Amuse

arsaequi.nl/maandblad AA20120080

DIGINOTAR: LESSONS TO BE LEARNT

Nico van Eijk*

Op 2 september 2011 verscheen tegen middernacht op de tv een balk boven in beeld met de mededeling dat er om 01.00 uur een extra uitzending van het NOS-journaal zou zijn. Was er een wereldramp gebeurd, was de regering gevallen? Overgeschakeld ontrolde zich een wat surrealistische enscenering. Minister Piet Hein Donner, minister van Binnenlandse Zaken en Koninkrijkszaken, eenzaam zittend achter een alledaags tafeltje, kwam met een verklaring waaruit moest worden opgemaakt dat het Internet niet langer veilig was. Maar we konden gerust weer gaan slapen want er waren adequate maatregelen getroffen, het land was gered!

Minister Piet Hein Donner kwam met een verklaring waaruit moest worden opgemaakt dat het Internet niet langer veilig was. Maar we konden gerust weer gaan slapen want er waren adequate maatregelen getroffen, het land was gered!

Met de verklaring was de DigiNotar-affaire een feit. Al langer gingen er geruchten dat er wat mis was met de 'veiligheidscertificaten' die worden gebruikt om bijvoorbeeld transacties en websites te authenticeren. Technisch een behoorlijk ingewikkelde aangelegenheid, maar kort gezegd komt het er op neer dat een website over een certificaat beschikt waarmee kan worden aangetoond dat men daadwerkelijk is wie men beweert te zijn.[1] Deze 'ssl-certificaten' worden getest via de browser (het hangslotje dat open of dicht staat). Naast dit soort certificaten zijn er ook andere, zoals Public Key Infrastructure (PKI)-certificaten. In Nederland gaat het bijvoorbeeld om 'PKI-Overheid', certificaten van de Nederlandse overheid. De certificaten worden gebruikt in de communicatie met burgers (belastingaangifte, UWV, DigiD) en door notarissen en deurwaarders (bijvoorbeeld registraties bij het kadaster).

DigiNotar wist al in juli dat hackers hadden ingebroken, maar pas eind augustus kreeg Govcert.nl,[2] dat zich bezighoudt met onder meer de bestrijding van cybercrime, een melding binnen – via een Duitse zusterorganisatie – dat er mogelijk wat mis was: een Iraanse internetgebruiker wilde naar Google.com gaan en kreeg een melding over een mogelijk frauduleus certificaat. Vervolgens ging het balletje rollen. Een onafhankelijk rapport bevestigde de inbraak en duidelijk werd dat niet alleen de 'internetcertificaten', maar ook de overheidscertificaten in het geding waren.

Konden we na de verklaring van Donner inderdaad weer gerust gaan slapen?

Konden we na de verklaring van Donner inderdaad weer gerust gaan slapen?[3] Het operationeel beheer van DigiNotar werd overgenomen, oftewel de overheid ging de onderneming leiden. In de tweede plaats werd een proces in gang gezet om op zo kort mogelijke termijn over te stappen naar andere PKI-certificatenleveranciers. Daarbij is gekozen voor een proces van geleidelijke overgang om de continuïteit zeker te stellen. Zo werd met Microsoft afgesproken dat de browser nog niet werd aangepast om DigiNotar-certificaten te weigeren.

Ook de Onafhankelijke Post- en Telecommunicatie Autoriteit (OPTA) kwam in actie. De OPTA is op grond van de Telecommunicatiewet belast met het toezicht op 'gekwalificeerde certificaten' (in de wandelgangen ook wel 'digitale handtekeningen' genoemd). De in het geding zijnde PKI-certificaten behoren tot deze gereguleerde certificaten. Aanbieders dienen zich te registreren bij OPTA en moeten uit hoofde van de wet aan allerlei voorschriften voldoen. OPTA kan eventueel besluiten om de registratie in te trekken. Dat is ook gebeurd in het geval van DigiNotar. De registratie is beëindigd per 14 september en DigiNotar is verplicht om de uitgegeven gekwalificeerde certificaten binnen 14 dagen in te trekken.[4] Zowel DigiNotar als de notarissen en deurwaarders hebben vervolgens – zonder succes – het besluit van OPTA aangevochten bij de voorzieningenrechter.[5] DigiNotar verkeerde ondertussen al in staat van faillissement.

* Prof.dr. N.A.N.M. van Eijk is verbonden aan het Instituut voor Informatierecht (IViR, Universiteit van Amsterdam) als hoogleraar informatierecht, in het bijzonder het media- en telecommunicatierecht.

1 Zie over de (technische) achtergronden onder meer: M.B. Voulon, 'Toezicht op certification service providers (CSPs)', *Computerrecht* 2012/1.

2 Govcert.nl is inmiddels opgegaan in Nationaal Cyber Security Centrum (NCSC), zie: *www.govcert.nl* en *www.ncsc.nl*. Op de website van Govcert is ook een dossier te vinden over DigiNotar.

3 Zie over de genomen maatregelen o.a.: *Kamerstukken II* 2011/12, 26 643, nrs. 188, 192, 194-210 en 214; *Handelingen II* 2011/12, nr. 102, item 7 (vragenuur); *Handelingen II* 2011/12, nr. 12, item 26 (DigiNotar).

4 Besluit OPTA van 13 september 2011 (kenmerk OPTA/ACNB/2011/202084_OV) en brief van 13 september 2011 (kenmerk OPTA/ACNB/2011/202111).

