[redacted] - BD/DGPOL/PBT/R&S

Van: [redacted] - BD/DGPOL/PBT/PT
Verzonden: woensdag 17 december 2014 16:05
Aan: [redacted]@politie.nl)
[redacted]@politie.nl)'; [redacted]@politie.nl)';
[redacted]@politie.nl)'; [redacted] - BD/DRC/CV
CC: [redacted]
Onderwerp: AO docs cybercrime jan 2015.docx
Bijlagen: AO docs cybercrime jan 2015.docx

Ha collega's,

Ik heb de q en a's voor het AO cybersecurity 22-1 die zien op politie ge-update en een paar nieuwe gemaakt (kwetsbaarheden en finfisher). De windows XP kan mi zo blijven.

[redacted], q en a's ihkv CC III bekijk jij?

Graag eerste werkweek januari (uiterlijk 7/1) jullie akkoord of wijzigingen. Dan verwerk ik deze op de 8e en zend het daarna door aan nctv.

Alvast dank, groet [redacted]

[redacted] - BD/DGPOL/PBT/R&S

Van: [redacted]@politie.nl> namens Bestuursondersteuning <Bestuursondersteuning@knp.politie.nl>
Verzonden: woensdag 17 september 2014 15:42
Aan: Parlementair - DGPOL; [redacted] BD/DGPOL/PBT/R&S
CC: Bestuursondersteuning
Onderwerp: Kamervragen spionagesoftware
Bijlagen: Antwoorden KV Spionagesoftware2014Z13948 OMenLE17sept.doc

[redacted]

Bijgaand vind je de conceptantwoorden + aanvullingen van de LE retour. Antwoorden zijn afgestemd met het OM. Wb vraag 7 daarop heb ik nog niet van alle eenheden reactie gekregen. Tussenstand is nu: Voor de Eenheden Noord-Holland, Noord-Nederland en Oost-Nederland en de Landelijke Eenheid is het antwoord op vraag 7 'nee' .

Gr.

[redacted]

Parlementaire zaken en Werkbezoeken
Politie | Den Haag | Staf | Bestuursondersteuning

Juliana van Stolberglaan 4-10, 2595 CL Den Haag

[redacted]

[redacted]

Van: [redacted]
Verzonden: woensdag 3 september 2014 16:16
Aan: [redacted] BD/DGPOL/PBT/R&S
Onderwerp: FW: Conceptbeantwoording Kamervragen over het gebruik van omstreden spionage .docx
Bijlagen: Conceptbeantwoording Kamervragen over het gebruik van omstreden spionage .docx

Hoi, [redacted] heeft wat tekstuele suggesties, zie bijlage. Ik vind zijn idee om eerst met 4 en 5 te beginnen wel een goed idee. Jij?

Met vriendelijke groet,

[redacted]
Coördinerend beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
Programma Politiële Taken

Turfmarkt 147 | 2511 DP | Den Haag | Noord 24e etage
Postbus 20301 | 2500 EH | Den Haag
.....
[redacted]
www.rijksoverheid.nl/venj
.....
Vrijdags afwezig
.....

Van: [redacted] - BD/PBT/PT
Verzonden: woensdag 3 september 2014 16:01
Aan: [redacted] - BD/PBT/PT
Onderwerp: Conceptbeantwoording Kamervragen over het gebruik van omstreden spionage .docx
Zie wat suggesties. M.i. beter beginnen met antwoorden die nu onder 4 en 5 staan (en dan samengevoegd0, dan de antwoorden van het 1e tekstblok en dan de rest. Dank, [redacted]

[redacted]

Van: [redacted]
Verzonden: dinsdag 9 juni 2015 12:31
Aan: Parlementair - DGPOL
CC: [redacted]@politie.nl); [redacted]@politie.nl); [redacted]- BD/DRC/CV
Onderwerp: FW: E-mail verzenden: kst-CVIII-N.pdf, Achtergrondinformatie kamervraag nr 2015Z09552.docx, Conceptantwoorden KV D66 encryptie zerodays 2jun2015.docx, Conceptantwoorden KV PvdA encryptie zerodays 2jun2015.docx
Bijlagen: Conceptantwoorden KV D66 encryptie zerodays 2jun2015.docx; Conceptantwoorden KV PvdA encryptie zerodays 2jun2015.docx; kst-CVIII-N.pdf; Achtergrondinformatie kamervraag nr 2015Z09552.docx

Collega, zou jij deze 2 setjes uit kunnen zetten bij de NP? De Kamervragen worden gecoördineerd door Nctv, DGRR heeft een voorzet gedaan voor beantwoording (dat is het antwoord in de D'66 set en hetgeen ik geel heb gemaakt in de PvdA set).

Het gaat om kamervragen over kwetsbaarheden (cyber). Hierover zijn eerder vragen gesteld finfisher. Eind 2014 is er blijkbaar een brief verzonden aan de TK waarin staat dat mivc en aivd belangendragers informeren bij constatering van een zero day. Vraag is nu of we dit ook zo (absoluut geformuleerd) kunnen doen in geval van politie. Tegelijkertijd is de lijn uitgezet en daarmee ook de verwachting naar wat politie zou moeten doen. Graag hoor ik van politie of politie zich kan vinden in de tekst, of dat er nuancering nodig is.

Alvast dank!

Met vriendelijke groet,

[redacted]
Coördinerend beleidsmedewerker

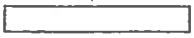
.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
Programma Politiële Taken

Turfmarkt 147 | 2511 DP | Den Haag | Noord 24e etage Postbus 20301 | 2500 EH | Den Haag
.....
[redacted]
[redacted]
www.rijksoverheid.nl/venj
.....
Vrijdags afwezig
.....

-----Oorspronkelijk bericht-----
Van: [redacted]- BD/DRC/CV
Verzonden: vrijdag 5 juni 2015 17:01
Aan: [redacted]- BD/DGPOL/PBT/PT; [redacted]@om.nl); [redacted]@klpd.politie.nl); [redacted]@knp.politie.nl); [redacted]@om.nl); [redacted]- BD/DRC/CV
Onderwerp: FW: E-mail verzenden: kst-CVIII-N.pdf, Achtergrondinformatie kamervraag nr 2015Z09552.docx, Conceptantwoorden KV D66 encryptie zerodays 2jun2015.docx, Conceptantwoorden KV PvdA encryptie zerodays 2jun2015.docx

Collega's, bij deze twee sets Kamervragen over een bericht van een 0-day en encryptie met een conceptantwoord. Bijgevoegd de berichtgeving met enkele links, en een Kamerbrief waarin is gemeld dat de diensten kwetsbaarheden melden aan "belanghebbenden". Die zin heb ik overgenomen en er bij gezet dat de politie dat ook doet. Commentaar is uiteraard welkom.

