Evaluatie van de rijkscrisisorganisatie tijdens de DigiNotar-crisis

Inhoud

Voorwoord

Op vrijdag 2 september 2011 wordt duidelijk dat de uitgifte, door het bedrijf DigiNotar, van Public Key Infrastructure-Overheid certificaten is gecompromitteerd door een inbraak in de bestanden van dit bedrijf. Nadat dit bekend is, wordt de crisisorganisatie van de rijksoverheid opgeschaald via de rijkscrisisstructuur. Het is het begin van een voor Nederland unieke 'cybercrisis' die de rijkscrisisstructuur gedurende twee weken in haar greep houdt.

Het Kabinet heeft in een brief aan de Tweede Kamer toegezegd dat de Inspectie Veiligheid en Justitie een evaluatie zal uitvoeren naar de rijkscrisisstructuur tijdens de DigiNotar-crisis. Dit rapport beschrijft op hoofdlijnen de opzet en het optreden van de rijkscrisis-organisatie en de besluitvorming binnen deze organisatie. Op basis van deze evaluatie en de conclusies die hier uit worden getrokken doet Inspectie VenJ tevens enkele aanbevelingen ter verbetering van de rijkscrisisorganisatie.

Naast dit onderzoek van de Inspectie Veiligheid en Justitie heeft ook de Onderzoeksraad voor Veiligheid een onderzoek afgerond. Dit onderzoek richt zich op de vraag hoe de overheid de veiligheid van digitale communicatie met burgers waarborgt. De beide onderzoeken zijn in goede afstemming met elkaar uitgevoerd.

De DigiNotar-crisis was een crisis die voor de buitenwereld geen spectaculaire beelden opleverde, maar wel een crisis die wat mogelijke gevolgen betreft een enorme impact had. Een veelheid aan organisaties in overheid en bedrijfsleven, heeft bijna twee weken met man en macht succesvol samengewerkt om de zorgen omtrent uitval van essentiële digitale datacommunicatie weg te nemen.

J.G. Bos
Hoofd van de Inspectie Veiligheid en Justitie

Samenvatting

De DigiNotar-crisis is de eerste digitale crisis waarmee de rijkscrisisorganisatie is geconfronteerd. In tegenstelling tot een acute crisis (brand, explosie) ontwikkelt deze crisis zich sluipenderwijs van 'probleem' tot 'nationale crisis'. Als na onderzoek blijkt dat door een digitale inbraak bij het bedrijf DigiNotar mogelijk ook zogeheten Public Key Infrastructure (PKI)-overheidscertificaten zijn gecompromitteerd besluit men op 2 september 2011 de rijkscrisisstructuur op te schalen. Gecompromitteerde PKI-overheidscerticaten hebben in potentie grote gevolgen voor de vitale infrastructuur. Dit is het begin van een aantal hectische weken voor de rijkscrisisorganisatie. Het levert voor de buitenwereld geen spectaculaire beelden op, maar is wel een crisis waarbij het gaat om het (herstel van) vertrouwen van burgers in overheidsdiensten, de PKI-overheidscertificaten en het voorkomen van ontwrichting van vitale processen.

Naar aanleiding van de DigiNotar-crisis zegt het Kabinet aan de Tweede Kamer toe dat de Inspectie Veiligheid en Justitie (Inspectie VenJ) een evaluatie zal uitvoeren naar de rijkscrisisstructuur tijdens de DigiNotar-crisis[1]. De onderzoeksvraag die in het kader van deze evaluatie is geformuleerd, luidt: 'heeft de rijkscrisisorganisatie tijdens de DigiNotar-crisis doeltreffend gefunctioneerd?'. Het doel van dit onderzoek is vierledig:

1. Het beschrijven op welke wijze de rijkscrisisstructuur volgens vooraf vastgelegde plannen is ingericht.
2. Het in beeld brengen van de wijze waarop de DigiNotar-crisis door de rijkscrisisorganisatie is opgepakt.
3. Het beschrijven op welke punten in de werkwijze verbeteringen nodig zijn.
4. Het vertalen van deze verbeterpunten in aanbevelingen.

Voor de beantwoording van de centrale onderzoeksvraag zijn in de eerste plaats de relevante plannen bestudeerd. Vervolgens is onderzocht, door het bestuderen van – onder andere – verslagen, rapporten, interne evaluaties en factsheets, hoe de feitelijke crisisbestrijding heeft plaatsgevonden. Ten slotte zijn, om het beeld te completeren, sleutelspelers uit de rijkscrisisorganisatie geïnterviewd[2].

De Inspectie VenJ concludeert dat de rijkscrisisorganisatie tijdens de DigiNotar-crisis doeltreffend heeft gefunctioneerd. Het doeltreffend functioneren van de rijkscrisisorganisatie is mede te danken aan de korte lijnen, de goede samenwerking en het doortastende optreden van de belangrijkste sleutelfunctionarissen.

Vanaf het begin van de crisis reageert de crisisorganisatie alert. De mogelijke gevolgen van de hack bij DigiNotar zijn snel onderkend. Hoewel men in het begin nog geen compleet beeld heeft van de dreiging schaalt men de crisisorganisatie vlot op. Hierdoor maak men snel een start met de beheersing van de (dreigende) crisis.

Tijdens de DigiNotar-crisis vormt het Operationeel Team het 'hart van de crisisorganisatie'. Dit team is niet vastgelegd in de planvorming, maar ontstaat tijdens deze crisis ad hoc. Het Operationeel Team speelt tijdens deze crisis een cruciale rol. Dit betreft zowel het onderkennen van de crisis, het uitdenken en uitrollen van de strategie, het uitzetten van de te ondernemen acties als ook de voorbereiding op te nemen besluiten. Tussen de leden van het Operationeel Team is sprake van vertrouwen en een goede samenwerking. Dit vertaalt zich in een doortastend optreden.

Tijdens de DigiNotar-crisis is er sprake van een vlotte en goed lopende informatievoorziening tussen de verschillende organisatieonderdelen. De juiste informatie is op het juiste moment bij de juiste functionaris. Dit is mede te danken aan de korte lijnen tussen de verschillende sleutelfunctionarissen van zowel de rijkscrisisorganisatie als ook de betrokken externe organisaties.

[1] Brief aan Tweede Kamer van 16 september 2011, kenmerk 2011-2000411239.
[2] Zie voor een overzicht van de geïnterviewde personen bijlage 3.

Door goede analyses en voorbereiding op de te nemen besluiten, zijn de Ministeriële Commissie Crisisbeheersing (MCCb) en de Interdepartementale Commissie Crisisbeheersing (ICCb) goed in staat om beslissingen te nemen. Het Adviesteam voert hierbij zijn rol niet conform planvorming uit. Het Operationeel Team en het Chief Information Officer-overleg nemen de rol van adviseur over.

Het Nationaal CrisisCentrum toont tijdens deze crisis aan, zowel inhoudelijk als praktisch de crisisbeheersingsorganisatie goed te kunnen ondersteunen en faciliteren.

Op basis van het onderzoek doet de Inspectie VenJ de volgende aanbevelingen aan de Nationaal Coördinator Terrorismebestrijding en Veiligheid:

1. Blijf investeren in een vaste kernbezetting van de rijkscrisisorganisatie, met deelnemers die door opleiding en oefening over de juiste crisiscompetenties beschikken.

2. Bezie de bemensing, werkwijze en status van het Adviesteam binnen de rijkscrisisorganisatie vanuit het oogpunt van doeltreffendheid. Indien waarde wordt gehecht aan het Adviesteam, organiseer het Adviesteam dan zo, dat het zijn rol als adviseur van de MCCb en de ICCb kan waarmaken.

7

Inleiding

1.1 Aanleiding en doel

Op vrijdag 2 september 2011 wordt tijdens een ingelaste Programmaraad Logius[3] duidelijk dat er digitaal is ingebroken bij het bedrijf DigiNotar. Er zijn onmiskenbare signalen dat certificaten, uitgegeven door het bedrijf DigiNotar zijn gecompromitteerd door de inbraak in de bestanden van het bedrijf. Concreet betekent dit dat de gebruiker van (overheids)sites niet langer de garantie heeft dat hij daadwerkelijk op de site van zijn keuze komt. Gebruikers kunnen bij het benaderen van de websites de melding krijgen dat deze websites niet langer betrouwbaar zijn.

[3] Logius is de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Logius biedt publieke dienstverleners een samenhangende ICT-infrastructuur. Hierdoor kunnen burgers en bedrijven betrouwbaar, snel en gemakkelijk elektronisch zaken met hen doen. Om dit te organiseren, levert Logius producten op het gebied van toegang, gegevensuitwisseling, informatiebeveiliging en standaardisatie.

Omdat een essentieel onderdeel van betrouwbare digitale informatievoorziening is aangetast en daardoor in potentie ernstige verstoringen kunnen optreden schaalt de rijksoverheid op vrijdagmiddag 2 september om 16:00 uur de rijkscrisisstructuur op. Dit is het begin van een aantal hectische weken waarin wordt geanticipeerd op de 'hack' en de mogelijke gevolgen daarvan. In de weken na 2 september wordt op verschillende niveaus en tussen veel verschillende organisaties van de overheid en het bedrijfsleven, intensief samengewerkt om de crisis te bezweren.

Het Kabinet zegt op 16 september 2011 in een brief aan de Tweede Kamer toe dat de Inspectie VenJ een evaluatie zal uitvoeren naar het functioneren van de rijkscrisisstructuur tijdens de DigiNotar-crisis[4].

Onderzoeksdoel

De evaluatie beoogt om uit de DigiNotar-crisis – op basis van de conclusies en aanbevelingen – lessen te trekken waardoor de crisisorganisatie op nationaal niveau bij dergelijke incidenten verder kan worden geoptimaliseerd. Dit oogmerk is terug te vinden in de onderzoeksdoelstellingen die door de Inspectie VenJ zijn geformuleerd:

1. Het beschrijven op welke wijze de rijkscrisisstructuur volgens vooraf vastgelegde plannen[5] is ingericht.
2. Het in beeld brengen van de wijze waarop de DigiNotar-crisis door de rijkscrisisorganisatie is opgepakt.
3. Het beschrijven op welke punten in de werkwijze verbeteringen nodig zijn.
4. Het vertalen van deze verbeterpunten in aanbevelingen.

Onderzoeksvraag

Op basis van de eerder genoemde toezegging aan de Tweede Kamer en de onderzoeksdoelstellingen is de navolgende centrale vraag geformuleerd.

- Heeft de rijkscrisisorganisatie tijdens de DigiNotar-crisis doeltreffend gefunctioneerd?

Onderzoeksopzet

Voor de beantwoording van de onderzoeksvraag zijn in de eerste plaats de relevante plannen bestudeerd. Vervolgens is onderzocht, door het bestuderen van – onder andere – verslagen, rapporten, interne evaluaties en factsheets, hoe de feitelijke crisisbestrijding heeft plaatsgevonden. Ten slotte zijn, om het beeld te completeren, sleutelspelers uit de rijkscrisisorganisatie geïnterviewd[6]. Ten behoeve van de interviews is een interviewprotocol opgesteld waarin de wijze van het interviewen als ook de wijze waarop met de informatie uit de interviews wordt omgegaan zijn vastgelegd.

4 Brief aan Tweede Kamer van 16 september 2011, kenmerk 2011-2000411239.
5 Dit betreft het Nationaal Handboek Crisisbesluitvorming en het Nationaal Crisisplan ICT.
6 Zie voor een overzicht van de geïnterviewde personen bijlage 3.

Om te beoordelen of de rijkscrisisorganisatie doeltreffend heeft gefunctioneerd is gebruik gemaakt van een analysekader waarin de feitelijke uitvoering door de rijkscrisisorganisatie is getoetst aan de beoogde doelstellingen. In het concept Toetsingskader Crisisbeheersing zijn een aantal kritische processen benoemd. Voor zover van toepassing zijn deze processen gebruikt als kader voor de analyse van de DigiNotar-crisis. Door de bevindingen uit hoofdstuk drie langs deze processen te analyseren, wordt een overzicht gegeven van de prestaties tijdens deze crisis. In het analysehoofdstuk wordt per proces een omschrijving gegeven van de kenmerken, de doelen en de beoogde prestaties van het proces. Vervolgens wordt geanalyseerd hoe in de praktijk invulling is gegeven aan het betreffende proces.

Op basis van het antwoord op de centrale vraag zijn aanbevelingen gedaan ter verbetering van de rijkscrisisorganisatie.

1.2 Reikwijdte van het onderzoek

Op basis van de toezegging van het Kabinet om de Inspectie VenJ een evaluatie te laten uitvoeren naar de rijkscrisisstructuur (en daarmee de crisisorganisatie) tijdens de DigiNotar-crisis, heeft de Inspectie VenJ een onderzoek gestart naar de opzet en het optreden van de rijkscrisisorganisatie en de besluitvorming binnen deze organisatie. De onderzoeksvraag is afgestemd met de Onderzoeksraad voor Veiligheid (OVV) die ook onderzoek naar de DigiNotar-crisis heeft verricht. Dit onderzoek richt zich op de vraag hoe de overheid de veiligheid van digitale communicatie met burgers waarborgt.

De geëvalueerde periode beslaat het moment vlak voor het opschalen van de rijkscrisis-structuur op 2 september 2011 tot en met het laatste Interdepartementale Commissie Crisisbeheersing (ICCb) overleg op 14 september. De nadruk van de evaluatie ligt op de eerste dagen waarin de crisisstructuur wordt opgebouwd, de strategie wordt bepaald en acties worden uitgezet.

De oorzaak van de crisis is voor deze evaluatie minder relevant. De Inspectie VenJ laat daarom de aanleiding (de 'hack') die tot de deze crisis heeft geleid buiten beschouwing. De evaluatie is gericht op de rijkscrisisorganisatie. De uitvoering van de uitgezette acties bij bijvoorbeeld lagere overheden (gemeenten / provincies) en het bedrijfsleven (VNO-NCW / MKB), alsmede de inhoud en kwaliteit van deze acties (of adviezen) blijven in deze evaluatie buiten beschouwing.

1.3 Leeswijzer

Dit rapport bestaat uit vijf hoofdstukken. Dit eerste hoofdstuk beschrijft de onderzoeksopzet. Het tweede hoofdstuk behandelt de planvorming met betrekking tot de rijkscrisisstructuur.

Het derde hoofdstuk neemt het optreden van de rijkscrisisorganisatie onder de loep. Het beschrijft op chronologische wijze de activiteiten die door de verschillende onderdelen (coördinatie- en besluitvormingsstructuren) van de rijkscrisisstructuur – al dan niet in onderlinge samenhang – zijn uitgevoerd.

Hoofdstuk vier bestaat uit analyses op basis van hoofdstuk twee en hoofdstuk drie. Ten slotte wordt de onderzoeksvraag beantwoord in hoofdstuk vijf. Ook doet de Inspectie VenJ in dit hoofdstuk aanbevelingen.

