Beveiliging kan sterk worden verbeterd

Veel kritiek op werkwijze DigiD

Elektronisch legitimeren wordt steeds meer geaccepteerd. Sinds enkele jaren kennen we in Nederland DigiD, maar regelmatig haalt DigiD op negatieve wijze de landelijke media. Hoe veilig is DigiD? Kan de beveiliging van DigiD worden verbeterd? Moet de overheid verantwoordelijk blijven voor de beveiliging van DigiD?

Arjan Hassing

De opkomst van internet heeft veel soorten van dienstverlening in de wereld veranderd. Zo ook de wijze waarop we ons kunnen legitimeren bij de overheid. De traditionele wijze van legitimeren bestaat uiteraard nog steeds – en is voorlopig ook nog niet weg te denken – maar al naar gelang het gebruik van internet steeds meer gemeengoed wordt, wordt elektronisch legitimeren ook steeds meer geaccepteerd. Het aantal personen dat een papieren inkomstenbelastingaangifte doet ligt in Nederland onder de 5 procent. De Nederlandse overheid stimuleert het gebruik van digitale dienstverlening en heeft de wens om vanaf 2017 papierloos te zijn. Sinds enkele jaren kennen we in Nederland DigiD (in België bestaat een vergelijkbaar initiatief: e-ID), maar regelmatig haalt DigiD op negatieve wijze de landelijke media. De DigiNotar-affaire[1] uit 2011 is waarschijnlijk het bekendste schandaal. Hoe veilig is DigiD? Kan de beveiliging van DigiD worden verbeterd? Moet de overheid verantwoordelijk blijven voor de beveiliging van DigiD?

Historie

DigiD is in Nederland in 2003 gelanceerd onder de naam NAV (Nieuwe Authenticatie Voorziening). In oktober 2004 werd de naam gewijzigd in DigiD, een afkorting van Digitale Identiteit. Vanaf 1 januari 2005 kunnen alle burgers van Nederland zich bij overheidsorganisaties identificeren via internet en kunnen alle overheidsinstellingen in Nederland zich aansluiten op DigiD. DigiD is gekoppeld aan het burgerservicenummer (BSN) en in beheer bij de gemeenschappelijke beheerorganisatie van de overheid: Logius.[2] Eind 2013 waren er ruim 10 miljoen DigiD's aan burgers in Nederland uitgegeven. DigiD is aanvankelijk ontwikkeld voor de overheid (gemeenten, Belastingdienst, UWV, SVB) maar de semi-overheid (zoals zorgverzekeraars, ziekenhuizen en onderwijsinstellingen) maakt er tegenwoordig ook gebruik van. Daarnaast zijn er initiatieven, door bijvoorbeeld notariskantoren, waardoor het gebruik onder voorwaarden ook buiten de overheid plaatsvindt.

Beveiligingsniveaus

DigiD heeft drie beveiligingsniveaus: basis, midden en hoog. Hoe hoger het beveiligingsniveau, hoe strenger de veiligheidsmaatregelen, maar ook hoe meer diensten er kunnen worden afgenomen.

- **Beveiligingsniveau basis:** DigiD van dit niveau is alleen gebruikersnaam en wachtwoord. Dit is het eenvoudigste en meest gebruikte type DigiD. Aan de gebruikersnaam wordt enkel de eis gesteld dat deze uniek is en uit minimaal zes karakters bestaat. Recentelijk zijn de eisen aan het wachtwoord strenger geworden: lengte minimaal acht karakters, minimaal één hoofdletter, één kleine letter, één cijfer en één leesteken. Periodiek wijzigen van het wachtwoord is niet verplicht gesteld.

Hoe werkt het?

