Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1469

Vragen van de leden **Remco Dijkstra** en **Arno Rutte** (beiden VVD) aan de Minister van Justitie en Veiligheid over *het bericht «Nederland is niet up-to-date»* (ingezonden 2 februari 2018).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid) (ontvangen 19 maart 2018). Zie ook Aanhangsel Handelingen, vergaderjaar 2017–2018, nr. 1269.

Vraag 1
Bent u bekend met artikel «Nederland is niet up-to-date»?[1]

Antwoord 1
Ja.

Vraag 2
Deelt u de mening dat fysieke vitale infrastructuur als luchthavens, elektriciteitscentrales en haven- en water infrastructuur ten alle tijden goed beschermd moeten zijn tegen cyberaanvallen? Hebben de Israëlische cybersecurityexperts uit het artikel die beweren dat de cyberveiligheid van deze cruciale infrastructuur in ons land onvoldoende op orde is gelijk? Zo ja, welke maatregelen neemt u? Zo nee, waarom niet?

Antwoord 2
De mening dat vitale infrastructuur goed beschermd moet zijn tegen cyberaanvallen onderschrijf ik volledig. Het beeld dat de cyberveiligheid van de cruciale infrastructuur in ons land onvoldoende op orde zou zijn herken ik niet. Dat neemt niet weg dat, zoals in de opeenvolgende jaarlijkse Cybersecuritybeelden Nederland[2] (CSBN) is aangegeven, de dreiging van cyberaanvallen serieus is en de weerbaarheid van onder meer de vitale infrastructuur verder verhoogd dient te worden. Mede met dit doel heeft dit kabinet structureel 95 miljoen euro gereserveerd voor cybersecurity.
Met de Cybersecuritywet, waarvan ik het voorstel op 15 februari jongstleden aan uw Kamer toezond, worden aanbieders van essentiële diensten in de loop van dit jaar verplicht te voldoen aan beveiligingseisen. Zij moeten adequate maatregelen nemen tegen inbreuken van buitenaf op hun netwerk-

[1] Telegraaf van 31 januari 2018
[2] Kamerstuk 26 643, nr. 477

ah-tk-20172018-1469
ISSN 0921 - 7398
's-Gravenhage 2018

en informatiebeveiliging. Als zich toch een cyberincident voordoet, moeten zij hun techniek en organisatie op orde hebben om het cyberincident van een passend antwoord te voorzien en de gevolgen ervan zo veel mogelijk te beperken.

Vraag 3
Is er sprake van een toename van het aantal cyberaanvallen? Dagelijks vinden aanvallen plaats, wat kunt u hierover zeggen?

Antwoord 3
Jaarlijks bied ik uw Kamer het CSBN van de NCTV aan. De afgelopen Cybersecuritybeelden Nederland en de jaarverslagen van de inlichtingen- en veiligheidsdiensten laten zien dat er sprake is van een serieuze dreiging. In het CSBN 2017 is geconstateerd dat de ontwikkeling van de weerbaarheid geen gelijke tred houdt met de ontwikkeling van de dreiging. Met het oog hierop wordt door dit kabinet geïnvesteerd in verdere verhoging van de weerbaarheid.

Vraag 4
Hoe blijft de Nederlandse overheid bij de tijd met betrekking tot de nieuwste ontwikkelingen op het gebied van cyberveiligheid? Kunt u aangeven of uitwisseling van kennis en/of samenwerking met andere bevriende landen juist zinvol is, of kleven hier ook nadelen aan? Welke lijn kiest het kabinet hierin en wie is verantwoordelijk voor een structurele en werkende aanpak om ongewenste cyberaanvallen op cruciale infrastructuur te voorkomen?

Antwoord 4
Laat ik voorop stellen dat de coördinerende verantwoordelijkheid op het gebied van cybersecurity binnen het kabinet bij mij als Minister van JenV belegd is. Uiteraard sta ik daarbij in nauw contact met de diverse collega's binnen het kabinet.
In de afgelopen jaren is vanuit de Nederlandse overheid reeds geïnvesteerd in cybersecurity. Zo is het NCSC binnen mijn ministerie al enige jaren belast met het verlenen van bijstand aan vitale organisaties en de rijksoverheid bij cyberdreigingen en -incidenten. In oktober 2017 zijn met de Wet gegevensverwerking en meldplicht cybersecurity de taken van het NCSC vastgelegd. Het NCSC vervult met het oog op genoemde wettelijke taken onder meer de rol van expertisecentrum. Vanuit het NCSC is er bijvoorbeeld dagelijks contact met andere Computer Emergency Response Teams (CERTS) en organisaties die deel uitmaken van de rijksoverheid en de vitale infrastructuur. Cybersecurity is van nature grensoverschrijdend. Daarom wordt nadrukkelijk ingezet op internationale samenwerking en wordt, met inachtneming van de verschillende wettelijke kaders, waar aangewezen informatie uitgewisseld, bijvoorbeeld met ander nationale CERTS.

Vraag 5
Hoe beoordeelt u de opmerking van een Israëlische specialist cybersecurity in het artikel dat andere Europese landen veel beter zijn ingespeeld op dit soort aanvallen dan Nederland? Is er grond voor die bewering? Zo ja, op welke wijze wordt werk gemaakt om op minstens hetzelfde beveiligingsniveau te komen als deze andere Europese landen? Zo nee, waarom niet?

Antwoord 5
Cybersecurity staat in Nederland hoog op de agenda en is een van de prioriteiten van dit kabinet. Zoals vorig jaar al bleek bij de door voormalig VS-Cybercommissaris Melissa Hathaway gepresenteerde *Cyber Readiness Index* [3] is Nederland goed op weg als het gaat om de digitale veiligheid, en dat juist de samenwerking tussen de overheid en de vitale sectoren in Nederland sterk ontwikkeld is. Dat neemt niet weg dat steeds flinke stappen gezet moeten worden om Nederland digitaal veilig te houden.

[3] http://www.potomacinstitute.org/academic-centers/cyber-readiness-index

Vraag 6
Welke resultaten denkt u te boeken met de 95 miljoen euro die is vrijgemaakt voor cybersecurity? Is dat voldoende en voor welke termijn? Waarop zal de nadruk komen te liggen? Welke plannen kan de Kamer verwachten? Op welke termijn en op welke manier wordt de Kamer geïnformeerd?

Antwoord 6
Met de 95 miljoen euro die het kabinet structureel gereserveerd heeft voor cybersecurity wordt een ambitieuze cybersecurity-agenda opgesteld. Deze agenda biedt het publiek-private kader voor de versterkte inzet op cybersecurity die door dit Kabinet is afgekondigd en bevat onder meer standaarden voor *Internet-of-things*-apparaten, het stimuleren van bedrijven om veiligere software te maken via software-aansprakelijkheid, het versterken van het Nationaal Cyber Security Centrum als aanspreekpunt van Computer Emergency Response Teams (CERT) van onder meer vitale sectoren, het stimuleren van cybersecurity-onderzoek en het verbeteren van voorlichtingscampagnes op het gebied van cyberhygiëne. Eind april van dit jaar zal de Nederlandse Cybersecurityagenda (NCSA) aan uw Kamer worden aangeboden.