2

De planvorming met betrekking tot de inrichting van de rijkscrisisstructuur

2.1 Algemeen

In het Nationaal Handboek Crisisbesluitvorming[7] zijn procedures en coördinatie- en besluitvormingsstructuren op rijksniveau vastgelegd voor de beheersing van (dreigende) crises. Naast het generieke Nationaal Handboek Crisisbesluitvorming zijn er crisisspecifieke plannen die de processen binnen een specifiek crisistype beschrijven. Voor het crisistype ICT bestaat het Nationaal Crisisplan ICT (NCP-ICT). Ten tijde van de DigiNotar-crisis is dit NCP-ICT nog niet formeel vastgesteld, maar maakt de in dit plan beschreven werkwijze wel deel uit van de aanpak. Daarom is dit plan wel meegenomen in dit evaluatieonderzoek. Inmiddels is dit NCP-ICT op 15 december 2011 formeel vastgesteld.

7 Nationaal Handboek Crisisbesluitvorming, 14 juni 2011.

Dit hoofdstuk zoomt in op zowel het generieke plan als het crisisspecifieke plan.
Aan de hand van deze plannen wordt de inrichting van de rijkscrisisstructuur besproken.

2.2 Het Nationaal Handboek Crisisbesluitvorming

Het nationale crisisbeheersingsstelsel is vastgelegd in het Nationaal Handboek Crisisbesluitvorming. Dit handboek heeft als doel: 'het vastleggen van procedures en eenduidige coördinatie- en besluitvormingsstructuren op rijksniveau voor de beheersing van (dreigende) crises'. Het is een generiek handboek en daarmee van toepassing op alle (dreigende) crisissituaties die een departementaal gecoördineerd optreden van de rijksoverheid vragen. Het handboek wordt regelmatig geëvalueerd, aangepast en opnieuw vastgesteld.

Het Nationaal Handboek Crisisbesluitvorming treedt in werking op het moment dat er sprake is van een nationale crisis. Dit is het geval wanneer één of meerdere vitale belangen (dreigen te) worden aangetast en de reguliere structuren en middelen niet toereikend zijn om de stabiliteit te handhaven. Er zijn vijf vitale belangen benoemd:

- territoriale veiligheid;
- economische veiligheid;
- ecologische veiligheid;
- fysieke veiligheid;
- sociale en politieke stabiliteit.

Deze vijf belangen zijn niet los van elkaar te zien, er is meestal sprake van een nauwe samenhang tussen deze belangen.

Achtereenvolgens worden in deze paragraaf de verschillende procedures en coördinatie- en besluitvormingsstructuren behandeld die in het Nationaal Handboek Crisisbesluitvorming staan beschreven.

Het Adviesteam

Elk ministerie draagt zorg voor de acties die binnen de eigen sector worden uitgevoerd. Het betreffende Departementaal Coördinatie Centrum (DCC) coördineert deze acties. Als sprake is van een (dreigende) crisis waarbij meerdere ministeries betrokken zijn, komt het Adviesteam bijeen.

Het Adviesteam wordt eventueel aangevuld met specifieke experts. De taken van dit team zijn onder andere het uitwisselen van informatie, het vormen van een beeld en oordeel over de situatie en het bezien of het noodzakelijk is om de Interdepartementale Commissie Crisisbeheersing (ICCb) en/of de Ministeriële Commissie Crisisbeheersing (MCCb) te activeren.

De Interdepartementale Commissie Crisisbeheersing

De ICCb wordt geactiveerd wanneer een (dreigende) crisis sector overstijgend is en/of in geval van een (mogelijke) opschaling van de crisiscommunicatie naar het nationale niveau. Dit gebeurt door één van de vaste leden van de ICCb of op verzoek van een Directeur-generaal (dg), Inspecteur- generaal (IG) of Secretaris-generaal (SG) van een ministerie. In de ICCb wisselt men op hoog ambtelijk niveau (dg/IG/SG) informatie uit en vormt men beelden en oordelen over de situatie. De ICCb bepaalt de strategische kaders en de kaders voor (publieks)voorlichting en woordvoering. De ICCb besluit over te nemen maatregelen en adviseert over het bijeenkomen van de MCCb. Zij geeft tevens advies aan de MCCb over te nemen maatregelen en de politieke consequenties daarvan.

De Ministeriële Commissie Crisisbeheersing

In een situatie die vraagt om sectoroverstijgende crisisbeheersing op politiek-bestuurlijk niveau kan de MCCb bijeen komen. Het verzoek tot activering van de commissie wordt gericht aan de minister van Veiligheid en Justitie (VenJ), die vervolgens overlegt met de minister-president over de activering, de samenstelling en het voorzitterschap. De MCCb komt onder andere bijeen om besluiten te nemen over adviezen van de ICCb, om de strategische kaders te bepalen en om de Staten-Generaal in te lichten. Daarnaast beraadslaagt de commissie over de politieke consequenties van genomen of te nemen besluiten en over adviezen ten behoeve van de ministerraad of andere overheden. Het MCCb neemt besluiten, de besluitenlijst moet worden goedgekeurd door de ministerraad.

Het Nationaal CrisisCentrum

Er is een permanent bezet Nationaal CrisisCentrum (NCC). Dit centrum vervult de functie van interdepartementaal facilitair communicatiecentrum en knooppunt van en voor de bestuurlijke informatie.

Het Nationaal Voorlichtingscentrum

De verantwoordelijkheid voor de crisiscommunicatie bij een (dreigende) crisis is in eerste aanleg belegd bij de betrokken departementale voorlichtingsdiensten. Het cluster Risico- en Crisiscommunicatie (cRC) van het NCC brengt in dit geval advies uit en stelt publieksinformatiemiddelen ter beschikking. Op last van de voorzitter van de ICCb, de MCCb of de eerstverantwoordelijke bewindspersoon wordt het Nationaal Voorlichtingscentrum (NVC) geactiveerd. Het NVC kent drie taakgroepen, de taakgroep Analyse, de taakgroep Advies en de taakgroep Aanpak. Deze taakgroepen zijn belast met het monitoren en analyseren van de media, het adviseren van de ICCb en de MCCb over de te volgen communicatiestrategie en de communicatieve gevolgen van de genomen besluiten. De taakgroep Aanpak is verantwoordelijk voor de uitvoering van de communicatiestrategie op rijksniveau. Het NVC wordt gevormd door medewerkers van het NCC en uit medewerkers die werkzaam zijn bij de directies Voorlichting van de ministeries en hun uitvoeringsorganisaties.

2.3 Het Nationaal crisisplan ICT

Al in de Nationale Risicobeoordeling van 2008/2009 en in de Bevindingenrapportage Nationale Veiligheid 2010 speelt een mogelijke crisis met betrekking tot ICT een rol. In de bevindingenrapportage staat:

'De digitalisering van de samenleving neemt steeds grotere vormen aan. Dat biedt veel kansen, maar zorgt ook voor nieuwe risico's. Risico's van kleinschalige criminaliteit tot cyberdefence/warfare en verstoring van de nationale veiligheid. Uitval van ICT voorzieningen kan leiden tot aantasting van onze vitale belangen. Te denken valt bijvoorbeeld aan economische schade bij uitval van het betalingsverkeer. Deze steeds dominantere rol van ICT in onze samenleving is aanleiding geweest om digitale veiligheid binnen de strategie Nationale Veiligheid als apart dreigingstype te identificeren.'

Experts achtten het destijds waarschijnlijk dat de verdediging tegen een dergelijke aanval tekort zou schieten, omdat het nagenoeg onmogelijk is om snel vast te stellen waar een aanval vandaan komt en wie daar achter zit. Op basis van deze risicobeoordeling is besloten een NCP- ICT op te stellen.

Het NCP-ICT omschrijft een ICT-crisis als 'een dreiging of crisis waarbij de bron ligt in het ICT-domein, waarbij één of meerdere vitale belangen in het geding zijn waarvoor de reguliere structuren niet toereikend zijn'. Een ICT-crisis kan voortkomen uit moedwillig handelen en niet-moedwillig handelen. De aanpak van een 'moedwillige crisis' en een 'niet-moedwillige crisis' komt grotendeels overeen. Echter bij een crisis veroorzaakt door moedwillig handelen zijn in verband met de opsporingsactiviteiten ook andere actoren actief.

Naast de planvorming voor de crisisbeheersingsstructuur is er in februari 2011 ook een Nationale Cyber Security strategie vastgesteld. Deze strategie bestaat uit twee delen. Het eerste deel bevat een analyse van het probleem omtrent de cyber security, de uitgangspunten en het te bereiken doel. Het tweede deel beschrijft een aantal actielijnen en activiteiten die het kabinet samen met andere partijen gaat uitvoeren om de cyber security te verbeteren.

Het NCP-ICT beschrijft de verschillende overleggen die een rol spelen bij een ICT-crisis, voor zover zij niet zijn opgenomen in de generieke planvorming.

De ICT Response Board

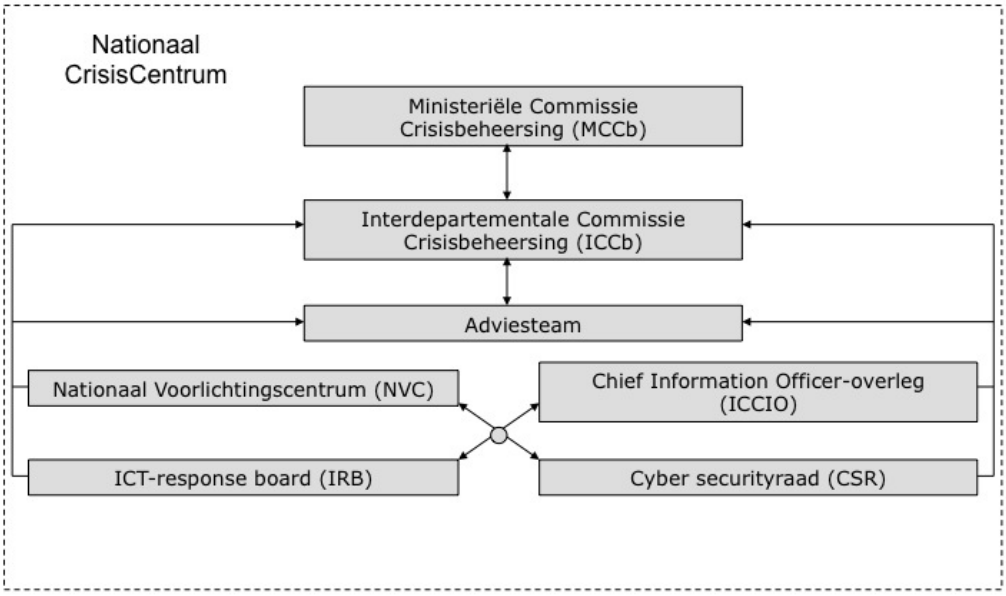
Bij een (dreigende) sectoroverstijgende ICT-crisis wordt de ICT Response Board (IRB) geactiveerd. Dit is een publiek-privaat samenwerkingsverband dat tijdens een (dreigende) ICT-crisis op basis van informatie-uitwisseling een analyse maakt van de crisis. Het IRB brengt indien nodig een advies uit aan het Adviesteam. De samenstelling van het IRB is flexibel.

De Cyber Security Raad

Naast de IRB is er een Cyber Security Raad (CSR). Dit is een publiek-privaat samenwerkingsverband op strategisch niveau. In een crisissituatie kan het worden geconsulteerd en fungeert in die hoedanigheid als 'klankbord'. De voorzitters zijn de Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de Chief Executive Officer (CEO) van de KPN.

Het Chief Information Officer-overleg

Het Chief Information Officer (CIO)-overleg, ook Interdepartementale Commissie CIO (ICCIO) genoemd, is een regulier overleg van alle CIO's van het Rijk en wordt voorgezeten door de CIO-Rijk van het ministerie van BZK. De ICCIO is verantwoordelijk voor de informatiebeveiliging van het Rijk. Tijdens een ICT-crisis die gevolgen heeft voor de bedrijfsvoering, heeft de ICCIO een coördinerende taak.



Figuur 1. Schematische weergave van de rijkscrisisstructuur volgens planvorming. Ten tijde van de DigiNotar-crisis waren de IRB, ICCIO en CSR uit het NCP-ICT nog niet formeel vastgesteld, maar maakten wel deel uit van de aanpak. Daarom zijn deze onderdelen wel meegenomen in deze schematische weergave.


3

De rijkscrisisorganisatie tijdens de DigiNotar-crisis

3.1 Algemeen

Om inzicht te krijgen in het functioneren van de rijkscrisisorganisatie tijdens de DigiNotar-crisis is in paragraaf 3.2 tot en met paragraaf 3.9 het optreden van de rijkscrisisorganisatie beschreven. Dit gebeurt aan de hand van een chronologische beschrijving op hoofdlijnen van de activiteiten die door de verschillende onderdelen (coördinatie- en besluitvormingsstructuren) van de rijkscrisisstructuur – al dan niet in onderlinge samenhang – zijn uitgevoerd.

3.2 Maandag 29 augustus tot vrijdagmiddag 2 september 2011

Van probleem tot nationale crisis

De DigiNotar-crisis ontwikkelt zich sluipenderwijs van 'probleem' tot 'nationale crisis'. In tegenstelling tot een acute crisis is de DigiNotar-crisis een langzaam ontwikkelende crisis. Direct betrokkenen geven in interviews[8] met de Inspectie VenJ aan dat dit twee oorzaken heeft. Allereerst ontbreekt een zichtbare calamiteit (zoals bij een brand of overstroming) en ten tweede betreft het zeer complexe materie waardoor de (mogelijke) gevolgen moeilijk zijn in te schatten.

De Nederlandse overheid ontvangt de eerste signalen dat er een probleem is met betrekking tot DigiNotar van Cert-Bund[9]. Dit gebeurt op maandag 29 augustus. Twee dagen daarvoor – op zaterdag 27 augustus – ontvangt Cert-Bund een melding dat een gebruiker in Iran op een Google-forum meldt dat hij bij het inloggen in zijn Gmail-account van zijn browser een waarschuwing heeft gekregen over de onbetrouwbaarheid van het certificaat[10]. Het certificaat is uitgegeven door DigiNotar.

Nadat Govcert van Cert-Bund het signaal met betrekking tot DigiNotar ontvangt op 29 augustus – omstreeks 12:30 uur – neemt Govcert direct met DigiNotar contact op het incident te melden, om inzicht te krijgen in de aard en omvang van de problematiek en om het betreffende certificaat in te laten trekken. Govcert maakt met DigiNotar de afspraak voor een conference call de volgende dag om de kwestie te bespreken.