Groet,



Achtergrondinformatie kamervraag nr 2015Z09552

Vragen van het lid Oosenbrug (PvdA) aan de staatssecretaris van Veiligheid en Justitie en de minister van Binnenlandse Zaken en Koninkrijksrelaties over het gebruik van een softwarefout door de Amerikaanse inlichtingendiensten (ingezonden 27 mei 2015)

Inhoudsopgave

Deze informatie wordt aangeleverd door de productie eenheid iv. Voor vragen of opmerkingen kun je contact opnemen met informatieplein@minvenj.nl.

Geciteerde bron

Het grootste gedeelte van veilige internetverbindingen is kapot

1) http://politiek.thepostonline.nl/2015/05/25/het-grootste-gedeelte-van-veilige-internetverbindingen-is-kapot/

Met update – De NSA is naar verluid een deel van hun spionagepraktijken op vooral hun landgenoten aan het afbouwen. Dat klinkt hoopgevend, maar is het nauwelijks. Al zou de organisatie acuut worden opgedoekt dan is de schade voor het bedrijfsleven, banken, burgers en overheden nog jaren voelbaar. Internet is onveiliger geworden. Het recht om op Amerikanen te spioneren ontleent de NSA aan de Patriot Act, een tijdelijke wet, die na de aanslagen van 11 september 2001 in het leven is geroepen. Daarna is de wet diverse malen verlengd, maar nu lijkt hij te verlopen omdat de verlenging niet geregeld is. Tot er een reparatiewet of een andere oplossing komt, worden wat praktijken afgebouwd.

Versleuteling kraken

Maar de echte pijn zit hem niet in wat de NSA al dan niet bij Amerikanen doet. Uit de gelekte documenten die klokkenluider Edward Snowden naar buiten bracht, wordt duidelijk dat er zwakheden in versleuteling zitten. Daarmee zou het mogelijk zijn een beveiligde verbinding razendsnel te ontcijferen.

Wat de Amerikanen nodig hebben is toegang tot het uitwisselen van sleutels bij het beginnen van een beveiligde verbinding. Daarna is alles eenvoudig te ontcijferen. Veel aandacht was er eerder niet voor dit probleem, omdat nog niet duidelijk was hoe dat kraken precies werkt. Het harde bewijs ontbrak.

Veel afluisteren

Inmiddels hebben wetenschappers onderzoek gedaan naar dit statement en achterhaald hoe die aanval werkt. Er is nu een wetenschappelijke paper geschreven, die dit helemaal uitlegt. Het blijkt dat grote delen van de beveiligde verbindingen volledig af te luisteren zijn. Het grootste gedeelte van onze beveiligde infrastructuur is daarmee kapot. Het duurt even voor je de totale impact doorgrond.
De zwakheid raakt VPN-verbindingen die door veel bedrijven worden gebruikt. Dus wie dacht bedrijfsgeheimen veilig over het internet te sturen moet daadwerkelijke vrezen voor economische spionage. Het raakt de veiligheid van onze banken, omdat veel van onze bancaire infrastructuur dit soort verbindingen gebruikt. Niet alleen voor internetbankieren, maar ook onderling.

Maar het gaat over veel meer, want dit lek raakt ook verbindingen tussen mailservers, het veilig internetbankieren en het veilig bezoeken van websites. Dat laatste werkt op twee niveaus: diverse webbrowsers zijn kwetsbaar voor het lek en ook webservers. Of uw webbrowser lek is kunt u online testen. Maar zelfs al is dat niet het geval is dan is het hoogst onzeker of de verbinding nog te vertrouwen is, omdat u niet ziet welke versleuteling u precies gebruikt.
Op hackersbijeenkomsten werd al begin deze eeuw gezegd dat cryptografie die vanuit de Verenigde Staten geëxporteerd mag worden door de NSA te kraken zou zijn. Dat was een verwachting, maar nooit bewezen. Nu we wetenschappelijk bewijs hebben, is die inschatting realistisch te noemen.

Breed misbruiken

Door het lek niet te dichten of publiek te maken, maar juist te misbruiken heeft de NSA internet ernstige schade toegebracht. Want grote delen van alles wat vertrouwelijk is, werkt met deze versleuteling en is nu kwetsbaar. In het donkerste scenario schatten de wetenschappers dat tweederde van de VPN-verbindingen niet meer veilig zijn.

Dat betekent niet dat het alleen te misbruiken is door de Amerikanen, maar ook door andere landen. Omdat het niet automatisch zo is dat internetverkeer de kortste

verbinding neemt, kun je niet uitsluiten dat vreemde mogendheden misbruik maken van onze vertrouwde verbindingen.

Moeilijk oplosbaar

Nu we het weten, kunnen we beginnen met het opruimen van de schade. Het oplossen van deze problemen is een enorme klus voor alle betrokkenen: overheden, bedrijfsleven en ook wijzelf. Er zullen nog veel testen moeten worden gedaan om te weten of de gebruikte beveiliging nog wel iets waard is.

Wanneer de NSA stelt het bijhouden van contactgegevens van Amerikanen af te bouwen dan betekent dat vervolgens dat de gevoelige inhoud van ons nog steeds wordt bekeken door onbevoegden. Zelfs al zou de NSA worden opgedoekt blijven wij kwetsbaar. Dit is het logisch gevolg van het investeren van honderden miljarden in spionage, terwijl aan beveiliging slechts een fractie wordt besteed.

Update 15.53 – PvdA-Kamerlid Astrid Oosenbrug zal de kwestie aan de orde stellen bij het Vragenuurtje dinsdag. Wordt vervolgd.

Mondelinge Vraag aangemeld voor morgen in het vragenuurtje n.a.v. dit bericht: http://t.co/oN1QnPyMsW #NSA #NCSC cc @brenno

— Astrid Oosenbrug (@AstridOosenbrug) May 25, 2015

2)**https://weakdh.org/imperfect-forward-secrecy.pdf**

Overig nieuws

PvdA stelt Kamervragen over gebruik softwarefout door NSA
https://www.security.nl/posting/429973/PvdA+stelt+Kamervragen+over+gebruik+softwarefout+door+NSA

woensdag 27 mei 2015, 16:47 door **Redactie**, 5 reacties

De PvdA heeft minister Plasterk van Binnenlandse Zaken en staatssecretaris Dijkhoff van Veiligheid en Justitie vragen gesteld over het gebruik van een recent onthuld encryptie-lek genaamd **Logjam** door de NSA. Via de Logjam-aanval kan een aanvaller, die zich tussen het slachtoffer en het internet bevindt, kwetsbare TLS-verbindingen naar een 512-bit encryptie downgraden. Hierdoor kan een aanvaller alle data over de versleutelde verbinding ontcijferen en zo lezen en aanpassen.

