Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2010–2011 **Aanhangsel van de Handelingen**

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

3626

Vragen van het lid **El Fassed** (GroenLinks) aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Buitenlandse Zaken over *internetcertificaten* (ingezonden 31 augustus 2011).

Antwoord van minister **Donner** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de ministers van Veiligheid en Justitie, van Buitenlandse Zaken, van Defensie en van Economische Zaken, Landbouw en Innovatie (ontvangen 13 september 2011).

Inleiding
In antwoord op het verzoek van het lid Heijnen in de regeling van werkzaamheden van 7 september 2011 (kenmerk 2011Z17081) deel ik u mee, mede namens de minister van Veiligheid en Justitie, dat het kabinet uw Kamer, zoals verzocht, per brief nader zal informeren over de gebeurtenissen, voorafgaande aan het plenaire debat hierover. In die brief zal ik ook ingaan op de belangrijkste berichten in de media over de veiligheid van overheidswebsites.

Vraag 1
Kent u het bericht[1] in onder meer Webwereld dat Iran erin is geslaagd om het internetverkeer van haar burgers naar Google.com af te tappen door middel van een vervalst beveiligingscertificaat bij de Nederlandse certificeringsautoriteit Diginotar?

Antwoord 1
Ja.

Vraag 2
Bent u ermee bekend dat het zogeheten «root-certificaat» van de uitgever van het door Iran vervalste certificaat, het bedrijf Diginotar, ongeldig is verklaard door Microsoft en Mozilla, en mogelijk door andere softwareleveranciers?

Antwoord 2
Het is ons bekend dat de certificaten van het bedrijf DigiNotar door de webbrowsers niet meer als betrouwbaar worden aangemerkt. Leveranciers van besturingssystemen en applicatiesoftware kunnen een update doorvoe-

[1] http://webwereld.nl/nieuws/107747/iran-kan-gmail-aftappen-door-nederlands-certificaat--update-2--.html

ah-tk-20102011-3626
ISSN 0921 - 7398
's-Gravenhage 2011

ren van hun systemen met als gevolg dat sommige websites en onderliggende systemen moeilijker – of in het geheel niet – bereikbaar zijn. Een aantal heeft dit ook gedaan.

Vraag 3
Kunt u toelichten op welke wijze door de overheid toezicht werd uitgeoefend op het functioneren van Diginotar? Doet u onderzoek naar de oorzaken van deze zaak?

Antwoord 3
In het stelsel van PKI-Overheid is voorzien dat certificaatleveranciers (CA) jaarlijks worden geaudit naar de opzet en werking van de eisen zoals vastgelegd in het Programma van Eisen PKI-Overheid. Deze audits worden uitgevoerd door gecertificeerde auditors. Zij rapporteren aan de Policy Authority (PA) van PKI-Overheid.
Daarnaast vindt er toezicht plaats door de OPTA[2] op basis van de Telecomwet, indien er sprake is van uitgifte van gekwalificeerde[3] certificaten ten behoeve van de elektronische handtekening. De DigiNotar certificaten waarbij het aangetoonde misbruik heeft plaats gevonden, zijn certificaten waar de OPTA geen bevoegdheid heeft om op toe te zien.
Het Kabinet neemt de structurele betekenis van de gebeurtenissen in ogenschouw. In het licht hiervan voert het ministerie van Binnenlandse Zaken en Koninkrijksrelaties onderzoek uit naar het gehele stelsel en proces rondom PKI-Overheid, inclusief het toezicht daarop. Het ministerie van ELI laat aanvullend daarop onderzoeken in hoeverre de problemen rondom DigiNotar ook consequenties hebben voor de wijze van toezicht op uitgifte van gekwalificeerde certificaten. De Tweede Kamer wordt hierover geïnformeerd zodra meer duidelijk is. Zoals in het regeerakkoord is gesteld zal de Staatssecretaris van Veiligheid en Justitie bovendien een wetsvoorstel indienen dat een meldplicht introduceert voor gebeurtenissen zoals deze bij DigiNotar zijn voorgekomen.

