Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2010–2011

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 188

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES EN VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 september 2011

Afgelopen vrijdag 2 september 2011 kreeg het Kabinet onmiskenbare signalen dat de uitgifte door het bedrijf DigiNotar van PKI-Overheid certificaten mogelijk gecompromitteerd was door een inbraak in de bestanden van het bedrijf, met als eventueel gevolg dat deze certificaten frauduleus uitgegeven zouden zijn. Nadat nadere informatie hierover was verkregen en ook met het bedrijf was gesproken is het Kabinet tot de conclusie gekomen dat de betrouwbaarheid van de certificaten en diensten van DigiNotar niet langer zonder meer gegarandeerd was en dat mitsdien het vertrouwen in het bedrijf DigiNotar moest worden opgezegd. Dit betekent dat op zo kort mogelijke termijn alle certificaten van het bedrijf moeten worden vervangen door certificaten van andere leveranciers. Voorts 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.

In aansluiting daarop is het Kabinet in overleg getreden met verschillende overheids- en bedrijfssectoren teneinde een volledig beeld te krijgen van de mogelijke risico's, de maatregelen die in verband daarmee nodig zijn en de stappen die nodig zijn om het vertrouwen in veilige digitale communicatie zo snel mogelijk te herstellen. Daarbij wordt intensief samengewerkt met en tussen ministeries, medeoverheden, VNO-NCW, MKB-Nederland, de Cybersecurityraad, ICT-Office, CIO-platform en diverse softwareleveranciers. Met deze brief wordt u geïnformeerd over de ontwikkelingen tot nu toe, de duiding ervan en de maatregelen die het Kabinet heeft genomen.

kst-26643-188
ISSN 0921 - 7371
's-Gravenhage 2011

Gebeurtenis

Op 27 augustus 2011 maakte een gebruiker in Iran op een Google forum melding dat hij bij het inloggen in zijn Gmail account van zijn browser een waarschuwing had gekregen over de onbetrouwbaarheid van het certificaat. Het gaat hierbij om certificaten die nodig zijn om de betrouwbaarheid van digitale communicatie te kunnen waarborgen. De certificaten dienen ter betrouwbare identificatie van websites (het zogenaamde «slotje») en beveiliging van verkeer tussen computers onderling. DigiNotar, een van de bedrijven die dit soort certificaten genereert, geeft twee soorten certificaten uit; de DigiNotar eigen merk certificaten en PKI-Overheid certificaten. Ten aanzien van de uitgifte van PKI-Overheid certificaten geldt een zwaarder veiligheidsregime. Naast certificaten biedt DigiNotar ook diensten aan die gebruik maken van door henzelf uitgegeven certificaten.

Op 29 augustus 2011 werd Govcert.nl (een onderdeel van het ministerie van Veiligheid en Justitie), onder verwijzing naar de eerderbedoelde blog van de Iraniër, door Cert-Bund (de Duitse evenknie van Govcert.nl) in kennis gesteld dat er mogelijk problemen waren met certificaten van DigiNotar. Cert-Bund meldde dat een posting was gedaan van een «vals» Google certificaat, afkomstig van DigiNotar, waarbij Google Chrome had aangegeven dat het een niet authentiek certificaat van Google betrof. Govcert.nl heeft het bedrijf DigiNotar hierop direct in kennis gesteld. Het bedrijf trok hierop het «vals»e Google.com certificaat in en verzocht op 30 augustus 2011 het bedrijf Fox-IT (een ICT beveiligingsbedrijf) om onderzoek hiernaar te doen. Fox-IT bracht op 2 september 2011 eerst aan DigiNotar en vervolgens aan Govcert.nl een eerste mondelinge rapportage met toelichting uit. Op maandag 5 september 2011 bracht Fox-IT zijn rapport uit. Dit rapport is als bijlage bij deze brief bijgevoegd[1].

