

Factsheet FS 2011-06

Frauduleus uitgegeven beveiligingscertificaat ontdekt

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.

Dit factsheet geeft een korte beschrijving van de situatie, risico's voor burgers en bedrijven en mogelijke maatregelen. Tenslotte beschrijft deze factsheet ook beknopt de werking van beveiligingscertificaten.

Zodra nieuwe feiten bekend worden zullen wij dit factsheet aanpassen. In de rechterbovenhoek van deze factsheet vindt u datum en tijdstip waarop de factsheet is gepubliceerd.

Wat is er gebeurd?

In juli 2011 is ingebroken op computersystemen van Diginotar. Daarna hebben de inbrekers honderden frauduleuze beveiligingscertificaten aangemaakt. Op dit moment is niet precies bekend hoeveel en welke certificaten frauduleus zijn uitgegeven.

Diginotar detecteerde deze inbraak op 19 juli 2011. Diginotar heeft deze informatie destijds niet naar buiten gebracht. Door een melding van GOVCERT.NL over de ontdekking van het frauduleus uitgegeven certificaat van google.com dat in het wild is gesignaleerd, is geconcludeerd dat in ieder geval één frauduleus certificaat niet was ingetrokken.¹

De eerste publieke signalen die uiteindelijk hebben geleid tot bekendmaking van dit incident, zijn in gang gezet door iemand in Iran die op 27 augustus 2011 op een Google forum aangaf hoe hij in probeerde te loggen op zijn gmail-account en van zijn browser² een waarschuwing kreeg over de betrouwbaarheid van het certificaat.³ Het bleek na verificatie inderdaad te gaan om een frauduleus certificaat. Het incident is, zoals later bekend werd, niet beperkt gebleven tot Google.com.

Op 2 september heeft de Nederlandse overheid bekend gemaakt het vertrouwen in certificaten van Diginotar op te zeggen. Dit in reactie op de uitkomsten van een onderzoek door Fox-IT op de systemen de Diginotar, nadat eerder bekend werd dat op die systemen was ingebroken.

De feiten op een rij:

- > De Nederlandse overheid zegt het vertrouwen in certificaten van Diginotar op.
- > Na inbraak bij Diginotar zijn waarschijnlijk honderden frauduleuze certificaten aangemaakt.
- > Een frauduleus certificaat voor google.com is daadwerkelijk door kwaadwillenden gebruikt.
- > Tussen de frauduleuze certificaten die bekend zijn, bevinden zich geen Nederlandse overheidscertificaten.
- > Bezoekers van websites kunnen meldingen krijgen dat websites niet meer vertrouwd worden.
- > Server-to-server communicatie die plaatsvindt op basis van Diginotar certificaten kan verstoord worden.
- > De Nederlandse Overheid neemt het operationeel beheer over bij Diginotar..
- > Meer informatie vind u op www.rijksoverheid.nl
- > Voor publieksvragen kunt u bellen met 0800-1351

¹ GOVCERT.NL is in een vroeg stadium ingelicht door CERT-Bund, een partner uit haar internationale CERT-netwerk.

² De forumposter maakte gebruik van Chrome als browser, welke als product van Google hardere checks geïmplementeerd lijkt te hebben wanneer gebruikers google.com of gerelateerde diensten bezoeken.

³ <http://www.google.co.uk/support/forum/p/gmail/thread?tid=2da6158b094b225a&hl=en>

Waarom zegt de overheid het vertrouwen in alle certificaten van Diginotar op?

Diginotar als bedrijf geeft twee typen certificaten uit: certificaten onder eigen naam, en certificaten voor de *Public Key Infrastructure (PKI)* van de Nederlandse overheid (PKIOverheid). Technisch gezien zijn dit twee aparte *root certificates*. In eerste instantie leek het erop dat alleen op de systemen voor Diginotar's eigen certificaten ingebroken was. Nader onderzoek heeft uitgewezen dat ook op de systemen voor PKIOverheidscertificaten was ingebroken.

Deze kennis is voor de Nederlandse overheid reden om het vertrouwen in alle certificaten van Diginotar op te zeggen. Hoewel uit het onderzoek niet blijkt dat na de inbraak op de systemen ook frauduleuze PKIOverheidscertificaten zijn aangemaakt, valt dit niet met voldoende zekerheid uit te sluiten.

De Nederlandse overheid trekt het Diginotar PKIOverheidscertificaat niet in, waarom?

De Nederlandse overheid vertrouwt de certificaten niet meer, maar trekt op dit moment geen certificaten in (er wordt geen certificaat 'gerevoket'). Door het intrekken van certificaten krijgt een gebruiker een waarschuwing dat de website geen vertrouwde website meer is. Echter wordt door het intrekken ook de communicatie tussen computersystemen verstoord.

Het gaat hier bijvoorbeeld om versleutelde gegevensuitwisseling tussen servers, voor interne bedrijfsprocessen en tussen bedrijven onderling. De continuïteit van dergelijke processen kan in gevaar komen bij terugtrekking van de certificaten. De certificaten worden hierbij meestal primair gebruikt voor versleuteling, en niet voor het vaststellen van de identiteit van de andere partij.

Wat gebeurt dan nu met de certificaten en wat doen browserfabrikanten?

De Nederlandse overheid neemt vanaf 3 september het beheer over van de systemen van Diginotar die betrokken zijn bij de certificaten. De systemen zullen nauwkeurig worden gemonitord om verder misbruik te voorkomen. Dit is een overgangsfase, die langzaam zal worden afgebouwd.