De burger kan op de website www.digid.nl een gebruikersnaam aanvragen. Het opgegeven adres moet in ieder geval hetzelfde zijn als wat in de Gemeentelijke Basisadministratie (GBA) staat als bekend woonadres van de aanvrager. De aanvrager kan zelf een DigiD-gebruikersnaam en wachtwoord kiezen. De gebruikersnaam dient uniek te zijn en Logius voert hierop controle uit. Vervolgens krijgt de burger een activeringscode op papier thuisgestuurd waarmee hij op zijn gebruikersnaam kan activeren. Met één inlogcode en bijbehorend wachtwoord kan de burger terecht bij de elektronische diensten van de aangesloten instellingen. Om een elektronische dienst af te nemen met DigiD wordt de burger van de website van de instelling doorgeleid naar de inlogpagina van DigiD. Hier logt de burger in en, nadat de identiteit is geverifieerd, kan de burger de dienst afnemen. De DigiD-website voert de controle op de identiteit uit, waardoor de afnemende websites die controle niet meer zelf hoeven uit te voeren. Een DigiD verloopt indien deze drie jaar niet wordt gebruikt. De burger krijgt een waarschuwingsmail zeven dagen voordat de driejaarstermijn verstrijkt.
Er wordt vooralsnog geen voorziening geboden voor vertegenwoordiging. Omdat DigiD strikt persoonlijk is, is het de eigenaar van een DigiD niet toegestaan zijn gebruikersnaam en wachtwoord aan een andere persoon uit te lenen. Gebruik van de DigiD van een ander, hoewel vanaf het internet nauwelijks te bewijzen valt of er mondeling toestemming is gegeven, wordt juridisch beschouwd als identiteitsfraude. Wel kan in sommige gevallen een andere persoon voor de authenticatie zorgdragen door zelf zijn eigen DigiD te gebruiken. In dat geval zal de overheidsorganisatie van wie een dienst wordt afgenomen – in aanvulling op DigiD – controle uitvoeren op de rechtmatigheid van de authenticatie ten opzichte van de dienst.

- **Beveiligingsniveau midden:** Het is mogelijk om DigiD via verificatie met behulp van sms uit te breiden. Daarvoor moet dan op de DigiD-website worden aangegeven dat authenticatie per sms wenselijk is, waarbij een mobiel telefoonnummer moet worden opgegeven. In dat geval moet na aanmelding op een DigiD-compatible website met DigiD-gebruikersnaam en wachtwoord, ook de per sms ontvangen eenmalig geldige transactiecode worden ingevoerd.

- **Beveiligingsniveau hoog:** Dit niveau bevindt zich nog in de ontwerpfase en krijgt de vorm van een elektronische identiteitskaart (eID). Dit beveiligingsniveau maakt gebruik van PKI-certificaten[3] waarbij een derde partij – de zwaar beveiligde certificaatautoriteit – de integriteit en authenticiteit van het certificaat waarborgt en daarmee instaat voor de identiteit van de certificaatbezitter.

ICT-beveiligingsassessment DigiD

Organisaties die over een DigiD-aansluiting beschikken dienen (gefaseerd) met ingang van 2012 jaarlijks hun ICT-beveiliging te (laten) toetsen middels een ICT-beveiligingsassessment DigiD. Deze assessment wordt onder verantwoordelijkheid van een Register EDP-Auditor (RE) uitgevoerd, welke is ingeschreven in het register van de NOREA.[4] Bij de uitvoering van ICT-beveiligingsassessments DigiD wordt de "Norm ICT-beveiligingsassessments DigiD" (d.d. 21 februari 2012) gehanteerd. Deze norm bevat een selectie van de 59 richtlijnen uit het document "ICT-beveiligingsrichtlijnen voor webapplicaties" van het Nationaal Cyber Security Centrum (NCSC) dat in samenspraak met publieke en private partijen is opgesteld. In de ICT-beveiligingsassessment worden 28 beveiligingsrichtlijnen getoetst en dient de Register EDP-auditor een oordeel te geven over de opzet en het bestaan[5] per beveiligingsrichtlijn. De Register EDP-Auditor schrijft een rapportage met de uitkomsten van zijn onderzoek en stemt de conceptrapportage af met de eigenaar van de DigiD-aansluiting. Laatstgenoemde zendt de rapportage naar Logius welke op basis hiervan besluit of de aansluiting operationeel blijft of niet.

Zwakheden in DigiD

De afgelopen jaren is er vanuit verschillende hoeken kritiek geuit op de huidige werkwijze van DigiD, met name rond de beveiliging van DigiD. De kritiek komt neer op de volgende punten:

1. Momenteel wordt een DigiD-activeringscode op aanvraag via de post uitgereikt (ofwel door de postbode in de brievenbus van de aanvrager gestopt). Aangezien er bij de uitreiking geen authenticatie tegen een legaal identiteitsbewijs

plaatsvindt, is er geen volledige zekerheid over de daadwerkelijke identiteit van de DigiD-gebruiker. Uitsluitend de DigiD-gebruikersnaam en het bijbehorende wachtwoord zijn benodigd ter identificatie van een persoon.

2. Mede omdat niet afgedwongen wordt om het wachtwoord periodiek te wijzigen is het uitlekken van de DigiD-gebruikersnaam en -wachtwoord voldoende om de identiteit van een persoon te misbruiken. Bijvoorbeeld fiscale partners die gezamenlijk aangifte doen moeten beide met hun DigiD een aangifte ondertekenen. Het ligt voor de hand dat de partner die de aangifte indient ook de DigiD van de andere partner kent en de digitale identiteit van die partner kan overnemen. In geval van scheiding is het aan te bevelen aan de niet-indienende partner zo snel mogelijk het wachtwoord te veranderen.