Uit het rapport blijkt dat al op 6 juni 2011mogelijk een eerste verkenning door een hacker heeft plaatsgevonden. Op 19 juni 2011 heeft DigiNotar een digitale inbraak gedetecteerd. Op 2 juli 2011 blijkt een eerste poging tot het genereren van een «vals» certificaat te hebben plaatsgevonden. Op 10 juli 2011 wordt daadwerkelijk een «vals» Google.com certificaat gegenereerd. Omstreeks 22 juli 2011 is DigiNotar een intern onderzoek gestart naar de geconstateerde incidenten. Het rapport daarvan was op 27 juli 2011 gereed. Zeker is dat vanaf 27 juli 2011 het «vals» gegenereerde Google.com certificaat actief is gebruikt. Tussen 4 en 29 augustus 2011 is er verder actief misbruik waargenomen van het «valse» Google.com certificaat. Tijdens het onderzoek door Fox-IT naar dit misbruik is een zogenoemd script aangetroffen met als «ondertekening» «My Signature as always: Janam Fadaye Rahbar»[2]. Het rapport bevat als bijlage een tijdlijn met het verloop van de feiten.

Reactie van de overheid

De overheid is noch op 19 juni 2011, noch op enig later moment door DigiNotar op de hoogte gesteld van de digitale inbraak. Pas door de kennisgeving van Cert-Bund aan Govcert.nl kreeg de Nederlandse overheid een eerste indicatie van mogelijke problemen. Zoals hiervoor beschreven heeft Govcert.nl hierop direct contact opgenomen met het bedrijf, waardoor de bovenbeschreven keten van onderzoek in gang werd gezet. Teneinde de ontwikkelingen te kunnen volgen, is vanaf dat moment dagelijks contact geweest tussen Govcert.nl en DigiNotar. Op dat moment bestond het beeld dat de problemen uitsluitend te maken hadden met het «eigen merk» certificaat van DigiNotar en niet met de PKI-Overheid certificaten. Op dinsdag 30 augustus 2011 heeft Govcert.nl hierover een factsheet gepubliceerd.

[1] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.
[2] Fox-IT rapport van 5 september 2011, blz. 13.

Uit een eerste mondelinge versie van het Fox-IT rapport van 2 september 2011 bleek Govcert.nl dat ook de PKI-Overheid certificaten mogelijk gecompromitteerd waren door de «inbraak». Als gevolg daarvan is de Rijksoverheid, via de gebruikelijke crisisstructuur van het Nationaal CrisisCentrum, opgeschaald. Vanaf vrijdagmiddag 2 september 2011 is meermalen zowel op hoogambtelijk niveau als op ministerieel niveau overlegd. Onder voorzitterschap van de minister van Veiligheid en Justitie waren meer in het bijzonder de minister van Binnenlandse Zaken en Koninkrijksrelaties, de staatssecretaris van Financiën en de minister van Economische Zaken, Landbouw en Innovatie betrokken bij dit crisisberaad. In het beraad van 2 september 2011 is besloten om in te grijpen.

Het Openbaar Ministerie is voorts onmiddellijk na berichtgeving over deze kwestie een feitenonderzoek gestart. DigiNotar heeft op maandag 5 september 2011 aangifte gedaan van de gepleegde «inbraak».

Betekenis van de ontstane situatie

De inbraak bij DigiNotar en het gebleken aanmaken en gebruik van «valse» certificaten vormen een ernstige aantasting van het vertrouwen en de integriteit van het digitale communicatieverkeer met potentieel grote gevolgen voor dit verkeer. Dit is het gevolg van het feit dat de aantasting van het vertrouwen in de certificaten van DigiNotar implicaties heeft 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 «valse» 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 «valse» certificaten maakt dat gebruikers er niet meer in alle gevallen zonder meer van uit kunnen gaan dat het een veilige internetcommunicatie betreft. In het geval dat onbedoeld een «valse» site wordt benaderd, kunnen de gegevens die een burger daaraan verstrekt in verkeerde handen terechtkomen, al zijn er tot dusver geen aanwijzingen dat dit in Nederland ook daadwerkelijk heeft plaatsgevonden. Hierdoor wordt het vertrouwen in het digitale communicatieverkeer ernstig aangetast.

Herstel van de ontstane situatie is niet zonder meer mogelijk door alle certificaten van het betrokken bedrijf uit te schakelen. Dit heeft potentieel grote gevolgen voor het digitale gegevensverkeer, met name voor het verkeer van machines onderling. Indien de leveranciers van besturingssystemen en applicatiesoftware het vertrouwen in door DigiNotar geleverde certificaten opzeggen, heeft dit potentieel tot gevolg dat de geautomatiseerde koppelingen tussen netwerken moeilijker of geheel niet meer tot stand komen. Dit levert een ernstige verstoring op van de uitwisseling van gegevens en kan een risico vormen voor de continuïteit van (bedrijfs)processen.