Browserfabrikanten zullen het vertrouwen in Diginotar certificaten ook intrekken, en daarvoor ook technische maatregelen in hun producten nemen. Sommige fabrikanten hebben dit al gedaan, anderen werken hieraan.

Zijn uw persoonsgegevens in gevaar?

Mogelijk heeft u in de afgelopen periode, na de inbraak bij Diginotar, persoonsgegevens verstuurd over een beveiligde verbinding met een website die een Diginotarcertificaat gebruikt.

Op basis van kennis over de inbraak, en over het waarschijnlijke motief van de inbreker, is het vrijwel uit te sluiten dat in het voorgaande scenario uw gegevens in Nederland zijn afgeluisterd of gestolen.

Wat betekent dit voor burgers en wat kunt u doen?

Wij raden u aan om zo spoedig mogelijk de updates van uw browser en besturingsstelsel te installeren, zodra deze beschikbaar zijn. U weet dan zeker dat uw browser onvertrouwde Diginotarcertificaten zal weigeren.

Als u een website bezoekt die een Diginotar-certificaat gebruikt, en daarmee een beveiligde verbinding opzet (dit gebeurt vanzelf), dan zult u een waarschuwing krijgen, omdat uw browser het certificaat niet vertrouwt en niet kan garanderen dat u met de juiste website een verbinding heeft.

Als dit gebeurt, dan raden wij u aan om verder contact met de website te verbreken. In het geval van niet-urgente zaken kunt u overwegen om te wachten en het over enkele dagen nog eens te proberen. In het geval van urgente zaken raden wij u aan contact op te nemen met de betreffende instantie.

Wat zijn de gevolgen voor bedrijven?

De intrekking van certificaten door Diginotar en softwarefabrikanten heeft twee gevolgen:

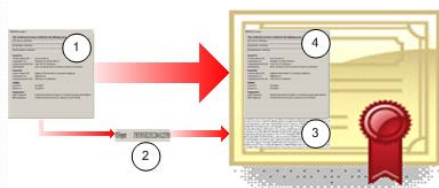
- Communicatie tussen computersystemen (intern, of tussen bedrijven) die gebruik maakt van Diginotarcertificaten (voor bijvoorbeeld versleuteling) kunnen verstoord worden als de certificaten niet meer vertrouwd worden door de betreffende programma's. Hierdoor kunnen bedrijfsprocessen verstoord raken. Dit is in het bijzonder een aandachtspunt bij programma's die op Windows draaien en mogelijk gebruik maken van Microsoft's *certificate trust list*. Let dus zeer goed op als Microsoft updates uitbrengt die aanpassingen maken in deze trust list en installeer deze alleen u zeker weet dat dit geen negatieve gevolgen heeft voor programma's en processen die daar gebruik van maken.
- Bezoekers van uw website kunnen een pop-up met een waarschuwing krijgen als ze gebruik maken van een beveiligde verbinding met uw website als u gebruikt maakt van DigiNotar certificaten. Dit is bijvoorbeeld het geval als bezoekers gevraagd wordt om persoonsgegevens op uw website in te vullen. Deze waarschuwing zal komen nadat gebruikers een browser update hebben geïnstalleerd.⁴ Hierdoor is de bezoeker niet meer in staat de betrouwbaarheid van uw website te verifiëren. Wellicht nemen zij contact met u op of maken zij geen gebruik meer van uw dienstverlening.

Wij raden u voor de continuïteit van uw dienstverlening aan om zo snel mogelijk over te stappen op een nieuw certificaat van een andere dienstverlener.⁵

Achtergrondinformatie over certificaten

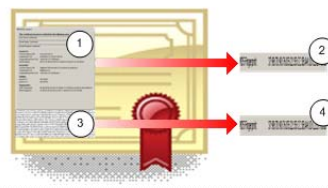
Om versleutelde digitale communicatie tot stand te brengen tussen een browser en een website wordt gebruik gemaakt van SSL/TLS certificaten. Als een certificaat ondertekend is door een officiële Certificate Authority (een *root CA*) wordt deze automatisch vertrouwd door alle gangbare browsers. Een CA stelt de spelregels voor wanneer zij (al dan niet na betaling) een certificaat als "door hen gecontroleerd" willen ondertekenen. Via een SSL/TLS certificaat worden websites en webverkeer beveiligd, wat tot uitdrukking komt in de 's' in *https* en het bekende 'slotje' of een gekleurde adresbalk. Hierdoor ontstaat aan de kant van de gebruiker vertrouwen dat hij te maken heeft met een authentieke en betrouwbare versie van de website.

Een digitale handtekening zetten en controleren



Ondertekenen

Een ondertekend certificaat wordt als volgt gemaakt. De Certificate Authority (CA) ontvangt gegevens van de aanvrager (1). Hierover berekent de CA een hash (2). De CA versleutelt de hash (3). Dit vormt samen met de oorspronkelijke gegevens (4) het ondertekende certificaat.



Controleren

Een browser controleert een certificaat als volgt. Van de oorspronkelijke gegevens op het certificaat (1) berekent de browser een hash (2). Daarna ontcijfert de browser de hash die door de CA is versleuteld (3). Als beide hashes (2 en 4) hetzelfde zijn dan is het certificaat niet gewijzigd en dus te vertrouwen.

⁴ In het verleden zijn ook Entrust certificaten uitgegeven door Diginotar. Voor deze certificaten krijgen alle gebruikers, ongeacht de status of versie van hun browser, een waarschuwing.

⁵ Op de website www.pkioverheid.nl kunt u een overzicht vinden van certificaatuitgevers voor de overheid.