Met het ICT-beveiligingsassessment wordt een grote mate van schijnveiligheid geboden

3. De ICT-beveiligingsassessment DigiD beslaat slechts 28 van de 59 beveiligingsrichtlijnen van het NCSC en toetst bovendien slechts op opzet en bestaan van beveiligingsrichtlijnen. Dat betekent dat als bij de onderzochte DigiD-aansluiting de 28 beveiligingsrichtlijnen effectief zijn ten tijde van het onderzoek, de auditor positief oordeelt en de aansluiting gehandhaafd blijft. Met een dergelijke assessment wordt een grote mate van schijnveiligheid geboden; waarschijnlijk hebben NOREA en Logius gekozen voor een praktische en snel uit te voeren assessment waarbij de kosten voor de instelling met DigiD-aansluiting beperkt blijven.

4. Het gebruiksgemak kan beter. Een burger gebruikt zijn DigiD nog maar beperkt, ongeveer een- à tweemaal per jaar. Dit leidt ertoe dat de burger zijn gebruikersnaam en/of wachtwoord vergeet of kwijtraakt. Dan moet een nieuw DigiD-account worden aangevraagd, waarbij het gehele registratieproces opnieuw moet worden doorlopen. Dit betekent extra werk voor de beheerorganisatie van DigiD, die nieuwe gegevens moet uitgeven voor dezelfde burgers. De burger moet extra handelingen verrichten en moet wachten op zijn nieuwe gegevens.

5. De overheid is eigenaar van DigiD maar is geen gerechtvaardigde partij in transacties buiten het overheidsdomein. Dat betekent dat DigiD niet buiten de overheid gebruikt zou kunnen worden omdat de overheid niets te maken heeft met transacties tussen een individuele burger en een webwinkel of weblog. De overheid wenst ook geen verantwoordelijkheid te hebben voor transacties tussen burgers en commerciële instanties.

6. De afhankelijkheid van één authenticatiedienst die door de overheid wordt geleverd maakt deze kwetsbaar. Er worden hoge eisen gesteld aan de beschikbaarheid, vertrouwelijkheid en integriteit die door het DigiD-platform geboden moeten worden, immers (1) een simpele DDoS-aanval[6] heeft vergaande consequenties voor de beschikbaarheid dienstverlening; (2) een grote databank met vertrouwelijke gegevens is een dankbaar doelwit voor aanvallers; (3) het is juridisch en organisatorisch lastig om commerciële partijen afhankelijk te laten zijn van de betrouwbaarheid van het aanmeld- en beheerproces voor DigiD bij de overheid.

Toekomst

Gegeven de punten van kritiek die in de voorgaande sectie zijn genoemd, dienen naar mijn mening de volgende oplossingsrichtingen te worden onderzocht:

1) Richt een PKI-infrastructuur in zodat het beveiligingsniveau 'hoog' wordt bereikt voor de authenticatie via DigiD. De certificaatautoriteit zou aanbesteed kunnen worden aan marktpartijen (zie punt 5).

2) Pas het proces van uitreiking van DigiD aan waarbij de aanvrager zich met een klassiek identiteitsbewijs dient te legitimeren om de activeringscode in ontvangst te nemen. De activeringscode zou niet meer per post verstuurd moeten worden maar bijvoorbeeld op het gemeentehuis opgehaald kunnen worden.

3) De strengere eisen aan wachtwoorden zijn een stap in de goede richting, maar technisch dient nog afgedwongen te worden dat de gebruiker periodiek – bijvoorbeeld elke zes maanden – zijn wachtwoord dient te veranderen. Bovendien mogen wachtwoorden niet lijken op de laatste tien gebruikte wachtwoorden;

4) Laat de IT-auditor de DigiD-aansluiting toetsen op alle 59 beveiligingsrichtlijnen van het normenkader voor webapplicaties van het NCSC en bovendien een toets doen op de werking van de beveiligingsrichtlijnen. Een volgende stap zou kunnen zijn het beheersproces van beveiliging te toetsen in plaats van de feitelijk beveiligingsinstellingen.

5) Haal DigiD weg bij de overheid en geef het in handen van een onafhankelijke organisatie die zowel overheid als het commerciële bedrijfsleven kan bedienen. Naar mijn mening zou het beheer van DigiD aanbesteed moeten worden in de markt. Het toezicht op de onafhankelijk organisatie zou mijns inziens wel bij de overheid belegd moeten worden.

6) Stel hoge eisen aan de onafhankelijke organisatie als het gaat om beschikbaarheid, vertrouwelijkheid en integriteit. Veel grote rekencentra in Nederland voldoen reeds aan hoge eisen op genoemde gebieden en ondergaan in de praktijk periodiek reeds zware ISAE 3402- en ISO 27001-audits.

