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

3537

Vragen van het lid **Verhoeven** (D66) aan de Ministers van Buitenlandse Zaken en van Justitie en Veiligheid over *het bericht «WhatsApp Rushes to Fix Security Flaw Exposed in Hacking of Lawyer's Phone»* (ingezonden 29 mei 2019).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid), mede namens de Minister van Buitenlandse Zaken (ontvangen 26 juli 2019). Zie ook Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 3137.

Vraag 1
Bent u bekend met het artikel «WhatsApp Rushes to Fix Security Flaw Exposed in Hacking of Lawyer's Phone?[1]

Antwoord 1
Ja.

Vraag 2
Bent u bekend met de hacksoftware van NSO Group? Wat is uw mening over de wenselijkheid van het bestaan van een markt in hacktools die apparaten en software die gebruikt worden door honderden miljoenen mensen, onveilig houden door gevonden onbekende kwetsbaarheden niet te laten dichten, maar open te houden om te kunnen hacken?

Antwoord 2
Ik ben er mee bekend dat de NSO Group software produceert die kan worden gebruikt om geautomatiseerde werken binnen te dringen.
Het is onwenselijk dat apparaten of software die door miljoenen mensen worden gebruikt kwetsbaar zijn. De omvang en complexiteit van software voor maatschappelijk gebruik is fors toegenomen. Veel gebruikte applicaties hebben tegenwoordig tientallen miljoenen regels broncode. Kwetsbaarheden zijn daarom talloos en wijdverbreid.[2] Het beleid van de regering is gericht op een open, vrij en veilig internet en daarmee op vermindering van het aantal onbekende kwetsbaarheden.[3] Uitgangspunt is dat onbekende kwetsbaarhe-

[1] https://www.nytimes.com/2019/05/13/technology/nso-group-whatsapp-spying.html
[2] Kamerstuk 26 643, nr. 428, p. 2
[3] Kamerstuk 34 372, nr. G, p. 4

ah-tk-20182019-3537
ISSN 0921 - 7398
's-Gravenhage 2019

den aan de leverancier of fabrikant worden gemeld.[4] De overheid stimuleert het melden van kwetsbaarheden, onder meer met het beleid voor *responsible disclosure*. Het is aan de producent om deze kwetsbaarheid te verhelpen door herstel van zijn software aan te bieden door een patch of update en het is vervolgens aan de gebruiker om zijn software te updaten.[5]
De verkoop van binnendringsoftware aan bepaalde partijen, waaronder regimes die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht, is onwenselijk. De regering wil bovendien de markt voor onbekende kwetsbaarheden niet bevorderen, dat zou negatieve gevolgen voor de veiligheid van het internet kunnen hebben.[6] Nederland spant zich internationaal in om cybersurveillancegoederen in relatie tot mensenrechtenschendingen onder exportcontrole te brengen. Zie hiervoor mijn antwoord op vraag 5.

Vraag 3
Bent u het ermee eens dat wereldwijd hacksoftware, waaronder hacksoftware gemaakt door NSO Group, gebruikt wordt om dissidenten, journalisten en mensenrechtenactivisten af te luisteren? Wat is uw mening over deze ontwikkeling? Kunt u daarbij ook ingaan op het onderzoek van de Electronic Frontier Foundation en Citizen Lab over het gebruik van hacksoftware van NSO Group in Mexico?

Antwoord 3
Het onderzoek van de Electronic Frontier en Citizen lab schrijft over het gebruik van binnendringsoftware bij het schenden van de mensenrechten van mensenrechtenverdedigers en journalisten. Het kabinet wijst dergelijke schendingen af, ongeacht of hierbij gebruik wordt gemaakt van binnendringsoftware of niet.

Vraag 4
Kunt u uitsluiten dat NSO Group hacksoftware verkoopt aan dubieuze regimes? Kunt u een lijst geven van landen waarvan u zeker weet dat zij hacksoftware hebben gekocht van NSO Group?

Antwoord 4
Ik heb geen inzicht in het klantenbestand van de NSO Group en kan dus geen uitspraken doen over het verkoopbeleid van de NSO Group.

Vraag 5
Aan welke regelgeving omtrent de export van hacksoftware moeten Europese bedrijven die dergelijke software maken voldoen? Bent u van mening dat deze regelgeving voldoende is om misstanden te voorkomen, zoals het misbruik van hacksoftware om dissidenten, journalisten of mensenrechtenactivisten af te luisteren?

Antwoord 5
Bepaalde cybersurveillancegoederen en -technologieën staan ingevolge het potentiele gebruik in civiele of militaire toepassingen onder exportcontrole. Dit geldt ook voor goederen voor het maken en besturen van binnendringsoftware. Verder is de verkoop van technologie voor de ontwikkeling van «intrusion software», software die gebruik maakt van kwetsbaarheden, onderhevig aan exportcontrole op grond van afspraken in het Wassenaar Arrangement. Deze goederen zijn hierdoor opgenomen in de controlelijst van de Europese Dual-use verordening. Een bedrijf dat binnen de EU gevestigd is, is verplicht voor het exporteren van deze goederen en technologie buiten de EU een vergunning aan te vragen. Vergunningen kunnen worden afgewezen indien er zorgen bestaan ten aanzien van het eindgebruik in relatie tot mensenrechtenschendingen. Nederland spant zich internationaal in om aanvullend cybersurveillancegoederen in relatie tot mensenrechtenschendingen onder exportcontrole te brengen. In het Wassenaar Arrangement vergt dit consensus van alle deelnemende landen.

---

[4] Kamerstuk 34 372, nr. G, p. 4
[5] Kamerstuk 34 372, nr. G, p. 4
[6] Kamerstuk 34 372, nr. G, p. 11

Vraag 6
Bent u het ermee eens dat de Nederlandse overheid geen hacksoftware zou moeten kopen die tevens gebruikt wordt door dubieuze regimes of voor het afluisteren van journalisten, dissidenten of mensenrechtenactivisten?

Antwoord 6
Als Minister van Justitie en Veiligheid kan ik mij alleen uitlaten over de Nederlandse opsporing. Voor de opsporing van strafbare feiten zijn in het huidige Regeerakkoord «Vertrouwen in de toekomst» afspraken gemaakt voor de aanschaf van binnendringsoftware. Voor de uitvoering van de Wet Computercriminaliteit III komt 10 miljoen euro extra beschikbaar. Daarbij zal slechts in een specifieke zaak hacksoftware worden ingekocht door opsporingsdiensten. Leveranciers van dergelijke software worden gescreend door de AIVD en leveren niet aan dubieuze regimes. [7] Het gaat dan om landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht.[8] Om deze reden voert de politie een toets uit voordat over wordt gegaan tot de aanschaf van binnendringsoftware. In deze toets wordt de leverancier gevraagd niet te hebben geleverd aan landen waartegen vanuit de EU of de VN restrictieve sancties bestaan en wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontroleregime bestaat waar mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning.

[7] Regeerakkoord 2017–2021 Vertrouwen in de Toekomst
[8] Handelingen I 2017/18, 34, item 5, p. 29