Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

> Retouradres Postbus 16950 2500 BZ Den Haag

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

Nationaal Coördinator Terrorismebestrijding en Veiligheid
DCS

Oranjebuitensingel 25
2511 VE Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Ons kenmerk
367400

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 25 maart 2013
Onderwerp Beantwoording van schriftelijke vragen over het Mandiant-rapport met kenmerk 2013Z03557

Hierbij bied ik u, mede namens de Ministers van Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken en Defensie de antwoorden aan op schriftelijke Kamervragen die zijn gesteld door de leden Bonis, Oosenbrug en Eijsink (allen PvdA over het Mandiant Intelligence Center-rapport over massale cyber-spionage in de Verenigde Staten door een groep hackers (APT1) in Shanghai (2013Z03557 van 25 februari 2013)

De Minister van Veiligheid en Justitie,

I.W. Opstelten

2013Z03557

Vragen van de leden Bonis, Oosenbrug en Eijsink (allen PvdA) aan de ministers van Buitenlandse Zaken, van Veiligheid en Justitie en van Defensie over het Mandiant Intelligence Center-rapport over massale cyber-spionage in de Verenigde Staten door een groep hackers (APT1) in Shanghai (ingezonden 25 februari 2013)

Nationaal Coördinator Terrorismebestrijding en Veiligheid
DCS

Datum
20 maart 2013

Ons kenmerk
367400

Vraag 1
Heeft u kennis genomen van het rapport van het Amerikaanse computerbeveiligingsbedrijf Mandiant "APT1: ExposingOne of China's Cyber Espionage Units" van 19 februari 2013?

Antwoord
Ja.

Vraag 2
Hoe beoordeelt u de conclusie van het rapport dat een groep hackers in Shanghai – naar Mandiant's overtuiging aantoonbaar in dienst van de Chinese krijgsmacht als Unit 61398 – zes jaar lang systematisch honderden terabytes aan data heeft gestolen van tenminste 141 bedrijven, organisaties en overheidsinstanties, voornamelijk, doch niet uitsluitend in de Verenigde Staten?

Antwoord
Wij beschikken voor deze conclusie niet over sluitend bewijs. Wel past het rapport in het beeld dat wij hebben van de aard en omvang van digitale spionage.

Vraag 3
Welke gevolgtrekkingen verbindt u aan de conclusie van het rapport dat de APT1-groep zich speciaal richt op het compromitteren van bedrijven en organisaties in allerlei takken van nijverheid in Engelssprekende landen, waaronder qua bedrijvigheid in principe ook Nederland gerekend kan worden?

Vraag 4
Acht u het aannemelijk dat de onderhavige groep dan wel andere Chinese hackers op grote schaal informatie ontfutselen aan bedrijven en instellingen in Nederland? Zo ja, welke maatregelen staan u voor ogen om deze dreiging het hoofd te bieden?

Vraag 6
Zijn er bij het NCSC concrete gevallen bekend van computerspionage-activiteiten van Chinese hackers in Nederland? Zo ja, zijn er aanwijzingen dat deze opereren in opdracht van de Chinese overheid?

Nationaal Coördinator Terrorismebestrijding en Veiligheid
DCS

Datum
20 maart 2013

Ons kenmerk
367400

Antwoord vragen 3, 4 en 6
In de opeenvolgende Cyber Security Beelden, die mede zijn gebaseerd op informatie van de inlichtingen- en veiligheidsdiensten, van het Nationaal Cyber Security Centrum (NCSC) is aangegeven dat digitale spionage en cybercriminaliteit de grootste dreigingen voor overheid en bedrijfsleven vormen. Ook in de jaarverslagen van 2011 van de inlichtingen- en veiligheidsdiensten is vermeld dat spionage zich in toenemende mate in het digitale domein afspeelt. Daarbij is bekend dat statelijke actoren, waaronder China,proberen gevoelige politieke, militaire, technisch-wetenschappelijke en economische informatie te verkrijgen. Naar aanleiding van het AIVD-jaarverslag van 2011, waarin melding wordt gemaakt van spionage-activiteiten door de Chinese inlichtingendienst in Nederland, is er ambtelijk contact geweest met de Chinese overheid.

Gelet op de geavanceerde ICT-infrastructuur en de aard van de Nederlandse economie is het waarschijnlijk dat de digitale cyberactiviteiten in aard en omvang zullen toenemen en, zoals in de Nationale Risico Beoordeling is vermeld, in potentie een aanzienlijke dreiging vormen voor de Nederlandse economie en de nationale veiligheid. De AIVD en MIVD bundelen daarom hun krachten in de gezamenlijke sigint-cyber eenheid en investeren in digitale onderzoekscapaciteit en –expertise. Het betreft hier ondermeer uitbreiding van de detectiecapaciteit teneinde het zicht op cyberspionage in Nederland te vergroten. Daarnaast investeert Defensie in cybercapaciteiten. Bij al deze activiteiten wordt nauw samengewerkt met het NCSC, waarbij het NCSC zijn achterban actief waarschuwt voor kwetsbaarheden en adviseert over te nemen maatregelen. Door de snelle technologische ontwikkelingen binnen het cyberdomein, wordt thans door de Evaluatiecommissie Wiv 2002 onderzocht of het wettelijke instrumentarium van de inlichtingen- en veiligheidsdiensten toereikend is om de huidige dreigingen effectief het hoofd te bieden.

