Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

Aanhangsel van de Handelingen

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

## 751

Vragen van het lid **Berndsen-Jansen** (D66) aan de minister van Veiligheid en Justitie over *de hackplannen van de minister* (ingezonden 14 november 2012).

Antwoord van minister **Opstelten** (Veiligheid en Justitie) (ontvangen 7 december 2012). Zie ook Aanhangsel Handelingen, vergaderjaar 2012–2013, nr. 739

Vraag 1
Heeft u kennisgenomen van het artikel in het Nederlands Juristenblad waarin ernstige kanttekeningen worden geplaatst bij uw plannen om de politie computers te laten hacken?[1]

Antwoord 1
Ja.

Vraag 2
Wat is uw reactie op de kritiek in het artikel dat door het plaatsen van zogenoemde «policeware» op computers sprake is van een vorm van identiteitsdiefstal door opsporingsinstanties?

Antwoord 2
In mijn brief van 5 oktober 2012 (Kamerstukken 2012/13, 28 684, nr. 363) heb ik aangegeven dat opsporingsinstanties op afstand een geautomatiseerd werk binnen zouden moeten kunnen treden ten behoeve van de opsporing van ernstige strafbare feiten. In het artikel wordt door de auteur betoogd dat het plaatsen van zogenaamde *policeware* niet alleen computervredebreuk omvat, maar ook identiteitsfraude. Voor het installeren van *policeware*op de computer zijn immers gebruikersrechten nodig. Hierbij is volgens de auteur sprake van totale controle over de computer. In reactie op deze kritiek merk ik op dat het binnentreden, genoemd in mijn brief, is gericht op het vaststellen van het strafbaar handelen van de verdachte en niet op het onder de identiteit van de verdachte verrichten van handelingen teneinde bij derden de indruk te wekken dat de verdachte die handelingen verricht. In die zin is er naar mijn mening geen sprake van identiteitsdiefstal.
Wel is het juist dat er handelingen worden verricht om toegang te verkrijgen tot gegevensbestanden van de verdachte. Dit handelen in het kader van de opsporing dient op zodanige wijze te worden vastgelegd dat achteraf

[1] Nederlands Juristenblad, 9 november 2012, «Policeware»

ah-tk-20122013-751
ISSN 0921 - 7398
's-Gravenhage 2012

verantwoording kan worden afgelegd over de rechtmatigheid van de bewijsverkrijging. Essentieel hierbij is dat de handelingen van de politie controleerbaar zijn. Dat wil zeggen dat deze handelingen worden vastgelegd ten behoeve van de verantwoording van opsporingshandelingen in een strafzaak. In dat kader zal ook nader onderzocht worden in hoeverre gebruik kan worden gemaakt van een *secure logging* faciliteit. Dit vormt uiteraard ook onderwerp van de voorbereiding van het wetsvoorstel, waar ik thans niet op kan vooruitlopen. Overigens kan nog worden opgemerkt dat in relatie tot rechtmatig politieoptreden bezwaarlijk kan worden gesproken van identiteitsfraude. Immers, de politie is ook bevoegd tot huiszoeking en pleegt daarbij geen huisvredebreuk. Met de voorgenomen wetswijziging zal de politie geen strafbare handeling plegen wanneer een computer wordt betreden en doorzocht, omdat het vereiste van de wederrechtelijkheid ontbreekt.

Vraag 3
Hoe beschouwt u de praktische problemen waar in het artikel op wordt gewezen, in het bijzonder ten aanzien van de rol van de rechter-commissaris die, gezien de digitale aard van hacking, niet als vergelijkbaar kan worden geacht met de «off line» werkelijkheid van huiszoeking?

Antwoord 3
Met betrekking tot de rol van de rechter-commissaris zijn de verschillen tussen de analoge en digitale wereld mijns inziens niet zo groot als de auteur in zijn artikel stelt. Ook nu is het reeds zo dat de rechter-commissaris voorafgaand aan een doorzoeking van een woning zijn toestemming moet verlenen en de beperkingen aangeeft. Hij is daarbij niet altijd daadwerkelijk aanwezig bij de operatie. Daar komt bij dat ook nu de rechter-commissaris reeds machtigingen dient af te geven voor het plaatsen van technisch geavanceerde hulpmiddelen als een internettap of een richtmicrofoon.
Het argument dat verdachten later kunnen aanvoeren dat de politie belastende informatie zelf creëert en op de computer van de verdachte heeft geplaatst is, zoals bij de beantwoording van vraag 2 reeds aan de orde is gekomen, op zichzelf niet nieuw. De door de auteur genoemde risico's worden serieus genomen. Bij de voorbereiding van de wettelijke regeling zal de nodige aandacht worden besteed aan de praktische problemen rond de toepassing van deze bevoegdheid. Daarbij zal ook de *secure logging* faciliteit worden betrokken.