De onderzoekers die het probleem ontdekten stelden dat de NSA de kwetsbaarheid mogelijk heeft gebruikt om toegang tot VPN-verbindingen te krijgen. PvdA-Kamerlid Oosenbrug

vraagt (**pdf**) Plasterk en Dijkhoff of ze ook van mening zijn dat de NSA deze kwetsbaarheid heeft gebruikt om toegang tot beveiligde informatie te krijgen. Ook wil ze weten hoe de bewindslieden staan tegenover het gebruik van kwetsbaarheden door overheden in plaats van die aan de leverancier te melden.

Onbekende kwetsbaarheden

Plasterk en Dijkhoff moeten verder antwoord geven op de vraag of Nederlandse inlichtingendiensten en de politie ook gebruik van onbekende kwetsbaarheden maken en op welke wijze de Nederlandse overheid omgaat met al dan niet bewust aangebrachte kwetsbaarheden in software en hardware. Oosenbrug wil daarnaast weten of de bewindslieden actief de opsporing van dergelijke kwetsbaarheden ondersteunen, of er bij aanbestedingen met de mogelijke aanwezigheid van dit soort lekken rekening wordt gehouden en of dergelijke lekken altijd worden gemeld. De vragen zouden binnen drie weken moeten worden beantwoord.

Logjam computer bug could wreak havoc

http://www.usatoday.com/story/tech/2015/05/20/logjam-computer-bug-freak-encryption/27642479/


Elizabeth Weise, USATODAY *1:18 p.m. EDT May 20, 2015*

(Photo: luckyraccoon, Getty Images/iStockphoto)

SAN FRANCISCO -- A computer bug named LogJam that has roots in 20-year-old U.S. government policies could make upwards of 20,000 websites unavailable as security fixes are rolled out.

The bug's existence was disclosed Tuesday in a paper published Tuesday and reported by the *Wall Street Journal*.

LogJam could allow attackers to see or change information on a website that looks secure. When it is fixed, some older, un-updated websites may not work.

Experts caution that there's no indication anyone has actually made use of the flaw and say it affects a small percentage of websites, as most have changed the few lines of code necessary to fix it..

The bug comes on the coattails of FREAK, a bug that was disclosed in March.

LogJam makes use of a flaw intentionally built into computers due to U.S. government regulations in the 1980s and 1990s that made exporting strong encryption software illegal, because they were considered potential weapons. While the ban has mostly been lifted, the less-strong encryption option is still built into some computers and software.

The LogJam bug allows one computer to tell another it must use easier-to-break "export" encryption, which is relatively simple for today's computers to crack. An operation that might have taken days or weeks takes a modern computer just hours.

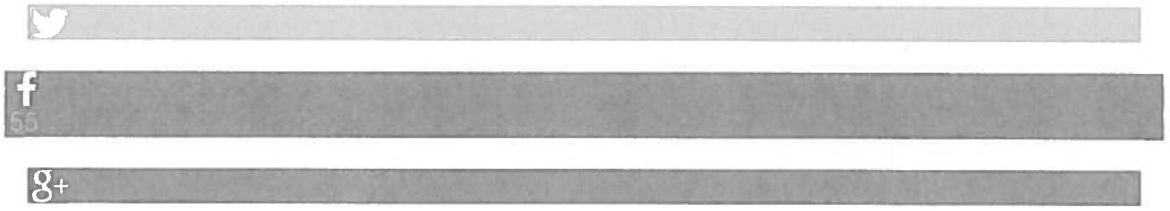
The bug can also trick a website into thinking it is using strong encryption when it's actually using a weak version.

"It's a good move for browsers to raise the bar on encryption key strength as computing power increases," said Branden Spikes, founder of Spikes Security, which develops technology for secure online web browsing.
Microsoft patched the LogJam vulnerability last week and patches for other popular browsers should be released soon.
Tod Beardsley, an engineer at security firm Rapid7, said the good news is that the usual bunch of Internet criminals can't really make use of LogJam.
"The only two groups really in a position to take advantage of this vulnerability are criminals on coffee shop wifi networks and state actors who already control a huge chunk of the local Internet," he said.

'Logjam' crypto bug could be how the NSA cracked VPNs

http://www.theregister.co.uk/2015/05/20/logjam_johns_hopkins_cryptoboffin_ids_next_branded_bug/

Johns Hopkins crypto boffin spots FREAK-like protocol bug



41

20 May 2015 at 05:25, Richard Chirgwin

Updated A team led by Johns Hopkins crypto researcher Matthew Green* thinks they might have an explanation for how the NSA attacked VPN services: flaws in how TLS implements Diffie-Hellman crytography.

In what's bound to be the next big branded bug, Green says servers that support 512-key "export-grade" Diffie-Hellman (DH) can be forced to downgrade a connection to that weak level. The server – and therefore the client – will both still believe they're using stronger keys such as 768-bit or 1024-bit.

Like so many things – including the similar FREAK flaw – the bug is ancient: a 20-year-old SSL bug that was inherited by TLS.

Green has hosted a site discussing what's being called "Logjam", Weakdh.org, with a detailed academic paper here (PDF).

Green's already been in touch with the major browser vendors, and says they're in the process of implementing a more restrictive policy on the size of Diffie-Hellman groups they will accept.

Logjam is another exploit of the 1990s-era crypto-wars: "To comply with 1990s-era U.S. export restrictions on cryptography, SSL 3.0 and TLS 1.0 supported reduced-strength DHE_EXPORT ciphersuites that were restricted to primes no longer than 512 bits", the paper notes.

Because "export grade" hangs around in ciphersuites, "a man-in-the-middle can force TLS clients to use export strength DH with any server that allows DHE_EXPORT."

"The attack affects any server that supports DHE_EXPORT ciphers, and affects all modern web browsers. 8.4% of the Top 1 Million domains were initially vulnerable," Green writes at the Logjam site.

Where 512-bit keys are supported, after an initial long computation, Green writes that "an academic team can break a 768-bit prime and that a nation-state can break a 1024-bit prime. Breaking the single, most common 1024-bit prime used by web servers would allow passive eavesdropping on connections to 18 per cent of the Top 1 Million HTTPS domains. A second prime would allow passive decryption of connections to 66 per cent of VPN servers and 26 per cent of SSH servers."

That's where the spooks come in: "A close reading of published NSA leaks shows that the agency's attacks on VPNs are consistent with having achieved such a break."

