Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam

M +31(0)654386680
E ot.vandaalen@bof.nl
W www.bof.nl

Bankrekening 55 47 06 512
Bits of Freedom, Amsterdam
KVK-nr. 34 12 12 86

Commissie Binnenlandse Zaken

Betreft
Hoorzitting over de digitale inbraak bij DigiNotar

Datum
Amsterdam, 13 september 2011

1. Op 15 september vindt in de Tweede Kamer een hoorzitting over de digitale inbraak bij Diginotar plaats. Bits of Freedom verdedigt de grondrechten op privacy en communicatievrijheid op internet. Omdat de inrichting van het certificaatsysteem belangrijke implicaties heeft voor privacy op internet, volgen wij het Diginotar-incident met veel belangstelling. Bits of Freedom maakt graag van de gelegenheid gebruik om de problemen van het huidige certficaatsysteem en de rol van de Nederlandse overheid met u te delen:

   - Het huidige certificaat-systeem is inherent onveilig. Het is gebaseerd op de veronderstelling dat ongeveer 650 vertrouwde certificaatverstrekkers in de hele wereld geen valse certificaten verstrekken. Dat vertrouwen is onterecht, zoals het incident bij Diginotar onderstreept.
   - Meer toezicht op Diginotar en andere certificaatverstrekkers kan dit fundamentele probleem niet oplossen. De Nederlandse overheid kan hoogstens Nederlandse certificaatverstrekkers (iets) beter controleren. Omdat die controle de overige honderden certificaatverstrekkers echter niet raakt is het effect daarvan echter verwaarloosbaar.
   - In plaats daarvan moet het huidige certificaatsysteem fundamenteel worden herzien. Het certificaatsysteem is internationaal in gebruik voor talloze toepassingen. Het systeem zal dan ook op internationaal niveau moeten worden herzien. Daarbij spelen vele, uiteenlopende belangen.
   - De Nederlandse overheid moet deze herziening stimuleren. Ze kan dit doen door (i) op internationaal niveau de urgentie van de herziening van het huidige certificaat-systeem te benadrukken en (ii) onafhankelijk wetenschappelijk onderzoek naar de herziening van het certificaatsysteem te financieren. De overheid moet daarnaast bij het formuleren van beleid rekening houden met het feit dat het huidige certificaatsysteem maar een beperkte mate van veiligheid kan garanderen.

   Wij lichten deze punten hieronder toe.

Het huidige certificaat-systeem is inherent onveilig

2. Een systeem om de veiligheid van communicatie te waarborgen is van belang voor een goede werking van de informatiemaatschappij, onder meer voor online diensten, logistieke processen, communicatie tussen burgers en overheid en communicatie tussen burgers onderling.

3. Het huidige systeem werkt als volgt: als bezoeker A een verbinding legt met website B, krijgt bezoeker A een certificaat toegestuurd van website B. Met behulp van dit certificaat wordt een veilige verbinding opgezet tussen bezoeker A en website B. De fundamentele vraag is echter: hoe weet bezoeker A dat dit geen vals certificaat is van C, die zich voordoet als B? In dat geval zou het verkeer tussen A en B namelijk juist *niet* veilig zijn.

4. De belangrijkste manier om dit te garanderen, is door gebruikers erop te attenderen wanneer een mogelijk vals certificaat wordt gebruikt bij het opzetten van de verbinding. De gebruiker krijgt bij het huidige certificaatsysteem een waarschuwing als een website een certificaat gebruikt dat afkomstig is van een bedrijf dat niet op een witte lijst van vertrouwde certificaatverstrekkers staat (zie de **bijlage 1** voor een toelichting). Deze lijst wordt bijgehouden in internetbrowsers, zoals Internet Explorer en Firefox.

