GOVCERT.NL

Factsheet FS 2011-07

DigiNotar certificaten en machine-to-machine (M2M) communicatie

Op 29 augustus 2011 is bekend geworden dat een frauduleus uitgegeven certificaat van DigiNotar in omloop is voor Google.com, als gevolg van een inbraak. Op 2 september zijn de uitkomsten van een nader onderzoek door Fox-IT gedeeld met de overheid, waarna de overheid het vertrouwen in de certificaten van DigiNotar heeft opgezegd.

DigiNotar is een van oorsprong Nederlands bedrijf dat zogenaamde SSL-certificaten uitgeeft. Deze certificaten dienen ter identificatie van websites en beveiliging van webverkeer. De ontdekking van het frauduleuze certificaat heeft er uiteindelijk toe geleid dat het *Root Certificate Authority* certificaat en de *sub root* van DigiNotar door verschillende softwarefabrikanten niet meer vertrouwd wordt.

De feiten op een rij:

- De Nederlandse overheid zegt het vertrouwen in certificaten van DigiNotar op, maar trekt PKIoverheid certificaten niet in.
- Software fabrikanten stellen updates beschikbaar.
- Machine-to-machine (M2M) communicatie die plaatsvindt op basis van DigiNotar certificaten kan verstoord worden.
- Als u gebruikmaakt van Diginotar certificaten, dan zult u over moeten stappen op een alternatieve aanbieder voor nieuwe certificaten en het installeren van updates uitstellen.
- Als u geen gebruik maakt van Diginotar certificaten kunt u direct beschikbare updates installeren.

Een uitgebreide beschrijving van de huidige situatie kunt u terugvinden in FS 2011-06. Dit factsheet richt zich specifiek op de mogelijke impact voor machine-to-machine (M2M) communicatie en de stappen die u kunt doorlopen om de impact op die communicatie te beperken.

Wat is er aan de hand?

Als gevolg van de inbraak bij DigiNotar heeft de Nederlandse overheid het vertrouwen in alle certificaten uitgegeven door DigiNotar opgezegd. De overheid heeft echter besloten om de PKIoverheid certificaten uitgegeven door DigiNotar niet in te trekken om te voorkomen dat M2M communicatie verstoord wordt. M2M communicatie vindt uitsluitend plaats tussen machines onderling. Het gaat hier bijvoorbeeld om versleutelde gegevensuitwisseling tussen servers, voor interne bedrijfsprocessen en tussen bedrijven onderling. Door een verstoring van M2M communicatie zou communicatie verbroken worden of niet op gang komen en worden bedrijfsprocessen geraakt.

Een verstoring kan ontstaan omdat meerdere software fabrikanten het vertrouwen in DigiNotarcertificaten hebben ingetrokken, en daarvoor ook technische maatregelen in hun producten hebben opgenomen of gaan opnemen. Dit gebeurt op verscheidene manieren afhankelijk van het operating system en de software fabrikant. Het grootste onderscheid is centraal (Microsoft) vs. decentraal (Linux).

Microsoft

Microsoft Windows maakt gebruik van een “Certificate Store” waarin zowel vertrouwde als niet-vertrouwde certificaten zijn opgenomen. Naast Browsers kunnen ook andere applicaties hier gebruik van maken. Binnen de Certificate Store zijn verschillende lijsten aanwezig met certificaten. De root Certificate Authorities (CA’s) zijn opgeslagen in de lijst met “Trusted Root Certification Authorities”. In deze lijst zijn onder meer de Diginotar root CA en de Staat der Nederlanden root CA’s aanwezig. Het Diginotar root CA is door Microsoft uit deze lijst verwijderd.

Een andere lijst binnen de Cerificate Store is een lijst van “Untrusted Certificates”. Deze lijst biedt de mogelijkheid om certificaten die geen root certificate zijn toch te weigeren. De Diginotar PKIOverheid

Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postbus 117
2501 CC Den Haag

T 070 888 7 555
E info@govcert.nl
I www.govcert.nl

sub-CA certificaten die onder de Staat der Nederlanden roots vallen zijn hierin door Microsoft opgenomen.

Microsoft heeft een update uitgebracht die de DigiNotar certificaten blokkeert op Windows systemen. De update wordt voor Windows-installaties in Nederland niet verplicht, maar als optioneel aangeboden. Op de Patch Tuesday van 13 september 2011 zal de update echter niet meer als optioneel aangemerkt worden en ook op Nederlandse Windows-installaties automatisch geïnstalleerd worden.

De Microsoft update kan na installatie eenvoudig worden teruggedraaid door een roll-back van de patch te doen. Daarna worden de Diginotar certificaten door het systeem weer vertrouwd. Doe dit alleen als het noodzakelijk is.