Tot slot

'Leuker kunnen we het niet maken' luidt de slogan van de Belastingdienst en dat geldt in mijn ogen ook voor DigiD. De beveiliging van DigiD kan sterk worden verbeterd en bovendien dient DigiD naar mijn mening bij de overheid weggehaald te worden. Die aanpassingen zullen gepaard gaan met hogere kosten en die zullen op de een of andere manier weer afgewenteld worden op de burger. De ontwikkelingen lijken echter onvermijdelijk en dat er misbruik van DigiD wordt gemaakt wil ook niemand. Schandalen zoals in de afgelopen jaren dienen voorkomen te worden als het vertrouwen in DigiD in de toekomst op peil moet blijven. De toekomst zal het leren; over vijf jaar zal ik nogmaals een artikel over DigiD schrijven…

Drs. Arjan Hassing RE RA (ahassing@controlsolutions.com) is partner bij ControlSolutions International. Daarvoor was hij werkzaam als accountant en IT-auditor bij Deloitte en EY. Hassing is tevens docent Bestuurlijke Informatievoorziening aan de Tilburg University. In genoemde rollen heeft hij veel ervaring opgedaan met vraagstukken op het gebied van audit, risk en compliance.

[1] In 2011 kwam DigiNotar, het bedrijf dat de beveiligingscertificaten van onder meer DigiD leverde, ernstig in opspraak nadat aan het licht was gekomen dat er onder meer vanuit Iran een hack was gezet bij het bedrijf, dat vervolgens had nagelaten de overheid en zijn andere klanten daarvan op de hoogte te stellen. Getronics PinkRoccade heeft inmiddels de certificering van DigiD-verbindingen overgenomen.

[2] Logius is een onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en beheert sinds 2006 generieke ICT-voorzieningen. Logius levert diensten aan andere overheidsorganisaties en organisaties met een publieke taak. Voorbeelden van deze diensten zijn DigiD, Digipoort, MijnOverheid en eHerkenning. Deze producten zijn bijna allemaal bij de stichting ICTU ontwikkeld en door Logius in beheer genomen. Het doorontwikkelen en het bevorderen van het gebruik van de producten behoort ook tot het takenpakket van Logius.

[3] Een public key infrastructure (PKI) is een systeem waarmee uitgiften en beheer van digitale certificaten kan worden gerealiseerd. Door de toepassing van een deugdelijke PKI is het mogelijk dat een certificaat dat door een certificaatautoriteit (CA) wordt beheerd, door de eigenaar ervan wordt gebruikt in de relatie met een ander individu. De CA waarborgt de integriteit en authenticiteit van het certificaat en staat in voor de identiteit van de certificaatbezitter. Aangezien de CA de kopieën van de verstrekte certificaten bevat, alsmede identificerende kenmerken van de identiteiten aan wie ze zijn verstrekt, is het van groot belang dat de fysieke opslagruimte op een zeer goede manier is beveiligd, zowel logisch (toegangsrechten binnen het systeem) als fysiek (wie is in staat het opslagsysteem te benaderen).

[4] NOREA is de Nederlandse Orde van Register EDP-Auditors en de beroepsorganisatie van IT-auditors in Nederland. NOREA beheert het register van gekwalificeerde IT-auditors en geeft opdrachtgevers en derden de mogelijkheid om vast te stellen of iemand op grond van zijn opleiding en ervaring heeft voldaan aan de eisen die door de beroepsorganisatie worden gesteld. Daarnaast heeft NOREA de volgende doelstellingen: bevorderen van de kwaliteit van de beroepsbeoefening; het bevorderen van de ontwikkeling van het vakgebied; het behartigen van gemeenschappelijke belangen van de leden.

[5] Opzet: beschrijving van de beveiligingsrichtlijn in een handboek, procedure of ander document.
Bestaan: waarneming van de aanwezigheid van de beveiligingsrichtlijn op één bepaald moment.
Werking: het bestaan van de beveiligingsrichtlijn gedurende een langere periode.

[6] Distributed denial-of-service-aanvallen (DDoS-aanvallen) zijn over het algemeen pogingen om een website, internetdienst of server ervan te weerhouden aanvragen van reguliere gebruikers te behandelen door meerdere computers tegelijk de aanval uit te laten voeren. Een veel voorkomende vorm van dit soort aanvallen is het verzadigen van het doelsysteem met externe communicatieverzoeken, zodat het niet kan reageren op legitieme verzoeken of zodat het zo traag wordt, dat het niet meer effectief te gebruiken valt.