

## Voorlopige bevindingen en aanbevelingen n.a.v. DigiNotar-inbraak

Van: NOREA-bestuur

Datum: 2 december 2011

### 1. Aanleiding en adviesvraag

Het NOREA-bestuur heeft met grote bezorgdheid kennis genomen van de gevolgen en ontwikkelingen naar aanleiding van de DigiNotar-inbraak, zoals deze sinds 3 september 2011 via persberichten, kamerbrieven alsmede het rapport van Fox-IT in de openbaarheid zijn gebracht.

Deze ontwikkelingen raken aan de kern van ons vakgebied. Op 19 september heeft het bestuur aan de Raad voor Beroepsethiek van de NOREA verzocht om een nadere analyse en interpretatie van de feiten en omstandigheden, rekening houdend met de doelstellingen, risico's en kansen voor de Orde. Vragen die in elk geval beantwoord moeten worden zijn de volgende:

- Zijn de assurance-opdracht(en), waarbij expliciet wordt verwezen naar "in accordance with attestation standards of the Dutch Institute of EDP-Auditors, NOREA" en/of de accreditatie van DigiNotar door PwC op grond van het normenkader TTP.nl op goede gronden uitgevoerd, in het perspectief van de conclusies die in het rapport van Fox-IT zijn geformuleerd;
- Heeft het management van DigiNotar (waaronder gekwalificeerde Register EDP-auditors) de juiste belangenafweging gemaakt tussen het belang van DigiNotar en het algemeen maatschappelijk belang door de inbraak tussen 19 juli en 27 augustus 2011 niet in de openbaarheid te brengen (op grond van de Gedragscode aanvaardt de IT-auditor te allen tijde de verantwoordelijkheid op te treden in het algemeen belang);
- Is het normenkader van TTP.nl alsmede de beveiliging door middel van SSL-certificaten toereikend voor de beveiliging van 'trusted' overheidscommunicatie en onze kritische infrastructuur.

Op 30 november jl. zijn door de Raad voor Beroepsethiek, op basis van publiekelijk beschikbare stukken en zonder een inhoudelijk onderzoek uit te voeren, enkele voorlopige bevindingen en aanbevelingen aan het bestuur gepresenteerd. Ondanks het voorlopige karakter van deze bevindingen, acht het bestuur het van belang om onze leden en externe relaties hieromtrent te informeren. Aan de Raad voor Beroepsethiek wordt gevraagd om haar onderzoeksactiviteiten uit te breiden met een meer inhoudelijk onderzoek, waarbij naast zelfstandige conclusies ook de bevindingen en conclusies van andere/ toekomstige (externe) onderzoeken kunnen worden betrokken.

### 2. De rol van de externe auditor(s)

Het beroep van IT-auditor vindt haar oorsprong binnen de accountancy. Daar is het gebruikelijk een bevestiging te geven bij een historische financiële verantwoording van de geld- en goederenstroom, te weten de jaarrekening. Het Burgerlijk Wetboek legt deze taak bij de accountant met de intentie zo vertrouwen te geven aan de maatschappij. Ondanks dat internationale regelgeving zoals de Amerikaanse Sarbanes-Oxley wetgeving en in andere landen soortgelijke regelgevingen IT niet expliciet noemen, wordt de IT-auditor wereldwijd geacht mee te werken aan deze op het verleden gerichte aanpak. De IT-auditor wordt voor een deel van haar werkzaamheden getraind in het vaststellen dat gedurende een bepaalde periode in het verleden de maatregelen effectief waren geïmplementeerd en hebben gewerkt. Dit uit zich vooral bij het ondersteunen van een externe accountant en andere assurance werkzaamheden.

Vorenstaande benadering is in 2008 ook gevolgd blijktens het *Independent Auditors' report* dat is afgegeven op 17 december 2008 door Pricewaterhouse Coopers Advisory N.V. Dit rapport is gericht op de assertion die door het management is afgegeven d.d. 17 november 2008 en betrekking heeft op de periode 14 mei 2007 tot en met 17 november 2008. In dit rapport wordt gebruik gemaakt van *Richtlijn Assurance-opdrachten door IT-auditors (3000)* welke richtlijn ontleend is aan de IFAC Standaard 3000: *Assurance engagements*. De verwijzing naar de regelgeving vanuit de beroepsorganisatie NOREA is derhalve terecht.

