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

2062

Vragen van het lid **Middendorp** (VVD) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over *de internationale cyberaanval en de ICT van de Overheid* (ingezonden 18 mei 2017).

Antwoord van Minister **Plasterk** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 12 juni 2017).

Vraag 1
Kent u het bericht «Waarschuwing voor grote internationale gijzelsoftware-campagne»?[1]

Antwoord 1
Ja

Vraag 2 en 3
Wat wordt er op dit moment concreet gedaan om te zorgen dat ICT-systemen van de rijksoverheid zelf niet geïnfecteerd raken?
Is alle software bij de rijksoverheid voldoende veilig en actueel? Zo nee, welke actie gaat u hiervoor ondernemen?

Antwoord 2 en 3
Mij zijn geen gevallen bekend van besmettingen bij de rijksoverheid. Ook bij het Nationaal Cyber Security Centrum (NCSC) zijn geen besmettingen gemeld, zoals de Minister van Veiligheid en Justitie in zijn brief van 2 juni heeft aangegeven. Niettemin heeft de aanval van Wannacry malware en zijn impact ertoe geleid dat bij verschillende organisaties van de Rijksdienst is en wordt nagelopen of ook echt op alle relevante plekken de relevante patches zijn toegepast.
Meer in het algemeen is bij de Rijksdienst een stelsel van regelgeving voor informatiebeveiliging van toepassing. Maar daarmee zijn we er niet. In de strategische I-agenda Rijksdienst is daarom «Verstandige aandacht voor informatiebeveiliging en privacy» één van de vijf thema's.
Verder informeert en waarschuwt het NCSC organisaties binnen de rijksoverheid zodat ook een dreiging van een passend antwoord kan worden voorzien.

[1] http://nos.nl/artikel/2172840-waarschuwing-voor-grote-internationale-gijzelsoftware-campagne.html

ah-tk-20162017-2062
ISSN 0921 - 7398
's-Gravenhage 2017

Ten slotte wil ik opmerken dat beveiliging en beheer van ICT een cyclisch proces is. Dat betekent dat acties ten behoeve van beveiliging niet eenmalig zijn, maar voortdurend, en met regelmaat terugkeren.

Vraag 4
Kan er een overzicht verstrekt worden van de ICT-systemen die draaien onder de verantwoordelijkheid van Binnenlandse Zaken en Koninkrijksrelaties met een beeld van de laatste stand? Hoe wordt het delen van expertise over het voorkomen van dit soort cyberaanvallen met andere ministeries georganiseerd?

Antwoord 4
Ik beschik over een omvangrijk overzicht van alle ICT-systemen waarvoor ik opdrachtgever en verantwoordelijk ben. Dit overzicht is zeer divers van aard, en bevat naast de grote systemen zoals DigiD ook een veelheid aan componenten die ten dienste staan van de (interne) bedrijfsvoering of kleinere systemen; alles bij elkaar bestaat dit overzicht uit ongeveer 800 elementen. Wat betreft de stand van zaken: van alle elementen in dit overzicht is mijn beeld dat zij niet getroffen zijn door het Wannacryvirus.
De rijksoverheid maakt gebruik van de expertise van het NCSC. Hierbij verwijs ik nogmaals naar de hiervoor genoemde brief van mijn collega van Veiligheid en Justitie.

Vraag 5
Welke lessen trekt u uit deze cyberaanval? Wat gaat de rijksoverheid anders doen inzake de eigen ICT-systemen ten opzichte van de huidige aanpak, om ervoor te zorgen dat de Rijks- en mede-overheden in de toekomst niet geraakt worden door cyberaanvallen?

Antwoord 5
Zoals ik hierboven opmerkte, zijn mij geen gevallen bekend van Wannacry besmettingen bij de rijksoverheid. Niettemin constateert de Algemene Rekenkamer helaas ook tekortkomingen in de informatiebeveiliging. De CIO-Rijk is hierover in gesprek met de CIO's, waarbij specifieke aandachtspunten per departement worden besproken. In het tweede halfjaarlijkse gesprek zal de CIO Rijk de voortgang bespreken op deze aandachtspunten. De Kamer zal eveneens over de voortgang worden geïnformeerd.
Ten aanzien van medeoverheden geldt dat informatiebeveiliging een verantwoordelijkheid is het betreffende bestuursorgaan, dat dus ook zelf verantwoordelijk voor het nemen van eventuele extra maatregelen.