> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Directie Dienstverlening, Regeldruk en Informatiebeleid

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

Kenmerk
2011-2000411239

Datum 16 september 2011
Betreft Digitale Inbraak DigiNotar

Digitale informatie-uitwisseling is een essentieel onderdeel geworden voor het functioneren van de Nederlandse samenleving. Het gaat hierbij zowel om het economische verkeer als om het functioneren van de overheid. De inbraak bij DigiNotar heeft de kwetsbaarheid van betrouwbare digitale informatievoorziening duidelijk gemaakt: zowel bedrijfsleven als overheid heeft hiervan de nadelen van ondervonden. Door een essentieel onderdeel (het verstrekken en toetsen van de betrouwbaarheid van digitale certificaten), te corrumperen, konden in potentie ernstige verstoring optreden. Dankzij de coöperatieve medewerking van vele organisaties in zowel het publieke als private domein, zijn ernstige verstoringen voorkomen.

In deze brief informeert het Kabinet u nader over de stand van zaken ten aanzien van de DigiNotar problematiek, de op de korte termijn te nemen maatregelen alsmede de richting voor de maatregelen op de langere termijn.

Stand van zaken DigiNotar problematiek
In de brief van 5 september 2011 is uw Kamer geïnformeerd over de digitale inbraak bij het bedrijf DigiNotar en de genomen maatregelen. Belangrijk onderdeel van de maatregelen was het overstappen naar andere certificaten. Wereldwijd maken softwareontwikkelaars wijzigingen (zogenaamde updates of patches) zodra certificaten niet meer vertrouwd kunnen worden. Op het overstappen stond en staat een grote tijdsdruk vanwege de patch die Microsoft op dinsdag 13 september 2011 zou uitbrengen. Uitvoering van de patch heeft als resultaat dat DigiNotar certificaten niet meer als betrouwbaar worden aangemerkt. Op verzoek van het kabinet heeft Microsoft deze patch voor Nederland uitgesteld tot de 13de, waar de rest van de wereld deze patch al geautomatiseerd kreeg aangeboden op 6 september 2011.

Deze patch is inmiddels uitgevoerd en heeft tot beperkte verstoringen geleid. Kritieke processen die afhankelijk zijn van machine-machine communicatie en die inmiddels zijn overgegaan op andere certificaten, bleken uit nadere tests ongevoelig te zijn voor de patch of hadden adequate terugval opties. Bij enkele gemeenten hebben zich problemen voorgedaan bij digitale loketten. De Orde van Advocaten heeft medio vorige week al besloten over te stappen op papieren informatie-uitwisseling met de rechtbanken.

Een aantal organisaties heeft besloten de patch van Microsoft handmatig tegen te houden om daarmee meer tijd te verkrijgen voor de overstap op andere certificaten.

De OPTA heeft als toezichthouder op het systeem van gekwalificeerde certificaten per 14 september 2011 12:00 uur de registratie van DigiNotar om gekwalificeerde certificaten uit te geven ingetrokken. Dit houdt in dat DigiNotar twee weken de tijd krijgt om zijn uitgegeven gekwalificeerde certificaten in te trekken en geen nieuwe gekwalificeerde certificaten meer mag uitgeven. Aan deze intrekking is de vereiste procedure voorafgegaan die direct is gestart na het bekend worden van het Fox-IT rapport.

De komende periode zal de verdere uitfasering van de DigiNotar certificaten vorm krijgen. Dit vindt plaats in nauwe afstemming met alle betrokken partijen. Enkele specifieke projecten kunnen hierdoor vertraging op lopen. Dit geldt onder andere voor de taxibranche. De wetgeving rondom de boordcomputer taxi treedt op 1 oktober 2011 in werking. De boordcomputerkaarten zouden gebruik gaan maken van DigiNotar certificaten. Aangezien dat niet meer tot de mogelijkheid behoort, zullen de boordcomputers met een vertraging van ongeveer 6 maanden op de markt komen.

De vermoedelijke hacker heeft, via openbare bronnen, geclaimd bij meer certificatenleveranciers digitaal te hebben ingebroken. Dit maakt dat er niet alleen onderzoek loopt naar de feitelijke inbraak bij DigiNotar, maar dat het onderzoek breder is getrokken en daarmee ook een internationale context heeft. Zoals in de eerdergenoemde brief van 5 september 2011 is gemeld leidt het Openbaar Ministerie een onderzoek naar de vraag wie er betrokken is bij het hacken van DigiNotar. Daarnaast doet de AIVD samen met zijn nationale en internationale partners, in het belang van de nationale veiligheid, onderzoek naar de digitale inbraak bij DigiNotar en de gevolgen daarvan. Daarbij wordt met name gekeken naar het motief en de werkwijze van de dader en de (on)mogelijkheden van het gebruik van onrechtmatig verkregen gegevens. Dit past binnen de A-taak van de inlichtingendienst. Tot slot heeft Govcert.nl intensief contact met andere CERTS waarbij enerzijds (inter)nationale partners worden geattendeerd op mogelijke andere claims van de vermoedelijke DigiNotar- hacker en kennis en expertise wordt gedeeld die van waarde is voor de hierboven genoemde onderzoeken.