Govcert licht op maandagavond om 23:05 uur het NCC in over de problemen bij DigiNotar. Govcert geeft aan dat de systemen van het bedrijf zijn 'gehackt' en dat certificaten van DigiNotar mogelijk zijn vervalst.

Op dinsdag 30 augustus neemt Govcert contact op met Logius van het ministerie van BZK. Ook neemt Govcert contact op met de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Op dat moment is de mogelijke impact van de gecompromitteerde certificaten nog niet duidelijk. Uit de conference call met DigiNotar eerder die dag omstreeks 09:30 uur, blijkt op dat moment niet dat de zogeheten PKI-overheidscertificaten[11] zijn gecompromitteerd. DigiNotar geeft tijdens de conference call met Govcert aan dat alleen de 'eigen merk[12]' certificaten zijn gecompromitteerd.

8 Zie bijlage 3.

9 Cert-Bund is de Duitse evenknie van Govcert en maakt net als Govcert deel uit van het wereldwijde netwerk van overheids- en private 'Computer Emergency Response Teams' (CERTs). Dit netwerk monitort voortdurend meer dan duizenden bronnen op internet.

10 Zie bijlage 4 voor een uitleg over certificaten en hun betekenis.

11 Zie bijlage 4 voor een uitleg over certificaten en hun betekenis.

12 Zie bijlage 4 voor een uitleg over certificaten en hun betekenis.

De PKI-overheidscertificaten zijn vooralsnog als 'trusted' aan te merken. DigiNotar heeft op dat moment het bedrijf Fox-IT[13] opdracht gegeven om nader onderzoek naar de 'hack' te doen.

Govcert heeft vanaf dinsdag 30 augustus en de daaropvolgende dagen (woensdag 31 augustus en donderdag 1 september) de operationele coördinatie van het incident. Daarnaast houdt Govcert zich bezig met het inschatten van de mogelijke crisisdreiging. Daarnaast worden de relevante diensten, sleutelfunctionarissen en overige instanties zoals de IRB geïnformeerd c.q. gealerteerd. Om in beeld te krijgen wat de precieze stand van zaken is met betrekking tot DigiNotar heeft men verschillende malen conference calls met DigiNotar. In deze contacten komen geen nieuwe feiten aan het licht. Men wacht het rapport van Fox-IT af.

Op donderdag 1 september is overleg tussen BZK/DRI (Programmadirectie Dienstverlening, Regeldruk en Informatiebeleid)[14] als opdrachtgever voor PKI-overheid en BZK/OBR (Organisatie Bedrijfsvoering Rijk)/Logius als opdrachtnemer en Govcert. Het is duidelijk dat aan betrokkenen een´slecht weerwaarschuwing´ moet worden gegeven. In dit overleg spreekt men drie acties af.

Ten eerste spreekt men af dat Logius haar gebruikers adviseert zich voor te bereiden op de mogelijkheid dat er overheidscertificaten van DigiNotar zijn gecompromitteerd. Daarbij is het van belang dat de gebruikers uitzoeken of, en welke, PKI-overheidscertificaten binnen de eigen organisatie aanwezig zijn en voor welke processen deze certificaten worden gebruikt. Tevens moet Logius de gebruikers adviseren om na te denken over de mogelijke gevolgen indien blijkt dat de PKI-overheidscertificaten niet meer kunnen worden vertrouwd. Ten tweede spreekt men in het overleg tussen BZK/DRI, BZK/OBR en Govcert af om het NCC voor te bereiden op een mogelijke opschaling van de crisisorganisatie. Ten derde last men een extra programmaraad Logius in op vrijdagmiddag 2 september.

Op vrijdagochtend 2 september spreekt Govcert met DigiNotar in een conference call af om de voorlopige bevindingen van Fox-IT 's middags te bespreken. Dezelfde ochtend schaalt Govcert om 10:30 uur de IRB op om inzicht te krijgen in de gevolgen van mogelijk gecompromitteerde PKI-overheidscertificaten.

Omstreeks 10:00 uur vindt een overleg plaats tussen de directeur Nationale Veiligheid, de NCTV en het hoofd NCC. In dit overleg besluiten zij om medewerkers van het NCC bij het IRB-overleg te laten aansluiten. Tevens besluiten zij om contact op te nemen met de dgOBR, die 's middags in het ingelaste overleg van de programmaraad Logius aanwezig is. Dit gebeurt om even voor 14:00 uur vlak voor de programmaraad Logius. Een van de betrokken zegt hierover:

[13] Fox-IT is een bedrijf in IT-security en expert op het gebied van informatiebeveiliging en digitaal rechercheonderzoek.

[14] Vanaf 1 november 2011 de directie Burgerschap en Informatiebeleid (B&I).

'Het woord crisis is toen nog niet in de mond genomen, maar het was ons duidelijk dat het niet zomaar een incident betrof'.

Vlak voor het begin van de programmaraad Logius is er overleg tussen de NCTV en de dgOBR. Zij bespreken op dat moment al mogelijke scenario's als mocht blijken dat de PKI-overheidscertificaten van DigiNotar niet meer zijn te vertrouwen. Om 14:00 uur start het overleg van de programmaraad Logius. Op praktisch hetzelfde moment vindt de mondelinge briefing van Fox-IT aan DigiNotar en Govcert plaats over haar voorlopige bevindingen[15] met betrekking tot 'de hack'. Fox-IT maakt bekend dat uit hun onderzoek blijkt dat de 'eigen merk'- certificaten zijn gecompromitteerd en dat niet kan worden uitgesloten dat óók PKI-overheidscertificaten zijn getroffen.

De informatie dat mogelijk ook de PKI-overheidscertificaten zijn gecompromitteerd wordt omstreeks 15:00 uur gedeeld in de programmaraad Logius. In dit overleg zijn inmiddels al verschillende scenario's besproken waaronder het 'worst case' scenario. Dit worst case scenario bevat acties die men zal ondernemen als blijkt dat ook de PKI-overheidscertificaten onbetrouwbaar zijn. De strategie is in dat geval het overnemen van het beheer van DigiNotar en het ontwikkelen van een 'migratietraject' van de DigiNotar-certificaten naar certificaten van andere (betrouwbare) certificeerders.

Omstreeks 15:00 uur hebben de NCTV en de dgOBR telefonisch contact. Zij besluiten om 17:00 uur op het NCC bij elkaar te komen voor overleg. Het hoofd NCC en de directeur Nationale Veiligheid schuiven hierbij aan. Na kort beraad besluit men de rijkscrisisstructuur in werking te stellen.

3.3 Vrijdagavond 2 september tot en met zaterdagnacht 3 september 2011

De inrichting van de rijkscrisstructuur en eerste acties

Op vrijdagmiddag is om 17:00 uur op het NCC een eerste overleg tussen de directeur Nationale Veiligheid, de NCTV, het hoofd NCC en de dgOBR. Hierbij zijn ook een aantal uitvoeringsorganisaties betrokken zoals de Belastingdienst en het Kadaster. In dit overleg worden de eerste beelden gedeeld. Het is de betrokkenen op dat moment duidelijk dat er sprake is van een (in potentie) grote crisis die door de rijkscrisisorganisatie moet worden opgepakt. Het is niet uit te sluiten dat de negatieve impact op de economische infrastructuur groot is. Dit omdat de DigiNotar-certificaten die het berichtenverkeer tussen systemen in sociale- en economische processen beveiligen (bijvoorbeeld via Digipoort) en ook voor de beveiliging van gekwalificeerde elektronische handtekeningen worden gebruikt, mogelijk onbetrouwbaar zijn. De problemen als gevolg van de onbetrouwbare certificaten hebben – zo is de inschatting – gevolgen voor diverse organisaties, beroepsgroepen en gebruikers; zoals de Belastingdienst, gemeenten en gebruikers van DigiD.

[15] Zie interim rapport: DigiNotar Certificate Authority breach 'Operation Black Tulip', 5 september 2011.

Ook voor het bedrijfsleven waar duizenden certificaten van DigiNotar in omloop zijn heeft dit mogelijk grote gevolgen. Men onderkent dat de DigiNotar-crisis niet alleen een continuïteitsvraagstuk en een securityvraagstuk[16] betreft, maar dat het ook een vertrouwensvraagstuk betreft. Op deze drie vraagstukken richt men zich bij het uitzetten van de eerste acties. Daarbij hebben de aspecten 'borgen van de continuïteit' en 'het herstellen van het vertrouwen' in eerste instantie prioriteit.

De communicatieadviseurs van het NCC, Govcert en de ministeriële woordvoerder van het ministerie van BZK stellen gezamenlijk de woordvoeringslijn vast. Men gaat ook aan de slag met het opstellen van scenario´s op het terrein van communicatie. Ook is om 17:00 uur contact met de webredacteur van de site 'rijksoverheid.nl' om de plaatsing van nieuwsberichten over de DigiNotar-crisis op deze site voor te bereiden.

In de loop van vrijdagmiddag vindt verschillende malen interdepartementaal overleg plaats. Rond 20:00 uur komt voor de eerste keer de ICCb bijeen. In dit overleg wordt onder andere een voorstel aan de MCCb besproken om het vertrouwen in DigiNotar op te zeggen en de bewindvoering van het bedrijf over te nemen. Dit is in lijn met de strategie zoals eerder op de dag in de programmaraad Logius is besproken. Door het vertrouwen in DigiNotar op te zeggen 'isoleert' men het probleem tot DigiNotar, waardoor men het vertrouwen in andere certificaten en de PKI-overheid tracht te behouden. Door het overnemen van het operationele beheer van certificaten van DigiNotar door de Nederlandse overheid voorkomt men dat mondiale browsers en dienstenleveranciers zoals Adobe alle Staat der Nederlanden PKI-certificaten – ongeacht de uitgever – als onbetrouwbaar aanmerken. Tevens laat men daarmee aan 'de buitenwereld' zien dat men de crisis daadkrachtig ter hand neemt. In het verlengde van de gekozen strategie benoemt men een aantal acties, dit zijn:

- het beheer van de certificaten overnemen van DigiNotar;
- het monitoren van het oneigenlijk gebruik;
- het op gang brengen van de transitie van gebruikers van DigiNotar naar andere (betrouwbare) certificeerdeers;
- de communicatie naar publiek, private partijen en overheid.

Om 20:00 uur is de woordvoeringslijn, het eerste persbericht en de eerste aanzet voor een lijst met mogelijke vragen en antwoorden gereed. Ook spreekt men in de ICCb af om vanaf zaterdag 3 september om 09:00 uur het publieksinformatienummer te activeren.

De MCCb komt – nadat het Kabinet van de eerste inventarisatie en uitgezette activiteiten op de hoogte is gebracht – om 21:00 uur bijeen onder voorzitterschap van de minister van Veiligheid en Justitie.

Naar aanleiding van het advies van de ICCb is op vrijdagavond na de bijeenkomst van de MCCb, door middel van een conference call, contact opgenomen met de 'board of directors' van de Amerikaanse eigenaar van DigiNotar, Vasco Data Security International.

[16] De Inspectie VenJ hanteert de terminologie zoals is gebruikt tijdens de DigiNotar-crisis.

In dit overleg met Vasco Data Security International komt men overeen dat de bedrijfsvoering door de Nederlandse overheid wordt overgenomen.

In de nacht van vrijdag 2 september op zaterdag 3 september geeft de minister van BZK een persconferentie. Hierin geeft hij aan dat de betrouwbaarheid van overheidswebsites op dat moment niet is te garanderen. De minister zegt tijdens deze persconferentie het vertrouwen in de certificaten van DigiNotar op. De minister geeft daarbij aan dat het Kabinet het operationeel beheer van de systemen voor certificaten bij DigiNotar heeft overgenomen. Het doel van deze overname is drieledig. Ten eerste om het certificeringsproces van intrekken, administreren en voor zover nodig beperkt uitgeven zeker te stellen voor zolang dit nodig is om op een ordelijke manier te kunnen verhuizen naar andere (PKI)certificeerders. Ten tweede om het vertrouwen in PKI-overheidscertificaten – zover niet besmet – overeind te houden. Ten derde om als overheid het signaal af te geven dat men 'er boven op zit' en de zaken onder controle heeft.

3.4 Zaterdag 3 september 2011

De verdere vormgeving van de rijkscrisisstructuur en de samenwerking daarbinnen
Op zaterdag 3 september krijgt de rijkscrisisstructuur verder vorm. Het benoemen van de primaire aandachtsgebieden van de crisis op vrijdag 2 september ('continuïteit', 'security' en 'vertrouwen') resulteert in een praktische werkwijze waarbij de aandachtsgebieden 'continuïteit' (en inhoud) en 'security' worden verdeeld en gecoördineerd door de dgOBR respectievelijk de NCTV. De directeur Nationale Veiligheid bewaakt hierin het totaalbeeld van de beide aandachtsgebieden. Gezamenlijk met het hoofd NCC vormt dit driemanschap het 'operationeel team (OT)', dat het hart van de crisisorganisatie vormt.

Op zaterdagochtend om 10:00 uur komt het Adviesteam voor de eerste keer bijeen op het NCC. Het Adviesteam stelt zich op de hoogte van de stand van zaken en gaat aan de slag met het opstellen van omgevingsanalyses en het maken van scenario's. In de loop van de zaterdag komt het Adviesteam verschillende keren bij elkaar. Daarbij worden afspraken gemaakt hoe de Crisis Beleidsadviseurs (CBA's) de eigen departementen informeren en hoe zij de activiteiten tussen de departementen en het NCC afstemmen.

Het ontwikkelen van scenario's door het Adviesteam stuit op problemen. Het blijkt dat de CBA's in het Adviesteam onvoldoende inzicht hebben in de (ingewikkelde) materie met betrekking tot de mogelijke gevolgen van de gecompromitteerde certificaten. Het is voor het Adviesteam niet mogelijk om de gevolgen te overzien en deze te verwerken in scenario's. Voor het Adviesteam is het een nadeel dat de informatie (bijvoorbeeld welke organisaties van de gecompromitteerde certificaten gebruik maken) gefragmenteerd binnenkomt, hierdoor verandert het zicht op de problematiek frequent.

De CIO-rijk is op vrijdag 2 september door de dgOBR op de hoogte gebracht van de problemen met de certificaten bij DigiNotar. De CIO-rijk wordt op zaterdagochtend door de dgOBR verzocht het netwerk van CIO's te activeren en hen te betrekken bij het organiseren van het herstel van de continuïteit van het elektronische berichtenverkeer en het beperken van de schade die ontstaan is door de gecompromitteerde certificaten van DigiNotar. Dit gebeurt omstreeks 11:00 uur.