5 Rb. Den Haag (vzr.) 27 september 2011, LJN: BT6349 en BT6781. Zie voor noot bij BT6781: *Computerrecht* 2012/1.

Wat leert de DigiNotar-affaire ons? Een aantal juridische observaties

De hele affaire begon vanwege gecorrumpeerde ssl-certificaten. Deze zijn het meest voorkomend bij alledaags internetgebruik. Het blijkt evenwel dat juist deze certificaten nauwelijks juridisch zijn ingekaderd. Ze behoren namelijk niet tot de gekwalificeerde certificaten waar de regulering rond elektronische handtekeningen betrekking op heeft. Het is de vraag of men zich dit voldoende heeft gerealiseerd (of kon realiseren) toen in 1999 de Europese richtlijn inzake elektronische handtekeningen tot stand kwam, die aan de basis ligt van wat er in de Telecommunicatiewet is geregeld.[6]

De hele affaire begon vanwege gecorrumpeerde ssl-certificaten. Deze zijn het meest voorkomend bij alledaags internetgebruik. Het blijkt evenwel dat juist deze certificaten nauwelijks juridisch zijn ingekaderd

Wijzigingen van de Telecommunicatiewet, die momenteel bij de Eerste Kamer voorliggen, geven nieuwe instrumenten om regels te stellen ten aanzien van de risico's voor de veiligheid en integriteit van netwerken en diensten.[7] Echter, certificaten vallen hier buiten. Hetzelfde geldt voor bestaande en toekomstige regels over data-lekken.

Bij de maatregelen die wel genomen zijn – het operationeel overnemen van DigiNotar en het migreren naar veilige certificaten – zijn kanttekeningen te plaatsen: in de eerste plaats met betrekking tot het operationeel overnemen van DigiNotar. Trad de overheid hier op in een publiekrechtelijke of privaatrechtelijke hoedanigheid? Het eerste lijkt voor de hand te liggen en daarmee is de kwestie van het ontbreken van een juridische grondslag des te interessanter. In de tweede plaats zijn er juridisch boeiende verwikkelingen geweest met betrekking tot de migratie. Hoe heeft de belangenafweging plaatsgevonden tussen enerzijds het waarborgen van de continuïteit en anderzijds de risico's die waren verbonden aan de mogelijk gecompromitteerde certificaten (deze vraag kan overigens ook gesteld worden ten aanzien van het uitstel dat door OPTA werd verleend)? En hoe moeten we het overleg tussen Donner en Microsoft positioneren over het nog niet verwerken van de gecompromitteerde certificaten?

Wat te doen?

De DigiNotar-affaire heeft ons weer eens met de neus op de feiten gedrukt. De veiligheid van het Internet is geen abstracte aangelegenheid en inbreuken kunnen grote consequenties hebben. Certificaten moeten zekerheid bieden voor wat betreft de toegang tot websites en het doen van transacties. De toenemende afhankelijkheid van het Internet en het ontbreken van alternatieven maakt een en ander alleen maar meer kritisch.

Een goede analyse en verdere studie is absoluut noodzakelijk, overgaan tot de orde van de dag is geen optie meer. Is het systeem van digitale handtekeningen, dat tot stand kwam in een tijd dat Internet nog niet zo prominent aanwezig was, wel afdoende? Is het probleem dat er een slechte naleving is en kan het aanscherpen van het toezicht een oplossing bieden, of moet het systeem als zodanig overboord en worden vervangen door bijvoorbeeld een vergunningstelsel? Echter, de gereguleerde gekwalificeerde certificaten zijn maar een deel van de problematiek. Mijns inziens moet er meer vanuit de risico's worden gedacht en is het beter om te kijken naar 'kritische' certificaten waarop specifieke voorwaarden van toepassing moeten zijn (ten aanzien van de partijen die deze uitgeven, mogelijk in combinatie met een verplichting voor marktpartijen om veilige certificaten te gebruiken).[8] Kortom, het juridisch kader, dat zich nog vooral concentreert op enkele klassieke partijen in de waardeketen tussen aanbieders van informatie en de afnemers, dient beter deze waardeketen als geheel te reflecteren, dus met inachtneming van activiteiten zoals de verlening van certificaten en de rol van browsers.

De DigiNotar-affaire heeft ons weer eens met de neus op de feiten gedrukt. De veiligheid van het Internet is geen abstracte aangelegenheid en inbreuken kunnen grote consequenties hebben

Bevoegdheden en handhavingsmaatregelen vragen eveneens om een kritische analyse. Juridische grondslagen ontbraken met betrekking tot essentiële stappen in de DigiNotar-affaire. Het overnemen van operationele processen en onderhandelen met marktpartijen in het kader van publiekrechtelijke belangen dient een wettelijke inkadering te hebben, al was het maar om enerzijds adequaat handelen mogelijk te maken en anderzijds misbruik te voorkomen. Ik geef maar als suggestie mee dat in de energiesector het fenomeen van de stille curator bestaat, die de controle van een onderneming kan overnemen teneinde de continuïteit van de dienstverlening zeker te stellen.[9] Ten slotte is ten aanzien van de genomen maatregelen een meer transparante belangenafweging gewenst en moet duidelijk zijn hoe overgangsmaatregelen zich tot de risico's (en mogelijke aansprakelijkheden) verhouden.

6 Richtlijn 99/93/EG, *PbEG* 2000 L 13/12; *Kamerstukken II*, 2000/01, 27 743; *Stb.* 2003, 199 (Wet elektronische handtekeningen).

7 *Kamerstukken* 2010/12, 32 549 (zie met name hst. 11A).

8 Zie in dit verband ook de reactie van de Europese Commissie in antwoord op vragen uit het Europees Parlement over DigiNotar: vraag van 9 september 2011 (Judith Sargentini) met antwoord van 19 oktober 2011, E-007985/2011. De Europese Commissie geeft aan een en ander mee te zullen nemen bij de voorgenomen herziening van de Richtlijn Elektronische Handtekeningen.

9 Art. 13a Elektriciteitswet.