Vervolgacties

Binnen het kader van de afhandeling van de DigiNotar problematiek zijn enkele aanvullende acties in gang gezet die op de korte termijn worden geëffectueerd. Het gaat hierbij om het stellen van nadere eisen aan certificatenleveranciers die onder het PKI(-Overheid) stelsel certificaten verstrekken. Dit zal op basis van de contracten met deze leveranciers vorm krijgen. De OPTA zal nader overleg voeren met door de Raad van Accreditatie toegelaten auditorganisaties (PWC en KPMG) over de wijze waarop de audits kunnen bijdragen aan een vergroting van de zekerheid ten aanzien van de kwaliteit van de certificaat verstrekkende organisaties.

De DigiNotar problematiek heeft de kwetsbaarheid van de digitale datacommunicatie aangetoond. Het Kabinet benadrukt dat internet met het systeem van certificaten een mondiaal systeem is, dat niet eenzijdig vanuit Nederland kan worden bepaald. Specifiek de certificatensystematiek is ontwikkeld in een periode met een ander dreigingsbeeld en op basis van de techniek van

enkele jaren geleden. Daarom kiest het Kabinet voor een aanpak waarin drie sporen zijn te onderscheiden.

Spoor 1. Vergroten van de weerbaarheid tegen (al of niet opzettelijke) inbreuken
Binnen het bestaande systeem dient de weerbaarheid tegen al of niet opzettelijke inbreuken vergroot te worden. Hierbij kan gedacht worden aan het opnemen van meerdere certificaten binnen één systeem (redundancy) zodat makkelijk kan worden overgeschakeld, het meer expliciet maken van vereisten waaraan certificatenleveranciers moeten voldoen, het vergroten van kennis en veiligheidsbesef bij organisaties met een essentiële functie in het stelsel van digitale datacommunicatie en dienstverlening van en met de overheid alsmede het actiever (laten) toetsen van de feitelijke veiligheid. Tevens zal in samenwerking met het Ministerie van Economische Zaken, Landbouw en Innovatie een onderzoeksopdracht uitgezet naar het gehele stelsel en proces rondom PKI-Overheid, inclusief het toezicht daarop. Dit onderzoek gaat ondermeer over de veiligheid van de digitale dienstverlening van en aan bedrijven als wel over de veiligheid van digitale overheidsdienstverlening aan burgers, inclusief de betekenis van de uitkomsten van de analyse voor de huidige toezichtsarrangementen.

De handreikingen van Govcert.nl over de beveiliging van overheidswebsites zullen – aangepast met de DigiNotar ervaringen – nadrukkelijk onder de aandacht worden gebracht van de houders van websites bij de centrale en decentrale overheden. Eveneens zal vorm gegeven worden aan een meldplicht voor ICT incidenten voor organisaties die cruciale maatschappelijke functies vervullen.

Spoor 2. Vergroten van herstelvermogen bij onverhoopte geslaagde inbreuken
Gegeven het feit dat internet per definitie niet als volledig veilig te beschouwen is alsmede internationaal bepaald wordt, kunnen inbreuken op die veiligheid nooit geheel worden uitgesloten. Het herstelvermogen om de consequenties van dergelijke inbreuken snel weg te kunnen nemen dient te worden vergroot. Daartoe worden aanvullende instrumenten ontwikkeld die de overheid de mogelijkheid geven afdoende in te grijpen. Kaderstelling en toezicht zijn daarvan essentiële elementen. Deze denklijn wordt nader uitgewerkt en voorzien van de juiste operationele en juridische instrumenten. Daarbij wordt ook gekeken naar het verder versterken van onderzoek en expertise bij de overheid zoals ook is ingezet in de Nationale Cybersecurity strategie.

Spoor 3. Structurele systeemverbeteringen op mondiaal niveau
De huidige werking van internet in het algemeen en het daarvoor geldende certificatensysteem zijn voor een belangrijk deel bepaald door de huidige technologische ontwikkelingen en de wijze waarop deze in de praktijk worden geïmplementeerd. Voor een deel is dit ook vastgelegd in EU regelgeving. Beïnvloeding van deze technische ontwikkelingen en de EU regelgeving vereist een actieve opstelling van Nederland. Het Kabinet heeft het op zich genomen om de ervaringen van de DigiNotar problematiek actief uit te dragen in de relevante gremia (internationale CERT-netwerk waar Govcert.nl deel van uitmaakt, EU (JBZ-Raad)) en te bewerkstellingen dat structurele verbeteringen op systeemniveau plaatsvinden.

Daarnaast zullen de al lopende initiatieven zoals de Cyber Security Dreigingsanalyse, de oprichting van het Nationale Cyber Security Centrum (NCSC) en het invoeren van de E-ID (electronische identiteit) met de nieuwe inzichten worden verrijkt en voortgezet. Uw Kamer zal over de uitwerking van deze lijnen nader worden geïnformeerd.

Tot slot heeft het Kabinet, zoals gebruikelijk bij de opschaling van de Rijkscrisisstructuur, de Inspectie Openbaar Orde en Veiligheid, gevraagd om een evaluatie te maken van het functioneren van de crisisstructuur.

Afsluiting
Het Kabinet acht een betrouwbare digitale communicatie van wezenlijk belang en stelt alles in het werk om dit te borgen.

Het Kabinet zal de Tweede Kamer binnen enkele weken informeren over de korte termijn maatregelen en opzet en uitvoering van het lange termijn onderzoek.

De minister van
Binnenlandse Zaken en
Koninkrijksrelaties,

J.P.H. Donner

De minister van
Veiligheid en
Justitie,

I.W. Opstelten