Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

Aanhangsel van de Handelingen

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

2127

Vragen van het lid **Belhaj** (D66) aan de Minister van Defensie over *het bericht dat het Pentagon hackers uitnodigt de digitale beveiliging te doorbreken* (ingezonden 4 maart 2016).

Antwoord van Minister **Hennis-Plasschaert** (Defensie) (ontvangen 1 april 2016).

Vraag 1, 2
Wat is uw reactie op het bericht «Ministerie van Defensie VS: hack ons»?[1] Hoe beoordeelt u de aanpak van het Pentagon om hackers uit te nodigen de digitale beveiliging van het ministerie te doorbreken? Kunt u uw antwoord toelichten?

Antwoord 1, 2
Ik heb kennis genomen van het bericht. Het «Hack the Pentagon»-initiatief van het Amerikaanse Ministerie van Defensie past in het «Cybersecurity National Action Plan» dat president Obama in februari heeft ontvouwd.[2] Het gaat overigens nog slechts om een *pilot*-programma, in het kader waarvan gekwalificeerde en vooraf geregistreerde *hackers* gedurende een gelimiteerde periode worden uitgenodigd de veiligheid van de openbare websites van het ministerie te testen. Andere digitale systemen zijn uitdrukkelijk van de *pilot* uitgezonderd.

Vraag 3
Bent u bereid de Tweede Kamer te zijner tijd te informeren over de uitkomsten van de aanpak van het Pentagon?

Antwoord 3
Het *pilot*-programma gaat in april van start. Mocht het Amerikaanse Ministerie van Defensie de uitkomsten openbaar maken, dan ben ik gaarne bereid deze te zijner tijd met uw Kamer te delen.

[1] NOS, 3 maart 2016, http://nos.nl/artikel/2090319-ministerie-van-defensie-vs-hack-ons.html.
[2] US White House, 9 februari 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

ah-tk-20152016-2127
ISSN 0921 - 7398
's-Gravenhage 2016

Vraag 4, 5
Vindt u het verstandig om deze nieuwe aanpak die het Pentagon hanteert ook in Nederland te proberen? Zo nee, waarom niet?
Hoe beoordeelt u de aanpak van betalen per gevonden lek? Is het raadzaam om dit ook toe te passen voor Defensie?

Antwoord 4, 5
Het gaat om een vernieuwend initiatief, waarvan de resultaten mogelijk ook voor ons land interessant zijn. Alvorens een dergelijke aanpak echter in Nederland kan worden overwogen, zullen de risico's en de kansen zorgvuldig tegen elkaar moeten worden afgewogen. De ervaringen in de Verenigde Staten met het *pilot*-programma kunnen bij deze afweging behulpzaam zijn. Mocht Defensie tot een soortgelijke aanpak willen overgaan, dan zal de Tweede Kamer hierover worden geïnformeerd.
Als er kwetsbaarheden worden gevonden, kunnen deze volledig publiekelijk bekend worden gemaakt (*full disclosure*) of op een meer beheerste wijze (*responsible disclosure*). In het geval van *full disclosure* bestaat de kans dat het veiligheidsrisico groter wordt, doordat bijvoorbeeld ook tegenstanders of criminelen worden geattendeerd op een kwetsbaarheid. Mede om deze reden heeft het kabinet voor de aanpak van *responsible disclosure* gekozen (Kamerstuk 26 643, nr. 264). Deze door het Nationaal Cyber Security Centrum (NCSC) opgestelde leidraad dient om het toepassen van *responsible disclosure* bij alle partijen te stimuleren. Bij het opstellen van deze leidraad zijn zowel onderzoekers als publieke en private partijen betrokken. In de *cybersecurity*-aanpak van Defensie is het betalen per gevonden lek op dit ogenblik niet van toepassing.

Vraag 6
Op welke wijze vindt er op dit moment samenwerking plaats tussen uw ministerie en hackers? Kunt u uw antwoord toelichten?

Antwoord 6
Er is geen consensus over de vraag wanneer iemand zich een «hacker» kan noemen. Vast staat wel dat onder de samenwerkingspartners van Defensie zich experts bevinden met dezelfde kennis en kwalificaties als personen die in het algemeen als «ethisch hacker» worden aangemerkt. In de voortgangsrapportage over de uitvoering van de Defensie Cyber Strategie van 15 maart 2016 (Kamerstuk 33 321, nr. 7) heb ik het belang van samenwerking nogmaals onderstreept. Nauwe samenwerking met nationale en internationale partners is van wezenlijk belang om de doelen van Defensie in het cyberdomein te bereiken. Defensie werkt in dat verband intensief samen met publieke en private partners, kennisinstellingen en de academische wereld in binnen- en buitenland.