Vraag 4
Kunt u de consequenties van deze zaak toelichten voor de dienstverlening en het interne functioneren van de Nederlandse overheid en andere klanten van Diginotar? Hebben burgers overlast ondervonden van deze zaak en zo ja, in hoeveel gevallen en op welke wijze?

Antwoord 4
De gevolgen van de reactie door internetdienstverleners op het bekend worden van de door DigiNotar afgegeven gecompromitteerde certificaten voor het vertrouwen in het digitale communicatieverkeer zijn groot, ook al is de materiële betekenis van die afgifte mogelijk veel beperkter. Alleen partijen die gebruik maken van certificaten of diensten van DigiNotar lopen het risico dat systemen of communicatie uitvallen. Tot nu toe is geconstateerd dat sommige websites (tijdelijk) uit de lucht zijn.
DigiNotar is niet het enige bedrijf dat certificaten en diensten voor internetverkeer genereert. De certificaten van andere bedrijven worden niet geraakt door de gebeurtenissen bij DigiNotar.
Het Kabinet heeft het operationele beheer van de systemen voor certificering bij DigiNotar gecontroleerd overgenomen, zodat de certificaten gefaseerd kunnen worden ingetrokken en het gebruik van de door hacker aangemaakt en gebruikte certificaten kan worden gemonitord en kan worden bestreden waar dit wordt waargenomen.

---

[2] De Onafhankelijke Post en Telecom Autoriteit (OPTA) voert toezicht uit op de aanbieders van gekwalificeerde certificaten. Deze certificatendienstverleners worden geplaatst in een openbaar register.

[3] Gekwalificeerde certificaten zijn bruikbaar in het elektronische verkeer tussen bedrijven onderling en tussen bedrijven en overheid. PKI-overheidscertificaten worden alleen ingezet in het elektronische verkeer van burgers en bedrijven met de overheid en tussen overheidsinstellingen.

Vraag 5
Acht u het uitgesloten dat Iran of enige andere partij erin kan zijn geslaagd om zich via Diginotar toegang te verschaffen tot vertrouwelijke communicatie van de Nederlandse overheid? Welke stappen heeft u gezet om zich daarvan te vergewissen?

Antwoord 5
Het Kabinet onderzoekt wie betrokken zijn bij het hacken van DigiNotar. Voor een beschrijving van genomen besluiten en ingezette acties verwijs ik naar de Kamerbrief «Digitale inbraak DigiNotar» van 5 september 2011.

Vraag 6
Bent u van plan om Iran op deze zaak aan te spreken?

Antwoord 6
Het Kabinet onderzoekt momenteel wie betrokken zijn bij het hacken van DigiNotar. Op grond van de uitkomsten van dit onderzoek beraadt het Kabinet zich op passende vervolgstappen.

Vraag 7
Acht u het in het licht van deze zaak verstandig om nieuwe certificaten van de Nederlandse overheid toe te vertrouwen aan particuliere bedrijven? Zo nee, overweegt u om certificaten direct door de Nederlandse overheid te laten uitgeven? Zo ja, welke aanvullende eisen overweegt u te stellen aan deze bedrijven? Kunt u dat toelichten?

Antwoord 7
Het feit dat de hacker certificaten namens DigiNotar oneigenlijk heeft aangemaakt, heeft geen gevolgen voor andere certificaatleveranciers. Wanneer de certificaten op een juiste, zorgvuldige wijze zijn gegenereerd, ongeacht door welk bevoegd bedrijf, is er op dit moment geen enkele aanleiding om te twijfelen aan de betrouwbaarheid en veiligheid van deze certificaten en al het internetverkeer dat met behulp van deze certificaten heeft plaatsgevonden.
Tegelijkertijd is het Kabinet van oordeel dat de structurele betekenis van de gebeurtenissen in ogenschouw moeten worden genomen. Als onderdeel daarvan voert het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een onderzoek uit naar het gehele stelsel en proces rondom PKI-Overheid, inclusief het toezicht daarop. Daarnaast zal de DigiNotar problematiek ook geëvalueerd worden met het oog op de gewenste betrouwbaarheid van digitale dienstverlening van en aan bedrijven. De Tweede Kamer wordt hierover geïnformeerd zodra hierover meer duidelijkheid is.