Rijksauditdienst
Ministerie van Financiën

De zaak 'DigiNotar': handelde de overheid adequaat?

Onderzoek naar alertheid en adequaatheid van handelen van de overheid ten tijde van de 'DigiNotar'-problematiek

Kenmerk: RAD/2012/161

Datum 8 maart 2012
Status Definitief

Colofon

Titel	De zaak 'DigiNotar': handelde de overheid adequaat?
Auteur	dhr. drs. J.P. Dirkx MBA
Opdrachtgever	mw. drs. B. Steenbergen, directeur Burgerschap & Informatiebeleid ministerie van BZK
Inlichtingen	**Rijksauditdienst** dhr. drs. J.P. Dirkx MBA T 06-48589862 F 070-4267635 j.p.dirkx@rad.nl

Managementsamenvatting

Wat is er door overheidspartijen[1] wel en niet goed gedaan ten aanzien van de beheersing van het stelsel van certificaten vallend onder PKIoverheid? Dat is kortgezegd de vraag die we in dit onderzoek pogen te beantwoorden. Daarbij maken we een onderverdeling naar de periode vóór het bekend worden van de digitale inbraak in de systemen van DigiNotar en de periode erna.

Door de afhandeling van de DigiNotar-affaire in september 2011 heeft bij de rijksoverheid een trendbreuk plaatsgevonden. De wijze van denken en omgaan met risico's van beveiliging van websites is veranderd. Samenwerking tussen overheidspartijen onderling en samenwerking tussen rijksoverheid en andere belanghebbende partijen (publiek, privaat, internationaal) hebben een belangrijke impuls gekregen.

Er is door de overheid snel en adequaat gehandeld om verdere schade te voorkomen. Zo werden burgers en bedrijven gewaarschuwd, werd Microsoft met succes benaderd om een voorziene patch (update) voor Nederland met een week uit te stellen, en werd de operationele bedrijfsvoering van DigiNotar met betrekking tot de uitgifte van certificaten overgenomen. Ook werd direct nader onderzoek ingesteld naar alle *ins and outs* rondom dit falen van de informatiebeveiliging. Vele belanghebbende partijen werden betrokken bij de bestrijding van de crisis. Ook dit gebeurde snel en adequaat.

Voorafgaand aan de digitale inbraak bij DigiNotar was er feitelijk geen sprake van extra alertheid in dit verband. Alle overheidspartijen vertrouwden, voor wat betreft het toezicht op PKI-overheid, op de activiteiten van de betreffende auditpartij, die op zijn beurt ook weer geaccrediteerd was. Wellicht mede als gevolg van dit vertrouwen, was een aantal standaardzaken niet aanwezig: zo was er geen risicoanalyse uitgevoerd over ketenpartners heen, was er onvoldoende inzicht in aantal en aard van de uitstaande PKIoverheid-certificaten, en was er geen helderheid over toezichtscriteria.

[1] Wanneer in dit rapport gesproken wordt over 'overheid', betreft dit steeds primair de *rijks*overheid.

1 Inleiding

1.1 Situatieschets

Door de DigiNotar-inbraak halverwege 2011 werd de Nederlandse overheid gesteld voor een andersoortig ICT-probleem dan tot nu toe was voorgekomen. Een - aanvankelijk niet ontdekte en pas na lange tijd bekend geworden - digitale inbraak (waarna aanwijsbaar misbruik was gemaakt van de aldus verkregen toegang) met potentieel zeer schadelijke gevolgen, niet alleen op het gebied van digitale veiligheid, maar ook op het niveau van persoonlijke veiligheid. De continuïteit van het maatschappelijk dataverkeer kwam door de (reacties op de) bekendwording van de inbraak onder druk te staan.