5. Dit systeem heeft een groot nadeel. Er staan namelijk ongeveer 650 bedrijven op de browserlijst van vertrouwde cerficaatverstrekkers, en die bedrijven komen uit alle landen. Al die bedrijven kunnen certificaten voor alle websites uitgeven, en browsers vertrouwen al deze certificaten: zo kan een Chinese certificaatverstrekker een certificaat voor google.com afgeven, maar ook een Nederlandse certificaatverstrekker – zoals Diginotar – kan dat doen. En het is naïef om erop te vertrouwen dat geen van deze certificaatverstrekkers een vals certificaat zal uitgeven, bijvoorbeeld omdat er ingebroken is en de inbrekers valse certificaten aanmaken, doordat een corrupte medewerker valse certificaten aanmaakt of onder druk van een overheid valse certificaten worden aangemaakt.

6. Denk hierbij aan Diginotar, die ondanks audits toch de meest basale beveiliging niet op orde had. Hun marketing doet overigens anders vermoeden: in ronkende taal schept Diginotar op over de beveiliging van haar systemen (**bijlage 2**). In werkelijkheid bleek haar beveiliging ver onder de maat, zoals het rapport van Fox-IT onderstreept.

> **Tussenconclusie: Het huidige certificaat-systeem is inherent onveilig, want het is gebaseerd op het vertrouwen dat ongeveer 650 certificaatverstrekkers over de hele wereld geen valse certificaten verstrekken, terwijl dat niet kan worden gegarandeerd – sterker nog, het is niet uitgesloten dat enkelen van die 650 certificaatverstrekkers op dit moment valse certificaten verstrekken.**

Meer toezicht op Diginotar kan dit fundamentele probleem niet oplossen

7. Het Diginotar-incident had verstrekkende gevolgen, maar is een symptoom van een fundamenteel probleem: het huidige certificaat-systeem is onveilig. Het uitgeven van valse certificaten, zoals bij Diginotar gebeurde, kan ook bij andere certificaatverstrekkers plaatsvinden. Zo bleek een half jaar geleden dat een grotere certificaatverstrekker, Comodo, ook valse certificaten had uitgegeven.

8. De belangrijkste conclusie van het Diginotar-incident is daarom, dat meer overheidsregulering of -toezicht het hierboven aangestipte fundamentele probleem niet kan verhelpen. De Nederlandse overheid zou Nederlandse certificaatverstrekkers in theorie aan strengere kunnen controles onderwerpen. Die verstrekkers zijn echter maar een fractie van de honderden certificaatverstrekkers in de hele wereld. Het systeem is ondertussen gebaseerd op het vertrouwen dat *al* de certificaatverstrekkers in de wereld geen valse certficaten verstrekken. Met andere woorden: extra overheidstoezicht op Nederlandse certificaatverstrekkers kan incidenten zoals bij Diginotar niet verhelpen.

> **Tussenconclusie: Meer toezicht op- of regulering van Nederlandse certificaatverstrekkers zal het fundamentele probleem van het aanmaken van valse certificaten niet kunnen voorkomen. Dit is dus slechts symptoombestrijding.**

9. Overigens is zeer de vraag of meer toezicht überhaupt een belangrijke bijdrage kan leveren aan de beveiliging van certificaatverstrekkers. Een systeem van audits levert maar een beperkte garantie op, zoals blijkt uit het Diginotar-incident waar ook periodiek audits werden uitgevoerd. In plaats daarvan zou, naast het controleren van de 'papieren werkelijkheid' ook de werkelijke beveiliging periodiek moeten worden gecontroleerd door middel van tests. Er kan worden overwogen om browserfabrikanten op te roepen om dit te eisen. Maar, zoals gezegd: ook dit is slechts een tijdelijke oplossing die het fundamentele probleem niet oplost.

Herziening certificaatsysteem noodzakelijk, maar is internationaal breed proces

10. Experts zijn het erover eens dat het huidige certificaatsysteem aan herziening toe is. Het is, zoals hierboven is toegelicht, fundamenteel onveilig. Dit klemt des te meer, nu door marktpartijen en belanghebbenden wel de suggestie van betrouwbaarheid wordt gewekt.

11. Het huidige certificaatsysteem is echter wereldwijd in gebruik. Het wordt gebruikt om websites te beveiligen. Het wordt in een iets aangepaste vorm gebruikt om de communicatie van interne processen te beveiligen (hierbij kan worden gedacht aan communicatie binnen de overheid, zoals uitkeringsinstanties, maar ook aan industriële processen, zoals JIT-manufacturing).

