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

3628

Vragen van de leden **Elissen, Hernandez** en **Kortenoeven** (allen PVV) aan de ministers van Veiligheid en Justitie, van Buitenlandse Zaken, van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie over *een blunder bij DigiNotar* (ingezonden 1 september 2011).

Antwoord van minister **Donner** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de ministers van Veiligheid en Justitie, van Buitenlandse Zaken en van Defensie (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 «Browsermakers geven nieuwe versie uit na DigiNotar blunder»?[1]

Antwoord 1
Ja.

Vraag 2
Heeft deze blunder gevolgen voor het gebruik van DigiD omdat DigiNotar het bedrijf is dat de beveiligingscertificaten levert waardoor burgers veilig gebruik kunnen maken van DigiD?

Antwoord 2
Het heeft gevolgen gehad voor het gebruik van DigiD. In de loop van dinsdag 6 september is DigiD overgeschakeld naar een andere certificaatleverancier. Voor die tijd kunnen burgers geconfronteerd zijn met waarschuwingen of meldingen dat de site niet langer vertrouwd kan worden.

[1] «Browsermakers geven nieuwe versie uit na DigiNotar blunder» (http://tweakers.net/nieuws/76445/browsermakers-geven-nieuwe-versies-uit-na-diginotar-blunder.html)

ah-tk-20102011-3628
ISSN 0921 - 7398
's-Gravenhage 2011

Vraag 3
Is er aanleiding om DigiNotar en andere «certificate authorities» aan nadere inspectie te onderwerpen om de privacy van Nederlandse burgers te waarborgen?

Antwoord 3
Het Kabinet heeft in de nacht van vrijdag op zaterdag het operationele beheer van systemen voor certificaten van DigiNotar overgenomen, teneinde de schade van de gebleken inbreuk op de integriteit van het internetverkeer te beperken en de beheersmaatregelen ter beperking van de gevolgen te kunnen treffen. Daardoor wordt een beheersbare migratie naar andere certificaten mogelijk zonder dat dit voor zover bekend additionele risico's schept.
Op dit moment wordt prioriteit gegeven aan het beheersen van het huidige incident en de gevolgen daarvan. Tegelijkertijd constateert het Kabinet 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. De Tweede Kamer wordt hierover geïnformeerd zodra hierover meer duidelijkheid is.

Vraag 4
Gaat de blunder bij DigiNotar naar uw verwachting gevolgen hebben voor de electronische dienstverlening van de overheid? Gaan burgers en/of overheidsonderdelen hier hinder van ondervinden? Zo nee, waarom niet?

Antwoord 4
De inbraak bij DigiNotar en de door de hacker daarbij aangemaakte en gebruikte certificaten vormen een ernstige aantasting van het vertrouwen in en de integriteit van het digitale communicatieverkeer. De aantasting van het vertrouwen in de certificaten van DigiNotar kan potentieel grote implicaties hebben voor zowel het verkeer tussen mens en machine als voor het verkeer tussen machines onderling.
Voor het digitale communicatieverkeer ontstaat door het aanmaken en gebruik van boven genoemde certificaten het risico dat het voor de internetgebruiker niet meer zichtbaar is of hij te maken heeft met een betrouwbare website of computer, blijkend uit het certificaat («slotje») op het scherm. De mogelijke introductie van deze certificaten maakt, dat gebruikers er niet meer in alle gevallen zonder meer van uit kunnen gaan, dat het een veilige internetcommunicatie betreft. In dergelijke gevallen kan de burger worden doorgeleid naar een niet bedoelde site, waarbij de gegevens die de burger verstrekt, in verkeerde handen terechtkomen. Hierdoor wordt het vertrouwen in het digitale communicatieverkeer ernstig aangetast.
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.
Er zijn tot dusver echter geen aanwijzingen dat dit in Nederland ook daadwerkelijk heeft plaatsgevonden.

Vraag 5
Heeft het feit dat bedrijven als Mozilla, Microsoft[2] en Google het vertrouwen in DigiNotar hebben opgezegd gevolgen voor de samenwerking tussen de Nederlandse overheid en DigiNotar?

Antwoord 5
Het Kabinet heeft het vertrouwen in het bedrijf DigiNotar en alle door hen geleverde diensten en certificaten opgezegd en het operationele beheer van het systeem voor het verstrekken van certificering overgenomen. Alle door het bedrijf afgegeven certificaten voor publieke en semi-publieke organisaties worden vervangen door certificaten van andere certificatenleveranciers nadat

[2] «Microsoft Security Advisory (2607712)» (http://www.microsoft.com/technet/security/advisory/2607712.mspx)

is gebleken dat de certificaten en diensten van de andere certificatenleveranciers betrouwbaar zijn.

Vraag 6
Klopt de uitspraak van woordvoerder Jochem Binst dat de blunder van Diginotar geen gevolgen heeft voor het werk dat DigiNotar voor de overheid doet? Zo ja, kunt u dit toelichten?

Antwoord 6
Zie het antwoord op vraag 5.

Vraag 7
Klopt het dat DigiNotar gehackt is, zoals op F-secure wordt gemeld?[3]

Antwoord 7
Er heeft een hack (digitale inbraak) bij DigiNotar plaatsgevonden. Zie feitenrelaas in brief d.d. 5 september.

Vraag 8
Gaat u onderzoeken of Iran achter de (geslaagde) hackpoging van DigiNotar zit? Zo nee, waarom niet? Zo ja, is hier sprake van cybercrime of cyberwarfare?

Antwoord 8
Het Kabinet onderzoekt momenteel wie betrokken zijn bij het hacken van DigiNotar. Mede in het licht van de uitkomst daarvan zal het Kabinet beslissen over passende vervolgstappen.

Vraag 9
Gaat u onderzoeken of er mensenrechten in Iran zijn geschonden doordat Iran een Nederlands certificaat heeft weten te bemachtigen?

Antwoord 9
Zie het antwoord op vraag 8.

[3] «DigiNotar Hacked by Black.Spook and Iranian Hackers» (http://www.f-secure.com/weblog/archives/00002228.html)