De Nederlandse overheid heeft op diverse manieren belang bij een goede certificatenuitgifte en bij de beveiliging van elektronische communicatie. Allereerst is er het maatschappelijk belang; veiligheid van de digitale infrastructuur is een maatschappelijke topprioriteit. Dit is natuurlijk tevens een internationale kwestie, waarbij dan ook waakzaamheid geboden is vanwege mogelijke terroristische en/of aanvalsgerichte acties door andere staten. Dan is er het belang van het kunnen garanderen van een veilig internetverkeer tussen burger en overheid, tussen bedrijfsleven en overheid alsmede tussen overheidsonderdelen. Ook had de overheid een contract met de betreffende certificatiedienstverlener, DigiNotar, om diensten aan te bieden in het kader van PKIoverheid.

1.2 Onderzoek

Naar aanleiding van deze digitale inbraak ontstonden bij de beleidsverantwoordelijke directie Burgerschap & Informatiebeleid (B&I)[2] onder meer de volgende vragen: welke maatregelen waren van kracht ten tijde van de inbraak, welke maatregelen werden direct na het bekend worden van de inbraak genomen, en welke maatregelen zouden genomen moeten worden om te voorkomen dat zich in de toekomst iets soortgelijks

[2] De programmadirectie Dienstverlening, Regeldruk en Informatiebeleid (DRI) van het ministerie van BZK was tot 1 november 2011 beleidsverantwoordelijk voor PKIoverheid. Per 1 november 2011 is DRI opgegaan in de directie Burgerschap & Informatiebeleid (B&I).

kan voordoen? Inmiddels zijn met betrekking tot deze ‘DigiNotar-problematiek’ verschillende onderzoeken vanuit de overheid gestart.

Dit rapport, in opdracht van B&I, betreft een onderzoek met de volgende hoofdvraag:

Hebben de betrokken overheidspartijen in het stelsel van PKIoverheid (betreft zowel gekwalificeerde als niet-gekwalificeerde certificaten), gegeven de bestaande taken en verantwoordelijkheden van die partijen binnen genoemd stelsel, alert gereageerd inzake ‘DigiNotar’?

Deze hoofdvraag kan worden uitgesplitst in twee deelvragen:

1. Waren alle betrokken overheidspartijen in voldoende mate alert c.q. reageerden zij, gegeven hun verantwoordelijkheden, alert en adequaat op signalen dat er bij de certificaatuitgevende partij DigiNotar sprake zou kunnen zijn van een niet toereikend beveiligingsregime? [Tijdvak: januari 2010 tot medio 2011.]
2. Was er - na het bekend worden in augustus 2011 - sprake van alert en adequaat reageren door de betrokken overheidspartijen op de geconstateerde digitale inbraak bij DigiNotar in juli 2011? [Tijdvak: eind augustus 2011 tot medio september 2011.]

Ten behoeve van het onderzoek zijn interviews gehouden met diverse betrokkenen en heeft desk research plaatsgevonden. Het betreft een vraaggestuurd onderzoek, waarbij geen assurance wordt verleend.

1.3 Afbakening

Dit onderzoek staat overigens los van een door BZK en EL&I geïnitieerd - en door Logica uitgevoerd - onderzoek naar opzet, inrichting en werking van het PKIoverheid-stelsel, en naar het toezicht op Nederlandse gekwalificeerde certificaten die buiten dit stelsel vallen. In dit RAD-onderzoek ligt daarom minder de focus op de aard van het genoemde stelsel, maar meer op het gedrag van de overheid (alertheid en adequaatheid van handelen).
Direct na het bekend worden van de inbraak zag de overheid in dat de kans op maatschappelijke ontwrichting aanzienlijk was, en dat er verdere maatregelen getroffen

moesten worden. Daarbij was niet alleen het aspect 'continuïteit' van belang, maar ook het aspect 'veiligheid'. Mede omdat uit afstemming gebleken is dat dit laatste aspect voor een aanzienlijk deel wordt meegenomen in het onderzoek door de Inspectie Veiligheid & Justitie (naar het functioneren van de rijkscrisisstructuur in de dagen volgend op het bekend worden van de digitale inbraak), ligt de focus in dit RAD-onderzoek meer op het continuïteitsaspect.