12. Doordat het huidige certficaatsysteem zo breed wordt ingezet, zal het systeem ook op internationaal niveau moeten worden herzien. Daarbij spelen vele, uiteenlopende belangen. Verschillende oplossingen worden overwogen, die allemaal voor- en nadelen hebben. De internationale gemeenschap heeft nog geen duidelijke keuze voor een specifiek systeem gemaakt.

Nederlandse overheid moet actieve bijdrage leveren aan discussie certificaat-systeem

13. De Nederlandse overheid kan als geen ander meepraten over de gevolgen van een onbetrouwbaar communicatiesysteem. Zij begrijpt uit eigen ervaring wat de verstrekkende gevolgen van het falen van het certificaatsysteem kunnen zijn. Zij heeft bovendien – evenals andere overheden, bedrijven en burgers – belang bij een veiliger certificaatsysteem.

14. De Nederlandse overheid moet de herziening van het certificaatsysteem daarom stimuleren. Ze kan dit doen door (i) op internationaal niveau de urgentie van de herziening van het

huidige certificaat-systeem te benadrukken en (ii) onafhankelijk wetenschappelijk onderzoek naar de herziening van het certificaatsysteem te financieren. De overheid moet daarnaast bij het formuleren van beleid rekening houden met het feit dat het huidige certificaatsysteem maar een beperkte mate van veiligheid kan garanderen.

> **Aanbeveling: De Nederlandse overheid moet op internationaal niveau de urgentie van de herziening van het certificaatsysteem benadrukken en onafhankelijk wetenschappelijk onderzoek naar de herziening van het certificaatsysteem financieren.**

We vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Ot van Daalen

Bijlage 1: de werking van het huidige certificaat-systeem

Een veilig communicatiesysteem garandeert drie dingen:

- **Authenticiteit**: als gebruiker A communiceert met website B, moet A zeker zijn dat hij ook daadwerkelijk met website B communiceert, en niet met C die het internetverkeer tussen A en B onderschept en zich voordoet als B.
- **Integriteit**: als gebruiker A informatie krijgt van website B, moet A zeker zijn dat de informatie die afkomstig is van B niet onderweg is veranderd, bijvoorbeeld doordat C het verkeer onderweg onderschept en manipuleert.
- **Vertrouwelijkheid**: als gebruiker A communiceert met website B, moet A zeker zijn dat de informatie die A en B uitwisselen niet in begrijpelijke vorm kan worden uitgelezen, bijvoorbeeld door C die het verkeer onderschept.

Het huidige certificaatsysteem is gebaseerd op de volgende controles om vast te stellen dat een certificaat vals is:

- In een certificaat wordt vermeldt voor welke website het geldt. Bijvoorbeeld: in het certificaat dat google.com gebruikt, staat vermeld dat het voor gebruik door google.com is bedoeld. Het probleem is echter dat iedereen een certificaat voor iedere website kan aanmaken: ook Bits of Freedom kan een certificaat aanmaken voor google.com. Ook C zou dus een certificaat van google.com kunnen aanmaken en gebruiken om het verkeer tussen A en B onderscheppen.
- Een oplossing voor dit probleem is om alleen vertrouwen te hebben in certificaten van bedrijven die controleren of een verzoeker ook recht heeft op een certificaat: deze bedrijven geven het certificaat voor google.com ook alleen maar aan Google, en niet aan de Iraanse overheid. Zo kan worden voorkomen dat C een vals google.com certificaat gebruikt om het verkeer tussen A en B te onderscheppen.
- Maar wie zijn deze vertrouwde certificaatverstrekkers? Het is niet haalbaar te verwachten dat elke internetgebruiker zelf een lijst van vertrouwde verstrekkers samensteld. In plaats daarvan worden lijsten van "algemeen vertrouwde" certificaatverstrekkers in webbrowsers, zoals Internet Explorer, Firefox en Google Chrome, ingebouwd. Browsers kunnen een certificaatverstrekker toevoegen aan deze vertrouwde lijst, als deze voldoet aan een aantal eisen op het gebied van informatiebeveiliging en audits. Diginotar was zo certificaatverstrekker die voldeed aan de eisen van de browserfabrikanten: Diginotar stond dus op de lijst van vertrouwde certificaatverstrekkers die in de browsers was ingebouwd.
- De gebruiker krijgt bij het huidige certificaatsysteem een waarschuwing als een website een certificaat gebruikt dat afkomstig is van een bedrijf dat niet op de witte lijst van vertrouwde certificaatverstrekkers van de browsers staat.

