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

3199

Vragen van de leden **Oosenbrug** (PvdA) en **Verhoeven** (D66) aan de Staatssecretaris van Veiligheid en Justitie over *het gebruik van software van het Hacking Team door de Nationale Politie (NP)* (ingezonden 13 juli 2015).

Antwoord van Staatssecretaris **Dijkhoff** (Veiligheid en Justitie) (ontvangen 28 augustus 2015). Zie ook Aanhangsel Handelingen, vergaderjaar 2014–2015, nr. 3033

Vraag 1
Heeft u kennisgenomen van het bericht «Nationale Politie geïnteresseerd in spionagesoftware Hacking Team»?[1] Herinnert u zich antwoorden op eerdere vragen over vergelijkbare software van 13 oktober 2011 en 7 oktober 2014?[2]

Antwoord 1
Ja.

Vraag 2
Klopt het dat het bedrijf Hacking Team een productpresentatie zou houden voor de NP over hun producten? Is deze presentatie doorgegaan, na de ingrijpende inbraak bij het bedrijf?
Maakt de NP of andere overheidsdiensten al gebruik van de software van dit bedrijf? Zo ja, wat zijn de gevolgen van de inbraak voor dit gebruik?
Klopt het dat de programma's om computers binnen te dringen meer mogelijkheden hebben dan de wet in Nederland toestaat om te gebruiken? Zo ja, hoe verzekert u zich ervan dat de software die de NP bezit om computers binnen te dringen alleen gebruikt wordt voor de doeleinden die de wet nu al toestaat en niet voor verdergaande, onwettige doeleinden?
Beschikt de NP over de broncode van de software die ze gebruikt om computers binnen te dringen? Zo ja, is de robuustheid en de veiligheid van deze software op basis van de broncode onderzocht? Zo nee, hoe wordt de correcte en veilige werking van deze software dan gecontroleerd?
Zijn de inbraak bij het bedrijf Hacking Team, de daaruit gebleken ernstig tekortschietende beveiliging en de eerdere vraagtekens bij de deugdelijkheid van vergelijkbare software voor u aanleiding de keuring en de inzet van deze

[1] Nu.nl, 9 juli 2015
[2] Aanhangsel Handelingen, vergaderjaar 2011–2012, nr. 1374

ah-tk-20142015-3199
ISSN 0921 - 7398
's-Gravenhage 2015

categorie software te heroverwegen? Zo nee, waarom niet? Zo ja, welke concrete stappen gaat u zetten?

Antwoord 2, 3, 4, 5 en 6
Zoals eerder is aangegeven in de beantwoording op de vragen van het lid Oosenbrug (PvdA) over het gebruik van een softwarefout door de Amerikaanse inlichtingendiensten (kenmerk 2015Z09552), brengt het verstrekken van informatie over welke specifieke software de opsporingsdiensten beschikken, testen en gebruiken grote risico's met zich mee voor de inzetbaarheid van die middelen. Dit geldt dus ook voor het verstrekken van informatie omtrent de broncode, de robuustheid en de daarmee samenhangende veiligheidsvraagstukken. Ik kan hier derhalve geen informatie over verstrekken. Ik hecht er aan om te benadrukken dat er altijd gehandeld wordt binnen de bestaande wet- en regelgeving.
Voor het opsporen van bepaalde strafbare feiten kunnen op bevel van het Openbaar Ministerie (OM) bijzondere opsporingsbevoegdheden worden toegepast. Bij de inzet van dergelijke bevoegdheden dient het belang van de opsporing proportioneel te zijn aan de inbreuk die de bevoegdheid maakt op de persoonlijke levenssfeer van de verdachte of derden. Bovendien dient het te verkrijgen bewijs niet door de inzet van een andere, lichtere bevoegdheid te kunnen worden verkregen (subsidiariteit). Bij de inzet van ingrijpende bevoegdheden is machtiging van de rechter-commissaris vereist. De proportionaliteit en subsidiariteit van de inzet van de bevoegdheid, en het gebruik van het technisch hulpmiddel dat wordt ingezet ter uitvoering voor de bevoegdheid, worden hierbij getoetst.
De politie beschikt over software die fysiek geïnstalleerd kan worden op de computer van een verdachte, waarmee ten behoeve van opsporingsdiensten toegang kan worden verkregen tot die computer en waarmee gegevens daarvan kunnen worden overgenomen. De inzet van dit middel beperkt zich, gelet op de bepalingen van het Wetboek van Strafvordering, tot het opnemen van vertrouwelijke communicatie (op basis van artikel 126l van het Wetboek van Strafvordering). Inzet ten behoeve van een heimelijke doorzoeking van gegevensdragers is binnen de wettelijke kaders niet toegestaan. Voorts is het onder bepaalde omstandigheden op basis van artikel 125i van het Wetboek van Strafvordering op basis van een machtiging van de rechter-commissaris mogelijk om op afstand een computersysteem te betreden, met als uitsluitende doel de computer te doorzoeken op vooraf bepaalde gegevensbestanden en deze zo nodig in beslag te nemen door ze vast te leggen. In een aantal strafzaken waarin het ging om zeer ernstige feiten is hiervan sprake geweest.
Inzet kan slechts plaatsvinden na voorafgaande goedkeuring door het OM. Ik zie op dit moment geen aanleiding om het beleid dan wel wet- of regelgeving omtrent de keuring en de inzet van dergelijke middelen aan te passen. De beschikbare technische hulpmiddelen voor het opnemen van vertrouwelijke communicatie worden voorafgaand aan de inzet gekeurd door de onafhankelijke keuringsdienst van de politie. Deze keuring is voornamelijk gericht op de authenticiteit en integriteit van het middel.