1.4 Opbouw rapport

In het hiernavolgende hoofdstuk wordt gekeken naar de periode voorafgaand aan de DigiNotar-affaire. Eerst wordt aangestipt hoe de processen verliepen op basis waarvan de overheid alert had moeten of kunnen zijn (voor zover het het PKIoverheid-stelsel betreft). Daarna volgen onze bevindingen aangaande dat wat voor verbetering vatbaar was in de betreffende periode.

Het derde hoofdstuk behandelt de periode direct na het bekend worden van de digitale inbraak bij DigiNotar. Allereerst wordt belicht welke adequate acties de overheid toen heeft ondernomen om de ontstane crisis het hoofd te bieden. Vervolgens wordt stilgestaan bij wat beter had gekund, waarna enkele slotopmerkingen volgen.

2 Periode voorafgaand aan DigiNotar-affaire

2.1 Hoe was de beheersing ten aanzien van het PKIoverheid-stelsel voorafgaand aan de DigiNotar-affaire?

We proberen hier allereerst de vraag te beantwoorden hoe, in de periode voorafgaand aan de DigiNotar-affaire, de processen verliepen op basis waarvan de overheid alert had moeten of kunnen zijn (voor zover het het PKIoverheid-stelsel betreft). Dit is niet los te zien van het functioneren van het stelsel van beheersing en toezicht dat van toepassing is voor PKIoverheid. Omdat Logica in haar onderzoek de opzet, inrichting en werking van het PKIoverheid-stelsel in al zijn facetten behandelt, volstaan wij hier met een korte beschrijving van zaken die tijdens ons onderzoek naar voren zijn gekomen.

Het stelsel van toezicht op de uitgifte van certificaten door (vertrouwde) certificatiedienstverleners en de toetreding van nieuwe certificatiedienstverleners voorziet in diverse toezichthoudende en controlerende partijen (overheid/niet-overheid) met elk zijn of haar eigen taken, bevoegdheden en verantwoordelijkheden (TBV's). Voor enkele overheidspartijen, waaronder OPTA, zijn deze TBV's vastgelegd in wet- en regelgeving, voor andere daarentegen is een en ander minder geformaliseerd vastgelegd.
Certificatiedienstverleners hebben voor wat betreft PKIoverheid een contractueel vastgelegde meldingsplicht richting Logius in het geval dat ernstige doorbrekingen van de dienstverlening aan de orde zijn (cyberincidenten).

Niet in alle gevallen is in voldoende mate gepreciseerd wat het houden van toezicht precies behelst en in welke mate men daarbij kan steunen op andere partijen. Het stelsel van toezicht berust *de facto* in grote mate op wederzijds vertrouwen. Daarbij is nauwe samenwerking en tijdige onderlinge verstrekking van betrouwbare informatie van cruciaal belang. Dit wordt mede ingegeven door de verschillende lagen die in dit stelsel zijn te onderscheiden en de verschillende soorten certificaten die worden verstrekt. Toezicht op c.q. controle van certificatiedienstverleners als geheel wordt ingevuld door geaccrediteerde[3] auditpartijen. OPTA houdt bij wet toezicht op alle gekwalificeerde certificaten, Logius ziet op alle PKIoverheid-certificaten; hierin zit een overlap (betreft gekwalificeerde PKIoverheid-certificaten). Basis voor het toezicht en de

[3] Accreditatie van en toezicht op de betreffende auditpartijen geschiedt door de Raad voor Accreditatie.

controle door de verschillende partijen is een stelsel van voorwaarden, vereisten, normen en standaarden, onder andere bestaande uit een Programma van Eisen, ETSI-normering, het TTP.NL-schema, de Telecommunicatiewet en het Besluit elektronische handtekeningen.

