Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

Aanhangsel van de Handelingen

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

1948

Vragen van de leden **Hijink** en **Lain** (beiden SP) aan de Staatssecretarissen van Infrastructuur en Milieu en van Veiligheid en Justitie over *de ICT-storing in het systeem van Amadeus waardoor overal ter wereld reserveringssystemen voor de luchtvaart uitvielen* (ingezonden 25 april 2017).

Antwoord van Staatssecretaris **Dijksma** (Infrastructuur en Milieu) mede namens de Staatssecretaris van Veiligheid en Justitie (ontvangen 24 mei 2017).

Vraag 1
Wat is uw reactie op het bericht dat een storing in het reserveringssysteem van Amadeus overal ter wereld voor overlast heeft gezorgd?[1]

Antwoord 1
Ik heb kennis genomen van het feit dat er een storing is geweest in het reserveringssysteem van Amadeus. Naar aanleiding van deze casus heb ik contact gehad met de luchtvaartsector. Uit de gesprekken blijkt dat er slechts sprake is geweest van een kortstondige verstoring die snel is verholpen.

Vraag 2 en 3
Bent u bekend met de oorzaak van deze storing? Was hier sprake van het moedwillig platleggen van het systeem door hackers of was er een andere oorzaak?
Kunt u aangeven of tijdens of na de storing privacygevoelige informatie van reizigers of luchtvaartpersoneel in verkeerde handen is gevallen?

Antwoord 2 en 3
Mij is uit informatie van betrokken partijen gebleken dat vanwege een lokaal hardware probleem in het data centrum bij Amadeus, de systemen bij Amadeus gedurende een korte tijd niet bereikbaar waren. Amadeus heeft hierop aan KLM bevestigd dat hier geen hack of een andere moedwillige actie aan ten grondslag lag. Hierbij is door Amadeus tevens aangegeven dat er door of als gevolg van de storing geen privacygevoelige informatie van reizigers of luchtvaartpersoneel in verkeerde handen is gevallen. Ook andere maatschappijen, voornamelijk in Europa, hebben last gehad van deze storing. Het verhelpen van storingen is uiteraard de verantwoordelijkheid van de eigenaar van desbetreffende systemen, zoals Amadeus.

[1] http://nos.nl/l/2169313

ah-tk-20162017-1948
ISSN 0921 - 7398
's-Gravenhage 2017

Vraag 4
Welke stappen worden ondernomen om nieuwe storingen in de toekomst te voorkomen? Zijn de systemen van Amadeus in uw ogen voldoende beveiligd tegen hackers en voldoet de technologie nog wel aan de eisen van deze tijd?

Antwoord 4
De verantwoordelijkheid voor de informatiebeveiliging ligt in dit geval bij de eigenaar van systemen. In het openbaar worden over de veiligheid van individuele systemen geen mededelingen gedaan, juist gelet op de veiligheid. Wel kan ik u aangeven dat tussen de betrokken private partijen onderling sprake is van contractuele afspraken. In het contact met het Ministerie van Infrastructuur en Milieu is door KLM aangegeven dat storingen altijd samen met Amadeus geëvalueerd worden en er afspraken worden gemaakt over verbeterstappen. Deze specifieke storing is door Amadeus onderzocht en er zijn maatregelen genomen. KLM heeft contractuele afspraken met Amadeus over de beschikbaarheid van de systemen, inclusief boeteclausules als Amadeus daar niet aan voldoet.

Vraag 5
Welke gevaren ziet u in de wereldwijde inzet van het reserveringssysteem van Amadeus? Is de gevoeligheid van het systeem niet te groot als een storing direct leidt tot vertraging en uitval van vluchten overal ter wereld?