Anyone running a Web or mail server need to disable export-grade cipher suites and generate a new and unique 2048-bit Diffie-Hellman group. Users need to watch for browser upgrades, and developers need to use the latest libraries and reject Diffie-Hellman groups shorter than 1024 bits. ®

***Bootnote:** Matthew Green contacted the author to ask that credit be more appropriately distributed. He said most of the work on Logjam was carried out by INRIA, the University of Michigan, Microsoft and the University of Pennsylvania. ®

[redacted]

Van: [redacted] - BD/DGPOL/PBT/PT
Verzonden: woensdag 24 september 2014 16:57
Aan: [redacted] - BD/DGPOL/PBT/PT
Onderwerp: FW: KV Spyware
Bijlagen: Conceptbeantwoording Kamervragen over het gebruik van omstreden spionagesoftware door de politie 24092014 (schoon).docx

Ha [redacted], dit is laatste versie. Kan ik mij in vinden. Heb [redacted] nog gevraagd waarom jouw suggestie om antwoorden om te draaien niet is verwerkt. Groet

Met vriendelijke groet,

[redacted]
Coördinerend beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
Programma Politiële Taken

Turfmarkt 147 | 2511 DP | Den Haag | Noord 24e etage
Postbus 20301 | 2500 EH | Den Haag
.....
[redacted]
[redacted]
www.rijksoverheid.nl/venj
.....
Vrijdags afwezig
.....

Van: [redacted] - BD/PBP/ARBVW
Verzonden: woensdag 24 september 2014 14:28
Aan: [redacted] - BD/PBT/PT
Onderwerp: KV Spyware
Hoi [redacted]
Na nader contact met [redacted] en [redacted] (DGRR) heb ik nog een aantal wijzigingen doorgevoerd in de beantwoording. Bijgaand tref je de bijgewerkte versie. Ben je akkoord met deze versie? Indien nodig kunnen we even contact hebben.

Met vriendelijke groet,

[redacted]
Beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
Programma Arbeidsvoorwaarden
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
T [redacted]
[redacted]
www.rijksoverheid.nl/venj
.....
Voor een veilige en rechtvaardige samenleving
.....

[redacted]

Van: [redacted]- BD/DGPOL/PMP/FMI
Verzonden: vrijdag 8 augustus 2014 10:15
Aan: [redacted]- BD/DGPOL/PBT/PT
CC: [redacted]- BD/DGPOL/PBT/PT
Onderwerp: FW: Media-analyse vrijdag 8 augustus 2014

[redacted]

Ik stel voor om het bericht over geheime spionagesoftware alsnog te verifiëren bij Bestuurszaken. Beide berichten suggereren dat de nationale politie de bedoelde software zonder wettelijke basis gebruikt. Hierbij enige achtergrondinformatie.

- Gamma Group is an international manufacturer of surveillance & monitoring systems with technical and sales offices in Europe, Asia, the Middle East and Africa. We provide advanced technical surveillance, monitoring solutions and advanced government training as well as international consultancy to National and State Intelligence Departments and Law Enforcement Agencies. Through in-house developments and strategic partnerships with many leading security companies, we provide government agencies with customized solutions based on their national security requirements.
- FinFisher, een softwareprogramma waarmee computers kunnen worden geïnfecteerd om op afstand bestanden te kopiëren, beeldschermkopieën te maken en toetsaanslagen te registreren. Voor meer informatie zie http://nl.wikipedia.org/wiki/FinSpy

[redacted]

Van: Postbus DGPOL Media-Analyse - DGPOL
Verzonden: vrijdag 8 augustus 2014 9:22
Aan: Postbus DGPOL Media-Analyse - DGPOL; [redacted] -

CC: 'Bestuursondersteuning' (Bestuursondersteuning@knp.politie.nl); [redacted] - BD/DV/P&B
Onderwerp: Media-analyse vrijdag 8 augustus 2014

'Nederlandse politie gelinkt aan geheime spionagesoftware'
Bronnen: http://www.nu.nl/binnenland/3847389/nederlandse-politie-gelinkt-geheime-spionagesoftware.html
http://www.volkskrant.nl/vk/nl/2664/Nieuws/article/detail/3715207/2014/08/08/Politie-gebruikt-mogelijk-omstreden-spionagesoftware.dhtml
Kern: De Nederlandse politie lijkt spionagesoftware af te nemen van Gamma International. Dat hebben hackers ontdekt toen zij inbraken bij het Duits-Britse bedrijf dat geheime software aan overheden en opsporingsautoriteiten verkoopt. Het zou gaan om het omstreden programma FinFisher, schrijft de Volkskrant vrijdag.

Nog geen knipselkrant beschikbaar:
http://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/cisfacilitair/cisbibliotheekdiensten/cisknipselkrant_6

Met vriendelijke groet,

[redacted]
Regie & Strategie

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
DGPOL
Turfmarkt 147 | 2511 DP | Den Haag | VenJ 24ste etage
Postbus 20301 | 2500 EH | Den Haag
Biedjma Khodabaks | b.khodabaks@minvenj.nl | **T** 06 38 82 50 46
.....
M [redacted]
www.rijksoverheid.nl/venj
.....
Voor een veilige en rechtvaardige samenleving
.....

Van: - BD/DRB/TR
Verzonden: dinsdag 14 oktober 2014 11:11
Aan: - BD/DGPOL/PBT/PT; - BD/DRC/CV
Onderwerp: FW: Mondelinge vraag van het lid GESTHUIZEN.docx

Zie nog deze input van de politie. Het bevestigt de lijn die al in jullie beider Q&A's stond.

Groeten,

Van: @politie.nl]
Verzonden: dinsdag 14 oktober 2014 11:05
Aan:
CC: - BD/DJOA/BJZ; ; Bestuursondersteuning; Mailbox Bestuursondersteuning Landelijke Eenheid (LE)
Onderwerp: RE: Mondelinge vraag van het lid GESTHUIZEN.docx

Er vanuit gaande dat de veiligheidslekken bedoeld worden die net in het nieuws waren (de bijlage zat er niet bij), denk ik dat het antwoord idd nee is. beperkingsgrond artikel 11, eerste lid

beperkingsgrond artikel 10, tweede lid, aanhef en onder c

Ik zal voor de zekerheid nog even bij DLR en DLOS checken.
Groet,

Van:
Verzonden: dinsdag 14 oktober 2014 10:39
Aan:
CC: -B; Bestuursondersteuning
Onderwerp: Fw: Mondelinge vraag van het lid GESTHUIZEN.docx
Urgentie: Hoog

zie vraag 3. M.i. Is het antwoord NEE. Klopt dat? Gr

Van: BD/DJOA/BJZ [mailto:]
Verzonden: Tuesday, October 14, 2014 10:33 AM W. Europe Standard Time
Aan:
Onderwerp: RE: Mondelinge vraag van het lid GESTHUIZEN.docx

Dat is inderdaad aan OM, en in het verlengde ook de vraag wat de politie feitelijk doet. Maar er zijn meer invalshoeken aan deze mondelinge vraag, en we hebben nog steeds niet scherp welke kan Gesthuizen op wil. Zie deze driedeling die ik maakte:

1) Gesthuizen wil weten of politie en justitie ook informatie over veiligheidslekken kopen. Dan hebben we het over de inzet van een controversieel opsporingsmiddel -> DGRR.

