Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

Aanhangsel van de Handelingen

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

286

Vragen van de leden **Berndsen-Jansen** en **Verhoeven** (beiden D66) aan de Minister van Veiligheid en Justitie over *het hacken van servers door de politie terwijl de zogenaamde «hackwet» nog niet door de Kamer is behandeld* (ingezonden 26 augustus 2014).

Antwoord van Minister **Opstelten** (Veiligheid en Justitie) (ontvangen 20 oktober 2014). Zie ook Aanhangsel Handelingen, vergaderjaar 2013–2014, nr. 34.

Vraag 1
Klopt de berichtgeving dat een groot internationaal onderzoek loopt naar Blackshades, software waarmee onder meer malware kan worden gemaakt?[1]

Antwoord 1
De berichtgeving klopt in zoverre dat in diverse Europese landen, de VS en Canada strafrechtelijke onderzoeken hebben gelopen of lopen tegen (ver)kopers en/of verspreiders en/of vervaardigers van software die hoofdzakelijk geschikt is gemaakt of ontworpen is tot het plegen van kort gezegd computercriminaliteit als bedoeld in de artikelen 138ab, eerste lid, 138b en 139c WvSr.

Vraag 2
Heeft het Openbaar Ministerie (OM) in het kader van onderzoek naar Blackshades opdracht gegeven tot het hacken van de server van Blackshades? Zo ja, kunt u toelichten wat de wettelijke basis is van die opdracht en op grond waarvan die opdracht geoorloofd is?

Antwoord 2
Het Openbaar Ministerie heeft geen opdracht gegeven om de server van Blackshades te betreden. De politie heeft onder verantwoordelijkheid van het Openbaar Ministerie en na daartoe te zijn gemachtigd door een rechter-commissaris op afstand een server betreden en deze server vervolgens doorzocht ter vastlegging van gegevens op grond van artikel 125i van het Wetboek van Strafvordering.
Het is onder bepaalde omstandigheden op basis van artikel 125i van het Wetboek van Strafvordering met een machtiging van de rechter-commissaris

[1] http://www.nu.nl/weekend/3858563/huiszoeking-aanschaffen-omstreden-software.html

ah-tk-20142015-286
ISSN 0921 - 7398
's-Gravenhage 2014

mogelijk om op afstand een computersysteem te betreden, met als uitsluitende doel de computer te doorzoeken op vooraf bepaalde gegevensbestanden en deze zonodig in beslag te nemen door ze vast te leggen. In twee strafzaken waarin het ging om zeer ernstige feiten is hiervan sprake geweest. Ik verwijs tevens naar de beantwoording van de vragen van het lid Gesthuizen (SP) aan de Minister van Veiligheid en Justitie over het gebruik van omstreden spionagesoftware door de politie (Aanhangsel Handelingen, vergaderjaar 2014–2015, nr. 202).

Vraag 3
Hoe vaak heeft het OM tot op heden aan de politie opdracht gegeven servers en computers te hacken in het kader van een opsporingsonderzoek en waar was in die gevallen de bevoegdheid tot het hacken op gebaseerd?

Antwoord 3
De politie verricht opsporingsonderzoek op basis van het Wetboek van Strafvordering. De term «hacken» komt daarin niet voor. De politie heeft, zoals in het antwoord op de vorige vraag beschreven, op basis van artikel 125i van het Wetboek van Strafvordering in slechts enkele (uitzonderlijke) gevallen, met machtiging van de rechter-commissaris, een geautomatiseerd systeem betreden en gegevens van een server waarvan de locatie en het eigenaarschap onbekend waren, veilig gesteld. Een van die onderzoeken betreft het onderzoek Blackshades.

Vraag 4 en 5
In hoeverre is het huidige Wetboek van Strafrecht en het Wetboek van Strafvordering toereikend als wettelijke grondslag voor het door de politie toegang verschaffen tot servers en computers van verdachten?
Klopt het dat uw voorstel tot «Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)» juist beoogt in een wettelijke grondslag te voorzien voor het hacken van servers en computers door justitie ten behoeve van het opsporingsonderzoek? Zo ja, hoe verhoudt de huidige praktijk waarin opdracht wordt gegeven tot het hacken van een server in kader van een opsporingsonderzoek, zich tot dit wetsvoorstel?

Antwoord 4 en 5
De huidige wettelijke regeling, zoals toegelicht in het antwoord op vraag 2, dient te worden aangevuld, hetgeen gebeurt in het wetsvoorstel Computercriminaliteit III. Doel van dat wetsvoorstel is het juridisch kader voor de opsporing en vervolging van cybercrime meer toe te snijden op de opsporing en vervolging van computercriminaliteit en de nieuwe werkwijzen van criminelen. De huidige samenleving en de snelle veranderingen van techniek om met elkaar te communiceren en informatie te delen of op te slaan overal ter wereld, vereisen dat opsporingsautoriteiten met die veranderingen mee ontwikkelen (zie ook mijn brief van 15 oktober 2012 aan de kamer inzake wetgeving bestrijding cybercrime)(Kamerstuk 28 684, nr. 363).
Het wetsvoorstel voorziet naast diverse veranderingen en aanvullingen in een nieuwe bevoegdheid waarin een opsporingsambtenaar zich, na een daartoe gegeven bevel van een officier van justitie, onder strikte voorwaarden heimelijk en op afstand de toegang mag verschaffen tot een geautomatiseerd werk om in dat geautomatiseerde werk bepaalde bevoegdheden toe te passen. Dit binnendringen in een geautomatiseerd werk is een verdergaande bevoegdheid dan het doorzoeken ervan en noodzakelijk voor de opsporing van veel vormen van internetcriminaliteit.

Vraag 6
Op welke termijn verwacht u het wetsvoorstel «computercriminaliteit III», dat sinds mei 2013 in consultatie is, bij de Tweede Kamer in te dienen?

Antwoord 6
Het wetsvoorstel wordt begin volgend jaar ingediend bij de Tweede Kamer.