Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Nationaal Coördinator Terrorismebestrijidng en Veiligheid
Programma Dreigingen & Capaciteiten

Schedeldoekshaven 200
2511 EZ Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl

Kenmerk
2012-0000129857

Uw Kenmerk
2012Z03111

Bijlagen
1

Datum 20 maart 2012
Betreft Beantwoording kamervragen gesteld door lid Elissen naar aanleiding van een nieuwsbericht over digitale spionage van China en Rusland

Hierbij bied ik u, mede namens de Ministers van Buitenlandse Zaken, van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie, de antwoorden aan op de schriftelijke vragen van het lid Elissen (PVV) over digitale spionage van China en Rusland. Deze vragen zijn ingezonden op 17 februari 2012 (kenmerk 2012Z03111).

De Minister van Veiligheid en Justitie,

I.W. Opstelten

2012Z03111
Antwoorden op vragen van het lid Elissen (PVV) aan de Ministers van Veiligheid en Justitie en van Buitenlandse Zaken over digitale spionage van China en Rusland

Datum
20 maart 2012

Kenmerk
2012-0000129857

1
Bent u bekend met het bericht 'Traveling Light in a Time of Digital Thievery'?[1]

Ja

2
Is het in uw beleving waar dat reizigers met waardevolle informatie een groot risico lopen dat hun apparaten in China en Rusland gemanipuleerd worden zodat deze landen informatie kunnen bemachtigen? Zo ja, hoe groot is dit risico? Welke landen maken zich nog meer schuldig aan dit soort activiteiten?

Er is een reële kans dat waardevolle informatie op deze wijze gestolen wordt door buitenlandse inlichtingendiensten. Buitenlandse inlichtingendiensten beschikken over een breed scala aan middelen om aan informatie te komen. Zo worden bestanden gekopieerd van gegevensdragers (laptops, mobiele telefoons, pda's enzovoorts); wordt telefoon- en dataverkeer afgeluisterd (vast en mobiel) en wordt gebruik gemaakt van camera's of microfoons in bijvoorbeeld hotelkamers. De AIVD en MIVD hebben in dit kader verschillende brochures uitgebracht waarin wordt gewaarschuwd voor het risico op spionage bij reizen naar het buitenland en waarin wordt aangegeven wat reizigers zelf kunnen doen om het risico te verkleinen.[2]

In de jaarverslagen van de AIVD en MIVD wordt aangegeven dat het risico op spionage onverminderd aanwezig is, daarbij geldt dat met name het risico op digitale spionage toeneemt. Ook uit het Cyber Security Beeld Nederland (CSBN) van het Nationaal Cyber Security Centrum (NCSC) komt de dreiging van cyberspionage door statelijke actoren prominent naar voren.[3] Het CSBN laat zien dat er sprake is van een toenemende dreiging van digitale spionage. Zowel overheden als private organisaties zijn regelmatig doelwit van digitale spionage geweest, ook in Nederland. Deze cyberaanvallen zijn gericht op het verkrijgen van vertrouwelijke informatie van economische of politieke waarde, of op direct geldelijk gewin.[4]

China, Rusland en Iran zijn in het meest recente jaarverslag van de AIVD genoemd als landen waarvan de buitenlandse inlichtingendiensten spionageactiviteiten ondernemen. Nadere informatie over landen die zich schuldig maken aan spionage kan ik niet verstrekken aangezien dat raakt aan het kennisniveau en de bronnen van de AIVD en de MIVD. Deze informatie is gerubriceerd en kan ik in het openbaar niet met u delen. U kunt er echter van uitgaan dat naast de genoemde landen ook andere landen heimelijke inlichtingenactiviteiten ondernemen in Nederland. De inlichtingendiensten doen hier onderzoek naar en treden op waar nodig.

3

1 1) 'Traveling Light in a Time of Digital Thievery' (Bron: http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-ofdigital-espionage.html?_r=2&pagewanted=all)

2 De brochures: Spionage in Nederland. Wat is het risico? , Spionage bij reizen naar het buitenland. Wat is het risico? , eerste druk 2004 en Digitale Spionage. Wat is het risico?, eerste druk 2010

3 Voor de ontwikkeling van het CSBN zijn inzichten gebundeld waarover AIVD, MIVD, KLPD, NCTV en Govcert.nl op basis van hun taak beschikken. Deze zijn daarna aangevuld met de kennis die met hen is gedeeld door de private partijen waarmee zij samenwerken.

4 Bij de Kamerbrief d.d. 23 december 2011 (Kamerstuk 26643, nr 220) ontving uw Kamer dit CSBN.

Treft de Nederlandse overheid speciale maatregelen wanneer ambtenaren, diplomaten of politici naar China of Rusland afreizen om te voorkomen dat deze landen op digitale wijze spioneren? Geeft u het Nederlandse bedrijfsleven voorlichting over dit onderwerp of biedt u op andere wijze ondersteuning of bescherming? Zo nee, waarom niet?