Voordat een certificatiedienstverlener überhaupt over mag gaan tot het verstrekken van certificaten moet deze zich eerst door een onafhankelijke, geaccrediteerde auditpartij laten certificeren en aantoonbaar voldoen aan alle geldende voorwaarden. Van geaccrediteerde certificerende instellingen (auditpartijen) mag worden verwacht dat zij de certificatie op betrouwbare en deskundige wijze uitvoeren; om dit te kunnen waarborgen zijn, naast de geldende gedrags- en beroepsregels (RA/RE), in het TTP.NL-schema eisen opgenomen waaraan de certificerende instelling en specifiek het auditteam moeten voldoen. Bij een gecertificeerde, operationele certificatiedienstverlener voert de certificerende instelling vervolgens eens in de drie jaar een volledig onderzoek uit op basis van de TTP.NL- en ETSI-normen. Jaarlijks wordt naar deelgebieden gekeken, eventueel voorzien van een herstelplan (op basis van major/minor nonconformities). Doorgaans resulteert dit in een goedkeurende verklaring. Het laatste auditrapport met betrekking tot DigiNotar is van maart 2011.

Gebleken is dat in het stelsel van toezicht zwaar wordt gesteund op de deskundigheid en het oordeel van de betreffende auditpartij. Er wordt daarbij volledig vertrouwd op een goede werking van het toezichtsstelsel als geheel. Gezien de ontstane crisis is het de vraag of en in hoeverre hierop nog vertrouwd kan en mag worden en of de huidige wijze van toezicht en controle in essentie goed genoeg kan functioneren om een dergelijke crisis in de toekomst te voorkomen.

2.2 Wat was niet optimaal, in de periode voorafgaand aan de DigiNotar-affaire?

Geen van de overheidspartijen heeft de DigiNotar-crisis voorzien. In de periode voordat de crisis plaatsvond is het certificatensysteem als geheel door de overheid niet kritisch geanalyseerd op mogelijke tekortkomingen. Zo is er geen (expliciete) risicoanalyse geweest waarbij de onderscheiden ketenpartners, hun onderlinge verwevenheid, afhankelijkheid en verantwoordelijkheden in kaart zijn gebracht, waarbij dit alles is beoordeeld en naar aanleiding waarvan nadere acties zijn uitgezet.

Er was geen inzicht in het aantal PKIoverheid-certificaten van DigiNotar dat per overheidspartij was uitgegeven. Ook was onbekend voor welke processen de PKIoverheid-certificaten werden gebruikt en was onduidelijk wat de implicaties zouden (kunnen) zijn als deze certificaten gecompromitteerd zouden raken. Als onderdeel van het PKI-stelsel van uitgegeven en ingetrokken certificaten wordt bijvoorbeeld ook een zogeheten trustlist gehanteerd door (de ontwikkelaars van) browsers. Deze browserleveranciers maken zelfstandig een afweging over de betrouwbaarheid van certificatiedienstverleners en het plaatsen van het betreffende rootcertificaat op de trustlist. Als browserleveranciers zo'n rootcertificaat zouden verwijderen van de trustlist, dan zou dat voor de gebruikers van de betreffende browser vergelijkbaar zijn met het ongeldig verklaren c.q. intrekken van alle certificaten die door een bepaalde certificatiedienstverlener zijn uitgegeven.

Er was vooraf geen regie-organisatie ingericht, gericht op het omgaan met crises als de DigiNotar-affaire, met afstemming van de onderlinge taken en bevoegdheden.

De verantwoordelijkheid voor PKIoverheid ligt bij het ministerie van BZK, bij de directie B&I (tot 1 november 2011: programmadirectie DRI). Deze directie is verantwoordelijk voor het beleid, maar de beleidsuitvoering c.q. de rol van Policy Authority voor PKIoverheid is belegd bij Logius. B&I kon niet via documentatie inzichtelijk maken welke rollen de betrokken partijen hebben, inclusief de eigen rol van B&I. DigiNotar werd vóór het bekend worden van de hack als een vertrouwde partij beschouwd, die door een externe auditor beoordeeld werd en 'goed' is bevonden. B&I was in de veronderstelling dat de betreffende omgevingen bij DigiNotar gescheiden waren en heeft daarnaast vertrouwd op de auditor. B&I heeft sinds begin 2010 eenmaal per twee weken overleg met Logius, maar hiervan worden geen vastleggingen gemaakt. Tijdens dit overleg komt onder andere het beheer van het Programma van Eisen aan de orde.