Het OT werkt de ingezette strategie (het organiseren van de overgang van DigiNotar naar andere certificatenverstrekkers) op zaterdagochtend nader uit. Men besluit de transitie van DigiNotar naar andere certificeerders niet centraal, maar door de betrokken organisaties zelf te laten regelen. Dit doet men omdat het organiseren van het transitietraject – gezien de hoeveelheid certificaten en de diversiteit van de betrokken organisaties – tot een enorme bureaucratie zou leiden. Daarnaast wil het OT zich niet mengen in een mogelijke discussie welke organisaties bij de overgang van DigiNotar naar andere certificeerders voorrang moeten hebben. Zij spreken af dat Logius bij de 'beheerste overgang' naar andere certificeerders monitort of er geen bottlenecks ontstaan (omdat iedereen massaal weggaat bij DigiNotar) en dat alle betrokken organisaties terecht kunnen bij andere certificeerders.

De ICCb bevestigt in haar overleg van zaterdagochtend (omstreeks 11:30 uur) de ingezette strategie. De ICCIO heeft hierbij een leidende rol. De dgOBR geeft aan dat het operationeel beheer om 10:00 uur die ochtend is overgenomen en dat de landsadvocaat bezig is met het organiseren van de volmacht. De ICCb bespreekt ook de te volgen lijn met betrekking tot publieksvoorlichting en besluit een lijst met vragen en antwoorden (Q&A's) te plaatsen op de site rijksoverheid.nl. Ook besluit de ICCb minister van BZK te adviseren tussen 15:00 uur en 16:00 uur met een nieuwe reactie over de DigiNotar-crisis naar buiten te treden. Tevens spreekt men af om op maandag 5 september de Tweede Kamer per brief te informeren over de DigiNotar-crisis. De ICCb geeft aan dat de uitwerking van scenario's door het Adviesteam noodzakelijk is. De scenario's moeten uiterlijk op zondagochtend (4 september) gereed zijn.

In de loop van de zaterdag is op het NCC tussen betrokkenen van de departementen overleg. Het is hun duidelijk dat bij de rijkscrisisstructuur ook andere bestuurslagen moeten worden betrokken, zoals de gemeenten, de provincies en ook private partijen zoals het VNO-NCW. Vooral het netwerk van de CIO's wordt hiervoor gebruikt. Men bereikt vlot vrijwel alle betrokken partijen, ondanks dat het weekend is. De communicatie naar de andere bestuurslagen neemt men actief ter hand. Per brief[17] worden de voorzitters van de veiligheidsregio's, de burgemeesters en de commissarissen van de Koningin op de hoogte gebracht van de stand van zaken met betrekking tot DigiNotar en de genomen besluiten en ingezette acties.

Ondanks dat in een korte tijd veel personen van diverse organisaties voor overleg bij de verschillende onderdelen van de crisisstructuur aanschuiven, levert dit geen grote problemen op.

[17] Brief van de minister van Veiligheid en Justitie, 3 september 2011, betreffende 'Vertrouwen in DigiNotar certificaten door Rijksoverheid opgezegd'.

Daarbij is het een voordeel dat het NCC zowel inhoudelijk als praktisch de diverse (bestuurlijke) overleggen binnen de crisisstructuur ondersteunt, bijvoorbeeld door het voeren (of het organiseren) van secretariaten. Hierdoor kunnen betrokkenen direct goed aan de slag en blijkt men in staat – ook als diverse overlegstructuren naast elkaar bestaan en circa honderd personen aanwezig zijn – de werkzaamheden in goede banen te leiden.

3.5 Zondag 4 september 2011

Het uitrollen van de strategie

Op zondag 4 september werkt men verder aan de overgang naar andere certificeerders conform de uitgezette strategie. Daarbij heeft de ICCIO samen met Logius een leidende rol. Ook is een belangrijk aspect om een volledig beeld te krijgen van alle diensten[18] van DigiNotar, waarbij de vraag is of en in hoeverre deze diensten nog veilig zijn.

Naast het herstellen van de continuïteit, blijven ook het 'herstellen van de het vertrouwen' en het 'security-vraagstuk' belangrijke uitgangspunten bij het organiseren en uitzetten van de activiteiten.

Communicatie naar de diverse doelgroepen (o.a. de bancaire sector) over de stand van zaken en ingezette activiteiten blijft aandacht vragen. Het mediabeeld wordt permanent gemonitord door het NVC en blijkt 'vrij rustig'. Het NVC constateert dat de DigiNotar-crisis in de landelijke pers niet veel stof doet opwaaien. Wel constateert men dat op de zogeheten 'expertwebsites' steeds meer technische vragen komen.

Het 'security-vraagstuk' krijgt meer nadruk als blijkt dat ook in andere domeinen sporen op servers zijn achtergelaten van de 'hack'. Bij nadere bestudering van het Fox-IT rapport blijkt dat de hacker waarschijnlijk dezelfde (persoon) is als de zogeheten 'Comodo-hacker' die in maart 2011 heeft ingebroken bij Comodo (een ander certificeringsbedrijf). De Fox-IT onderzoekers schrijven in hun onderzoek te vermoeden dat er een link tussen de twee inbraken bestaat, omdat in een script een 'fingerprint'[19] is aangetroffen die bij beide hacks hetzelfde blijkt. Bij de aanval op Comodo zijn, net als bij DigiNotar, valse certificaten gegenereerd. De vraag die dit oproept is of er ook bij andere certificatenverstrekkers is ingebroken. Het is daarom belangrijk dat dit vlot wordt uitgezocht, omdat anders mogelijk nieuwe onrust ontstaat. Daarbij worden de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), het Korps landelijke politiediensten (KLPD) en Govcert ingeschakeld.

[18] Naast certificaten leverde DigiNotar ook diensten, veelal gebaseerd op versleuteling en/of certificaten. Voorbeelden van DigiNotar diensten zijn: 'privacy services' (bijvoorbeeld anonimisering en pseudonimisering) en 'Authenticatie diensten' (bijvoorbeeld Eazy ID, authenticatie met behulp van mobiele telefoon).

[19] Een 'fingerprint' is een spoor (bijvoorbeeld door een gebruikte methodiek/techniek) dat de hacker achterlaat in een systeem waarin hij inbreekt waardoor het mogelijk is hem bij een nieuwe inbraak te identificeren als dezelfde hacker.

Mede door de onduidelijkheid over welke certificaten zijn gecompromitteerd, overwegen de grote browserleveranciers, waaronder Microsoft, het vertrouwen op te zeggen in álle DigiNotar certificaten, inclusief in de PKI-overheidscertificaten. Het voornemen van Microsoft is om op 'patch-Tuesday'[20] een update uit te brengen die de DigiNotar certificaten blokkeert op Windows systemen. Door het toepassen van deze update worden de door DigiNotar uitgegeven certificaten door de webbrowsers niet meer vertrouwd. Het gevolg hiervan is dat mogelijk alle communicatie die gebruik maakt van DigiNotar-certificaten wordt onderbroken. De gevolgen hiervan zijn in potentie bijzonder groot. Bijvoorbeeld voor de financiële wereld, omdat hierdoor mogelijkerwijs normaal betalingsverkeer niet meer mogelijk is. In de ICCb van zondagmiddag 16:00 uur geeft men aan dat het van belang is om deze update enige tijd uit te stellen om zo de maatschappelijke impact te minimaliseren en tijd te winnen voor het transitietraject naar nieuwe certificeerders.

In de ICCb verwoordt men het probleem dat hier speelt als volgt:

'Vraagpunt is hierbij in hoeverre je via de vertrouwenslijn het vertrouwen in DigiNotar-certificaten overeind houdt en in hoeverre je bij Microsoft uitstel kunt krijgen voor een revoke'[21].

'Als je zegt 'het is veilig' en Microsoft doet een revoke, dan schaad je vertrouwen. Als je zegt 'het is niet veilig' veroorzaak je wellicht zelf schade'.

Belangrijk aspect is om het vertrouwen van de financiële sector te behouden. Als deze wegvalt heeft dit grote gevolgen; maar:

'Als je doorgaat met business as usual, wie neemt dan de verantwoordelijkheid als het achteraf toch niet veilig bleek te zijn?'.

De ICCb besluit met Microsoft over een mogelijke uitstel van de update in gesprek te gaan. Daarbij hebben de CIO-Rijk en Govcert het voortouw. Men spreekt in de ICCb af de nieuwe feiten aan de MCCb voor te leggen, waarbij men aan de MCCb tevens de vraag voorlegt op welke wijze over de voorgenomen update extern moet worden gecommuniceerd.

Als de MCCb om 18:00 uur bijeenkomt is de voorgenomen update van Microsoft het voornaamste onderwerp van gesprek. In dit overleg spreekt men af dat de gekozen strategie van gefaseerde overgang gehandhaafd blijft. De MCCb geeft aan dat een nieuw worst case scenario (alle diensten van DigiNotar zijn gecompromitteerd/hacks bij meerdere leveranciers) moet worden ontwikkeld waarbij gekeken moet worden of de gevolgde lijn houdbaar is.

[20] Patch Tuesday is de tweede dinsdag van de maand, waarop Microsoft de maandelijkse beveiligingsupdates voor de Windowssystemen en andere Microsoft-producten uitgeeft, via Windows Update.

[21] Het laten vervallen of ongeldig verklaren van een certificaat.

Ook stelt de MCCb dat het van groot belang is dat Microsoft de update uitstelt. Communicatie over de voorgenomen update is onverstandig zolang de gesprekken met Microsoft nog gaande zijn. Het voornemen is om op maandag (5 september) de Tweede Kamer te informeren over de stand van zaken.

In het OT bespreekt men om 22:00 uur de te volgen koers met betrekking tot Microsoft. Tevens bespreekt het OT de wijze van communiceren naar het publiek en de communicatie richting (specifieke) sectoren. Govcert informeert bijvoorbeeld door middel van factsheets de (internationale) ICT-sector. Het NVC blijft – zo spreekt het OT af – de spin in het web bij alle vormen van communicatie naar de verschillende doelgroepen.

Als de ICCb bijeenkomt om 01:00 uur in de nacht van zondag op maandag (4 op 5 september) is nog geen duidelijkheid over het voornemen van Microsoft om de 'patch' uit te stellen.

'Microsoft kan nog geen uitsluitsel geven of ze dinsdag een patch zullen doen.'

In de ICCb blijkt dat Microsoft 'worstelt' met het al dan niet uitvoeren van de update en eigenlijk de patch wél wil uitvoeren. Daarbij is een overweging van Microsoft dat zij beducht is voor een achterstand ten opzichte van andere partijen (die wel een update uitvoeren) waarmee de vertrouwenspositie van Microsoft in gevaar komt. Op maandagochtend (5 september) zal Microsoft over de 'patch' een besluit nemen.

In de ICCb bespreekt men tevens de impact van het mogelijk opzeggen van het vertrouwen van de PKI-overheidscertificaten door Microsoft. Bij de CIO's is de vraag uitgezet in welke sectoren van de samenleving de meeste problemen zijn te verwachten. De CIO's benoemen vijf probleemgebieden. Dit zijn:

- financieel-fiscale problemen (betalingsverkeer);
- problemen in de rechtsorde keten (m.b.t. deurwaarders, dagvaardingen, processen verbaal);
- problemen in de sector openbaar bestuur (GBA-raadpleging en problemen met DigiD);
- problemen in de sociaal economische sector (arbeidsbureaus, UWV, DUO);
- veiligheidsproblemen (politie).

In de ICCb komt het aspect 'communicatie' uitgebreid aan de orde. De communicatie met de diverse sectoren verloopt via de CIO's. Het NVC ontwikkelt hiervoor een specifieke boodschap. Govcert communiceert met het zogeheten 'expert-circuit'. Door VNO-NCW en het Ministerie van Financiën is overleg gevoerd met een representatieve groep van bedrijven en koepelorganisaties van het bedrijfsleven over de mogelijke gevolgen van de update door Microsoft.

3.6 Maandag 5 september 2011

Het in kaart brengen, analyseren en beoordelen van de knelpunten
Maandagochtend 5 september omstreeks 08:00 uur geeft Microsoft aan af te zien van de geautomatiseerde update op dinsdag 6 september. Deze update stelt Microsoft een week uit. Concreet betekent dit, dat Microsoft de 'patch' niet als 'verplicht' aanbiedt aan haar gebruikers maar als 'optioneel'. De gebruiker moet dus zelf bewust kiezen om de update te installeren.

Het uitstel van de geautomatiseerde update geeft organisaties meer tijd om de certificaten van DigiNotar te vervangen. Hierdoor voorkomt men dat, door een abrupte beëindiging van de mogelijkheid om van DigiNotar-certificaten gebruik te maken, het communicatieverkeer tussen machines onderling ('server-to-server') wordt verstoord. Hierdoor zouden websites en onderliggende systemen moeilijker of in het geheel niet meer bereikbaar zijn.

In de ICCIO die deze maandagochtend omstreeks 09:00 uur plaatsvindt, staat het in kaart brengen van de processen die geraakt worden en waar de problemen zich voordoen centraal. Ook de informatie van DigiNotar (lijst met certificaten) wordt verder geanalyseerd. Men bespreekt de afspraken die zijn gemaakt in de ICCb en de MCCb. Dit zijn ten eerste de afspraken met betrekking tot de mogelijke schade die wordt geleden door bedrijven. Ten tweede de sectorspecifieke afspraken ten aanzien van de 'coulance' richting burgers en bedrijven indien zij, door het ontbreken van een veilige internetverbinding, niet in staat zijn op tijd hun gegevens aan te leveren. Men besluit de landsadvocaat een voorstel te laten opstellen over eventuele aansprakelijkheidsverdeling bij geleden schade. Punt van aandacht is de communicatie naar de specifieke sectoren en mede-overheden. Een voorbeeld is een bestuurlijke brief vanuit het NCC voor de gemeenten waarin ook technische informatie staat hoe de overgang naar nieuwe certificaten plaats kan vinden.

In het overleg van het Adviesteam dat deze maandagochtend om 10:00 uur plaatsvindt, staat vooral informatie-uitwisseling centraal over de stand van zaken met betrekking tot de DigiNotar-crisis en de uitgezette acties. Men bespreekt hoe men informatie van- en naar de departementen moet organiseren (bijvoorbeeld het doorsturen van verslagen van de ICCIO-, de ICCb- en de MCCb-overleggen aan de DCC's, en het 'voeden' van het OT met de actuele stand van zaken binnen de eigen departementen).

In het overleg van het OT van 10:00 uur bespreekt men wat de 'toon en strekking' moet zijn van de brief die deze maandag naar de Tweede Kamer wordt gestuurd. Deze brief zal later op de maandag omstreeks 15:00 uur in de ICCb worden besproken.

Het OT bespreekt in dit overleg de activiteiten die op dat moment zijn uitgezet via 'twee sporen', dat zijn:

- Het in kaart brengen (via de CIO's) door de departementen van de problemen binnen de eigen sectoren (op basis waarvan prognoses over ontwikkelingen kunnen worden opgesteld).
- Het analyseren van de lijst met certificaten van DigiNotar (via de CIO's), waardoor (na analyse) een beeld ontwikkeld kan worden welke instanties betrokken zijn en welke processen daar spelen.