Het gaat bij dit alles niet om handelingen en reacties die alleen Nederland betreffen, maar die tot wereldwijde reacties kunnen leiden en ook beïnvloed worden door deze internationale reacties. Nederland, inclusief Nederlandse bedrijven, vormt een onderdeel van het wereldwijde systeem van internetverkeer. Incidenten die Nederland raken hebben directe en indirecte uitstralingseffecten op dat wereldwijde systeem. De reactie van veelal mondiaal werkende bedrijven laat zien dat de afspraken die binnen dat systeem bestaan ten behoeve van het borgen van een veilig en betrouwbaar internetverkeer strikt worden gehandhaafd:

bedrijven, certificeerders en browsers accepteren niet dat frauduleuze certificaten in omloop zijn of blijven en passen hun systemen hierop aan.

De gevolgen van de door DigiNotar afgegeven gecompromitteerde certificaten voor het vertrouwen in het digitale communicatieverkeer zijn groot, ook al is de materiële betekenis mogelijk veel beperkter. DigiNotar is immers beslist niet het enige bedrijf dat certificaten en diensten voor internetverkeer genereert. De certificaten van andere bedrijven worden niet geraakt door de gebeurtenissen bij DigiNotar. Ook gebruikt de overheid certificaten van andere leveranciers dan DigiNotar. Alleen partijen die gebruik maken van certificaten of diensten van DigiNotar lopen het risico dat systemen of communicatie uitvallen.[1] Het aantal potentieel getroffen bedrijven is weliswaar groot (er is sprake van enkele tienduizenden certificaten van DigiNotar) maar voor zover het verkeer plaatsvindt tussen sites met niet «valse» certificaten is er geen inbreuk. Uit de omstandigheid dat thans DigiNotar-certificaten gecompromitteerd blijken te kunnen zijn, mag niet worden geconcludeerd dat alle historische transacties van DigiNotar gecompromitteerd zijn geweest.

Genomen besluiten en ingezette acties

De volgende maatregelen zijn genomen om de ontstane situatie zo snel mogelijk te beheersen:

Technische maatregelen

- Het Kabinet heeft het vertrouwen opgezegd in het bedrijf DigiNotar en alle door hen geleverde diensten en certificaten en het operationele beheer van de systemen voor het verstrekken van certificering overgenomen. ICT-veiligheidsspecialisten worden hierbij betrokken om de overgangsfase zo snel mogelijk af te ronden.
- Er is per direct een eerste inventarisatie gemaakt van de mogelijke gevolgen en passende beheersmaatregelen.
- Alle door het bedrijf afgegeven certificaten voor publieke en semi-publieke organisaties worden vervangen door certificaten van andere certificatenleveranciers nadat is gebleken dat de certificaten en diensten van de andere certificatenleveranciers betrouwbaar zijn. Voor private partijen geldt dat zij zelf een keuze voor een leverancier moeten maken.

Juridische maatregelen

- De landsadvocaat is vanaf vrijdag 2 september 2011 betrokken.
- Het Openbaar Ministerie heeft een feitenonderzoek ingesteld.
- De OPTA is intensief betrokken.
- Het Kabinet onderzoekt wie betrokken zijn bij het hacken van DigiNotar.
- Het bedrijf DigiNotar wordt aangesproken op de verantwoordelijkheid en/of aansprakelijkheid wegens nalatigheid.

Uitgangspunt is dat de certificaten van DigiNotar niet langer betrouwbaar zijn en het gebruik daarvan zo snel mogelijk uit het communicatieverkeer moet verdwijnen. Een abrupte beëindiging van het gebruik zou evenwel in het verkeer tussen machines onderling vermoedelijk leiden tot potentieel ernstige verstoringen. Daarom is in dat verkeer een beheerste migratie nodig. Daartoe is in de eerste plaats het operationele beheer van de certificaten bij DigiNotar gecontroleerd overgenomen, zodat de certificaten gefaseerd kunnen worden ingetrokken en het gebruik van «valse» certificaten kan worden gemonitord en kan worden bestreden waar dit wordt waargenomen.

