Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017 **Aanhangsel van de Handelingen**

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

1184

Vragen van de leden **Gesthuizen** en **Van Raak** (beiden SP) aan de Ministers van Veiligheid en Justitie en van Binnenlandse Zaken en Koninkrijksrelaties over *Russische hackers die gebruikmaken van Nederlandse server* (ingezonden 4 januari 2017).

Antwoord van Minister **Plasterk** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de Minister van Veiligheid en Justitie (ontvangen 13 februari 2017). Zie ook Aanhangsel Handelingen, vergaderjaar 2016–2017, nr. 1046.

Vraag 1 en 2
Wat is uw reactie op het bericht dat Russische hackers gebruik zouden hebben gemaakt van een Nederlandse server?[1]
Op welke manier gaat u zich hierover uitgebreid op de hoogte laten stellen? Bent u bereid ook de Kamer hierover op de hoogte te houden?

Antwoord 1 en 2
Het kabinet doet in het openbaar geen uitspraken over specifieke casussen. We worden als bewindspersonen langs geëigende kanalen geïnformeerd over ontwikkelingen en incidenten.
Het kabinet zal uw Kamer blijven informeren over ontwikkelingen omtrent cyberdreigingen, onder meer via het Cyber Security Beeld Nederland (CSBN) en de jaarverslagen van de AIVD.
In algemene zin kan worden aangegeven dat het kabinet, onder meer in het CSBN 2016 heeft geconstateerd dat statelijke actoren steeds meer inzetten op digitale middelen voor spionage-, beïnvloedings- en sabotagedoeleinden. Zoals in jaarverslagen van de AIVD is vermeld wordt Nederland misbruikt als doorvoerhaven voor digitale aanvallen. Nederland beschikt over veel bandbreedte, een van 's werelds grootste internetknooppunten en legio mogelijkheden voor het huren van server(ruimte)s.

Vraag 3
Klopt het dat dit soort aanvallen niet kunnen worden voorkomen? Zo nee, waarom niet? Wat wordt ondernomen teneinde dergelijke aanvallen zoveel mogelijk te voorkomen?

[1] Nos.nl, 2 januari 2017, http://nos.nl/l/2151180

ah-tk-20162017-1184
ISSN 0921 - 7398
's-Gravenhage 2017

Antwoord 3
Het wijdverspreide en steeds toenemende gebruik van digitale technologie maakt het onmogelijk om alle digitale aanvallen te voorkomen. Wat betreft het voorkomen van dergelijke aanvallen, voor zover zij zijn gericht op politieke partijen, verwijzen wij u naar het antwoord op vraag 2 in de beantwoording van de vragen van de van de vaste Kamercommissie voor Binnenlandse Zaken van 23 januari 2017.[2] Het verhogen van bewustzijn rondom cybersecurity neemt hierin een belangrijke plaats in.
Verwezen zij in dit verband ook naar het bij uw Kamer aanhangige voorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten. Met de modernisering van deze wet zal de overheid op grotere schaal zicht kunnen krijgen op digitale aanvallen, daardoor de reikwijdte daarvan eerder kunnen vaststellen en beter in staat zijn tegenmaatregelen te treffen.

Vraag 4
Klopt het dat spionnen gebruik hebben gemaakt van kwetsbaarheden in het mailverkeer van de Amerikaanse Democratische partij? Hoe worden dergelijke kwetsbaarheden in het Nederlandse mailverkeer voorkomen of opgelost?

Antwoord 4
Ten aanzien van de Russische activiteiten en intenties jegens de Amerikaanse presidentsverkiezingen verwijs ik naar het openbare rapport dat de Amerikaanse inlichtingengemeenschap op 6 januari jl.publiceerde.
Zoals ook aangegeven in reactie op eerdere vragen van de vaste Kamercommissie voor Binnenlandse Zaken met name vraag 2, zijn politieke partijen zelf primair verantwoordelijk voor het organiseren van hun informatiebeveiliging. Wel werkt het kabinet, zoals eveneens is aangegeven, permanent aan het vergroten van het bewustzijn rondom cybersecurity, in het bijzonder ook in relatie tot de verkiezingen in maart 2017. Zo is er in dat verband bijvoorbeeld vanuit de NCTV, in samenwerking met de inlichtingen- en veiligheidsdiensten, contact met politieke partijen over hun digitale veiligheid.

[2] Kamerstuk 26 643, nr. 441, Brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, 23 januari 2017 (https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2017Z00892&did=2017D01817).