2) Gesthuizen wil weten of de Minister kan bevestigen dat dit soort handel is veiligheidslekken plaatsvindt en wat hij daaraan doet. Dat valt dan uiteen in een deel het dichten van het lek (-> NCTV) en een deel strafrecht (-> DGRR).
3) Gesthuizen wil weten of de "spionagesoftware" uit de eerder schriftelijke vragen gebruik maakt of iets te maken heeft met deze handel in veiligheidslekken. -> DGPOL

[redacted]

Van: [redacted]@politie.nl]
Verzonden: dinsdag 14 oktober 2014 10:29
Aan: [redacted] BD/DJOA/BJZ
Onderwerp: Re: Mondelinge vraag van het lid GESTHUIZEN.docx

Voor mijn helderheid: vraag is toch wat politie mag ikv opsporing? Dat is aan OM.

Van: [redacted] BD/DJOA/BJZ [mailto:c.jetten@minvenj.nl]
Verzonden: Tuesday, October 14, 2014 10:27 AM W. Europe Standard Time
Aan: [redacted]
Onderwerp: FW: Mondelinge vraag van het lid GESTHUIZEN.docx

Van: [redacted] BD/DJOA/BJZ
Verzonden: dinsdag 14 oktober 2014 10:00
Aan: Bestuursondersteuning (Bestuursondersteuning@knp.politie.nl)
Onderwerp: FW: Mondelinge vraag van het lid GESTHUIZEN.docx
Urgentie: Hoog

Beste collega's,

Kunnen jullie even meekijken met deze Q&A voor een eventueel mondeling vragenuur over het volgende: "Mondelinge vraag van het lid GESTHUIZEN (SP) aan de minister van Veiligheid en Justitie over de handel in veiligheidslekken (Radio 1 Argos, 11 oktober 2014) en de antwoorden op eerdere schriftelijke vragen over het gebruik van omstreden spionagesoftware door de politie (AH 202)

Dank alvast,
[redacted]

Ministerie van Veiligheid en Justitie
DG Politie – Programma Regie & Strategie
Turfmarkt 147 – Noordtoren 24e etage
Postbus 20301 - 2500 EH Den Haag
[redacted]

Van: [redacted] - BD/PBT/PT
Verzonden: maandag 13 oktober 2014 18:35
Aan: [redacted] BD/DJOA/BJZ; [redacted] - BD/PBT/PT
CC: [redacted] BD/PR&C/R&S
Onderwerp: Mondelinge vraag van het lid GESTHUIZEN.docx

Hoi Zie bijgaand mijn opzetje voor het dossier van de minister.

Als we antwoord willen hebben op de vraag of de politie gebruik maakt van veiligheidslekken ihkv opsporing dan moeten we die vraag nog expliciet uitzetten bij politie via parlementaire box bij bestuurszaken. Daarover heb ik nu niks opgenomen, omdat ik dat echt eerst bevestigd zou willen zien.

Groet [redacted]

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Veiligheid en Justitie

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Security and Justice

---------- Disclaimer ---------- De informatie verzonden met dit e-mailbericht (en bijlagen) is uitsluitend bestemd voor de geadresseerde(n) en zij die van de geadresseerde(n) toestemming kregen dit bericht te lezen. Kennisneming door anderen is niet toegestaan. De informatie in dit e-mailbericht (en bijlagen) kan vertrouwelijk van aard zijn en binnen het bereik van een geheimhoudingsplicht en/of een verschoningsrecht vallen. Indien dit e-mailbericht niet voor u bestemd is, wordt u verzocht de afzender daarover onmiddellijk te informeren en het e-mailbericht (en bijlagen) te vernietigen. ----------
----

[redacted] - BD/DGPOL/PBT/R&S

Van: [redacted] - BD/DGPOL/PMP/F&C
Verzonden: dinsdag 14 juli 2015 11:42
Aan: [redacted] - BD/DGPOL/PBT/PT
Onderwerp: FW: Nieuwe Kamervraag inzake het gebruik van software van het Hacking Team door de Nationale Politie (NP)
Bijlagen: DetailRapport.doc; het_gebruik_van_software_van_het_Hacking_Team_door_de_Nationale_Politie[1].docx

Urgentie: Hoog

Hoi [redacted]

Dit is de set waar het om gaat.
De NCTV heeft ze ook al gezien.
Ik heb ook contact met DGRR over deze set.

Volgens mij is voor vraag 2 en 3 input van de NP nodig.
Vraag 4 lijkt heel veel op de set van oktober over finfisher.
Bij vraag 5 vraag ik mij af of je hier wel iets op moet zeggen, lijkt mij niet wenselijk om hier openbaar inzicht in te bieden.
Voor vraag 7 heeft [redacted] van FMI na het nieuwsbericht een uitvraag gedaan. De NCTV neemt die ook mee in hun beantwoording, net als 8 en 9.

Het lijkt mij zinvol om als er informatie is dat wel relevant voor de staatssecretaris is, maar je niet wilt publiceren in een aparte nota bij te voegen.

Graag hoor ik of jij naast input op de vragen 2 en 3 nog input nodig hebt op andere vragen vanuit bestuursondersteuning. Dan kan ik dat verzoek vandaag nog aan ze doen.

Groet,
[redacted]

Van: [redacted] - BD/PR&C/R&S
Verzonden: dinsdag 14 juli 2015 9:33
Aan: [redacted] - BD/DGPOL/PMP/F&C
Onderwerp: FW: Nieuwe Kamervraag inzake het gebruik van software van het Hacking Team door de Nationale Politie (NP)

NCTV heeft de set al opgemerkt.

Van: NCTV Staf - NCTV
Verzonden: dinsdag 14 juli 2015 7:19
Aan: [redacted] BD/NCTV/DCS/ACSB
CC: [redacted] - BD/NCTV/DCS/ACSB; [redacted] - BD/NCTV; [redacted] - BD/DCS; [redacted] - BD/DCS/NCSC; [redacted] - BD/DSB/AS; Parlementair - DGPOL; [redacted] BD/PR&C/R&S; NCTV Staf - NCTV
Onderwerp: FW: Nieuwe Kamervraag inzake het gebruik van software van het Hacking Team door de Nationale Politie (NP)

Zie vragen die primair bij DgPol liggen. Vragen 7, 8 en 9 hebben relatie met DCS.