Vanuit het perspectief van toezicht is er geen standpunt over de mate waarin afwijkingen door certificatiedienstverleners van de voorgeschreven normen al dan niet acceptabel zijn; in de praktijk is er overigens bijna geen certificatiedienstverlener die nooit afwijkingen heeft. Bij het overheidstoezicht werd zwaar geleund op de auditor, waarbij de mate van diepgang van de auditwerkzaamheden - variërend van beoordeling van hoofdzakelijk de management controlcyclus tot beoordeling van met nadruk ook de technische implementatie - geen factor van betekenis vormde; men kan overigens ook vragen stellen bij het feit dat audits bij certificatiedienstverleners nooit onverwachts plaatsvinden.

Uit hoofde van zijn toezichthoudende functie op gekwalificeerde certificaten wordt door OPTA onder meer het auditrapport van de auditor jaarlijks omstreeks augustus opgevraagd. Het laatste auditrapport met betrekking tot DigiNotar, van maart 2011, was - vóór het bekend worden van de DigiNotar-crisis - nog niet opgevraagd. OPTA vervult zijn toezicht op basis van informatie uit auditrapportages, op signalen van de auditor of op signalen van Logius. De grondslag voor het toezicht door OPTA wordt gevormd door wet- en regelgeving alsmede door vigerende normen. Dit alles is vaak op hoofdlijnen geformuleerd. Mede hierdoor kan tussen partijen (bijvoorbeeld tussen Logius en OPTA) al snel een verschil van inzicht ontstaan over de daadwerkelijke invulling van een en ander.

Er is een trend dat de overheid delen van haar eigen dienstverlening uitbesteedt. De vraag die gesteld kan worden is of de gedachte van marktwerking ('laat het over aan de markt') wel in alle gevallen mogelijk en/of wenselijk is en of het in eigen beheer houden, gegeven de publieke taak van de overheid en de mogelijke maatschappelijke impact, in voorkomende gevallen niet een wenselijker optie is. De indruk is dat er teveel wordt vertrouwd op een ‘goede’ naam in plaats van te focussen op kwaliteit.

De taken van de programmadirectie DRI waren vooral coördinerend en structurerend van aard; DRI was meer gericht op het uitvoeren van projecten dan op beleidsontwikkeling. Ook was het DRI-programma eind 2010 bijna afgerond. Dit heeft een rol gespeeld bij de beleidsontwikkeling m.b.t. de certificaten; het denken over certificaten en beveiliging was een dossier waaraan geen hoge prioriteit (meer) werd toegekend. De gedachte was dat de beleidsontwikkeling was afgerond en dat hieraan voorlopig niets meer hoefde te gebeuren; beheer van PKIoverheid was in goede handen bij Logius.

3 Periode direct na bekend worden DigiNotar-inbraak

Vanwege het door DigiNotar verzwijgen van de geconstateerde inbraak werd pas in een veel te laat stadium duidelijk dat er problemen waren met de betrouwbaarheid van certificaten. Bovendien waren niet direct omvang en verstrekkendheid van de problematiek bekend; welke typen certificaten waren door de inbraak geraakt en konden daarmee niet meer als veilig worden beschouwd?

3.1 Wat ging er allemaal goed na het bekend worden van de inbraak?

De overheid heeft zijn tanden laten zien. Deels als reactie op het verzwijgen van de digitale inbraak door DigiNotar werden in snel tempo verregaande maatregelen getroffen. Bij dit soort gevallen van cybercrime is snelheid van handelen een vereiste.