Daarnaast komen in dit overleg ook aspecten als 'aansprakelijkheid' en 'de communicatie naar de mede-overheden' ter sprake. In het OT besluit men een overleg in te plannen met de vier grote gemeenten (G4), de Vereniging Nederlandse Gemeenten (VNG), het Interprovinciaal Overleg (IPO) en de Unie van Waterschappen.

Om 14:00 uur komt het OT wederom bijeen. Bespreekpunt is onder meer het gezamenlijke persbericht dat met Microsoft wordt voorbereid. Ook de tekst die men opneemt bij de update is onderwerp van gesprek. De tekst vraagt om (zeer) nauwkeurige juridische bestudering in verband met mogelijke aansprakelijkheid en claims indien de tekst niet 'waterdicht' is.

Daarnaast vragen een aantal andere processen om aandacht. Zoals het hanteerbaar maken van de gedetailleerde informatie van de CIO's en het vervolgens benoemen van de meest kwetsbare sectoren en processen. Ook de communicatie vanuit de Rijksoverheid en de communicatie naar specifieke sectoren bespreekt men in het OT. Als uit de analyses van de ICCIO duidelijk is welke sectoren en processen kwetsbaar zijn, worden, op basis van deze informatie, deze specifieke sectoren (bijvoorbeeld ziekenhuizen) per brief geïnformeerd.

In het overleg van de ICCb dat omstreeks 16:00 uur plaatsvindt bespreekt men de uitgestelde automatische update van Microsoft. In de ochtend van dinsdag 6 september zal Microsoft de updates voor Nederland klaarzetten, maar niet automatisch uitvoeren. Nederland heeft bedongen een extra boodschap bij de update te plaatsen. Deze luidt:

'Update staat nu klaar, als u geen gebruik maakt van DigiNotar certificaten, kunt u gewoon de update installeren. Indien u wel gebruik maakt van DigiNotar certificaten, dan kunt u ervoor kiezen deze update niet te installeren.'

Tevens is de communicatie met medeoverheden, en meer in het bijzonder de gemeenten, een punt van aandacht. Zij blijken niet altijd te weten wat ze moeten doen. Ook in andere sectoren bestaat op enkele punten onduidelijkheid over de te volgen koers. Afgesproken wordt dat men inventariseert wat de problemen zijn met de gemeenten. Daarnaast verstuurt het NCC een bestuurlijke brief aan het einde van deze maandag naar de decentrale overheden.

Bij de bankensector zijn geen problemen gesignaleerd. In de fiscale sector verwacht men wel problemen. Hierover vindt met de VNO-NCW overleg plaats. Ook elders signaleert men problemen, zoals bij de digitale afgifte van exportproducten door de Kamer van Koophandel en bij de Rijksdienst voor het Wegverkeer, die geen contact krijgt met postkantoren.
De problemen die eventueel ontstaan bij de overgang naar andere certificaten monitort men permanent. Bij het wisselen van certificaten zal – zo is de afspraak – indien dit noodzakelijk is een prioriteitstelling moeten plaatsvinden op basis van een maatschappelijke afweging door de MCCb.

Het bespreken en aanpassen van de (concept) brief aan de Tweede Kamer neemt veel tijd in beslag. Het is duidelijk dat het lastige materie betreft waar de schrijversgroep niet helemaal vat op heeft. Na de nodige aanpassingen zal de brief aan de MCCb worden voorgelegd. De ICCb spreekt af dat tot nader orde – tenzij dit noodzakelijk blijkt te zijn – de ICCb en de MCCb geen nieuwe overleggen plannen. Het OT zal vooralsnog de regie van de activiteiten op zich nemen.

In de MCCb die omstreeks 16:30 uur start bespreekt men de brief aan de Tweede Kamer. Eveneens omarmt men de gekozen koers met betrekking tot de Microsoft-update.

In het OT-overleg van maandagavond om 19:15 uur komt het persbericht dat gezamenlijk met Microsoft zou worden uitgebracht ter sprake. Microsoft heeft alsnog bezwaren geuit tegen het aanvankelijke voornemen om met een gezamenlijk persbericht naar buiten te treden. De overweging van Microsoft is dat de schijn kan ontstaan dat Microsoft zich (op veiligheidsgebied) laat leiden door een derde partij (de Nederlandse Staat). Er worden gescheiden persberichten voorbereid. De tekst die meegaat met de 'patch' is een aspect waarover Microsoft, Govcert en de landsadvocaat in gesprek zijn.

Op maandagavond – omstreeks 21:00 uur – informeert het Kabinet namens de ministers van BZK en van VenJ de Tweede Kamer met een brief[22] over de DigiNotar-crisis. In deze brief zet het Kabinet de feiten uiteen die hebben geleid tot deze crisis. Men geeft aan wat de gevolgen zijn van de 'valse certificaten' voor het digitale communicatieverkeer en de invloed daarvan op overheid, bedrijven en burgers. Tevens geeft het Kabinet in deze brief aan wat de besluiten en acties zijn om de crisis te bestrijden.

Op maandagavond, 21:30 uur, geeft de minister van BZK een tweede persconferentie.
In deze persconferentie zet de minister gedetailleerd uiteen wat de stand van zaken is met betrekking tot de DigiNotar-crisis. De minister gaat daarbij onder andere in op het ontstaan van de crisis en de maatregelen die zijn genomen om de ontstane situatie (zo snel mogelijk) te beheersen.

[22] Brief 5 september 2011, betreffend 'digitale inbraak DigiNotar'.

Ook informeert het Kabinet op maandagavond de bestuurlijke partners (gemeenten, VNG, IPO etc.) door middel van een tweede (bestuurlijke) brief. In deze brief geeft het Kabinet onder andere aan welke stappen zij moeten nemen indien zij getroffen zijn door gecompromitteerde certificaten van DigiNotar ('handelingsperspectief').

3.7 Dinsdag 6 september 2011

Het voortzetten van de strategie en inspelen op nieuwe ontwikkelingen

Via de website pastebin.com laat de hacker via een 'posting'[23] weten dat hij nog vier andere 'Certificate Authorities' (zoals DigiNotar) gehackt heeft. Dit vereist extra onderzoek waarbij onder andere Govcert, de AIVD, het KLPD en het OM zijn betrokken. Om het OT met deze nieuwe feiten en het onderzoek naar de achtergronden en motieven van de hacker niet extra te belasten, splitst men het OT in een OT-Veiligheid (OT-V) en een OT-Continuïteit (OT-C). Het OT-V wordt belast met het onderzoek naar de hacker. Het OT-C is primair verantwoordelijk voor de bestrijding van de crisis langs de uitgezette lijnen.

In het overleg van het Adviesteam dat op dinsdagochtend om 10:00 start passeren de uitgezette activiteiten (o.a. de bestuurlijke brief) de revue. Het Adviesteam stelt zich op de hoogte van de verschillende activiteiten en bespreekt hoe deze binnen de departementen kunnen worden uitgezet en gecommuniceerd.

Het OT-C komt dinsdagmiddag om 12:30 uur bijeen. Of de hacker inderdaad bij meerdere certficaatverstrekkers heeft ingebroken en welke gevolgen dit voor de continuïteit heeft, is op dat moment niet bekend. Het lijkt er op dat men de crisis in de hand heeft, in die zin dat men inzicht heeft in de problemen die er spelen en de beheerste overgang van DigiNotar naar andere certificeerders in volle gang is en goed werkt. Er is dan ook geen reden om wat betreft het aspect 'continuïteit' een andere koers te varen. Communicatie naar de verschillende doelgroepen blijft een punt van aandacht, omdat er veel vragen over de DigiNotar-crisis binnenkomen. Dit betreffen zowel vragen vanuit de samenleving (bijvoorbeeld over DigiD) als ook technische detailvragen met betrekking tot de migratie en de update van Microsoft. Het NVC coördineert alle acties met betrekking tot de communicatie.

Ook de ICCIO dat omstreeks 14:00 uur plaatsvindt, bevestigt het beeld van het eerdere overleg van het OT-C dat de problematiek bij de ketens steeds inzichtelijker wordt. Dat neemt niet weg dat er zowel bij mede-overheden als het bedrijfsleven veel vragen leven over het aanvragen van certificaten. Het coördineren hiervan vraagt om permanente afstemming tussen direct betrokkenen (de ICCIO, Logius, het OT-C, het NCC en de certificaatverstrekkers) en gerichte communicatie naar bedrijfsleven en mede-overheden.

In een teleconferentie tussen de leden van de CSR op dinsdagmiddag bespreekt men de DigiNotar-crisis. Over het algemeen zijn de leden van mening dat de aanpak van de crisis

[23] Een vermelding in een blog of internet forum zonder een schermnaam of - meer algemeen - met behulp van een niet-identificeerbare pseudoniem.

goed verloopt. Een van de leden stelt bijvoorbeeld dat er goed is geacteerd en gecommuniceerd vanuit de crisisorganisatie. Wel adviseert de raad om na te denken over scenario's met het oog op een mogelijke internationale verbreding van het probleem.

In de middag van 6 september laat het Kabinet via de website rijksoverheid.nl weten dat DigiD weer veilig kan worden gebruikt. Het bericht luidt:

'Zoals bekend gemaakt is de overheid bezig de veiligheid van DigiD weer te garanderen door het vervangen van zogenoemde beveiligingscertificaten. Hierdoor worden mogelijke gevolgen van de Diginotar-problematiek opgelost. Op dit moment zijn vervanging en testen zodanig gevorderd dat DigiD weer veilig kan worden gebruikt door mensen die al een DigiD hebben'.

Op dinsdagavond om 19:00 uur voert Microsoft de software-update voor Nederland uit zoals met de Nederlandse overheid is afgesproken. Dat betekent dat Microsoft de update niet automatisch installeert, maar dat de gebruiker hiervoor bewust moet kiezen (optioneel).

3.8 Woensdag 7 september 2011

Herstellen van vertrouwen; gerichte communicatie en vervangen certificaten
In de ochtend van woensdag 7 september publiceert Govcert omstreeks 10:00 uur het nieuwsbericht op verschillende sites over de update van Microsoft. Onder de kop 'Microsoft update blokkeert DigiNotar certificaten' wordt bericht over de update van Microsoft. Het bericht luidt:

'Microsoft heeft een update uitgebracht die de DigiNotar certificaten blokkeert in Windows. De update wordt voor Windows-installaties in Nederland niet verplicht, maar als optioneel aangeboden. Door het toepassen van de update worden de malafide, door DigiNotar uitgegeven certificaten niet meer vertrouwd. Hierdoor kan communicatie die gebruik maakt van DigiNotar certificaten onderbroken worden.'

In het OT-C dat woensdagmiddag om 12:30 uur start, blijkt dat de 'patch' van Microsoft, op een aantal uitzonderingen na, goed is verlopen. Logius inventariseert welke sites zijn 'plat gegaan'.

Ook de overgang van DigiNotar naar andere certificeerders verloopt in principe goed. De certificeerders houden zich aan de gemaakte afspraken. Men prioriteert niet, maar handelt volgens het ''first come, first serve' principe. Uit het verslag van de OT-C blijkt dat er regelmatig overleg plaatsvindt tussen rijksvertegenwoordigers, gemeenten, provincies en (o.a.) VNO-NCW. Men merkt daarbij op dat: 'de ketens elkaar goed weten te vinden'.

De hacker heeft – zo is inmiddels bekend – ook digitaal ingebroken bij het bedrijf 'Globalsign'. Hoewel dit wel mogelijk gevolgen heeft; 'gevolgen kunnen mondiaal groot zijn', zijn de gevolgen voor Nederland beperkt. In Nederland werkt men weinig met de certificaten van Globalsign;

'Er is geen aanleiding voor het OT-C om aan te nemen dat de door de Rijksoverheid aangewezen certificeerders onveilig zijn.'

Ook in de ICCIO om 14:00 uur bespreekt men de update van Microsoft. Met name bij de gemeente Amsterdam zijn er problemen. Of dit aan gebruikers ligt (die de 'patch' handmatig hebben doorgevoerd) of aan de gemeente onderzoekt men nader. In de ICCIO wordt bekend dat de 'hack' bij het bedrijf Globalsign geen effecten heeft op Nederland. Het bedrijf heeft per onmiddellijk de uitgifte van certificaten gestaakt en is in Nederland niet actief.

De ICCIO bespreekt uitvoerig de afspraken die er met de andere certificeerders zijn gemaakt met betrekking tot het uitgifteproces van certificaten. Daarbij staan aspecten als 'de doorlooptijden', 'de aanvraagprocedures van certificaten', 'het prioriteren van aanvragen' en 'het in kaart brengen van knelpunten' centraal. De voorzitter geeft aan dat: 'de feiten in kaart gebracht worden door Logius en dit overzicht (in de ICCIO) wordt gedeeld'.

Een belangrijk onderwerp in de ICCIO is de update die Microsoft op 13 september zal uitvoeren. In tegenstelling tot de handmatige update van dinsdag 6 september zal Microsoft deze update geautomatiseerd uitvoeren. Dit is dus een geheel andere (omgekeerde) situatie; bij deze update moeten gebruikers bewust actie ondernemen om de 'patch' niet door te voeren. Het is daarom van belang dat men in kaart brengt welke gebruikers de DigiNotar certificaten nog niet hebben vervangen en waar zich problemen kunnen voordoen. De ICCIO spreekt af dat de leden een overzicht opstellen ('top 5, dan wel top 10') van de sectoren waar de meeste problemen zijn te verwachten. Tevens moeten de leden inzicht geven in de planning van het vervangen van de DigiNotar-certificaten.

In de loop van woensdag communiceert de rijkscrisisorganisatie verschillende berichten over de DigiNotar-crisis, de update door Microsoft en de technische gevolgen daarvan richting publiek, bedrijfsleven en mede-overheden. Zo plaatst Govcert om 16:00 uur een achtergrondartikel voor burgers en het midden- en klein bedrijf onder de kop 'wat voor gevolgen hebben valse certificaten voor mij?' op de website 'waarschuwingsdienst.nl'.[24] Ook publiceert Govcert op hun website een factsheet over 'DigiNotar certificaten en machine-to-machine (M2M) communicatie' en de stappen die men kan doorlopen om de impact op die communicatie te beperken. Via het publieksinformatienummer 0800-1351 en de website 'rijksoverheid.nl' verschaft de rijkscrisisorganisatie permanent actuele informatie over de gevolgen van de DigiNotar-crisis en de wijze waarop burgers op mogelijke problemen kunnen anticiperen.

[24] De website 'waarschuwingsdienst.nl' geeft adviezen en actuele informatie over computer- en internetgebruik. De website wijst om mogelijke bedreigingen en bescherming daartegen. Waarschuwingsdienst.nl is een dienst van Govcert.nl.

