Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

Aanhangsel van de Handelingen

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

372

Vragen van het lid **Van den Bosch** (VVD) aan de Minister van Defensie over *het bericht «Hacker steelt Australische JSF-bestanden»* (ingezonden 13 oktober 2017).

Antwoord van Staatssecretaris **Visser** (Defensie) (ontvangen 9 november 2017).

Vraag 1
Bent u bekend met het artikel «Hacker steelt Australische JSF-bestanden»?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u bevestigen dat er bij de Australische krijgsmacht informatie is gestolen over het F-35 project? Onderschrijft u de lezing van uw Australische collega dat hierbij geen sprake is geweest van diefstal van uiterst geheime informatie die de nationale veiligheid in gevaar brengt? Kunt u uw antwoord toelichten?

Antwoord 2
In het desbetreffende artikel wordt gesproken over een inbraak in het computernetwerk van een Australische leverancier. Deze is bij het F-35 programma betrokken via commerciële contracten met onderleveranciers van de Amerikaanse hoofdcontractanten. De Australische krijgsmacht is geen partij bij die contracten. Uit onderzoek dat Australië naar de toedracht van het incident heeft ingesteld, is gebleken dat de F-35 gegevens waartoe mogelijk toegang is verkregen geen gerubriceerde (geheime) informatie bevatten.

Vraag 3
Had hierbij informatie gestolen kunnen worden die de Nederlandse nationale veiligheid had kunnen bedreigen, nu of in de toekomst? Zo ja, heeft u de garantie dat dit niet gebeurd is?

[1] https://www.telegraaf.nl/nieuws/784928/hacker-steelt-australische-jsf-bestanden

ah-tk-20172018-372
ISSN 0921 - 7398
's-Gravenhage 2017

Antwoord 3
Het verlies van niet-gerubriceerde informatie brengt de nationale veiligheid niet in gevaar.

Vraag 4
Om wat voor documenten ging het wel en welke waarde kunnen die documenten hebben voor derden, waaronder andere landen? Geven de documenten bijvoorbeeld belangrijke informatie over technische specificaties, waarmee derden een F-35 of onderdelen daarvan zouden kunnen ontwerpen/bouwen, of waarmee offensieve of defensieve capaciteiten van de F-35 kwetsbaar worden? Kunt u uw antwoord toelichten?

Antwoord 4
Er zijn geen details over de niet-gerubriceerde F-35 informatie verstrekt. Informatie benodigd voor het ontwerp en de bouw van complexe onderdelen, alsmede informatie over de capaciteiten van de F-35 is hoog-gerubriceerd (geheim/zeer geheim). Tot dergelijke informatie is blijkens het onderzoek geen toegang verkregen.

Vraag 5
Welke protocollen bestaan er binnen de internationale F-35 projectgroep bij eventuele diefstal van informatie? Zijn deze effectief gebleken?

Antwoord 5
Verlies van informatie wordt behandeld als een veiligheidsincident, waarnaar het desbetreffende partnerland en/of het *Joint Program Office* (JPO) altijd een onderzoek instelt. Hierbij bepaalt de ernst van het incident de omvang en diepgang van het onderzoek. Onderzoeksuitkomsten die relevant zijn voor de internationale F-35 projectgroep, waartoe ook Nederland behoort, worden aan de groepsleden beschikbaar gesteld om soortgelijke incidenten in de toekomst te voorkomen. Aangezien het bij dit incident informatie van een commerciële partij betrof, zijn de *International Traffic in Arms Regulations (ITAR)* van toepassing en is in eerste instantie melding gemaakt van het incident in de commerciële keten van de Australische leverancier, andere betrokken contractpartijen en de hoofdcontractant.

Vraag 6
Bestaan er binnen de internationale F-35 projectgroep bepaalde voorwaarden op het gebied van cybersecurity om als partnerland beschikking te krijgen tot de geheime informatie aangaande het F-35 project? Zo ja, voldeed Australië aan deze voorwaarden? Zo ja, dienen deze voorwaarden in het licht van dit hack dan verder aangescherpt te worden?

Antwoord 6
Het JPO ziet erop toe dat de beveiligingsmaatregelen, ook op het gebied van cybersecurity, die partnerlanden moeten toepassen op informatie die betrekking heeft op het F-35 programma, correct worden uitgevoerd. Daartoe dienen landen aan hoge veiligheidseisen te voldoen, wat voor Australië het geval is. Cybersecurity heeft bij het JPO en de F-35 partnerlanden hoge prioriteit en is een voortdurend punt van aandacht. Indien nodig worden de veiligheidseisen en maatregelen aangescherpt. Daarnaast is in de *Amerikaanse International Traffic in Arms Regulations* (ITAR) vastgelegd aan welke eisen commerciële bedrijven moeten voldoen voor de bescherming van informatie.

Vraag 7
Kunt u garanderen dat alle F-35 informatie in Nederland veilig is voor diefstal? Heeft u informatie gehad van uw Australische collega over dit hack en heeft dit geleid tot aanpassingen c.q. intensivering van de Nederlandse cybersecurity?

Antwoord 7
Nederland voldoet aan alle veiligheidseisen die het JPO partnerlanden oplegt voor de bescherming van F-35 informatie. Verder verwijs ik naar het antwoord op vraag 5.

Vraag 8
Wordt er nader onderzoek gedaan naar wie achter de hack heeft gezeten? Kunt u uw antwoord toelichten?

Antwoord 8
Om veiligheidsredenen kan ik niet op deze vraag ingaan en verwijs ik naar het antwoord op vraag 5.