[1] In het systeem voor de initialisatie van nieuwe pinautomaten zijn wel sporen gevonden van een poging tot inbraak, maar deze poging is niet geslaagd. De DigiNotar certificaten hiervoor zijn daarom wél betrouwbaar (bron rapport FOX-IT).

Naast het Kabinet nemen evenwel ook andere partners (zoals bijvoorbeeld leveranciers van besturingssystemen en applicatiesoftware) binnen het systeem van internetverkeer maatregelen om het bestaan en/of gebruik van frauduleuze certificaten en diensten tegen te gaan. Deze maatregelen kunnen de bedoelde verstorende effecten hebben welke nu juist voorkomen moeten worden met de beheerste migratie. Leveranciers van besturingssystemen en applicatiesoftware kunnen bijvoorbeeld een update doorvoeren van hun systemen met als gevolg dat sommige websites en onderliggende systemen moeilijker – of in het geheel niet – bereikbaar zijn. Daarom is het Kabinet in overleg getreden met de softwareindustrie en bedrijfsleven over de DigiNotar problemen die onder andere optreden bij server-to-server verkeer. In nauwe samenwerking is besloten de risico's zoveel mogelijk te minimaliseren. Daarbij hebben softwareleveranciers en overheid moeilijke keuzes moeten maken om de bereikbaarheid van de Nederlandse overheid en samenleving zo betrouwbaar mogelijk te laten zijn.

Een van de directe gevolgen is dat een geplande softwareupdate van Microsoft voor Nederland op expliciet verzoek van de overheid beheerst wordt ingevoerd. Dat geeft organisaties en bedrijven meer tijd om de certificaten te vervangen zodat de geplande softwareupdate op een ander moment zal worden uitgevoerd.

Daarnaast is het Kabinet in nauw overleg getreden met de medeoverheden en het bedrijfsleven – en daarbinnen met de afzonderlijke sectoren – teneinde een beeld te krijgen van die sectoren die potentieel geraakt worden en de problemen die zich daarbij voordoen. Op deze wijze tracht het Kabinet de problemen die zich voordoen te isoleren, en geleidelijk aan risico's te elimineren of te mitigeren. Op basis van dit overleg kan geconcludeerd worden dat een aantal sectoren niet geraakt worden door de problemen met de DigiNotar certificaten (geldverkeer, Schiphol, NS). Weliswaar zijn er inmiddels enkele sectoren die met verstoringen te maken hebben, maar tot dusver is niet gebleken van grote, niet beheersbare problemen.

In dit kader zijn de volgende *afstemmingsmaatregelen* genomen.
- Omdat DigiNotar ook bedrijven als klant heeft, is er intensief en voortdurend overleg met ministeries, medeoverheden, VNO-NCW, MKB-Nederland, CIO-platform, ICT-Office en diverse softwareleveranciers.
- Met het oog op de doorwerking op de verschillende sectoren wordt interdepartementaal overleg gevoerd met de betreffende sectoren en met de gemeentelijke en provinciale overheden.
- Het overleg met de andere certificaatleveranciers is eveneens gaande.

Handelingsperspectief voor overheden, bedrijven en burgers

Het Kabinet heeft andere overheden door middel van een bestuurlijke brief geïnformeerd en geadviseerd over hoe te handelen in de huidige situatie.

Het Kabinet raadt organisaties aan om na te gaan of ze gebruik maken van DigiNotar certificaten en/of diensten. Indien dit het geval is, wordt hen geadviseerd deze zo snel mogelijk om te zetten. Via de website www.logius.nl wordt informatie verstrekt die nodig is om DigiNotar certificaten te kunnen vervangen.

De CIO's (Chief Information Officers) van Rijk en decentrale overheden zijn aangewezen om de omzetting van de certificaten van DigiNotar aan te sturen. Zij inventariseren gebruikte certificaten en mogelijk te nemen

maatregelen. Indien nodig worden alternatieve certificaten aangeschaft en wordt de migratie daarheen in gang gezet. Dit alles onder hoge tijdsdruk, om de migratieperiode zo kort mogelijk te houden en zo de veiligheid en betrouwbaarheid van het internetverkeer te waarborgen.

