Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019 **Aanhangsel van de Handelingen**

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

56

Vragen van het lid **Arno Rutte** (VVD) aan de Minister van Justitie en Veiligheid over *het artikel «New defense bill bans the U.S. government from using Huawei and ZTE tech»* (ingezonden 17 augustus 2018)

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid) (ontvangen 25 september 2018) Zie ook Aanhangsel Handelingen, vergaderjaar 2017–2018, nr. 3166.

Vraag 1
Kent u het artikel «New defense bill bans the U.S. government from using Huawei and ZTE tech»?[1]

Antwoord 1
Ja.

Vraag 2
Deelt u de analyse van de Amerikaanse regering dat het gebruik van Chinese apparatuur van 2 bepaalde fabrikanten, daar waar het gaat om een «substantieel of essentieel onderdeel van een system, evenals technologie die gebruikt wordt voor het routeren of bekijken van gebruikersdata» een gevaar kan vormen voor de nationale veiligheid en daarom verboden wordt? Zo ja, welke maatregelen gaan er door u genomen worden en op welke termijn? Zo nee, waarom is de Nederlandse veiligheidsafweging anders dan de Amerikaanse veiligheidsafweging?

Antwoord 2
De Nederlandse overheid beziet de risico's die verbonden zijn aan dergelijke producten en bedrijven op een zorgvuldige 'case by case' basis, waarbij in ieder geval de volgende criteria worden betrokken:
– Is er sprake van een statelijke actor die zich richt tegen Nederlandse belangen?
– is er sprake van wetgeving die een bedrijf verplicht om op enigerlei wijze samen te werken met die betreffende actor?

Nederland maakt hierin een eigenstandige afweging. Gezien de nationale veiligheidsbelangen en de belangen van het bedrijfsleven wordt niet

[1] https://techcrunch.com/2018/08/13/new-defense-bill-bans-the-u-s-government-from-using-huawei-and-zte-tech/

ah-tk-20182019-56
ISSN 0921 - 7398
's-Gravenhage 2018

vooruitgelopen of gespeculeerd over al dan niet mogelijke toekomstige maatregelen.

Vraag 3
Heeft u kennisgenomen van het feit dat het in het artikel genoemde verbod ook geldt voor Hytera, het bedrijf dat de technologie voor het netwerk en de portofoons voor C2000 levert?

Antwoord 3
Ja.

Vraag 4
Als in de Verenigde Staten het gebruik van technologie van Hytera voor communicatiediensten van de overheid als een gevaar voor de nationale veiligheid wordt gezien, hoe kan de Nederlandse nationale veiligheid dan na ingebruikname van het nieuwe C2000 wél gewaarborgd zijn?

Antwoord 4
Zoals eerder aan uw Kamer is gemeld[2] wordt C2000 gebruikt voor de reguliere communicatie tussen de hulpverleningsdiensten: politie, brandweer, ambulance en Koninklijke Marechaussee. Het beveiligingsniveau voor deze gebruikersgroepen is bepaald op het niveau «departementaal vertrouwelijk». Ook het beveiligingsniveau van het vernieuwde netwerk zal als zodanig worden ingericht. De communicatie via het C2000-netwerk is versleuteld en maakt gebruik van afgeschermde verbindingen. Er zijn bij het classificatieniveau passende maatregelen genomen om sabotage te herkennen en te voorkomen. Versleuteling gebeurt door de leveranciers van de randapparatuur en deze versleuteling wordt door de politie in het netwerk gezet. Gebruikers bepalen zelf de leveranciers van de randapparatuur. Gebruikers kunnen extra versleuteling toepassen indien nodig.
Gelet op de vragen die zijn gerezen door de betrokkenheid van een Chinese aandeelhouder bij de ontwikkeling van C2000 heb ik Xebia gevraagd om een security audit uit te voeren op de technische ICT-oplossing die Hytera als onderdeel van de vernieuwing van C2000 realiseert. Daarnaast ben ik in gesprek met het Nationaal Bureau Verbindingsbeveiliging (NBV) van de AIVD om mij hierover te adviseren. Ik zal passende maatregelen nemen wanneer daartoe aanleiding is.
Uiteraard houd ik de veiligheid van de systemen die gebruikt worden goed in de gaten en heeft het kabinet aandacht voor ontwikkelingen in technologieën en kwetsbaarheden daarin, en de noodzaak scherp te blijven op de beveiliging hiervan. Ook de internationale ontwikkelingen rond Chinese technologiebedrijven worden door mijn departement gevolgd.

Vraag 5
Overweegt u, in navolging op het verbod op Kaspersky software bij overheidsdiensten, ook in Nederland een verbod op het gebruik van essentiële diensten van Chinese makelij? Zo ja, welke consequenties heeft zo'n besluit voor de korte en de middellange termijn, in het bijzonder met het oog op C2000? Zo nee, waarom niet?

Antwoord 5
Zie het antwoord op vraag 2.
Het dreigingsbeeld op het terrein van digitale risico's heeft geleid tot een aangescherpte afweging ten aanzien van het gebruik van specifieke digitale producten en diensten. Nederland maakt hierin een eigenstandige afweging, op basis van factoren zoals deze ook bij het nemen van de voorzorgsmaatregel rondom Kaspersky antivirussoftware zijn gebruikt.

[2] Kamerstuk 25 124, nr. 90