Vele vormen van samenwerking zijn benut: tussen overheidspartijen onderling, tussen publieke en private partijen, en tussen internationale partners. Ook is op een gegeven moment de wetenschap betrokken; zo werd op 4 september professor Bart Jacobs, hoogleraar Computerbeveiliging (Radboud Universiteit Nijmegen), ingeschakeld voor advies.

In de Programmaraad van Logius, die op vrijdagmiddag 2 september 2011 bij elkaar werd geroepen, waren in dit verband relevante *key players* vertegenwoordigd. Dit was zeer bevorderlijk voor een snelle informatie-uitwisseling en vervolgens ook voor een goed gedragen besluitvorming. Precies ten tijde van de Programmaraad-bijeenkomst werd namelijk ook duidelijk dat Fox-IT het gecompromitteerd zijn van PKIoverheid-certificaten niet kon uitsluiten. Jaap Uijlenbroek, de directeur-generaal Organisatie & Bedrijfsvoering Rijk, werd nu helemaal een belangrijke spin in het web.[4] GOVCERT.NL[5] - dat al vanaf het begin van de crisis, op maandag 29 augustus 2011, in alle opzichten stevig de vinger aan de pols hield, met name ook richting DigiNotar - zorgde er direct voor dat de kwestie opgeschaald kon worden naar het niveau van crisis, waarna de rijkscrisisstructuur werd geactiveerd. Ook Logius had al die hele week een belangrijke rol gehad, onder meer door klanten te informeren, en door hen

[4] Tijdens de afwikkeling van de crisis werd zowel een 'Operationeel Team Continuïteit' (OTC) als een 'Operationeel Team Veiligheid' (OTV) geformeerd. Het OTC stond onder leiding van Jaap Uijlenbroek, het OTV onder leiding van Erik Akerboom (Nationaal Coördinator Terrorismebestrijding en Veiligheid).

[5] GOVCERT.NL was juist een maand eerder afgesplitst van Logius.

proactief te vragen om toch alvast te inventariseren waarmee hun PKIoverheid-certificaten in verband stonden.

Gegeven de ontstane situatie is er zeer proactief gehandeld door de overheid. Vastliggende alsook (juridisch) niet geheel duidelijk belegde taken, bevoegdheden en verantwoordelijkheden (van afzonderlijke partijen) waren in deze crisissituatie feitelijk van minder belang dan samenwerking en coördinatie tussen partijen. Door de aanvankelijke onduidelijkheid over de verstrekkendheid van de hack en het pogen te anticiperen op zich mogelijk ontwikkelende scenario's ontstond een nieuwe, geheel eigen dynamiek. Men heeft niet geaarzeld om vergaande maatregelen te treffen. Voorbeelden daarvan zijn: het op zeer korte termijn overnemen van het feitelijke beheer van het bedrijf DigiNotar door de overheid (via overleg met de eigenaar Vasco Data), en het succesvol overleggen met Microsoft om specifiek voor Nederland een automatische update uit te stellen.

De DigiNotar-hack wordt binnen de overheid wel ervaren als een *wake up call*. Tegelijkertijd heeft de DigiNotar-problematiek - uiteraard gegeven het feit dat uiteindelijk geen grote schade is opgetreden op in ieder geval het gebied van continuïteit - gefungeerd als een uitstekende, levensechte oefening om partijen samen te brengen op het complexe gebied van de beveiliging van de digitale infrastructuur.

Enig geluk heeft niet ontbroken bij de aanpak van de ontstane crisis. Zo was het achteraf bezien niet ongunstig dat het mogelijk gecompromitteerd zijn van de PKIoverheid-omgeving bij DigiNotar duidelijk werd op een vrijdag; daardoor kon het weekend benut worden voor de meest belangrijke, initiële maatregelen. In de aanpak stonden personen aan het roer met de juiste kennis en vaardigheden en met de benodigde contacten. Er was sprake van een goede mix van persoonlijkheden. Wat de aanpak van de crisis ook ten goede kwam, was het feit dat vlak voor het DigiNotar-incident de oefening Cyberstorm III had plaatsgevonden, met ook deelname van de zich vormende ICT Response Board waarin zowel de publieke als de private sector vertegenwoordigd is. Tevens kon de Interdepartementale Commissie van CIO’s (ICCIO) relatief eenvoudig uitgebreid worden tot een zogeheten “ICCIO-plus” met ook CIO’s van lagere overheden en VNO-NCW.