Vraag 4
Hoe verhoudt het plaatsen van «policeware» op computers zich tot antivirussoftware waarmee ook «policeware» kan worden gedetecteerd op de computer/tablet/smart phone van burgers? Kan de antivirussoftware deze «policeware» gewoon verwijderen of bent u voornemens van antivirusbedrijven te eisen dat zij dergelijke policeware niet detecteren, vermelden en verwijderen en daarmee onvolledige bescherming bieden aan hun klanten?

Antwoord 4
Het voorkomen van het ontdekken door antivirussoftware van de door de auteur genoemde «*policeware»* is een gecompliceerd technisch probleem. De verhouding tussen het plaatsen van *policeware* en het functioneren van antivirus*software*wordt, als onderdeel van de praktische problemen rond de toepassing, betrokken bij de voorbereiding van het wetsvoorstel.

Vraag 5
Wat vindt u van het idee om, net als in Duitsland, in wetgeving te expliciteren dat grondrechten van burgers, zoals bijvoorbeeld het recht op confidentialiteit en integriteit van eigen computersystemen, worden gewaarborgd en inbreuken onder specifieke omstandigheden vanuit dit uitgangspunt steeds gerechtvaardigd moeten zijn?

Antwoord 5
Bij het heimelijk op afstand binnendringen van een geautomatiseerd werk door de opsporingsdiensten, kunnen verschillende grondrechten in het geding zijn. Dit betreft het recht op eerbiediging van de persoonlijke levenssfeer (art. 10 WG) en de onschendbaarheid van het briefgeheim (art. 13 GW). Deze grondrechten zijn niet absoluut, beperking van deze rechten is

onder omstandigheden mogelijk, mits bij wet voorzien. Het belang van de opsporing van strafbare feiten vormt een zwaarwegend algemeen belang dat aanleiding kan vormen tot het stellen van beperkingen aan de bovengenoemde grondrechten. De regeling van het aftappen en opnemen van telecommunicatie in het Wetboek van Strafvordering (art. 126m/t Sv), vormt daarvan een voorbeeld. In het licht van de geldende grondrechten zie ik weinig meerwaarde in een explicitering in wetgeving dat de confidentialiteit en integriteit van eigen computersystemen worden gewaarborgd en dat inbreuken op dit recht onder specifieke omstandigheden gerechtvaardigd moeten zijn. De bevoegdheid tot het op afstand heimelijk doorzoeken van geautomatiseerde werken ten behoeve van de opsporing van ernstige strafbare feiten zal met strikte waarborgen worden omkleed. In het wetsvoorstel zal zorgvuldig worden omschreven wanneer, hoe en onder welke omstandigheden gebruik kan worden gemaakt van de opsporingsbevoegdheden. Dit biedt de burger waarborgen voor een zorgvuldige toepassing van de nieuwe bevoegdheden.
Wat niet in het artikel van de auteur vermeld staat, maar wat ik voor de volledigheid wel wil opmerken, is dat in de Duitse wetgeving een bevoegdheid is opgenomen tot het op afstand doorzoeken van computers. Dit betreft de zogenaamde Verdeckter Eingriff in informationstechnische Systeme, die onder bepaalde voorwaarden kan worden verricht door het Bundeskriminalamt (§ 20k BKAG). Daarmee wordt dus inbreuk gemaakt op het door de auteur aangehaald recht op confidentialiteit en integriteit van eigen computersystemen. Daarbij is voorzien in een uitgebreide protocolverplichting.

Vraag 6
Hoe beschouwt u de suggestie om in geval van criminele hackers over te gaan tot het reactief verstoren van de ICT-infrastructuur van aanvallers indien sprake is van een acuut bedreigende agressie?

Antwoord 6
Ik beschouw dit als een belangwekkende suggestie. In mijn eerdergenoemde brief aan Uw Kamer van 15 oktober, waarover ook de auteur in zijn artikel spreekt, ben ik nader ingegaan op de noodzaak van het op afstand ontoegankelijk maken van gegevens, ook als de gegevens zich in het buitenland bevinden. De auteur wijst op de noodzaak tot het ondernemen van snelle, effectieve actie tegen criminele *hackers* die uit het buitenland opereren. Deze verstoringsbevoegdheid zou reactief ingezet worden, in situaties waarin sprake is van aanvallen gericht tegen personen of infrastructuur in Nederland. Deze suggestie zal worden betrokken bij de voorbereiding van het eerdergenoemde wetsvoorstel.

Vraag 7
Bent u bereid deze vragen te beantwoorden voorafgaande aan het algemeen overleg in de Kamer over de nationale cyber security strategie op 29 november 2012?

Antwoord 7
Ja, nu dit algemeen overleg is geagendeerd op 6 december 2012