Op 1 november 2010 heeft PricewaterhouseCoopers Certification B.V. een *Certificate* afgegeven dat is gebaseerd op TTP.NL '*Scheme for management system certification of Service Providers issuing Qualified Certificates for Electronic Signatures, Public Key certificates and / or Time-stamp token*', versie 8.1 d.d. juni 2010. Hierbij wordt expliciet aangegeven dat het management systeem van DigiNotar B.V. voor het uitgeven van certificaten voldoet aan de vereisten zoals gespecificeerd in: (1) qualified certificate policy QCP+ specified in ETSI TS 101 456 (v. 1.4.3) en (2) normalized certificate policies NCP+, EV specified in ETSI TS 102 042 (v. 2.1.2).

Het certificaat heeft een houdbaarheidsperiode van 1 november 2010 tot en met 31 oktober 2013, waarbij opgemerkt wordt dat gedurende die periode jaarlijks '*surveillance*' audits zullen worden uitgevoerd. Werd in het rapport van 17 december 2008 gewezen op de inherente beperking van het onderzoek te weten het risico van het projecteren van de uitkomsten naar de toekomst, is dat in het certificaat achterwege gebleven. De verwijzingen die in het rapport van 17 december 2008 zijn gemaakt naar regelgeving en gehanteerde criteria zijn in lijn met de vereiste transparantie dienaangaande.

Aan de formele vereisten is derhalve door PwC voldaan. Of de beoordeling en certificering ook in materiëel opzicht adequaat is geweest vergt nader inhoudelijk onderzoek.

### **3. De rol van het management van DigiNotar**

Door het management van DigiNotar is zoals hiervoor al werd vermeld op 17 november 2008 een assertion afgegeven die in het Independent auditors's report wordt bevestigd. Dit is evenwel niet het geval geweest bij het afgeven van het certificaat. Dit impliceert dat het certificaat kwalificeert als een 'direct report' terwijl het audit rapport uit 2008 kwalificeert als een 'assertion report'. In een 'direct report' richt de onderzoeker zich rechtstreeks tot de processen en procedures en niet tot een eventuele uitspraak van het management.

In het kader van de toegang tot gegevens zijn een aantal vereisten uit de ETSI TS 101 456 gesteld aan het systeem, te weten vereisten 7.4.6. '*System Access management*'. Hier wordt gesteld dat : '*the CA shall ensure that CA system access is limited to properly authorized individuals*'. De digitale inbraak heeft aangetoond dat kwetsbaarheden in deze vereiste bestaan.

Het is zonder een inhoudelijk onderzoek niet mogelijk aan te geven in hoeverre voldaan is aan de daarop volgende vereisten onder de punten 7.4.6.A) tot en met 7.4.6.L). Ook al zou zijn voldaan aan alle hiervoor genoemde vereisten heeft het er, zonder hiernaar verder onderzoek te hebben gedaan en zonder te beschikken over niet-publiekelijk beschikbare informatie, alle schijn van dat voor het maatschappelijk verkeer niet op een juiste wijze invulling is gegeven aan de vereisten 7.4.6.I) en 7.4.6.K) die stellen dat: '*continuous monitoring and alarm facilities shall be provided to enable the CA to detect, register and act in a timely manner upon any unauthorized and/or irregular attempts to access its resources*'.

Hetzelfde geldt voor vereiste 7.4.8 e), namelijk: '*In the case of compromise the CA shall as a minimum provide the following undertakings:*

- *Inform the following of the compromise: all subscribers and other entities with which the CA has agreements or other form of established relations, among which relying parties and CAs. In addition, this information shall be made available to other relying parties.*
- *Indicate that certificates and revocation status information issued using this CA key may no longer be valid.'*

Deze regel is weliswaar niet aangekruist in de kolommen in de standaard, maar kan niet anders gelezen worden als een belangrijke handeling in het kader van vertrouwen binnen het maatschappelijk verkeer.

Voor het trekken van conclusies en het doen van aanbevelingen is nader inhoudelijk onderzoek noodzakelijk, incl. hoor en wederhoor van de IT-auditors die deel hebben uitgemaakt van het DigiNotar-management.