De Nederlandse overheid heeft vanaf zaterdag 3 september 2011 de feitelijke operationele bedrijfsvoering van DigiNotar op het gebied van certificaten overgenomen. Dit was eigenlijk 'een sprong in het diepe' (want juridisch bezien niet volledig

uitgekristalliseerd)[6], maar achteraf kan geconstateerd worden dat deze handelwijze een juiste zet is geweest. Betrouwbare, eerstehands informatie vanuit het bedrijf kon daardoor op dezelfde dag (zaterdag 3 september 2011) gedeeld worden met de beleidsbepalers in het Nationaal Crisis Centrum.

Over het algemeen is er goede en tijdige communicatie geweest vanuit de overheid naar burgers en instanties toe.

3.2 Wat had beter gekund in de periode na het bekend worden van de inbraak?

Daar waar BZK een gecontroleerde migratie naar andere certificatiedienstverleners wenste, nam OPTA het besluit om de registratie van DigiNotar om gekwalificeerde certificaten uit te geven per 14 september 2011 in te trekken. Hierdoor moest DigiNotar alle uitstaande gekwalificeerde certificaten van DigiNotar intrekken. Dat betekende dat alle dienstverlening met die certificaten per die datum geen doorgang meer kon vinden. Dit heeft geleid tot rechtszaken tegen OPTA door belanghebbende partijen, zelfs inclusief andere overheidsorganisaties.
Hoewel de intrekking van de bovengenoemde registratie van DigiNotar - bezien vanuit het perspectief van OPTA - op zich verklaarbaar was, had er meer oog kunnen zijn voor de continuïteit van (in ieder geval) de PKIoverheid-dienstverlening. Hierbij had gedacht kunnen worden aan het bieden van alternatieven c.q. het treffen van maatregelen om uitwijkvoorzieningen te creëren, teneinde ‘de winkel open te houden’.

De overheid beschikte niet over een lijst waaruit bleek van welke certificaten de diverse afnemers van PKIoverheid gebruik maakten. Dit overzicht was nodig voor het kunnen uitvoeren van een *impact assessment.* Nadat de crisis was uitgebroken, werd deze slag binnen korte tijd alsnog gemaakt.

Aan afnemers van PKIoverheid-certificaten is gedurende de week van 29 augustus 2011 door de overheid verteld dat de PKIoverheid-omgeving bij DigiNotar - voor zover bekend - niet gecompromitteerd was. Dit bleek op vrijdag 2 september 2011 echter onwaar te zijn; het kon toen niet meer worden uitgesloten dat de PKIoverheid-omgeving gecompromitteerd was.

[6] Feitelijk was bijv. op dat moment bij de overheid ook niet bekend welke andere (certificatie)dienstverlening DigiNotar bood (naast die van PKIoverheid).

3.3 Tot slot

Er is veel in beweging op het terrein van cyber security bij de Nederlandse overheid. De ICT Response Board (IRB) is van start gegaan, een publiek-privaat samenwerkingsverband dat ingezet kan worden bij dreiging van een ICT-crisis; deze IRB is ondergebracht bij het Nationaal Cyber Security Centrum (NCSC). Steeds meer taken zijn nu belegd bij het ministerie van Veiligheid & Justitie. Bevoegdheden ter bestrijding van cybercrime worden uitgebreid.

Zaken op het gebied van digitale beveiliging worden door de overheid vrij vaak aan private partijen overgelaten. Het is van belang om de betreffende taken meer geaggregeerd bij de overheid te hebben. Daarbij zal meer specialistische kennis bij de overheid opgebouwd moeten worden.

Rijksauditdienst,
Projectleider

dhr. drs. J.P. Dirkx MBA