan uw Kamer aangeboden voorstel voor de Cybersecuritywet (Kamerstuk 34 883), met daarin onder meer zorg- en meldplichten voor aanbieders van essentiële diensten en digitaledienstverleners. Ik stuur uw Kamer, mede gelet op de implementatiedeadline, op zeer korte termijn mijn beantwoording van het verslag betreffende dit wetsvoorstel. De meer sturende rol van de overheid als wetgever komt ook terug in de ambities van de NCSA.

Vervolgproces

De uitvoering van deze NCSA zal in nauwe samenwerking met publieke en private partijen worden vormgegeven. De NCSA kent nadrukkelijk een dynamisch karakter. Aan de hand van technologische en maatschappelijke ontwikkelingen, en het jaarlijkse Cybersecuritybeeld Nederland zal steeds gemonitord en getoetst worden of de NCSA nog optimaal toegesneden is op de actuele situatie. Het dreigingsbeeld wordt jaarlijks door de Nationaal Coördinator Terrorismebestrijding en Veiligheid opgesteld, en aan uw Kamer aangeboden. Over de voortgang van de NCSA wordt uw Kamer in

samenhang met het dreigingsbeeld periodiek geïnformeerd, voor het eerst in 2019. In 2021 zal bovendien een eerste overkoepelende evaluatie verricht worden.

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