#### **4. Aanbevelingen voor de beroepsorganisatie**

Ten aanzien van assurance-rapporten en certificaten bestaat een verwachtingskloof tussen het vertrouwen dat door het maatschappelijk verkeer daaraan wordt ontleend en de feitelijke werkzaamheden die door IT-auditors dienaangaande worden uitgevoerd. Het bestuur neemt de suggestie over om met de leden een discussie te starten over de verhoging van de toegevoegde waarde van het beroep door de focus te verschuiven van historisch (financiële) verantwoording naar het in kaart brengen van bestaande zwakheden in relatie tot relevante dreigingen vandaag en in de nabije toekomst, waarbij al dan niet gewezen wordt op de inherente beperkingen en de risico's van het projecteren van de uitkomsten van het onderzoek naar de toekomst. Voor een gebruiker van IT heeft een bevestiging van het goed functioneren van de processen gedurende de voorgaande periode weinig toegevoegde waarde. Het is voor die gebruiker veel belangrijker te weten dat de dienstverlener robuust genoeg is om de actuele bedreigingen het hoofd te bieden en dat de dienstverlening in de nabije toekomst ongestoord wordt gecontinueerd. Deze discussie dient later te worden uitgebreid naar overleg met de toezichthouders en de rijksoverheid. Het lijkt zaak te zijn om deze discussies in voldoende tempo te voeren met alle daarbij behorende transparantie. De Orde kan daarmee haar maatschappelijke betrokkenheid en relevantie vergroten.

NOREA is vertegenwoordigd in het College van Belanghebbenden TTP.nl. In dat verband is de discussie geopend over een zodanige aanpassing van het document en certificeringsschema uit juni 2010, zodat de lijsten met criteria zoveel mogelijk in lijn blijven met de technologische en politieke ontwikkelingen. Ook zal in dat overleg aandacht worden bepleit voor duidelijke aanwijzingen met betrekking tot de kosten van een certificatieonderzoek. In paragraaf 6.4 van het genoemde document wordt aangegeven dat een certificatieonderzoek 15 tot 20 mandagen in beslag neemt en een jaarlijks 'surveillance' audit 8 mandagen. NOREA is van mening dat het vooraf aangeven van het tijdsbeslag niet bevorderlijk is voor de kwaliteit van de uitgevoerde werkzaamheden. Het is volgens ons niet de taak van het College van Belanghebbenden TTP.nl om de kosten van een certificatieonderzoek te limiteren, maar om te borgen dat een certificaat de redelijke mate van zekerheid verschaft die het maatschappelijk verkeer daarvan verwacht.

Het bestuur overweegt een werkgroep in te stellen die richtlijnen ontwikkelt op welke wijze zwakheden en bedreigingen breder in kaart kunnen worden gebracht dan op dit moment gebruikelijk is en waarbij ook technologische en politieke ontwikkelingen nadrukkelijk worden meegenomen. Aangezien dit in feite een taak is voor het management van een organisatie, dat vanuit een realistische afweging van risico's haar besluiten neemt, is deze bijdrage van de IT-auditor een extra 'value' voor het management.

Ofschoon de beroepsorganisatie vertrouwelijkheid hoog in het vaandel heeft staan alsmede het uitgangspunt dat een IT-auditor slechts een uitspraak doet na afweging van het belang van alle partijen overweegt het bestuur in overleg te treden met de daartoe bevoegde instanties om een 'misbruik van IT'-meldpunt in te stellen alwaar het management en de IT-auditor, in de anonimiteit indien daar behoefte aan is, melding kan maken van misbruik, in de zin van misstanden en incidenten, van de IT in de meest brede zin des woords. De moderne maatschappij is momenteel dusdanig afhankelijk van de IT en de daarmee verband houdende communicatiehuishouding dat maatschappelijk gezien niet meer voorbij kan worden gegaan aan een adequaat uitgerust centraal meldpunt met een speciaal daartoe uitgeruste opsporingsinstantie.

Voorts heeft het bestuur het voornemen om met de overheid in overleg te treden om te bezien op welke wijze de belanghebbenden op een adequate en tijdige wijze op de hoogte gebracht kunnen

worden omtrent misbruik van IT, zoals is geconstateerd en beoordeeld door het meldpunt, opdat soortgelijke situaties zich niet gaan voordoen in andere situaties.

## **5. Aanbevelingen in relatie tot de rol van de rijksoverheid**

Het bestuur zal met de overheid in overleg te treden om bij het stimuleren van technologische oplossingen meer aandacht te besteden aan het inrichten van een toezichhoudende rol.

Daarbij zal een centraal orgaan worden bepleit dat de beschikking krijgt over en onderzoek doet naar gegevens en informatie ten aanzien van het elektronische verkeer nationaal en internationaal om zodoende tijdig betrokkenen te kunnen informeren over daadwerkelijke zwakheden en risico's welke optreden door het zich steeds verder ontwikkelen van de technologie.

Daarnaast zal de beroepsorganisatie proberen de overheid te overtuigen van de noodzaak meer proactief om te gaan met informatiebeveiliging voor haar eigen werkzaamheden. Als wordt gekozen voor een aanpak in de richting van een e-overheid, behoort de overheid daarbij de regie strak in handen te houden en te borgen dat de maatschappij kan vertrouwen op de technologische aanpak.