Vraag 7
Heeft u inzicht in de fouten en de kwetsbaarheden die door de software van het bedrijf Hacking Team gebruikt wordt? Zo nee, hoe probeert u hierover informatie te krijgen? Zo ja, wat doen het Nationaal Cyber Security Centrum en de rijksoverheid teneinde deze kwetsbaarheden en de risico's die daaruit voortvloeien weg te nemen?

Antwoord 7
De bedrijfsinformatie van Hacking Team, die op 5 juli 2015 openbaar werd, bevatte informatie over meerdere onbekende kwetsbaarheden, zogenaamde zero-days. Zodra deze kwetsbaarheden in software bekend werden, heeft het Nationaal Cyber Security Centrum (NCSC) hierover beveiligingsadviezen uitgebracht. Uiteraard blijft het NCSC de situatie nauwgezet volgen. Daarnaast worden vanuit het NCSC, conform haar reguliere verantwoordelijkheden, onderdelen van rijksoverheid en (andere) vitale organisaties in het algemeen op frequente basis geadviseerd over kwetsbaarheden in hard- en software en de wijze waarop deze kunnen worden verholpen.

Vraag 8 en 9
Deelt u de mening dat cybersecurity het meest gebaat is bij het dichten van ontdekte kwetsbaarheden in plaats van het instandhouden waardoor zij ook voor kwaadwillenden en dubieuze regimes bruikbaar zijn?
Ziet u ethische en technische bezwaren tegen het gebruik door de overheid van software, die nog ongepubliceerde kwetsbaarheden in computersystemen gebruikt teneinde toegang te verschaffen? Zo nee, hoe oordeelt u dan over het misbruik door exploit-kits van de kwetsbaarheden die het bedrijf Hacking Team gebruikte en de klandizie voor deze software van dubieuze regimes? Zo ja, hoe wilt u bijdragen aan een veilige ICT-infrastructuur waarin fouten en zwakke plekken in software en hardware zo snel mogelijk verholpen worden?

Antwoord 8 en 9
Ik deel de mening dat cybersecurity het meest gebaat is bij het dichten van ontdekte kwetsbaarheden. Ter versterking van de digitale veiligheid van Nederland en het beperken van de criminaliteit stimuleert de Nederlandse overheid het melden van kwetsbaarheden, onder meer met het beleid voor responsible disclosure. Dit beleid stimuleert het op verantwoorde wijze en actief openbaar maken van kwetsbaarheden door overheid, bedrijfsleven, beveiligingsonderzoekers en ethische hackers en het samen werken aan het verhelpen van deze kwetsbaarheden. Internationaal hecht het kabinet ook veel waarde aan responsible disclosure en zal het belang daarvan dan ook blijven uitdragen.
Ook neemt Nederland wereldwijd een leidende rol in bij de beperking op uitvoer van ICT goederen en software naar regimes met een slechte staat van dienst op het gebied van mensenrechten via onder andere multilaterale fora als de Global Conference on Cyberspace 2015 en het statement over het gebruik en de export van surveillance technologie van de Freedom Online Coalition 4.
Zoals reeds is aangegeven in mijn beantwoording op de vragen 2 t/m 6, is het onder bepaalde omstandigheden mogelijk om ten behoeve van de opsporing toegang te verschaffen tot computersystemen. Dit dient echter altijd voorzien te zijn van een wettelijke basis en van solide waarborgen. Voor een nadere toelichting op de wijze waarop overheidsdiensten omgaan met kwetsbaarheden verwijs ik u graag naar de beantwoording van de vragen van het lid Oosenbrug (PvdA) over het gebruik van een softwarefout door de Amerikaanse inlichtingendiensten (kenmerk 2015Z09552).