Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

Aanhangsel van de Handelingen

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

2104

Vragen van het lid **Hachchi** (D66) aan de staatssecretaris van Infrastructuur en Milieu over *het bericht «Kwaadwillende kan vliegtuig op afstand hacken»* (ingezonden 12 april 2013).

Antwoord van staatssecretaris **Mansveld** (Infrastructuur en Milieu) (ontvangen 1 mei 2013)

Vraag 1
Heeft u kennisgenomen van het bericht «Kwaadwillende kan vliegtuig op afstand hacken»?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u de Kamer informeren hoe het met de computerbeveiliging van de Nederlandse luchtvaartindustrie is gesteld?

Antwoord 2
In de luchtvaart wordt een veelheid aan computersystemen gebruikt, zoals bij radar, communicatie, GPS-satelliet navigatie, documentatie systemen (on-board manuals). Deze systemen worden qua prestaties en veiligheid veelal meegenomen in de technische certificatie van vliegtuigen, en regelmatig vernieuwd («update»). Technische specificaties terzake worden ontwikkeld door onder andere internationale luchtvaartgremia, zoals EASA, ICAO en Eurocontrol. Vaak gaat uitvoerig onderzoek vooraf aan vaststelling van dergelijke specificaties.
De eisen zijn veelal vastgelegd in sectorale wetgeving op het gebied van luchtvaartveiligheid, zoals bijvoorbeeld in Europese Luchtvaart wet- en regelgeving, alsook in (uitvoeringsregelingen onder) de Wet Luchtvaart.
De Inspectie Leefomgeving en Transport houdt op de implementatie van deze wetgeving toezicht. Het luchtvaartbedrijfsleven stelt zich bij de implementatie van deze wetgeving actief op.
De minister van Veiligheid en Justitie is coördinerend bewindspersoon voor nationale veiligheid en cyber security en verantwoordelijk voor het Nationaal Cyber Security Centrum (NCSC). Het NCSC faciliteert de Airport-Information

[1] http://tweakers.net/nieuws/88408/kwaadwillende-kan-vliegtuig-op-afstand-hacken.html

ah-tk-20122013-2104
ISSN 0921 - 7398
's-Gravenhage 2013

Sharing and Analysis Center (ISAC) waar informatie uitgewisseld wordt over ICT-kwetsbaarheden en oplossingen binnen de luchtvaartsector.

Vraag 3
Bent u het eens met de stelling dat de overheid hier een rol speelt vanwege het veiligheidsaspect ondanks dat het hier om vliegtuigen van private partijen gaat?

Antwoord 3
Ja, de transportsector in algemene zin, en de luchtvaartsector in het bijzonder, maakt deel uit van de nationale vitale infrastructuur (net als bijvoorbeeld de haven Rotterdam) en valt daarmee nadrukkelijk binnen het aandachtsgebied.
Voorts vertaalt deze verantwoordelijkheid zich in relevante wet- en regelgeving, alsmede toezicht en handhaving daarop (zie antwoord op vraag 2). Tevens wordt daarbij door middel van het inrichten en deelnemen aan crisisoefeningen binnen de luchtvaartsector de preparatie en respons op eventuele incidenten geoptimaliseerd.

Vraag 4
Hoe oud zijn de systemen gemiddeld in Nederlandse vliegtuigen en in vliegtuigen die op Nederlandse luchthavens vliegen? Wat is de hackgevoeligheid van deze vliegtuigen volgens u?

Antwoord 4
Zoals aangegeven bij vraag 2 wordt bij de vluchtuitvoering een veelheid aan systemen gebruikt, die qua prestaties en veiligheid over het algemeen worden meegenomen in de technische certificatie van vliegtuigen. Daarnaast worden deze systemen ook regelmatig vernieuwd («update») en gecontroleerd op hun functionaliteit.
Naar aanleiding van het onderzoek naar de hackgevoeligheid dat in de media werd aangehaald, en waarvan de resultaten werden gepresenteerd tijdens de «hackers» bijeenkomst in Amsterdam, thans het volgende: EASA en de FAA (de Amerikaanse federale luchtvaartautoriteit) hebben aangegeven dat de beveiliging van de simulatiesoftware die in het betreffende onderzoek is gebruikt wezenlijk lager is dan de gecertificeerde systemen die in de praktijk aan boord van vliegtuigen gebruikt worden. Bij voornoemd onderzoek betreft het nadrukkelijk een testopstelling en een theoretische kwetsbaarheid. De in de praktijk gebruikte en gecertificeerde systemen kennen een hogere mate van beveiliging, bijvoorbeeld waar het gaat om het aanpassen/beïnvloeden van bijvoorbeeld vluchtdata. In een reactie op voornoemd onderzoek geven EASA en FAA aan dat de ontwikkeling van gecertificeerde on-boardsystemen al ruim 30 jaar plaatsvindt op basis van strikte normen voor robuustheid die niet aanwezig zijn in simulatiesoftware.
Dit betekent dat niet op voorhand kan worden aangenomen dat de geconstateerde theoretische kwetsbaarheden in het onderzoek daadwerkelijk van toepassing zijn op on-board systemen.

Vraag 5
Wordt er al aan oplossingen gewerkt? Welke mogelijkheden ziet u om dit te versnellen?

Antwoord 5
Ondanks de verschillen tussen een gesimuleerde en echte omgeving (zie vraag 4) hebben betrokken partijen aangegeven om de gepresenteerde onderzoeks-resultaten te gaan testen in systemen in de praktijk, teneinde het risico zo klein mogelijk te maken. Daarnaast heeft het NCSC de relevante publieke en private partners vanuit haar expertise op het gebied van cyber security geïnformeerd over deze casus zodat de partners op grond van hun eigen verantwoordelijkheid maatregelen kunnen nemen.
Nederland speelt een actieve rol bij de internationale (luchtvaart) beleidsontwikkeling op dit terrein, en zal dit blijven doen. Daarin worden relevante technologische ontwikkelingen meegenomen, en worden initiatieven van internationale (luchtvaart) gremia zorgvuldig bezien. Daar waar het de luchtvaartveiligheid raakt zullen technologische ontwikkelingen uiteraard

versneld worden opgepakt om de hoge mate van veiligheid waar de luchtvaartsector om bekend staat blijvend op het hoge niveau te houden. Zie verder antwoord op vraag 4.

Vraag 6
Welke maatregelen neemt u voor de korte termijn om dit probleem aan te pakken?

Antwoord 6
Zie antwoord op vraag 4 en 5.