De overheid zal sectorspecifieke afspraken maken ten aanzien van de te betrachten coulance richting burgers en bedrijven indien zij niet in staat zijn op tijd hun gegevens via een veilige internetverbinding aan te leveren. Zo zal de Belastingdienst coulance betrachten in die gevallen waarin het Diginotar incident heeft geleid tot overschrijding van termijnen voor fiscale verplichtingen. Hierbij moet gedacht worden aan bijvoorbeeld het voorkomen van boetes wegens het te laat indienen van een aangifte. De komende periode werken de Belastingdienst en VNO/NCW samen aan de concrete invulling van die coulance bepaling.

In die gevallen dat een aanvrager niet via een veilige site contact kan leggen, wordt gezocht naar een passend alternatief.

Communicatie

Met deze brief informeert het Kabinet de Tweede Kamer over de actuele stand van zaken. De Tweede Kamer wordt zo snel mogelijk door het Kabinet geïnformeerd over het vervolg.

Daarnaast communiceert het Kabinet gericht met specifieke sectoren over potentiële gevolgen voor de betreffende sector. Zodra hierover meer informatie beschikbaar komt, worden deze gepubliceerd door de overheid en het bedrijfsleven via www.rijksoverheid.nl.

De gebruikers van DigiNotar certificaten worden per brief geattendeerd op de risico's van hun certificaten en worden geadviseerd deze zo snel mogelijk om te zetten. De CIO's informeren en adviseren departementen, decentrale overheden en hun sectoren eveneens over de risico's en hoe het beste te handelen. Daarnaast is voor de zakelijke markt meer informatie over het wijzigen van certificaten te verkrijgen via www.logius.nl of telefoonnummer 0900 5554555.

Govcert.nl onderhoudt een specifieke, meer technisch georiënteerde communicatielijn met de ICT-specialisten in binnen- en buitenland. Daarnaast zijn er zogenoemde factsheets beschikbaar via www.Govcert.nl. waarin meer technische achtergrondinformatie en handelingsperspectief wordt gegeven.

Publieksinformatie is te verkrijgen via www.rijksoverheid.nl en het publieksinformatienummer 0800–1351.

Langere termijn

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.
Zoals in het regeerakkoord is afgesproken zal de Staatssecretaris van Veiligheid en Justitie bovendien een wetsvoorstel indienen dat een meldplicht introduceert voor gebeurtenissen zoals deze bij DigiNotar zijn voorgekomen.

In dit kader wordt ook de op 30 juni van dit jaar geïnstalleerde Cybersecurityraad om advies gevraagd over de wijze waarop de veiligheid en integriteit van het digitaal communicatieverkeer in voldoende mate geborgd kan worden om gebeurtenissen als bij DigiNotar zoveel mogelijk te voorkomen en te beperken. Deze Raad heefttot taak om de regering en private partijen gevraagd en ongevraagd van advies te dienen over relevante ontwikkelingen op het gebied van digitale veiligheid. De Raad heeft daarbij nadrukkelijk aandacht voor het belang van privacy en fundamentele rechten zoals de vrijheid van meningsuiting en informatievergaring.

De recente ontwikkelingen worden ook meegenomen in de verdere vormgeving van de Nationale Cyber Security Strategie, in het bijzonder bij de vaststelling van het Dreigingsbeeld Nederland. Daarin wordt deze gebeurtenis meegenomen en worden tevens de juridische knelpunten en oplossingen benoemd.

Het Kabinet heeft in januari 2011 besloten om toe te werken naar één ICT-beveiligingsorganisatie onder verantwoordelijkheid van het ministerie van Veiligheid en Justitie. In dit kader is Govcert.nl reeds onderdeel geworden van het ministerie van Veiligheid en Justitie.

Tot slot

Het Kabinet acht een betrouwbare digitale communicatie van wezenlijk belang en stelt alles in het werk om dit te borgen. Bij de aanpak van de gevolgen van de gebleken aantasting van de integriteit van dit digitale communicatieverkeer treden overheid en bedrijfsleven thans eendrachtig op vanuit een gedeelde visie op ieders maatschappelijke verantwoordelijkheid. Voor het Kabinet is de bedreiging van het vertrouwen in en de integriteit van het internetverkeer onacceptabel.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,
J. P. H. Donner

De minister van Veiligheid en Justitie,
I. W. Opstelten