Bijlage 2

PINEWOOD
Specialist in netwerk- en databeveiliging

CASE STUDY:

DigiNotar
Internet Trust Services

DigiNotar verstevigt grip op secure omgeving met RSA enVision

Internet Trust Service Provider DigiNotar houdt zich in Nederland al tien jaar bezig met de ontwikkeling en levering van producten en diensten die zakelijk verkeer via internet meer zekerheid geven. De organisatie borgt alle stappen die nodig zijn voor het versturen van documenten en het sluiten van transacties via het web. Van het vaststellen van de identiteit van de betrokkenen en digitaal ondertekenen tot de veilige en betrouwbare opslag met logging. Al deze activiteiten leunen zwaar op de IT-infrastructuur, die vanzelfsprekend ook maximaal beveiligd moet zijn. Deze secure omgeving is in de loop der jaren uitgegroeid tot een complex geheel van systemen en appliances die uiteenlopende beheerinformatie genereren. Om deze omgeving effectiever te monitoren en automatisch op risico's te kunnen reageren, implementeert DigiNotar als een van de eerste Nederlandse organisaties een Security Information Event Management-oplossing (SIEM). Op advies van security-partner Pinewood is gekozen voor RSA enVision.

De producten en diensten van DigiNotar worden met notariële zekerheid geleverd aan de overheid, zakelijke dienstverleners als accountants, advocaten en notarissen, en andere bedrijven. Voorbeelden zijn identity management, elektronische handtekeningen, betrouwbare documentuitwisseling en elektronische archivering. Daarnaast levert de organisatie alle soorten identificatiemiddelen, van het eenvoudigste gebruikersnaam/wachtwoordsysteem en identificatie met een mobiele telefoon of bankkaart tot de zwaarste vorm van elektronische handtekening op smartcards. "Betrouwbaarheid, veiligheid en toetsbaarheid staan centraal in alles wat we doen", zegt Marcel Jak, Manager Sales & Consultancy bij DigiNotar. "Dat betekent dat we zelf natuurlijk aan de strengste normen en eisen op het gebied van beveiliging moeten voldoen, zowel fysiek als logisch. Fysiek houdt dat in dat de toegang tot onze opslagfaciliteit maximaal beveiligd is, onder andere met onafhankelijke biometrie, sluisdeuren et cetera. Voor logische toegangsbeveiliging speelt de toegangsautorisatie tot de systemen een grote rol. Onder andere met de toepassing van het 4 ogen-principe; voor essentiële handelingen is extra autorisatie vereist, bijvoorbeeld van de directie. Om zeker te weten dat we die beveiliging op orde hebben laten we externe auditers dat regelmatig testen."

Beschikbaarheid

Als relatief kleine organisatie die toch optimale beveiliging moet realiseren en in standhouden, laat DigiNotar zich op deelgebieden al zo'n tien jaar ondersteunen door specialisten van Pinewood. "De beveiliging van onze infrastructuur is de laatste jaren steeds specifieker geworden. Daarbij hebben we te maken met verschillende verkeersstromen. Intern en van en naar onze beveiligde omgeving. Naast diverse firewalls, antivirus- en antispamoplossingen gebruiken we ook IDS-applicaties (Intrusion Detection System). Verder zijn ook de kwetsbaarheden, bijvoorbeeld rondom phishing op poorten, op het DNS-vlak aangepakt met secure DNS-links. Een ander aspect van beveiliging dat steeds meer aandacht opeist, is de beschikbaarheid van onze systemen. Met load-balancing en goede uitwijkfaciliteiten garanderen we onze klanten dat ze altijd gebruik kunnen maken van onze diensten. Via onze authenticatiesystemen loggen onze klanten duizenden keren per dag aan op de beveiligde omgeving. Als dat om wat voor reden niet mogelijk is, heeft dat verregaande gevolgen voor de productiviteit van klantorganisaties. En dat geldt net zo goed voor de controle op de geldigheid van digitale handtekeningen of certificaten."