De AIVD en MIVD doen in het kader van de wettelijke taak onderzoek naar ongewenste inlichtingenactiviteiten van vreemde mogendheden. Over dit onderzoek informeren de AIVD en MIVD overheidsinstanties die maatregelen kunnen nemen. Tevens informeren de AIVD en de MIVD, in specifieke gevallen, díe instanties die doelwit zijn van de heimelijke inlichtingenactiviteiten, dit kunnen zowel overheden als bedrijven zijn.

Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) bevordert als onderdeel van de AIVD de beveiliging van vertrouwelijke informatie van de overheid. De AIVD geeft advies over informatiebeveiliging, beoordeelt beveiligingsproducten en ondersteunt bij de implementatie ervan. Ook dit advies kan gericht zijn tot zowel overheden als bedrijven.

Daarnaast gelden voor de beveiliging van waardevolle overheidsinformatie de regels die zijn vastgelegd in het 'Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie'. In dit voorschrift zijn ook beschermingsmaatregelen tegen dreigingen van digitale spionage inbegrepen.

Het ministerie van Buitenlandse Zaken heeft in het standaard opleidingsprogramma van diplomaten bewustwordingsactiviteiten op het gebied van integrale veiligheid, inclusief informatiebeveiliging en risico op spionage, opgenomen.

Toeleveranciers van de defensieorganisatie krijgen van de MIVD advies over informatiebeveiliging. Daarnaast worden aan defensieorderbedrijven eisen gesteld ten aanzien van informatiebeveiliging en worden cursussen voor beveiligingsfunctionarissen van deze bedrijven gegeven. Voor bedrijven die bijzonder interessant zijn voor buitenlandse inlichtingendiensten worden maatwerkbijeenkomsten georganiseerd om de bewustwording te vergroten.

In april 2010 heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties de Kwetsbaarheidsanalyse Spionage (KWAS) aangeboden aan de Tweede Kamer. Het kabinet heeft uw Kamer in zijn brief d.d. 22 februari 2011 op de hoogte gebracht van de aanpak naar aanleiding van dit onderzoeksrapport. [5] Dat betreft onder andere voorlichting aan bedrijfsleven en overheden over de risico's van spionage en de mogelijkheden om de weerbaarheid daartegen te vergroten. Daarvoor is de Handleiding Kwas ontwikkeld en wordt dit jaar een e-learning module beschikbaar gesteld.

4
Hoe beoordeelt u de uitspraak van de vice-president van beveiligingsbedrijf McAfee dat apparaten die door de Chinese overheid worden gecontroleerd nooit meer op het bedrijfsnetwerk aangesloten mogen worden? Worden apparaten van de Nederlandse overheid ook niet meer gebruikt wanneer deze aan de Chinese grens zijn gecontroleerd? Zo nee, waarom niet?

Er bestaat een risico dat apparaten die worden afgegeven aan derden, bijvoorbeeld bij grenscontroles, worden voorzien van middelen om heimelijk informatie weg te halen.

5 Kamerbrief d.d. 22 februari 2011 (Kamerstuk 30821, nr. 13)

Organisaties en overheden zijn zelf verantwoordelijk voor het maken van een risico-inschatting van het gebruik van dergelijke apparaten binnen het bedrijfsnetwerk en het implementeren van maatregelen die het weglekken van informatie kunnen voorkomen. De bovengenoemde Handleiding KWAS ondersteunt organisaties bij het maken van deze risico-inschatting.

5
Hoe beoordeelt u het hacken van telefoons, computers of andere communicatiemiddelen van Nederlandse staatsburgers door een vreemde mogendheid als China of Rusland? Kunt u uw antwoord toelichten?

Dergelijke inlichtingenactiviteiten kunnen de nationale veiligheid aanzienlijke schade toebrengen en de nationale belangen aantasten. Daarom vindt het kabinet dit soort activiteiten ontoelaatbaar. Constatering van dergelijke activiteiten leidt altijd tot het nemen van maatregelen.

6
Welke gevaren ziet u voor Nederland wanneer landen als China en Rusland (en eventueel ook andere landen) zich op grote schaal aan cyberspionage schuldig maken?

Informatie op economisch, technisch-wetenschappelijk, militair en politiek terrein kan als gevolg van spionage weglekken naar het buitenland. Deze spionage kan een dreiging tegen de staatsveiligheid en de nationale belangen van Nederland vormen. Het kan daarnaast leiden tot economische schade, het verlies van concurrentiepositie van Nederlandse bedrijven en de koppositie die Nederland in bepaalde sectoren bekleed.