[redacted]
Senior Stafadviseur

Ministerie van Veiligheid en Justitie
Nationaal Coördinator Terrorismebestrijding en Veiligheid
Turfmarkt 147| 2511 DP | Den Haag |
Postbus 16950 | 2500 BZ | Den Haag

www.nctv.nl

Van: MVJKamerverzoek-BSG@minvenj.nl [mailto:MVJKamerverzoek-BSG@minvenj.nl]
Verzonden: maandag 13 juli 2015 17:04
Aan:

CC: BD-Parlementaire Contactpersonen; Info PIV - DC/PIV; Informatieplein Justitie - DC/PIV; MVJBSG - BSG; BD-Paminco Internationaal
Onderwerp: Nieuwe Kamervraag inzake het gebruik van software van het Hacking Team door de Nationale Politie (NP)

Geachte mevrouw/heer,

Er is een nieuwe kamervraag aangemaakt op uw directie inzake "het gebruik van software van het Hacking Team door de Nationale Politie (NP)".

Wilt u svp een directie/medewerker koppelen aan dit stuk?

link naar detailrapport of zoek op ID-nummer 82720

Voor vragen kunt u een mail sturen naar MVJBSG@minvenj.nl of bellen naar tst. 6002.

Met dank & vriendelijke groet,
Paminco

Detailrapport(Kamervragen)
(ID 82720)

ID	82720
Invoerdatum	13-07-2015 17:04
Briefnr TK/EK	2015Z14018
Inkomend nr Jus	
Soort brief	Kamervraag TK
Brief datum	13-07-2015
EK/TK	TK
Kamerleden	Verhoeven, K. , Oosenbrug, mw. R.F.A.
Omschrijving/onderwerp	het gebruik van software van het Hacking Team door de Nationale Politie (NP)
Naar BSG	Nee
Primair	MVenJ
Secundair	
Bewindspersoon	Staatssecretaris van Veiligheid en Justitie
Lid bestuursraad	DGPol
Directie	STAF
Afdeling	(Geen)
Medewerker	(Geen)
Medebetrokken	
Mondelinge vragentermijn	24-08-2015
Einddatum	03-08-2015
Interne planning	
Te nemen actie	Schrift. Antwoord
Stand van zaken/ voortgangsinformatie	
Uitstel aangevraagd	Nee
Uitstel aangevraagd met	
Afgedaan met	
Relatie met	
Documenten	het gebruik van software van het Hacking Team door de Nationale Politie

[redacted]

Van: [redacted] - BD/DGPOL/PBT/R&S
Verzonden: woensdag 3 september 2014 14:51
Aan: [redacted] - BD/DGPOL/PBT/PT
Onderwerp: FW: spyware
Bijlagen: getContent.pdf

Met vriendelijke groet,

[redacted]
Beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
Programma Arbeidsvoorwaarden
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
[redacted]
www.rijksoverheid.nl/venj
.....
Voor een veilige en rechtvaardige samenleving
.....

Van: [redacted] - BD/PR&C/R&S
Verzonden: maandag 11 augustus 2014 16:30
Aan: [redacted] - BD/PBP/ARBVW; [redacted] - BD/PR&C/R&S
Onderwerp: FW: spyware

Hi [redacted],

Zie mijn bericht hieronder. Handig om even bij [redacted] na te gaan wat hij heeft opgevraagd. Bijgevoegd ook eerdere Kamervragen over dit onderwerp eind 2011.

Ter info

Gr [redacted]

Van: [redacted] - BD/PR&C/R&S
Verzonden: maandag 11 augustus 2014 13:59
Aan: [redacted] - BD/PBT/PT
CC: [redacted] - BD/PBP/I&I
Onderwerp: RE: spyware

Ok, dan laat ik dit verder aan jou, met verzoek [redacted] daarover te informeren.
Gr [redacted]

Van: [redacted] - BD/PBT/PT
Verzonden: maandag 11 augustus 2014 13:58
Aan: [redacted] - BD/PR&C/R&S
Onderwerp: RE: spyware

Hoi, ik heb vrijdag een [redacted] gevraagd ons van feitelijke info te voorzien. Graag daaraan refereren, ik spreek haar vanmiddag nog telefonisch. Inhoudelijk lijkt dit meer PT te zijn. Groet, [redacted]

Van: [redacted]- BD/PR&C/R&S
Verzonden: maandag 11 augustus 2014 13:54
Aan: [redacted]- BD/PBP/I&I; [redacted]- BD/PBT/PT
Onderwerp: spyware

[redacted],

Ik wil bij de NP informatie op gaan vragen over onderstaande. Voordat ik dat doe echter even een checkvraag of dossier Spyware bij I&I en/of PT is belegd en of er info beschikbaar is? Eerder is in de tijd van KLPD al over dit onderwerp gesproken.

'Nederlandse politie gelinkt aan geheime spionagesoftware'
Bronnen: http://www.nu.nl/binnenland/3847389/nederlandse-politie-gelinkt-geheime-spionagesoftware.html
http://www.volkskrant.nl/vk/nl/2664/Nieuws/article/detail/3715207/2014/08/08/Politie-gebruikt-mogelijk-omstreden-spionagesoftware.dhtml
Kern: De Nederlandse politie lijkt spionagesoftware af te nemen van Gamma International. Dat hebben hackers ontdekt toen zij inbraken bij het Duits-Britse bedrijf dat geheime software aan overheden en opsporingsautoriteiten verkoopt. Het zou gaan om het omstreden programma FinFisher, schrijft de Volkskrant vrijdag.

Met vriendelijke groet,

[redacted]
Regie & Strategie

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
DGPOL
Turfmarkt 147 | 2511 DP | Den Haag | VenJ 24ste etage
Postbus 20301 | 2500 EH | Den Haag
[redacted]
.....
[redacted]
www.rijksoverheid.nl/venj
.....
Voor een veilige en rechtvaardige samenleving
.....

[redacted]

Van: [redacted] - BD/DGPOL/PBT/PT
Verzonden: dinsdag 14 juli 2015 15:48
Aan: [redacted] - BD/DGPOL/PMP/F&C
Onderwerp: het_gebruik_van_software_van_het_Hacking_Team_door_de_Nationale_Politie1.docx
Bijlagen: het_gebruik_van_software_van_het_Hacking_Team_door_de_Nationale_Politie1.docx

Hoi [redacted],
DGRR staat voor 4 en 5 is dgrr aan de lat. Ik heb wel al een voorzet voor beantwoording gedaan nav eerdere kamervragen, finfisher. Met nog een vraag over de broncode. Zie het doc.