3.9 Donderdag 8 september 2011 tot en met woensdag 14 september 2011

De afwikkeling van de DigiNotar-crisis

De activiteiten vanaf donderdag 8 september tot en met woensdag 14 september staan vooral in het teken van de afwikkeling van de DigiNotar-crisis. De eerder genomen besluiten en uitgezette acties krijgen in deze dagen een vervolg. Er komt steeds meer inzicht in het verloop van de crisisbestrijding en de knelpunten daarbij. Onduidelijkheden zoals welke organisaties nog gebruik maken van DigiNotar-certificaten, welke sectoren mogelijk risico's lopen en hoe de overgang van DigiNotar-certificaten naar de certificaten van andere certificeerders verloopt, brengt men stelselmatig in beeld.

Het OT-C, de ICCIO en Logius hebben zeer frequent overleg met alle betrokkenen partijen over de voortgang van de transitie van de DigiNotar-certificaten naar de andere certificeerders. Hoewel blijkt dat het omwisselen van de certificaten niet bij alle certificeerders even soepel verloopt, heeft men een goed beeld van de knelpunten en onderneemt men hierop actie. Vragen als 'hoeveel certificaten zijn uitgegeven?' en 'wat is de gemiddelde doorlooptijd bij de overgang van de certificaten?' zijn in de overleggen van het OT-C – bijvoorbeeld op donderdag 8 en vrijdag 9 september - terugkerende onderwerpen.

Bij een aantal gemeenten dreigen problemen te ontstaan omdat deze de ICT niet op orde hebben en problemen ondervinden met hun websites. In het OT-C van donderdag 8 september besluit men daarom – in samenwerking met de VNG – zeven teams van specialisten op het terrein van ICT-infrastructuur en certificaten én met kennis op het bestuurlijk vlak samen te stellen. Deze 'vliegende brigades' moeten gemeenten bij de vervanging van certificaten bijstaan. Ook bij de advocatuur dreigen problemen te ontstaan omdat deze sector nog zeer veel (circa 13.000) certificaten moet omzetten. Het OT-C, de ICCIO en Logius inventariseren de problemen bij deze sector en bieden waar mogelijk ondersteuning aan. Over het algemeen (zo blijkt uit het verslag van de ICCIO van vrijdag 9 september) krijgt men steeds meer grip op de problemen.

Bij de communicatie met mede-overheden, bedrijfsleven – en daarbinnen met de afzonderlijke sectoren – en de 'thuisgebruikers' staat vanaf donderdag 8 september vooral de geplande geautomatiseerde update van Microsoft (op dinsdag 13 september) centraal. Via vooraankondigingen, factsheets en via publieksinformatie communiceert men met de verschillende doelgroepen. Niet alleen nationaal, maar ook internationaal wordt over de DigiNotar-crisis en de ondernomen activiteiten gecommuniceerd. Zo informeert Govcert via de CERT[25] -kanalen haar buitenlandse collega-organisaties over de ontwikkelingen.

[25] CERT: computer emergency response teams. Zie ook noot 9.

Ook via het International Watch and Warning Network[26] (IWWN) wisselt Govcert informatie uit over de effecten van een gecompromitteerde Certificate Authority zoals DigiNotar en hoe men om moet gaan met mogelijke problemen. Daarnaast monitort Govcert de (gevolgen van) updates van andere browsers dan die van Microsoft zoals Mozilla Firefox, Linux en Google Chrome.

In de dagen vanaf donderdag 8 september blijft het mediabeeld vrij rustig. In het OT-V geeft men aan:

'Zowel in de Nederlandse als buitenlandse kranten is weinig nieuws te vinden met betrekking tot het DigiNotar incident.'

In het OT-V van vrijdag 9 september richt men zich vooral op de mogelijke andere digitale inbraken van de 'hacker' die hij geclaimd heeft, zoals bij 'GlobalSign'. Vooralsnog zijn de effecten voor Nederland gering. De motieven en achtergronden van de hacker zijn onderwerp van uitgebreid onderzoek door onder andere de AIVD en het KLPD en vraagt veel capaciteit. Ook het onderzoek naar de (veiligheid van) andere certificaatverstrekkers is blijvend onderdeel van het onderzoek door de leden van het OT-V.

Op maandag 12 september komen om 08:00 uur het KLPD, het OM, Govcert en Fox-IT bijeen om de voortgang van hun onderzoeken te bespreken. Deze maandag staat grotendeels in het teken van de vooraankondiging naar verschillende partijen over de update van Microsoft op dinsdag 13 september. De verwachting is – zo blijkt uit de overleggen van het OT-V en het OT-C – dat de meest kritieke ketens (waaronder de vier grootste gemeenten) bijna op orde zijn voor wat betreft de overgang naar andere certificaten. Dit laat onverlet dat er nog steeds een aanzienlijk aantal (circa 29%) van de (kleinere) gemeenten de zaken nog niet op orde heeft.

In de ICCb van dinsdagmiddag 13 september om 12:30 uur spreekt men af om op woensdagmiddag (14 september) de balans op te maken van de update door Microsoft. Op dat moment kan men ook aangeven of het sein 'brand meester' kan worden gegeven. In de ICCb bespreekt men tevens de conference call met de CSR op dinsdagmiddag, waarbij men de raad vraagt om advies over het optreden op korte termijn als ook op langere termijn.

In het OT-V van woensdag 14 september om 10:00 uur komt onder andere de berichtgeving met betrekking tot de update van Microsoft ter sprake. Er zijn nagenoeg geen berichten over de gevolgen van de patch, op enkele lokale media na die berichten over problemen bij hun gemeenten. Wat betreft de hacker merkt men op dat deze niet meer actief is in de media (Twitter, Pastebin). Het OT-V spreekt af dat – 'tenzij de situatie dit noodzaakt' – er geen OT-V meer plaatsvindt. Men zal de ICCb en de MCCb adviseren om af te schalen.

[26] Het International Watch en Warning Network (IWWN) werd in 2004 opgericht om de internationale samenwerking op het gebied van de aanpak van computercriminaliteit, aanvallen en kwetsbaarheden te bevorderen. Het stelt de deelnemende landen in staat om informatie te delen, bewustzijn te creëren en de respons capaciteit te vergroten.

Ook in het OT-C komt op woensdag omstreeks 12:00 uur de Microsoft update ter sprake. Er komen een aantal knelpunten ter sprake maar:

'De duiding is dat heel beheerst wordt gemigreerd en gepatcht'.

In de ICCb van woensdag 14 september neemt de voorzitter (onder andere) de actuele stand van zaken door. De update van Microsoft is, op een aantal kleine problemen na, goed verlopen. Een aantal organisaties (waaronder de Belastingdienst) hebben de geautomatiseerde patch handmatig tegengehouden, waarmee 'tijd is gekocht' om rustig over te stappen naar andere certificaten. Wat betreft de hack bij GlobalSign vermeldt de ICCb dat er geen problemen zijn gesignaleerd voor Nederland en dat de hacker niets meer van zich heeft laten horen. Wat betreft de communicatie stelt de ICCb het Kabinet voor, de Tweede Kamer per brief te informeren. Tevens zal een persbericht worden uitgegeven over de stand van zaken. Daarbij is het belangrijk dat men aangeeft dat het probleem weliswaar (nog) niet over, maar wel beheersbaar is.

Wat betreft de voortgang van de rijkscrisisorganisatie besluit men de ICCb en de MCCb 'op een waakvlam' te zetten. Om de nafase gecoördineerd op te pakken zal een voorstel worden gedaan (door het ministerie van VenJ) waarbij het beleid, de onderzoeken die lopen en de openstaande continuïteitsvraagstukken worden meegenomen.

4

Analyse

Bij de crisisbeheersing gaat het uiteindelijk om de geleverde prestaties: is de crisis op adequate wijze aangepakt? Een vastgesteld toetsingskader voor de crisisbeheersing op nationaal niveau ontbreekt vooralsnog. 'Harde' normen voor de vaststelling of een crisis op nationaal niveau adequaat is bestreden zijn er niet.

In het concept Toetsingskader Crisisbeheersing[27] is een aantal kritische processen benoemd. Voor zover van toepassing zijn deze processen gebruikt als kader voor de analyse van de 'DigiNotar-crises'. Door de bevindingen uit hoofdstuk drie langs deze processen te analyseren, wordt een overzicht gegeven van de prestaties tijdens deze crisis. In dit analysehoofdstuk wordt per proces een omschrijving gegeven van de kenmerken, de doelen en de beoogde prestaties van het proces. Vervolgens wordt geanalyseerd hoe in de praktijk invulling is gegeven aan het betreffende proces. Naast deze kritische processen is in dit analysehoofdstuk ook gekeken of er tijdens de DigiNotar-crisis is gehandeld conform de (vastgestelde) plannen.

[27] Concept Toetsingskader Crisisbeheersing versie 0.8D

Door de beoogde prestaties te vergelijken met de feitelijke prestaties kan – ondanks het ontbreken van harde normen – een uitspraak worden gedaan over het functioneren van de rijkscrisisorganisatie tijdens de DigiNotar-crisis.

4.1 Praktijk en planvorming

Ter voorbereiding op een potentiële crisis worden afspraken vastgelegd in verschillende plannen. In hoofdstuk twee is beschreven welke plannen van toepassing zijn op de DigiNotar-crisis. In deze paragraaf wordt geanalyseerd op welke wijze de in de plannen vastgelegde structuren zijn gevolgd tijdens deze crisis. Het Nationaal Crisisplan ICT was ten tijde van de DigiNotar-crisis nog niet formeel vastgesteld, maar maakt wel onderdeel uit van de gebruikelijke structuur. Derhalve is dit plan wel meegenomen in deze analyse.

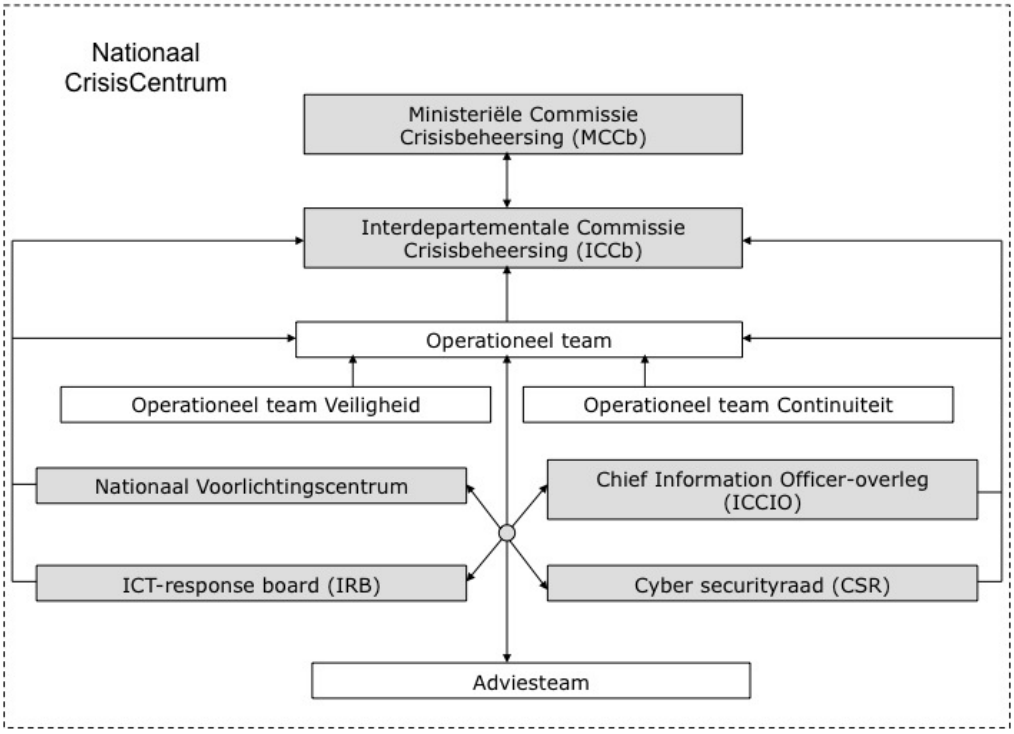
Tijdens de DigiNotar-crisis is de rijkscrisisstructuur opgeschaald. Zoals vastgelegd in het Nationaal Handboek Crisisbesluitvorming gebeurt dit langs de lijn van het MCCb, ICCb en het Adviesteam. Daarnaast is het NCC opgeschaald en is ook het NVC actief. Tevens zijn de crisisspecifieke gremia, zoals beschreven in het NCP-ICT, geactiveerd. Zo zijn er een ICT-Response Board, een CSR en de ICCIO actief.

Elk gremium heeft eigen taken en verantwoordelijkheden die zijn vastgelegd in bovengenoemde plannen. Uit de bevindingen blijkt dat deze taken en verantwoordelijkheden in de meeste gremia conform de planvorming zijn uitgevoerd; zo neemt de MCCb besluiten en informeert zij het Kabinet over deze besluiten en coördineert het NVC de communicatie naar zowel de burgers als de overige betrokkenen. De IRB en de CSR adviseren, volgens planvorming, bij het nemen van (strategische) besluiten.

Wel blijkt dat het Adviesteam moeite heeft met het vervullen van zijn rol zoals is vastgelegd in het Handboek Crisisbesluitvorming. Zo hebben de leden van het Adviesteam problemen met het ontwikkelen van scenario's. Door een gebrek aan specifieke ICT-kennis, waardoor zij onvoldoende inzicht hebben in de complexe materie, kan het Adviesteam de mogelijke gevolgen van gecompromitteerde certificaten niet in kaart brengen. Het Adviesteam functioneert tijdens de DigiNotar-crisis voornamelijk als schakel tussen de crisisorganisatie en de betrokken departementen en organisaties. De leden van het Adviesteam zorgen voor de terugkoppeling aan de eigen organisaties. Hiermee voorkomt men dat binnen de departementen ongecoördineerde activiteiten plaatsvinden, die niet zijn afgestemd met de rijkscrisisorganisatie.

Het OT neemt de rol van het Adviesteam voor een deel over. Het OT is niet vastgelegd in de planvorming, maar ontstaat tijdens deze crisis ad hoc. Tijdens de DigiNotar-crisis vormt het OT het 'hart van de crisisorganisatie'. Het OT houdt zich onder andere bezig met de uitwerking van de ingezette strategie.

Hoewel de taken van de ICCIO zich volgens het NCP-ICT beperken tot de continuïteit van de bedrijfsvoering, neemt de ICCIO ook een groot deel van de rol van het Adviesteam over. In de ICCIO is specifieke expertise aanwezig die bij het Adviesteam ontbreekt en worden scenario's en beelden ontwikkeld. Ook bij de overgang van DigiNotar naar andere certificeerders speelt de ICCIO een belangrijke rol.