Linux- en aanverwante systemen

Voor Linux bestaat geen eenduidig mechanisme. Daarnaast is de toepassing van identieke pakketten op verschillende Linux-versies uiteenlopend. Het certificatenbeheer is hierdoor veelal applicatiespecifiek. Drie veelvuldig gebruikte oplossingen voor SSL-implementatie in Linux- en aanverwante systemen zijn: OpenSSL, GnuTLS en Mozilla NSS. Zowel OpenSSL als GnuTLS maken geen gebruik van standaard lijsten van vertrouwde certificaten. Sommige Linux-distributies voegen echter wel een lijst met vertrouwde certificaten toe aan de OpenSSL-packages die zij distribueren.

Debian levert bijvoorbeeld met het *ca-certificates* package een lijst met vertrouwde root certificaten mee, waar het DigiNotar root certificaat binnenkort uit verwijderd zal worden. Aangezien *ca-certificates* alleen root certificaten bevat, heeft dit géén consequenties voor DigiNotar PKIoverheid-certificaten. *Ca-certificates* is overigens ook beschikbaar voor andere distributies zoals Ubuntu en CentOS.

NSS (Network Security Service) is een mechanisme dat onder andere gebruikt wordt door Firefox en Google Chrome. Met NSS wordt een NSSCKBI database met standaard certificaten meegeleverd. Daarin is het vertrouwen in diverse DigiNotar certificaten inmiddels al opgezegd. Gebruikers hebben echter de mogelijkheid om vanuit de applicaties die gebruik maken van NSS een uitzondering toe te voegen voor de DigiNotar certificaten.

Wat voor mogelijke impact heeft de situatie voor u?

Door het verschil in aanpak is de potentiële impact ook divers. Mocht u gebruikmaken van Microsoft producten, dan kunnen na het installeren van de update, problemen ontstaan. Machines die gebruik maken van DigiNotar certificaten voor wederzijdse communicatie zullen elkaar niet meer vertrouwen. Dit heeft gevolgen omdat er geen communicatie wordt opgezet tussen de systemen en er geen gegevenswisseling tussen de machines meer mogelijk is. Als één van de twee systemen de update gedraaid heeft kan dit probleem al optreden.

Voor Linux platformen is de kans dat er zich, naar aanleiding van automatische updates, problemen voordoen op het gebied van M2M moeilijker in kaart te brengen dan bij Microsoft. Op basis van de gebruikte oplossingen lijkt de kans op soortgelijke problemen qua omvang en impact als bij Microsoft onwaarschijnlijk.

Wat kunt u doen?

1. Maak allereerst een inventarisatie om te bepalen of uw systemen gebruik maken van DigiNotar certificaten. Beantwoord tijdens deze inventarisatie de volgende vragen:
    a. Maakt u gebruik van DigiNotar certificaten voor uw bedrijfsprocessen?
        i. Ja, ga verder met vraag b.
        ii. Nee, dan raden wij u aan om direct beschikbare updates te installeren.
    b. Waar staan de certificaten?
        i. Intern

Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postbus 117
2501 CC Den Haag

T 070 888 7 555
E info@govcert.nl
I www.govcert.nl

   ii. Extern (certificaat is aanwezig bij andere partij waarmee gecommuniceerd moet worden)
c. Wat is hun functie?
   i. Verificatie van identiteit
   ii. Versleuteling
d. Welke bedrijfsprocessen zijn afhankelijk van communicatie gebaseerd op DigiNotar certificaten?

2. Als u gebruik maakt van Diginotar certificaten, dan zult u over moeten gaan op nieuwe certificaten van een alternatieve leverancier. Hierdoor zult u het installeren van updates moeten uitstellen totdat de nieuwe certificaten gearriveerd zijn.

Migratietips

Tijdens het migreren zult u wellicht hinder ondervinden en kunnen uw bedrijfsprocessen hieronder lijden. De informatie uit de inventarisatie moet daarom meegenomen worden in de besluitvorming rondom de migratie. Om de gevolgen te beperken geven wij een aantal tips om de migratie voorspoediger te laten verlopen.

1. Afhankelijk van de hoeveelheid systemen en de aard van de afhankelijkheid van DigiNotar certificaten, kunt u ervoor kiezen om de overgang gefaseerd te laten verlopen. Dit houdt in dat u systemen parallel draait.
2. U kunt rekening houden met de timing en de migratie zoveel mogelijk laten plaatsvinden op momenten waarop de dienstverlening en bedrijfsprocessen het minst gebruik maken van de systemen.
3. U kunt communicatie inlichten of opzetten om het contact met klanten voor te bereiden zodat vragen en onbegrip beperkt blijven.