Groet, [redacted]

[redacted]

Van: [redacted] - BD/DGPOL/PBT/PT
Verzonden: woensdag 1 oktober 2014 16:23
Aan: [redacted] - BD/DGPOL/PBT/R&S
Onderwerp: http://computerworld.nl/beveiliging/83855-klpd-betaalde-2-7-miljoen-voor-finfisher-spyware?utm_source=SIM&utm_medium=email&utm_campaign=20140915-12%3A00%3A02_computerworld_cron&utm_content=&utm_term=_1711

Kijk, ik zie dit: hier heeft politie wel inhoudelijk gereageerd.. Hoe verhoudt zich dit tot het antwoord dat nu de lijn in is..

Met vriendelijke groet,

[redacted]
Coördinerend beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
Programma Politiële Taken

Turfmarkt 147 | 2511 DP | Den Haag | Noord 24e etage
Postbus 20301 | 2500 EH | Den Haag
.....
[redacted]
www.rijksoverheid.nl/venj
.....
Vrijdags afwezig
.....

[redacted]

Van: [redacted] - BD/DGPOL/PBT/PT
Verzonden: maandag 30 maart 2015 21:37
Aan: [redacted] - BD/DGPOL/PBT/PT
Onderwerp: RE: AO dataretentie

Gesthuizen heeft in verleden kV gesteld over finfisher, spionagesoftware. KV zijn beantwoord. Wat had ze precies? V Tongeren kan ik niet duiden. Misschien kun je even mondeling toelichten?

[redacted]

Vrijdags afwezig

Sent with Good (www.good.com)

From: [redacted] - BD/DGPOL/PBT/PT
Sent: woensdag 25 maart 2015 21:22:41
To: [redacted] - BD/DGPOL/PBT/PT
Subject: AO dataretentie

Ha [redacted], Gesthuizen vroeg hoe het zat met inbreken op computers ogv 125i Sv (Fin Fish?). Van Tongerrn had het over google en dgdog oid. Kan jij dit duiden? Vriendelijke groet [redacted]

Sent with Good (www.good.com)

[redacted]

Van: [redacted] - BD/DGPOL/PBT/R&S
Verzonden: woensdag 1 oktober 2014 16:58
Aan: [redacted] - BD/DGPOL/PBT/PT
Onderwerp: RE: http://computerworld.nl/beveiliging/83855-klpd-betaalde-2-7-miljoen-voor-finfisher-spyware?utm_source=SIM&utm_medium=email&utm_campaign=20140915-12%3A00%3A02_computerworld_cron&utm_content=&utm_term=_1711
Bijlagen: Lijnversie beantwoording Kamervragen over het gebruik van omstreden spionagesoftware door de politie 01102014.docx

Hoi [redacted],

Wat mij betreft is deze reactie in lijn met onze beantwoording. Het grootste deel van het bericht is door de website zelf geschreven. De woordvoerder van Politie doet geen uitspraken over specifieke software, in lijn met onze antwoorden. Voor de volledigheid heb ik de lijnversie van onze beantwoording nogmaals bijgevoegd.

[redacted]
Met vriendelijke groet,

[redacted]
Beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
Programma Arbeidsvoorwaarden
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
[redacted]
www.rijksoverheid.nl/venj
.....
Voor een veilige en rechtvaardige samenleving
.....

Van: [redacted] - BD/PBT/PT
Verzonden: woensdag 1 oktober 2014 16:23
Aan: [redacted] - BD/PBP/ARBVW
Onderwerp: http://computerworld.nl/beveiliging/83855-klpd-betaalde-2-7-miljoen-voor-finfisher-spyware?utm_source=SIM&utm_medium=email&utm_campaign=20140915-12%3A00%3A02_computerworld_cron&utm_content=&utm_term=_1711

Kijk, ik zie dit: hier heeft politie wel inhoudelijk gereageerd.. Hoe verhoudt zich dit tot het antwoord dat nu de lijn in is..

Met vriendelijke groet,

[redacted]
Coördinerend beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
Programma Politiële Taken

Turfmarkt 147 | 2511 DP | Den Haag | Noord 24e etage
Postbus 20301 | 2500 EH | Den Haag
.....
[redacted]

www.rijksoverheid.nl/venj

Vrijdags afwezig

Van: [redacted] - BD/DGPOL/PBT/PT
Verzonden: woensdag 7 januari 2015 14:40
Aan: [redacted] - BD/NCTV/DCS/ACSB
CC: [redacted] - BD/DCS; [redacted] - BD/NCTV/DCS/ACSB; [redacted] - BD/DRC/CV; [redacted] - BD/DRC/CV
Onderwerp: RE: input AO cyber security 22/1
Bijlagen: AO cybercrime jan 2015 def.docx

Hoi [redacted] zie bijgaand mijn input tbv het AO. Windows XP tekst heb ik voor de zekerheid nog langs onze info-club gezonden voor een check, dus dat volgt nog (evt voor onder de arm want ik denk dat het niet echt actueel meer is, maar voor de zekerheid..).

Met vriendelijke groet,

[redacted]
Coördinerend beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
Programma Politiële Taken

Turfmarkt 147 | 2511 DP | Den Haag | Noord 24e etage
Postbus 20301 | 2500 EH | Den Haag
.....
[redacted]
www.rijksoverheid.nl/venj
.....
Vrijdags afwezig
.....

Van: [redacted] - BD/NCTV/DCS/ACSB
Verzonden: woensdag 7 januari 2015 11:13
Aan: [redacted] - BD/PBT/PT; [redacted] - BD/DRC/CV; [redacted] - BD/DRC/CV
CC: [redacted] - BD/DCS; [redacted] - BD/NCTV/DCS/ACSB
Onderwerp: RE: input AO cyber security 22/1

Beste allen,

Nog de beste wensen voor 2015. Zouden jullie aub de onderstaande zaken aan willen leveren? Uiterlijk vrijdag alles binnen zijn, want volgende week moet het dossier de lijn in. Zouden jullie aub de heren in cc mee willen nemen in de mail, want ik ben beperkt bereikbaar de komende dagen.

Alvast bedankt.