Figuur 2. Een schematische weergave van de crisisstructuur tijdens de DigiNotar-crisis. De wit gekleurde organisatieonderdelen wijken af van de in de planvorming beschreven structuur. Zie figuur 1 voor de schematische weergave van de structuur volgens planvorming,

4.2 Het onderkennen en signaleren van de crisis

Dit proces heeft betrekking op het vroegtijdig onderkennen van een crisisdreiging en het tijdig informeren van relevante organisaties en sleutelfunctionarissen. Het doel van dit proces is het mogelijk maken van een zo snel mogelijke start van een adequate beheersing van de (dreigende) crisis. Anders dan bij een acute crisis moet men bij een crisis die geleidelijk tot stand komt, anticiperen op (indirecte) aanwijzingen voor een mogelijke crisis of meerdere omstandigheden die in combinatie tot een crisis kunnen leiden.

Vanaf het moment dat de eerste signalen van problemen met betrekking tot DigiNotar bij de Nederlandse overheid (Govcert) binnen komen, pakt men deze direct op. In tegenstelling tot een acute crisis bijvoorbeeld een grote brand, is in dit geval de aard van de dreiging niet direct duidelijk. De informatie over de ernst van de situatie wordt gefragmenteerd bekend. Men activeert, als op 2 september duidelijk wordt dat door de digitale inbraak bij DigiNotar mogelijk gecompromitteerde PKI-overheidscertificaten in omloop zijn, vrijwel direct de rijkscrisisstructuur. Op het moment dat men de crisisstructuur activeert, is er nog geen compleet beeld van de situatie. Er kan op dat moment niet worden uitgesloten dat er PKI-overheidscertificaten zijn gecompromitteerd, maar er kan ook niet worden bevestigd dat deze wèl zijn gecompromitteerd. Men gaat uit van een worst case scenario waarbij ook de PKI-overheidscertificaten zijn gecompromitteerd. Op basis van dit scenario bedenkt men een strategie en zet men acties uit. In lijn met de strategie waarbij herstel van het vertrouwen, de continuïteit en de veiligheid de primaire aandacht hebben, handelt men snel en proactief.

4.3 Het voorzien in informatie

Het proces 'voorzien in informatie' heeft betrekking op het verkrijgen van alle, voor de bestrijding van een (dreigende) crisis relevante informatie en het actief communiceren over deze informatie binnen de gehele crisisorganisatie. De juiste informatie moet op het juiste moment, in de juiste vorm, bij de juiste functionaris beschikbaar zijn. Het hoofddoel van dit proces is om alle betrokkenen in staat te stellen om op een adequate wijze hun werkzaamheden uit te voeren. Het is van belang dat de noodzakelijke gegevens zo snel mogelijk worden geregistreerd, verwerkt en verdeeld. De gegevens moeten zo snel mogelijk worden getoetst op consistentie, betrouwbaarheid en actualiteit. Wanneer dit is gebeurd moet de informatie worden verspreid onder de verschillende betrokkenen. Dit gebeurt zowel binnen de verschillende onderdelen als tussen de onderdelen van de rijkscrisisorganisatie. Ook tussen de verschillende niveaus (strategisch, tactisch en operationeel) moet de informatie worden gedeeld.

In het beginstadium van de DigiNotar-crisis is er sprake van veel en gefragmenteerde informatie over de mogelijke gevolgen van de hack. Al snel is er intensief overleg tussen Govcert, de NCTV de dgOBR, de directeur Nationale Veiligheid en het hoofd NCC. Hierdoor komt vlot de verschillende informatie bij elkaar en worden de eerste beelden gevormd over de situatie. Nadat op vrijdagmiddag 2 september de rijkscrisisstructuur is geactiveerd informeert men ook uitvoeringsorganisaties zoals de Belastingsdienst en het Kadaster.

De eerste dagen zijn de aard, omvang en de mogelijke gevolgen van de crisis nog niet duidelijk waardoor het beeld verschillende malen wijzigt. Men legt veel nadruk op het scherp krijgen van het beeld. Daarbij spelen de ICCIO en Govcert een belangrijke rol, bijvoorbeeld ten aanzien van de hoeveelheid certificaten van DigiNotar die nog in omloop zijn, de transitie naar andere certificeerders en het in kaart brengen van de mogelijk kwetsbare sectoren.

Ook het Adviesteam speelt hierbij, voor wat betreft de stand van zaken bij de departementen, een belangrijke rol. De verschillende onderdelen monitoren continu het beeld en houden deze actueel. Voor wat betreft de informatievoorziening binnen de crisisorganisatie heeft het NCC een faciliterende rol. Naast de bestuurlijke en operationele informatie is er binnen de crisisorganisatie ook behoefte aan ICT-specifieke kennis. De hiervoor benodigde informatie wordt verkregen via Govcert, Logius, de ICCIO en hun netwerken. In deze informatiebehoefte wordt goed voorzien.

Kenmerkend voor de informatievoorziening tijdens de DigiNotar-crisis zijn de korte lijnen tussen de verschillende deelnemers van de crisisorganisatie waarbij het OT een spilfunctie heeft. Dit draagt bij aan een soepele informatievoorziening en kent een praktische insteek (korte informele overleggen). Tevens heeft men oog voor het belang van de informatievoorziening naar de organisaties die niet direct tot de rijkscrisisstructuur behoren, zoals gemeenten, provincies en private partijen zoals VNO-NCW. De crisisorganisatie maakt tevens gebruik van de informatie van deze partijen om het eigen beeld scherp te krijgen.

Door de korte lijnen tussen de MCCb, de ICCb, het OT en de ICCIO is er sprake van een vlotte informatievoorziening waardoor alle betrokkenen op de hoogte zijn van de genomen besluiten en uitgezette acties. Ook nadat het OT is gesplitst in een OT-C en een OT-V, heeft men voldoende oog voor de onderlinge informatie uitwisseling.

4.4 Het analyseren, beoordelen en besluiten voorbereiden

Dit proces heeft betrekking op het verschaffen van inzichten over de betekenis van de crisis en haar effecten. Daarnaast zorgt dit proces voor het aanbieden van opties voor de te nemen maatregelen. Door dit proces op een juiste manier in te richten stelt dit het besluitnemend orgaan (bijvoorbeeld de ICCb of de MCCb) in staat besluiten te nemen. Het analyseren, beoordelen en het voorbereiden van besluiten is de schakel tussen de informatievoorziening en het proces van het nemen van besluiten en het aansturen. Er dient sprake te zijn van een actueel beeld als basis voor de analyse. Wanneer er besluiten zijn genomen dienen de uitkomsten van deze besluiten te worden teruggekoppeld ten behoeve van het actuele beeld.

Vanaf het eerste moment dat bij de Nederlandse overheid bekend is dat er digitaal is ingebroken bij DigiNotar probeert men de situatie te beoordelen en op waarde te schatten. Zo is Govcert vrijwel vanaf het begin actief in overleg met DigiNotar en Fox-IT om inzicht te krijgen in de stand van zaken. De informatie over de (omvang van de) hack en de mogelijke impact daarvan laat zich – ook door de complexiteit van de materie – op dat moment moeilijk duiden. Op basis van de eerste (imperfecte) informatie ondernemen de op dat moment betrokken organisatieonderdelen zoals BZK/DRI, BZK/OBR, Logius en Govcert, vlot actie om meer inzicht te krijgen in de omvang van de problematiek en de mogelijke effecten daarvan.

Zo spreekt men af dat Logius haar gebruikers vraagt om uit te zoeken of en welke PKI-overheidscertificaten binnen de eigen organisatie aanwezig zijn en voor welke processen deze certificaten worden gebruikt.

Als op vrijdagmiddag 2 september blijkt dat niet kan worden uitgesloten dat ook PKI-overheidscertificaten zijn gecompromitteerd wordt vrijwel direct door de dgOBR in samenspraak met de NCTV de situatie beoordeeld als potentieel zeer ernstig en bedenkt men een strategie die tijdens de crisis als uitgangspunt dient voor alle activiteiten. Een sterk punt is dat men daarbij een drietal prioritaire thema's benoemt (herstel vertrouwen, herstellen continuïteit en het veiligheidaspect) die – hoewel op dat moment nog veel onduidelijk is – zich goed lenen als vertrekpunt voor de te ondernemen acties.

Direct na het activeren van de rijkscrisisorganisatie op vrijdagmiddag om 17:00 uur op het NCC deelt en analyseert men de eerste beelden. Hiermee legt men de basis voor de beslissingen die later op de avond door de ICCb en de MCCb zijn genomen (opzeggen vertrouwen in DigiNotar, transitie naar andere certificeerders).

Het Adviesteam is vanaf het begin betrokken bij het opstellen van omgevingsanalyses en het maken van scenario's. Deze rol komt – mede door de complexiteit van de materie – niet uit de verf. Hierdoor kan het Adviesteam zijn rol als 'adviseur' van de ICCb en de MCCb niet (geheel) waarmaken. Een belangrijke rol bij het analyseren en beoordelen van de stand van zaken is weggelegd voor de ICCIO. De ICCIO en haar netwerk is gedurende de crisis een belangrijke bron van informatie bij het nemen van beslissingen over de vraag op welke wijze de ingeslagen koers (het transitietraject) vorm moet krijgen.

Het OT werkt op basis van de analyses en informatie van onder meer de ICCIO, Govcert, Logius en – in een later stadium op basis van de adviezen van de CSR en het IRB – de ingezette strategie nader uit en geeft deze gedurende de crisis vorm. Daarbij maakt men onder andere gebruik van de input van betrokken uitvoeringsorganisaties en VNO-NCW. Men is hierdoor in staat om op basis van duidelijke analyses de besluitvorming in de ICCb en de MCCb voor te bereiden.

Het verzamelen van actuele informatie, het duiden (analyseren) van deze informatie en het voorbereiden van beslissingen (door onder andere het OT) werkt goed. Men toetst regelmatig of men nog op de goede weg zit, analyseert wat de knelpunten zijn en werkt zowel binnen de rijkscrisisorganisatie – als ook met een groot aantal organisaties buiten de crisisorganisatie – intensief samen bij het zoeken naar oplossingen. Een voorbeeld daarvan is de wijze waarop de rijkscrisisorganisatie op basis van de analyses over de gevolgen van de update, de update (de patch) van Microsoft op dinsdag 6 september organiseert.

4.5 Het nemen van besluiten en aansturen

Onder dit proces wordt leidinggeven aan de crisisrespons verstaan. Het betreft het bepalen van de strategie, het nemen van besluiten, de aansturing van de uitvoering, het monitoren van de strategie en de besluiten, en op basis daarvan het mogelijk bijstellen van deze strategie en de besluiten. Het hoofddoel van dit proces is het bevorderen van een effectieve aanpak en coördinatie van de crisisorganisatie.

Aan daadkracht in de besluitvorming ontbreekt het tijdens de DigiNotar-crisis niet. Op basis van de eerste beelden die al voorafgaand aan de opschaling bekend zijn (in de ingelaste programmaraad Logius) nemen de dgOBR, de directeur Nationale Veiligheid, het hoofd NCC en de NCTV (die in een later stadium het OT vormen) de beslissing om de crisisstructuur op te schalen. Ook daarna besluit men vlot over de in te zetten strategie. Dit besluit legt men voor aan de ICCb en de MCCb. Zij gaan hiermee akkoord. Hierdoor is zonder tijdverlies stevig doorgepakt.

Kenmerkend voor de besluitvorming tijdens de DigiNotar-crisis is de wisselwerking tussen de verschillende besluitvormende organen. In de 'binnenste cirkel' van de crisisorganisatie (de MCCb, de ICCb, het OT) beschikt men, dankzij een goede informatievoorziening, over dezelfde beelden en analyses van de crisis. Hierdoor is de crisisorganisatie in staat de situatie snel te beoordelen en kan men snel besluiten nemen. Het feit dat de leden van het OT ook betrokken zijn bij de overleggen van de besluitvormingsorganen (de MCCb en de ICCb), draagt bij aan een vlotte besluitvorming. Ook het feit dat men al snel besluit om de generieke crisisstructuur uit te breiden met een crisisspecifieke structuur (onder andere met ICT-deskundigen) bevordert de noodzakelijke kennis op basis waarvan men besluiten neemt.

Bij de besluitvorming tijdens deze crisis, speelt naast de organisatiestructuur ook de menselijke factor een belangrijke rol. Uit de interviews[28] en uit de bevindingen blijkt dat de goede samenwerking en het onderlinge vertrouwen tussen de leidinggevenden van de verschillende onderdelen van de crisisorganisatie belangrijke pluspunten zijn. Het feit dat men elkaar kent van eerdere werkzaamheden en oefeningen draagt hieraan bij. Tevens blijkt dat de leden van de MCCb, de ICCb en het OT over de competenties beschikken om snel beslissingen te nemen en acties uit te zetten als de situatie daarom vraagt. Dit blijkt met name uit het overnemen van het operationeel beheer van DigiNotar en de acties om de automatische update van Microsoft uit te stellen.

Tijdens de DigiNotar-crisis vragen veel verschillende onderwerpen om een beslissing. Deze onderwerpen variëren van communicatie tot aan de wijze waarop men met de hack bij andere certificeerders moet omgaan. Hoewel deze onderwerpen sterk verschillen, kunnen de besluitvormende organen – dankzij een vlotte informatievoorziening en beeldvorming – toch besluiten nemen over deze uiteenlopende onderwerpen.

[28] Zie bijlage 3.

4.6 Communiceren over de crisis

Dit proces heeft betrekking op het informeren van de bevolking en andere doelgroepen zoals bedrijven en betrokken instellingen tijdens een crisis. Het hoofddoel van dit proces is het voorkomen of beperken van schade, onrust en overlast. Crisiscommunicatie moet gedrag bevorderen dat aansluit bij een effectieve beheersing van de crisis. Daarnaast moet het de zelfredzaamheid bevorderen en zorgen voor een juiste beleving van de crisis. Het is van belang dat de crisiscommunicatie zo snel mogelijk wordt ingezet. Dit gebeurt op basis van actuele omgevingsanalyses. De communicatiestrategie moet zo snel mogelijk worden uitgedacht en ingezet.

Al in een vroeg stadium van deze crisis speelt communicatie een belangrijke rol. Op vrijdagmiddag 2 september komen de verschillende communicatiedeskundigen van het NCC, Govcert en het Ministerie van BZK bijeen om de woordvoeringslijn op te stellen, de communicatiestrategie te ontwikkelen en voorbereidingen te treffen voor het plaatsen van persberichten op de website rijksoverheid.nl. Ook besluit men die dag om een publieks-informatienummer in te stellen.

Het herstellen van vertrouwen en van de continuïteit zijn belangrijke thema's binnen de vastgestelde strategie. De – gezien het tijdstip – verassende persconferentie om 01:00 uur in de nacht van vrijdag 2 september op zaterdag 3 september door de minister van BZK past geheel in deze strategie. Door het vertrouwen in DigiNotar op te zeggen, 'isoleert' men het probleem en houdt men het algemene vertrouwen in de PKI-overheidscertificaten overeind. Tevens laat de rijkscrisisorganisatie met deze persconferentie zien dat zij de crisis voortvarend aanpakt.