Volwassen security-organisatie

Het keuzetraject voor een SIEM-oplossing startte met een programma voor het beschrijven van de interne controlestructuur, zoals het vastleggen van procedures en de diverse verantwoordelijkheden en het toezicht daarop. “Elementaire vragen zijn dan: werkt de firewall? En wat gebeurt er als dat niet zo is? De antwoorden op deze vragen vergen een geïntegreerd platform voor het monitoren van de gehele IT-organisatie, inclusief maatregelen en rapportages.” Zo ontstond binnen DigiNotar de behoefte aan een intelligente oplossing die de enorme hoeveelheid gegevens van de onderdelen uit de complexe en bedrijfskritische beveiligingsomgeving van DigiNotar centraal kon verzamelen. Bovendien is het dan van belang dat de correlatie tussen deze gevarieerde informatie inzichtelijk is. “Zonder een dergelijk systeem moeten beheerders de log-informatie van elk afzonderlijk onderdeel beoordelen en zelf in relatie brengen met andere event-gegevens. Met behulp van RSA enVision beschikt DigiNotar over een compleet beeld van het functioneren van de security-organisatie. De belangrijkste systemen, risico’s en maatregelen zijn nu centraal te monitoren. De beschikbaarheid van informatie uit alle lagen van het netwerk biedt de beheer-organisatie de mogelijkheid om sneller en effectiever op te treden bij potentiële beveiligingsrisico’s. En belangrijker; risico’s zijn veelal te voorkomen. Zo streven we naar een volwassen risicomanagement en security-beheerorganisatie. ”

Omdat security verweven is met de gehele DigiNotar-organisatie is de implementatie van SIEM een lang-durig traject. Jak zegt daarover: “Het is essentieel om vooraf te definiëren wat je als beheerorganisatie wilt met de beschikbare informatie. Het onderling koppelen van de informatie uit verschillende systemen en log-bestanden moet namelijk wel toegevoegde waarde opleveren. Dat moet het monitoren van de goede werking van belangrijke security maatregelen vergemakkelijken of verbeteren. Daar doen we nu ervaring mee op.” De eerste SIEM-activiteiten zijn gericht op het secure netwerk voor de uitgifte en productie van digitale certificaten. Binnen deze omgeving zijn de Certificate Authorities en de ondersteunende productiesystemen en databases aan RSA enVision gekoppeld. DigiNotar zet RSA enVision nu bijvoorbeeld in om te monitoren of specifieke processen wel binnen de gestelde tijd gebeuren. “Bij het verstrekken en vooral het intrekken van een certificaat moet binnen vier uur een zogenaamde CRL-lijst (Certificate Revocation List) aangemaakt worden. Deze lijst geeft de status van de uit te geven certificaten weer, bijvoorbeeld of deze ingetrokken zijn. Met behulp van RSA enVision kunnen we dit proces monitoren, eventuele maatregelen nemen en bovenal bewijzen dat we die afspraken ook daadwerkelijk nakomen.”

Voortdurend aanscherpen

Hoewel DigiNotar een relatief kleine beheerorganisatie heeft, voert het de implementatie zelfstandig uit. Jak: “Pinewood heeft in de oriëntatiefase geadviseerd en levert waar nodig extra ondersteuning. Daarbij is het zeer praktisch dat hun specialisten ons als jaren op diverse vlakken ondersteunen en niet alleen onze IT-infrastructuur goed kennen, maar ook onze hands-on bedrijfscultuur. Dat vergemakkelijkt de samen-werking aanzienlijk. Hoewel we aan het begin van het SIEM-traject staan, zien we deze implementatie als een belangrijke stap in het voortdurende proces om de betrouwbaarheid van onze dienstverlening aantoonbaar ‘transparant’ te verbeteren. Juist als Internet Trust Service Provider moeten we op dat vlak voorop lopen en de beveiliging voortdurend aanscherpen.”

Marcel Jak