Groeten,

[redacted]

Van: [redacted] - BD/NCTV/DCS/ACSB
Verzonden: maandag 15 december 2014 13:26
Aan: [redacted] - BD/PBT/PT; [redacted] - BD/DRC/CV; [redacted] - BD/DRC/CV
Onderwerp: input AO cyber security 22/1

Beste [redacted],

Op 22 januari staat een AO cyber security gepland. Dat betekent dat begin januari het dossier bij elkaar moet komen richting de minister. Hieronder een aantal thema's die altijd opspelen of waarvan

het mogelijk aan de orde kan komen. Als er andere zaken zijn waarvan jullie denken dat het aan de orde zou kunnen komen, vul vooral aan. Zouden jullie aub uiterlijk dinsdag 6 januari input willen sturen voor het dossier in de bijgevoegde formats? Bijgevoegd ook de documenten die voor het vorige AO in maart gemaakt zijn, scheelt hopelijk werk.

Thema's:

- Stavaza capaciteitsopbouw THTC
- Aantal cyberzaken 2014
- Stavaza wetsvoorstel cybercrime III
- NL als bron van cybercrime
- Uitspraak zaak Groen Hart Ziekenhuis
- Stavaza migratie Windows XP politie? (vorig AO)
- Inzet Finfisher politie?

Alvast bedankt.

Groeten,

senior adviseur cyber security
Directie Cyber Security

Ministerie van Veiligheid en Justitie

De minister van Veiligheid en Justitie

Directoraat-Generaal Politie
Regie & Strategie

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj

Contactpersoon

nota

Beantwoording Kamervragen over het gebruik van omstreden spionagesoftware door de politie

Datum
24 september 2014

Ons kenmerk
566120

Dossiernummer
550115

Concipiënt

Gevraagde actie

Akkoord met verzending aan de Tweede Kamer van bijgevoegde antwoorden op Kamervragen.

Achtergrond

Het lid Gesthuizen (SP) heeft vragen gesteld naar aanleiding van het bericht dat de politie gebruik lijkt te maken van het softwareprogramma FinFisher van het bedrijf Gamma International. Digitale activisten zouden hier achter zijn gekomen door klantbestanden van het betreffende bedrijf te hacken. FinFisher is een computerprogramma dat op afstand ongemerkt op een computer (van bijvoorbeeld een verdachte) kan worden geïnstalleerd. FinFisher maakt het vervolgens mogelijk om de gebruiker van deze computer ongemerkt in de gaten te houden. Het bericht meldt dat het op afstand hacken en overnemen van computers door de politie niet is toegestaan.

Voorliggende antwoorden zijn met input van de NP en OM tot stand gebracht en afgestemd met DGRR, NCTV en DWJZ. Tevens is Directie Voorlichting ingelicht over deze antwoorden.

Toelichting

In de beantwoording geeft u aan dat de politie technische hulpmiddelen voor het opnemen van vertrouwelijke communicatie (bijvoorbeeld software) altijd vooraf laat keuren door een onafhankelijke keuringsdienst. Daarnaast is het gebruik met waarborgen omkleed. Zo moet de inzet voldoen aan de eisen van proportionaliteit en subsidiariteit en is goedkeuring van het OM nodig en bij ingrijpende gevallen een machtiging van de rechter-commissaris.

Directoraat-Generaal Politie
Programma
Arbeidsvoorwaarden

Datum
24 september 2014

Ons kenmerk
566120

U geeft voorts aan met welk doel en op welke manier de inzet van dergelijke middelen onder de huidige wettelijke kaders kan plaatsvinden. Ook zegt u desgevraagd dat het niet zo is dat vooruitlopend op de Wet Computercriminaliteit III door de politie wordt geëxperimenteerd met het overnemen van computers. Over of de politie al dan niet beschikt over specifieke software, zoals het genoemde FinFisher, doet u geen mededelingen, omdat het verstrekken van informatie over welke specifieke software de opsporingsdiensten van de politie beschikken, testen en gebruiken grote risico's met zich meebrengt voor de inzetbaarheid van die middelen. Immers: als algemeen bekend wordt welke softwareprogramma's de politie gebruikt, kunnen verdachten zich hierop gaan instellen en bijvoorbeeld voorzorgsmaatregelen nemen om te voorkomen dat deze software tegen hen wordt ingezet (onder andere door middel van bepaalde antivirus software).

beperkingsgrond artikel 10, tweede lid, aanhef en onder c
beperkingsgrond artikel 11, eerste lid

beperkingsgrond artikel 10, tweede lid, aanhef en onder c
beperkingsgrond artikel 11, eerste lid

Dit is in lijn met de beantwoording van eerdere Kamervragen over dit onderwerp[1].

[1]Kamervragen van de leden Schouw en Berndsen (D66) over het gebruik van spysoftware (13 oktober 2011) en Kamervragen van de leden Gesthuizen (SP) en El Fassed (GroenLinks) over het gebruik van spionagesoftware door de Nederlandse overheidsdiensten (25 oktober 2011)

Onderwerp	**Politie: Kwetsbaarheden software**
Dossierhouder	[redacted]
Bereikbaarheid	[redacted]
Minister	**V&J**
Vraagsteller	
Partij	

Vraag: Koopt politie kwestbaarheden of maakt de politie gebruik van kwetsbaarheden?

Antwoord:

- Kwetsbaarheden ontdekken is niet strafbaar. De verkoop van kennis hierover is niet verboden.
  Softwareproducenten betalen voor deze kennis om producten veiliger te maken. Maar ook cybercriminelen zijn bereid voor dergelijke kwetsbaarheden te betalen.
- Waar de handel in kwetsbaarheden zelf niet strafbaar is, is het treffen van voorbereidingen voor het begaan van strafbare feiten dat wel. Daar is sprake van als iemand bijvoorbeeld software voor handen heeft die is ontworpen om wederrechtelijk binnen te dringen in een computer en gegevens te stelen, én de bedoeling heeft daarmee strafbare feiten te plegen.
- De politie koopt geen kwetsbaarheden op de markt. De politie beschikt wel over software die fysiek kan worden geïnstalleerd op de computer van een verdachte. Het gebruik van deze software vindt plaats op basis van het Wetboek van Strafvordering.
- (Over de werkwijze van de inlichtingendiensten kan ik

geen uitspraken doen.).

Onderwerp	**Politie: Gebruik van spionagesoftware**
Dossierhouder	
Bereikbaarheid	
Minister	**V&J**
Vraagsteller	
Partij	

Vraag: Maakt de politie gebruik van spionagesoftware?

Antwoord:

- De politie beschikt over software die fysiek geïnstalleerd kan worden op de computer van een verdachte, waarmee toegang kan worden verkregen tot die computer en waarmee gegevens 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.
- Onder bepaalde omstandigheden is op basis van artikel 125i van het Wetboek van Strafvordering op basis van een machtiging van de rechtercommissaris 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.
- De beschikbare technische hulpmiddelen voor het opnemen van vertrouwelijke communicatie worden voorafgaand aan de inzet gekeurd door de onafhankelijke keuringsdienst van de politie.