Het NVC wordt op zaterdag 3 september geactiveerd. Vanaf dit moment voert het NVC de coördinatie over de communicatie naar diverse doelgroepen. Men heeft oog voor eenduidige communicatie onder regie van het NVC. Zo voorkomt men dat er tegenstrijdige berichtgeving ontstaat. Men hanteert gedifferentieerde communicatie met specifieke boodschappen voor de diverse doelgroepen. Er wordt onder andere gebruik gemaakt van factsheets, publieksnummers, Twitter en webpublicaties op diverse websites. Voor haar informatie gebruikt het NVC onder andere de (technische) expertise van Govcert en de ICCIO.

Ook monitort het NVC permanent het omgevingsbeeld. Dit omgevingsbeeld blijkt gedurende de gehele crisis vrij rustig en beheerst de reguliere media nauwelijks. Wel zijn er veel vragen op zogeheten 'expertwebsites'. Govcert voert de communicatie uit naar dit 'expertcircuit'.

De crisisorganisatie speelt snel in op vragen van de diverse doelgroepen. Zo verzendt men, wanneer op maandag 5 september blijkt dat met name gemeenten niet precies weten wat ze moeten doen, dezelfde dag nog een brief naar de bestuurlijke partners waaronder de gemeenten.

Deze brief beschrijft welke stappen zij moeten ondernemen als ze getroffen zijn door gecompromitteerde certificaten.

Via verschillende media worden burgers op de hoogte gehouden van de stand van zaken. Zo geeft de minister van BZK op maandagavond 5 september een tweede persconferentie en wordt op 7 september een bericht over het gebruik van DigiD geplaatst op de website rijksoverheid.nl. Vanaf vrijdagavond 2 september 2011 staat op deze website een apart informatiedossier, dat permanent werd vernieuwd. Zowel naar burgers als naar andere doelgroepen communiceert men met hoge frequentie nieuwe informatie.

Door bovenbeschreven wijze van communiceren stelt de crisisorganisatie zich transparant op en zijn betrokkenen op de hoogte van de stand van zaken en de ondernomen acties. Tevens weet men wat zijzelf moeten ondernemen om de gevolgen van de crisis zoveel mogelijk te beperken. Dit blijkt met name uit het verloop van de update van Microsoft op 6 september 2011.


5

Beantwoording onderzoeksvraag en aanbevelingen

De onderzoeksvraag luidt: Heeft de rijkscrisisorganisatie tijdens de DigiNotar-crisis doeltreffend gefunctioneerd? Deze vraag is beantwoord aan de hand van de analyses van de processen:

- **praktijk en planvorming;**
- **het onderkennen en signaleren van de crisis;**
- **het voorzien in informatie;**
- **het analyseren, beoordelen en besluiten voorbereiden;**
- **het nemen van besluiten en aansturen en**
- **het communiceren over de crisis.**

Conclusie

De rijkscrisisorganisatie heeft tijdens de DigiNotar-crisis doeltreffend gefunctioneerd.

Hoewel de rijkscrisisstructuur niet geheel conform planvorming is ingericht is dit zeker niet ten koste gegaan van het optreden. Het doeltreffend functioneren van de rijkscrisisorganisatie is mede te danken aan de korte lijnen, de goede samenwerking en het doortastende optreden van de belangrijkste sleutelfunctionarissen. Dit laat echter onverlet dat niet alle organisatieonderdelen tijdens deze crisis even rolvast hebben gehandeld.

De rijkscrisisstructuur is tijdens de DigiNotar-crisis grotendeels ingericht zoals beschreven in de planvorming. Er is een generieke structuur zoals beschreven in het Nationaal Handboek Crisisbesluitvorming die bestond uit de MCCb, de ICCb, het Adviesteam en het NVC. Daarnaast is deze generieke structuur uitgebreid met een crisisspecifieke structuur zoals beschreven in het NCP-ICT. Dit betreft de organisatieonderdelen de IRB, de CSR en de ICCIO. Dit plan is ten tijde van deze crisis nog niet vastgesteld. De rijkscrisisstructuur kent tijdens de DigiNotar-crisis een overleg dat niet is beschreven in de planvorming. Dit betreft het OT dat tijdens het verloop van de crisis is gesplitst in een OT-V en een OT-C.

De mogelijke gevolgen van de hack bij DigiNotar zijn snel onderkend. Hoewel men in het begin nog geen compleet beeld heeft van de dreiging schaalt men de crisisorganisatie vlot op. Hierdoor maak men snel een start met de beheersing van de (dreigende) crisis.

Tijdens de DigiNotar-crisis is sprake van een vlotte en goed lopende informatievoorziening tussen de verschillende organisatieonderdelen. De juiste informatie is op het juiste moment bij de juiste functionaris. Dit is mede te danken aan de korte lijnen tussen de verschillende sleutelfunctionarissen van zowel de rijkscrisisorganisatie als ook de betrokken externe organisaties.

Door goede analyses en voorbereiding op de te nemen besluiten, zijn de MCCb en de ICCb goed in staat om beslissingen te nemen. Het Adviesteam voert hierbij zijn rol niet conform planvorming uit. Het OT en de ICCIO nemen de rol van adviseur over.

Het OT speelt tijdens deze crisis een cruciale rol. Dit betreft zowel het onderkennen van de crisis, het uitdenken en uitrollen van de strategie, het uitzetten van de te ondernemen acties als ook de voorbereiding op te nemen besluiten in de MCCb en de ICCb. Tussen de leden van het OT is sprake van vertrouwen en een goede samenwerking. Dit vertaalt zich in doortastend optreden.

Tijdens de DigiNotar-crisis bestaat er een goede wisselwerking tussen de verschillende besluitvormende organen. De MCCb, de ICCb, het OT beschikken dankzij een goede informatievoorziening over dezelfde beelden en analyses van de crisis. Hierdoor is de crisisorganisatie in staat de situatie snel te beoordelen en kan men snel besluiten nemen.

Het NCC toont tijdens deze crisis aan zowel inhoudelijk als praktisch de crisisbeheersingsorganisatie goed te kunnen ondersteunen en faciliteren.

Door het snel en effectief inrichten van het NVC, zorgt de communicatie vanuit de overheid voor het beperken van schade, onrust en overlast. Dit geldt zowel voor de communicatie naar de burgers als voor de communicatie naar de overige doelgroepen.

Aanbevelingen

Aan de Nationaal Coördinator Terrorismebestrijding en Veiligheid:

1. Blijf investeren in een vaste kernbezetting van de rijkscrisisorganisatie, met deelnemers die door opleiding en oefening over de juiste crisiscompetenties beschikken.

2. Bezie de bemensing, werkwijze en status van het Adviesteam binnen de rijkscrisisorganisatie vanuit het oogpunt van doeltreffendheid. Indien waarde wordt gehecht aan het Adviesteam, organiseer het Adviesteam dan zo, dat het zijn rol als adviseur van de MCCb en de ICCb kan waarmaken.

Bijlagen

Bijlage I

Afkortingen

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
CA	Certificate Authority
CBA	Crisis Beleidsadviseur
CERT	Computer Emergency Response Team
CEO	Chief Executief Officer
CIO	Chief Information Officer
cRC	Cluster Risico- en Crisiscommunicatie
CSR	Cyber Security Raad
DCC	Departementaal Coördinatie Centrum
Dg	Directeur-generaal
DRI	Programmadirectie Dienstverlening, Regeldruk en Informatiebeleid
G4	De vier grootste gemeenten
ICCb	Interdepartementale Commissie Crisisbeheersing
ICCIO	Interdepartementale Commissie- CIO
IG	Inspecteur-Generaal
Inspectie VenJ	Inspectie Veiligheid en Justitie
IPO	Interprovinciaal overleg
IRB	Incident Respons Board
IWWN	International Watch and Warning Network
KLPD	Korps Landelijke Politiediensten
LOCC	Landelijk Operationeel Coördinatiecentrum
LOS	Landelijk Operationele Staf
M2M	Machine to Machine
MCCb	Ministeriële Commissie Crisisbeheersing
Ministerie van BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Ministerie van VenJ	Ministerie van Veiligheid en Justitie
NCC	Nationaal CrisisCentrum
NCP-ICT	Nationaal Crisisplan-ICT
NCTV	Nationale Coördinator Terrorismebestrijding en Veiligheid
NVC	Nationaal Voorlichtingscentrum
OBR	Organisatie Bedrijfsvoering Rijk
OM	Openbaar Ministerie
OT	Operationeel Team
OVV	Onderzoeksraad voor Veiligheid
PKI	Public Key Infrastructure
SG	Secretaris-generaal
VNG	Vereniging Nederlandse Gemeenten
VNO-NCW	Verbond van Nederlandse Ondernemingen- Nederlands Christelijk Werkgeversverbond

Bijlage II

Openbare bronnen

DigiNotar Certificate Authority breach 'Operation Black Tulip' Fox-IT, 5 september 2011
Nationaal Crisisplan ICT, versie 1.0, 15 december 2011
Nationaal Handboek Crisisbesluitvorming
Nationale Cyber Security Strategie, februari 2011
Nationale Risicobeoordeling, Bevindingenrapportage 2010, versie 1.0
Scenario's Nationale Risicobeoordeling 2008/2009
Toetsingskader Crisisbeheersing, conceptversie 0.8D

Bijlage III

Geïnterviewde functionarissen

Drs. E.S.M. Akerboom	NCTV	Ministerie van Veiligheid en Justitie
Drs. A. Borst EMPM	Hoofd NCC	Ministerie van Veiligheid en Justitie
Drs. R.W.C. Clabbers	Directeur Nationale Veiligheid	Ministerie van Veiligheid en Justitie
Drs. M. K. Delfgaauw	Adviseur crisiscommunicatie	Ministerie van Veiligheid en Justitie
MSc N. Ghaoui	Beleidsmedewerker NCC	Ministerie van Veiligheid en Justitie
Mr. M.W.I Hillenaar	CIO-Rijk	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Dhr. A. Jochem	Manager Security Team	Govcert
Drs. K.W. Keuzenkamp	Clusterhoofd	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Drs C.Y. Sikkema	Sr. Beleidsmedewerker NCC	Ministerie van Veiligheid en Justitie
Dr. J.J.M. Uijlenbroek	Directeur-generaal OBR	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Bijlage IV

Uitleg over certificaten en hun betekenis

Bron: Factsheets NCC

- **Waarvoor worden certificaten gebruikt?**

Certificaten worden gebruikt om communicatie over internet betrouwbaar en veilig te laten zijn. Met certificaten kan duidelijk worden gemaakt wie of wat de ontvanger of verzender van informatie is. Dat kan een website (slotje), een persoon of computer (inloggen/ authenticeren) of een elektronische handtekening (ondertekenen) zijn. De onderliggende techniek werkt in alle gevallen met sleutels (vandaar de naam Public Key Infrastructure).

De certificaten zijn openbare verklaringen (van een vertrouwde derde partij), die aangeeft wie er in het bezit is van welke sleutel. In het geval van 'het slotje' wordt zo'n sleutel ook nog eens gebruikt om de communicatie tussen gebruiker en een website te versleutelen ter voorkoming van afluisteren (een zogeheten secure socket layer of, afgekort SSL).

- **Wie geven certificaten uit?**

Een uitgever van certificaten, wordt ook wel certificatiedienstverlener genoemd. Er zijn verschillende certificatiedienstverleners. Voorbeelden zijn Verisign, Comodo, Thawte, Digidentity, Getronics, QuaVadis en ESG. DigiNotar is ook zo'n certificatiedienstverlener.

- **Uitgifte van certificaten door DigiNotar.**

DigiNotar gaf certificaten uit voor zowel websites(slotje), het herkennen van personen (inloggen) als voor de elektronische handtekening. Dat deed ze in verschillende productie straten, waaronder: 'eigen-merk'-certficaten.

- **Welke certificaten zijn er?**

Er zijn wettelijk gezien twee soorten certificaten: gekwalificeerde certificaten en andere certificaten, waaronder servercertificaten. Servercertificaten worden in computers gebruikt voor het opzetten van beveiligde verbindingen. De burger weet dan dat hij echt op de website van de desbetreffende organisatie zit en niet op een nep-site.

Een gekwalificeerd certificaat wordt door een persoon gebruikt om een elektronische handtekening te kunnen zetten. Een gekwalificeerd certificaat moet voldoen aan allerlei wettelijke eisen. Dat geldt niet voor andere (niet gekwalificeerde) certificaten. Zo moet een verlener van gekwalificeerde certificaten zich laten registeren bij de OPTA en moet een persoon die een gekwalificeerde certificaat wil hebben zich persoonlijk met een geldig legitimatiebewijs identificeren bij de uitgever van het certificaat (certificatiedienstverlener). De OPTA houdt toezicht op de regelgeving met betrekking tot gekwalificeerde certificaten die gebruikt worden voor elektronische handtekeningen.

-

- **Wat zijn PKI-overheidcertificaten?**

PKIoverheid is een nog zwaarder regime dan de voorafgaande 'gekwalificeerde' certificaten (omschreven in het zogeheten PKIoverheid Programma van Eisen). Het verklaart – middels een overeenkomst tussen de Staat en de certificatiedienstverlener – ondermeer het regime van de EU Richtlijn van toepassing op alle onder PKIoverheid uitgegeven certificaten, dus ook de website- (slotje) en inlog/authenticatie certificaten.
Daarnaast verplicht het certificering (die is onder de EU Richtlijn nog vrijwillig) conform zowel de EU Richtlijn als tegen het Programma van Eisen van PKIoverheid. Die certificering vindt plaats door een externe partij (BSI Management Systems B.V. en PriceWaterhouse-Coopers zijn hiertoe geaccrediteerd, zij zijn daartoe door de minister van Economische zaken,Landbouw en Innovatie aangewezen). Daarnaast is een jaarlijkse audit verplicht.

Overheden namen – net als bedrijven en andere organisaties – zowel Eigen merk, als PKI-overheidscertificaten af bij DigiNotar. Voorbeelden van bedrijven die Eigen merk certificaten afnamen zijn Nuon en EspritXB. Een voorbeeld van een overheidsorganisatie die Eigen merk certificaten afnam is de Belastingdienst, het betreft de zogeheten BAPI certificaten waarmee Fiscaal Intermediairs met de Belastingdienst praten.

Colofon

Afzendgegevens
Inspectie Veiligheid en Justitie

Lange Houtstraat 26
2511 CW Den Haag
Postbus 20301
2500 EH Den Haag
www.ivenj.nl

Foto's: Dhr. Rob Altena
Dhr. Thomas Abrahams
J-14397