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

3627

Vragen van het lid **Verhoeven** (D66) aan de minister van Binnenlandse Zaken en Koninkrijksrelaties over *de beveiliging van Digi-D en overheidswebsites* (ingezonden 31 augustus 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
Heeft u kennisgenomen van het bericht «Browsers dumpen Diginotar na Iraanse Gmail-tap» en specifiek het in de ban doen van het Diginotar certificaat door Firefox, IE en Chrome?[1]

Antwoord 1
Ja.

Vraag 2
Is het zo dat de Nederlandse staat via onder meer Digi-D ook gebruik maakt van de diensten en specifiek van certificaten van Diginotar? Kunt u een opsomming geven van de verschillende websites en diensten die hier gebruik van nemen?

Antwoord 2
Ja. De DigiNotar certificaten voor DigiD zijn inmiddels vervangen.
Het betreft enkele tienduizenden certificaten van DigiNotar waarvan de betrouwbaarheid thans ter discussie is gesteld. Daaronder valt een substantieel aantal certificaten dat in gebruik is bij de Nederlandse staat en dat wordt ingezet voor diverse overheidswebsites en -diensten. Alle door het bedrijf

[1] Webwereld.nl, 30 aug 2011.

ah-tk-20102011-3627
ISSN 0921 - 7398
's-Gravenhage 2011

DigiNotar uitgegeven certificaten voor publieke en semi-publieke organisaties worden of zijn inmiddels vervangen door certificaten van andere (PKI-) certificatenleveranciers. De CIO's (Chief Information Officers) van Rijk en decentrale overheden zijn aangewezen om de omzetting van de certificaten van DigiNotar aan te sturen. In de komende periode gaan alle websites en diensten gefaseerd en gecontroleerd over op nieuwe certificaten.

Vraag 3
Betekent de genoemde inbreuk dat de handtekening van Diginotar nu de facto waardeloos is geworden, dat browsers ook de beveiliging van Digi-D niet meer op waarde kunnen schatten en dat browsers beveiligingswaarschuwingen zullen geven bij veilige overheidswebsites? Biedt dit ruimte voor derde partijen om onveilige kopieën te maken van overheidswebsites die dan dezelfde melding zullen krijgen, maar in tegenstelling tot de originelen niet meer veilig zijn en die burgers kunnen misleiden?

Antwoord 3
Nee. Uit de omstandigheid dat thans DigiNotar-certificaten gecompromitteerd blijken te kunnen zijn, kan en mag niet worden geconcludeerd dat alle historische transacties van DigiNotar mogelijk gecompromitteerd zijn;
Inmiddels zijn DigiD.nl en mijn.belastingdienst.nl overgegaan naar een andere certificaatleverancier, waarvan de certificaten betrouwbaar zijn en worden vertrouwd door de softwareleveranciers;
Ja, het is mogelijk dat browsers in de omschakelperiode naar andere certificaten beveiligingswaarschuwingen geven bij veilige overheidswebsites en;
Ja, in de omschakelperiode naar andere certificaten is het mogelijk dat derde partijen onveilige kopieën kunnen maken van overheidswebsites (de zgn. omgeleide sites), die gebruik maken van de door de hacker oneigenlijk aangemaakte certificaat van DigiNotar. Om deze reden is het operationele beheer van het systeem voor het verstrekken van certificering 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.

Vraag 4
Kunt u via onafhankelijk onderzoek aantonen dat de beveiliging van overheidsdiensten zoals Digi-D en beveiligde websites nog altijd afdoende is?

Antwoord 4
De overheid neemt diverse maatregelen om de beveiliging van overheidsdiensten en -websites te beheersen. Zo heeft het Kabinet, na overleg met het moederbedrijf van DigiNotar, nog in de nacht van vrijdag op zaterdag het operationele beheer van systemen voor certificaten van het bedrijf overgenomen teneinde de schade van de gebleken inbreuk op de integriteit van het internetverkeer en de beheersmaatregelen ter beperking van de gevolgen van de gebeurtenis. Daardoor wordt een beheersbare migratie naar andere certificaten mogelijk zonder dat dit additionele risico's schept voor zover bekend.
Voor een overzicht verwijs ik u naar de Kamerbrief «Digitale inbraak DigiNotar» van 5 september 2011.