Antwoord 5
Digitalisering is doorgedrongen in de haarvaten van de samenleving. Het is daarom onontkoombaar dat er een bepaalde afhankelijkheid van ICT-systemen ontstaat, echter het gebruik van dergelijke systemen heeft ook nadrukkelijke voordelen. Zo leidt het gebruik van Amadeus door wereldwijde inzet tot grotere uniformiteit en wordt daardoor de efficiëntie aanzienlijk vergroot. Vanwege de afhankelijkheid is het van groot belang dat door de eigenaar in het licht van de eigen verantwoordelijkheid reeds maatregelen zijn getroffen om de continuïteit van dit systeem te borgen.

Vraag 6
Is er een inschatting te maken van de economische schade die deze storing heeft veroorzaakt? Welke gevaren voor de economie en voor reizigers ziet u voor de toekomst als een dergelijke storing zich opnieuw voordoet?

Antwoord 6
Een schatting is vanuit de overheid niet te geven. De economische schade heeft zich in ieder geval geuit in de vorm van tientallen vertraagde vluchten en een uur durende verstoring van de online ticketverkoop.

Vraag 7, 8 en 9
Klopt het dat luchtvaartmaatschappijen geen of weinig alternatieven hebben bij een grote uitval van digitale systemen? Hoe kwetsbaar maakt dit de hele sector in geval van toekomstige storingen?
In hoeverre is deze storing voor u een nieuwe waarschuwing dat onze samenleving steeds kwetsbaarder wordt voor ICT-storingen en acties van hackers? Zijn voor vitale infrastructuren voldoende off-line back-up voorzieningen aanwezig?
Bent u bereid extra maatregelen te nemen om cruciale digitale infrastructuur beter te beschermen en hierover in contact te treden met bedrijven en publieke organisaties die hiervoor verantwoordelijk zijn?

Antwoord 7, 8 en 9
In lijn met de conclusies in het Cybersecuritybeeld Nederland 2015[2] is het in algemene zin inderdaad zo dat er steeds minder fysieke alternatieven zijn op het moment dat digitale voorzieningen niet werken. Uiteraard maakt dit kwetsbaar. Dit is ook de reden waarom door de sector wordt gewerkt aan passende maatregelen. Zo zijn er draaiboeken om de negatieve gevolgen van grote verstoringen, zoals extreem weer, elektriciteitsstoring en uitval van

[2] Nationaal Cyber Security Centrum, Cybersecuritybeeld Nederland, 2015.

ICT-systemen, te beperken, alsmede contractuele afspraken tussen partijen onderling.
Ten overvloede wil ik benadrukken dat, zoals in antwoord op vraag 4 is aangeven, er in het geval van Amadeus geen sprake was van een aanval door een hacker, en dat het dus geen waarschuwing in die zin is. Het is echter wel een illustratie van de toegenomen afhankelijkheid van ICT-voorzieningen.
Op dit moment wordt door het Ministerie van Veiligheid en Justitie samen met de betrokken vakdepartementen gewerkt aan de totstandbrenging van de implementatiewetgeving betreffende de Netwerk- en informatiebeveiligingsrichtlijn (NIB-richtlijn), waarin voor aanbieders van essentiële diensten en digitale dienstverleners zorgplichten betreffende de continuïteit van hun dienstverlening alsook handhaving van de naleving daarvan zijn vastgelegd. Hierover wordt uw Kamer, conform eerder toezegging, op reguliere wijze door de Staatssecretaris van Veiligheid en Justitie geïnformeerd. Uiteraard staan we hierbij in nauw contact met de private sector. Dit in aanvulling op reguliere overlegstructuren.

Vraag 10
Deelt u de mening dat de overheid een grotere rol zou moeten spelen in het verbeteren van de cybersecurity in ons land? Dient de bescherming van publieke belangen niet gepaard te gaan met een actievere rol van de overheid in de bescherming van onze digitale infrastructuur?

Antwoord 10
De overheid heeft de afgelopen jaren ingezet op het verhogen van de digitale weerbaarheid, ofwel de cybersecurity, van de vitale infrastructuur. Zoals reeds aangeven, wordt door de implementatie van de NIB-richtlijn tevens invulling gegeven aan het realiseren van een beveiligingsverplichting voor de vitale infrastructuur.