Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

De Voorzitter van de Tweede Kamer
der Staten Generaal
postbus 20018
2500 EA Den Haag

Burgerschap en Informatiebeleid
Informatiebeleid

Schedeldoekshaven 200
2511 EZ Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl

Contactpersoon
J.F. Kootstra

T 070-4267114
john.kootstra@minbzk.nl

Kenmerk
2012-0000054694

Datum 2 februari 2012
Betreft Stand van zaken vervolgacties n.a.v. DigiNotar

Afgelopen september heeft het kabinet het vertrouwen in het bedrijf DigiNotar opgezegd. Aanleiding hiervoor was mogelijke compromittering van de PKIoverheid certificaten. Als gevolg daarvan kwam het vertrouwen in veilige communicatie in het geding. Het Kabinet heeft haar reactie op het incident middels meerdere brieven aan uw Kamer gemeld. Ook heeft het Kabinet gereageerd op de moties naar aanleiding van het plenaire debat van 13 oktober.[1]
Het Kabinet heeft ingezet op een driesporen beleid: het vergroten van de weerbaarheid tegen inbreuken; het vergroten van herstelvermogen bij geslaagde inbreuken; en structurele systeemverbeteringen op mondiaal niveau.
Ter voorbereiding op het Algemeen Overleg van 8 februari informeer ik u hierbij nader over de stand van zaken.

Het kabinet heeft meerdere onderzoeken opgestart, om grondig uit te laten zoeken waar de onvolkomenheden zitten en hoe passende maatregelen genomen kunnen worden. Onder mijn verantwoordelijkheid vallen de volgende onderzoeken:

- Evaluatie van het stelsel van PKIoverheid en het toezicht erop. Deze evaluatie die mede in opdracht van het ministerie van EL&I wordt uitgevoerd, evalueert ook het stelsel van gekwalificeerde certificaten, onder toezicht van de OPTA. In deze evaluatie wordt onderzocht welke risico's de stelsels bevatten; of het normenkader nog toereikend is; of het toezichtarrangement adequaat functioneert; en of er alternatieve technologieën zijn. Dit onderzoek wordt uitgevoerd door Logica. De uitkomsten van dit onderzoek worden in februari verwacht.
- Fox-IT heeft van DigiNotar opdracht gekregen technisch onderzoek te doen naar de hack. Het onderzoek is gestart op 30 augustus 2011. Een voorlopig rapport is op 3 september uitgebracht. Met het overnemen van het operationele beheer van de DigiNotar heeft het ministerie van BZK tevens het opdrachtgeverschap van dit onderzoek overgenomen. Fox-IT werkt aan de afronding van het definitieve rapport (planning eind februari).
- De Rijks Audit Dienst onderzoekt of de betrokken overheidspartijen in het PKIoverheid stelsel gegeven de bestaande taken en verantwoordelijkheden alert gereageerd hebben inzake DigiNotar. De resultaten van dit onderzoek worden in februari verwacht.

Uw Kamer kan conform eerdere toezegging uiterlijk 1 mei van dit jaar een reactie tegemoet zien op de uitkomsten van deze onderzoeken. Waar nodig zal ik de

[1] *Kamerstukken 26643, nr. 188, 189, 214*

reactie op deze onderzoeken met samen met andere bewindspersonen opstellen, gelet op de andere onderzoeken die elders lopen, zoals:

- onderzoek door de inspectie V&J naar de crisisbeheersingsaspecten, waarvan de resultaten in maart worden verwacht.
- onderzoek naar de veiligheid van diensten in de Digitale Agenda in opdracht van het ministerie van EL&I (gereed in februari).

De AIVD heeft tevens onderzoek gedaan naar de digitale inbraak. De Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) is hierover geïnformeerd.

Daarnaast heeft de Onderzoeksraad voor Veiligheid de uitnodiging van de Minister van V&J en ondergetekende geaccepteerd om onderzoek te doen naar de digitale veiligheid van de internetcommunicatie tussen overheid en burgers. In haar reactie heeft de Onderzoeksraad voor Veiligheid laten weten dat zij zich zal richten op de bestuurlijke en organisatorische processen waarmee overheden invulling geven aan digitale veiligheid. Het onderzoek zal naar verwachting voor de zomer gepubliceerd worden.

Vooruitlopend op de resultaten van de onderzoeken, heeft Logius in de rol van de *Policy Authority* van PKIoverheid naar aanleiding van de DigiNotar crisis het Programma van Eisen aangescherpt. Het betreft vooral nader invullende eisen op het gebied netwerkbeveiliging, computerbeveiliging en logging. Een eerste eis heeft betrekking op het voorkomen van ongeautoriseerde toegang tot PKIoverheid-diensten van certificatiedienstverleners (CSP's). CSP's moeten een fysieke en logische scheiding van omgevingen hebben en/of sterkere authenticatie per afzonderlijk PKI-proces gebruiken. Een tweede eis legt CSP's op om de afnemers van certificaten te wijzen op de maatregelen die afnemers zelf moeten nemen om de continuïteit van hun dienstverlening (op het gebied van het gebruik van certificaten) te waarborgen. Verdere eisen betreffen functiescheiding, een hoger niveau van beveiliging van webtoegang, automatische maandelijkse security scans, verplichte jaarlijkse penetratietesten, en uitgebreide logging en monitoring van de PKIoverheid omgeving.

Omdat internet niet als volledig veilig is te beschouwen en inbraken nooit geheel uitgesloten kunnen worden, is het belangrijk de kwetsbaarheid te verminderen en het herstelvermogen te vergroten. Als uitwerking van eerder aan de Tweede Kamer[2] aangekondigde maatregel zijn de CIO's *(Chief Information Officers)* van de departementen aangeschreven met het verzoek om uiterlijk 1 april 2012 te rapporteren over het beheer en gebruik van certificaten binnen de Rijksdienst. Daarbij gaat het zowel om het verbeteren van het beheer van de nu gebruikte certificaten, als om het beperken van de afhankelijkheid die het gebruik van certificaten van één leverancier met zich mee brengt. Dit kan onder andere door certificaten van meerdere leveranciers te gebruiken of voor kritische processen een reservecertificaat van een andere leverancier gereed te hebben.

Ook internationaal is DigiNotar kwestie besproken, bijvoorbeeld tijdens de Europese ministeriële *egovernment* conferentie te Poznan op 17 en 18 november vorig jaar. Hierbij is vooral de afhankelijkheid tussen het functioneren van de overheid en het gebruik van certificaten benoemd als onderwerp van Europese aandacht. De lessen van DigiNotar worden ook bij de voorbereidingen van de herziening van de richtlijn elektronische handtekeningen (1993/93/EG) ingebracht. Deze herziening van deze richtlijn wordt besproken in de Telecomraad, waarin de minister van EL&I Nederland vertegenwoordigt.

[2] *Kamerstuk 26643, nr. 189*

Om meer zicht te krijgen in alternatieven voor het SSL-stelsel is in het kader van ICA (international Council of IT in administrations) op initiatief van Nederland een werkgroep opgericht. De resultaten hiervan worden in november van dit jaar verwacht.

Met deze en komende acties wordt gewerkt aan blijvend vertrouwen in de veilige communicatie met de overheid als belangrijke randvoorwaarde voor een moderne, efficiënte en dienstverlenende overheid.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

Mevrouw mr. drs. J.W.E. Spies