In april 2010 heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties de Kwetsbaarheidsanalyse Spionage (KWAS) aangeboden aan de Tweede Kamer. Uw Kamer is per brief d.d. 22 februari 2011 (Kamerstuk 30821, nr 13) op de hoogte gebracht van de aanpak naar aanleiding van dit onderzoeksrapport. 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 eind 2012 een e-learning module beschikbaar gesteld.

Concrete gevallen van spionage kunnen schadelijk zijn voor de nationale veiligheid en de nationale belangen aantasten. Het kabinet vindt dit soort activiteiten ontoelaatbaar. Wanneer dergelijke activiteiten geconstateerd worden, zullen passende maatregelen genomen worden.

Vraag 5
Bent u bereid het Nationaal Cyber Security Centrum (NCSC) op te dragen in contact te treden met Mandiant om additionele inlichtingen te verkrijgen ten bate van de nationale veiligheid?

Nationaal Coördinator Terrorismebestrijding en Veiligheid
DCS

Datum
20 maart 2013

Ons kenmerk
367400

Antwoord
De inlichtingen- en veiligheidsdiensten staan in contact met internationale collega-diensten i.v.m. het Mandiant-rapport. Het NCSC heeft contact met de Amerikaanse CERT, die onder het Department of Homeland Security ressorteert en nader onderzoek doet naar het rapport. Op basis van de verstrekte gegevens worden zowel de Rijksoverheid, de defensie-industrie als de vitale sectoren actief geïnformeerd.

Vraag 7
Zijn er contacten met de Chinese autoriteiten over hackers-activiteiten vanuit China? Zo ja, hoe verlopen die?

Antwoord
In EU-verband zijn er contacten met China over cyberveiligheid. Tijdens de 14e EU-China Top van februari 2012 is besloten tot de oprichting van een EU-China Cyber werkgroep. In september 2012 vond het eerste overleg van deze EU-China werkgroep plaats, die vooral oriënterend van aard was en in het teken stond van mogelijke aandachtsgebieden, zoals de aanpak van cybercriminaliteit, bestaande internationale regelgeving en economische aspecten van cyberspace en mogelijke samenwerking. Dit jaar zal een tweede overleg in Brussel plaatsvinden.

Daarnaast is naar aanleiding van het AIVD-jaarverslag van 2011, waarin melding wordt gemaakt van spionage-activiteiten door de Chinese inlichtingendienst in Nederland, ambtelijk contact geweest met de Chinese overheid.

Vraag 8
Bent u bereid om internationaal aandacht te vragen voor de problematiek rondom cyber-spionage?

Antwoord
Nederland vraagt internationaal reeds actief aandacht voor de problematiek van cyberdreigingen, waaronder cyberspionage, zowel in bilaterale contacten als in EU- en NAVO-verband. Daartoe worden de Nederlandse cybersecurity strategie en het jaarlijkse Cyber Security Beeld Nederland gedeeld met andere landen. In Europees verband zet het kabinet zich onder meer in om een gedeeld dreigingsbeeld te realiseren.

Vraag 9
Hoe beoordeelt u de beginnende inspanningen in VN-verband om tot een multilateraal cyber-wapenbeheersingsregime te komen en, meer specifiek, de rol van China daarin? Is er sprake van Nederlandse betrokkenheid bij deze inspanningen?

Nationaal Coördinator Terrorismebestrijding en Veiligheid
DCS

Datum
20 maart 2013

Ons kenmerk
367400

Antwoord
Enkele landen, waaronder China, hebben in 2011 een aanzet gegeven tot het formuleren van een multilateraal cyberverdrag, wat onder andere in VN- en OVSE-verband naar voren is gebracht. Er is echter geen internationale overeenstemming over de noodzaak van een dergelijk verdrag en de eventuele invulling daarvan.Nederland is van mening dat bestaande regels van internationaal en Europees recht ten aanzien van het gebruik van digitaal geweld en criminaliteit voldoen. Hiertoe dient onder andere het Boedapest Verdrag over cybercrime. Nederland ondersteunt wel de ontwikkeling van gedragsnormen om uitwerking te geven aan de toepassing van internationaalrechtelijke bepalingen in het digitale domein. Nederland neemt daartoe actief deel aan de discussie over gedragsnormen in het digitale domein, allereerst om een open en vrij internet te behouden en tegenwicht te bieden aan landen die het vrije gebruik van internet en media aan banden willen leggen in naam van veiligheid en bestrijden van cybercriminaliteit. Tegelijkertijd onderkent het kabinet het belang om potentiële conflicten tussen landen als gevolg van cyberincidenten te voorkomen.

10
Bent u bereid om in EU-verband te pleiten voor een gemeenschappelijke aanpak van hackers-activiteiten afkomstig van buiten de EU?

Antwoord
De EU heeft recentelijk een integrale cybersecurity strategie gelanceerd waarin onder meer aandacht wordt geschonken aan het weerbaar maken van cyberspace, de risico's en dreigingen die uitgaan van het digitale domein en de adequate reactie op die dreigingen. De strategie gaat ook in op het externe beleid van de EU ten aanzien van cyberdreigingen. Nederland zal de geïntegreerde benadering blijven bewaken bij de uitvoering van de strategie, en een voortrekkersrol blijven spelen in de implementatie van deze strategie, onder andere via de *Friends of the Presidency* groep over cyberzaken.