Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

Aanhangsel van de Handelingen

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

3023

Vragen van het lid **Vuijk** (VVD) aan de Minister van Defensie over *het bericht «Nederlands-Duits defensiebedrijf gehackt door Chinezen»* (ingezonden 16 juni 2016).

Antwoord van Minister **Hennis-Plasschaert** (Defensie) (ontvangen 4 juli 2016).

Vraag 1
Bent u bekend met het bericht «Nederlands-Duits defensiebedrijf gehackt door Chinezen»?[1]

Antwoord 1
Ja.

Vraag 2
Klopt het dat geheime data van het Nederlands-Duitse bedrijf Rheinmetall Defence is gestolen bij een cyberaanval door Chinese hackers? Klopt het dat deze aanval al in 2012 gestart is? Zijn vanaf die datum gegevens gestolen? Graag een toelichting.

Antwoord 2
Het is niet aan het Ministerie van Defensie om dergelijke berichtgeving te ontkrachten of te bevestigen. Zoals in het meest recente jaarverslag van de MIVD is opgemerkt, is het bekend dat een aantal actoren actief probeert waardevolle (bedrijfs)informatie via het digitale domein te ontvreemden (Kamerstuk 33 321, nr. 7 van 15 maart 2016).
In het hier aangehaalde artikel bevestigen Rheinmetall Defence noch Fox-IT dat er data is gestolen als gevolg van digitale spionage. Uit het onderzoeksrapport dat Fox-IT publiek heeft gemaakt is evenmin gebleken dat Rheinmetall Defence slachtoffer is geweest van digitale spionage.

Vraag 3
Klopt het dat het Delftse bedrijf Fox-IT het lek aan het licht heeft gebracht? Werkt Fox-IT samen met andere overheidsinstellingen? Graag een toelichting.

[1] http://www.volkskrant.nl/buitenland/nederlands-duits-defensiebedrijf-gehackt-door-chinezen~a4320398/

ah-tk-20152016-3023
ISSN 0921 - 7398
's-Gravenhage 2016

Antwoord 3
Zie het antwoord op vraag 2.
Veel publieke en private partijen beschikken over expertise op het terrein van cyber security. Zo beschikt ook Fox-IT over expertise, maar Fox-IT is niet de enige. Ook Defensie werkt samen met Fox-IT, onder andere bij het opleiden van cyberprofessionals (zie ook Kamerstuk 33 321, nr. 7 van 15 maart 2016).

Vraag 4
Kunt u toelichten hoe de verantwoordelijkheidsverdeling tussen het Ministerie van Defensie en Nederlandse bedrijven is vormgegeven als het gaat om de bescherming van ICT-infrastructuur tegen malafide hackers? In hoeverre ziet het Ministerie van Defensie het als haar taak om ICT-infrastructuur van private (defensie)bedrijven te beschermen? In hoeverre moeten (defensie)bedrijven zelf waken over hun ICT-infrastructuur?

Antwoord 4
Hoewel in Nederland de bescherming van ICT-infrastructuur primair een eigen verantwoordelijkheid van iedere organisatie is, hecht Defensie grote waarde aan veiligheid in zijn keten van leveranciers en opdrachtnemers. Defensie heeft daarom de Algemene Beveiligingseisen voor Defensie Opdrachten, de zogenaamde ABDO, vastgesteld. In het ABDO zijn contractuele voorwaarden opgenomen die beschrijven aan welke veiligheidseisen moet worden voldaan voordat Defensie gerubriceerde opdrachten aan een opdrachtnemer of leverancier kan gunnen. Deze voorwaarden worden op dit moment geactualiseerd om onder andere de digitale dreiging beter te adresseren. De MIVD ziet toe op handhaving van deze eisen en voert audits uit bij de betrokken bedrijven.

Vraag 5
In hoeverre is het Ministerie van Defensie in staat om zich tegen hacks en vergelijkbare aanvallen te beschermen? In hoeverre is het Ministerie van Defensie in staat de private defensiesector tegen hacks en aanvallen te beschermen?

Antwoord 5
De dreiging van digitale spionage bij Defensie, toeleveranciers, bondgenootschappelijke netwerken en producenten van militair-relevante producten is aanzienlijk. Zoals eerder dit jaar in het jaarverslag van de MIVD gemeld, neemt deze dreiging in omvang en geavanceerdheid toe en worden actoren steeds agressiever (Kamerstuk 33 321, nr. 7 van 15 maart 2016). Defensie slaat dagelijks aanvallen af. Voortdurende versterking van de digitale weerbaarheid is niettemin geboden. Deze versterking maakt deel uit van de Defensie Cyber Strategie (Kamerstuk 33 321, nr. 5 van 23 februari 2015).
De maatregelen om de eigen informatietechnologie-systemen (IT-systemen) veilig te houden, maken deel uit van de diensten en producten die het Joint IV Commando (JIVC), waaronder het Defensie *Computer Emergency Response Team* (DefCERT), en de directie *Operations* van de Defensie Materieel Organisatie leveren. De MIVD heeft een belangrijke rol bij het tegengaan van spionage en sabotage. Defensie ontwikkelt doorlopend nieuwe beveiligingsmethodieken om nieuwe dreigingen (vroegtijdig) te kunnen onderkennen en af te slaan.
Defensie wisselt dreigingsinformatie uit in het *Information Sharing and Analysis Centre* (ISAC) voor de defensie-industrie[2] en deelt deze tevens waar mogelijk met de private sector door tussenkomst van het Nationaal Cyber Security Centrum (NCSC), waarbij het NCSC zich richt op de rijksoverheid en de vitale infrastructuur. Defensie draagt ook op andere manieren bij aan de digitale veiligheid van Nederland, zoals het op verzoek van NCSC beschikbaar stellen van cyberprofessionals bij incidenten, maar het beschermen van de private sector is geen taak van Defensie.

[2] https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/inhoud/industrieveiligheid