DigiD, weg ermee

Zo hebben de afnemers van DigiD waarschijnlijk gedacht toen ze ontdekten hoeveel werk het was om het DigiD assessment van Logius uit te voeren. Logius, de beheerder van DigiD, droeg eind 2012 alle afnemers van DigiD op om een onafhankelijk assessment over hun gegevensbeveiliging uit te laten voeren. De directe aanleiding tot deze maatregel was een aantal veiligheidsincidenten die het gebruik van DigiD ernstig in diskrediet brachten.

Niet voldoen aan de eis van Logius voor eind 2013 zou uitsluiting van het gebruik van DigiD tot gevolg kunnen hebben. Inmiddels zitten we in 2014. Afgelopen week vroegen wij Logius hoe de stand van zaken was. Hun woordvoerder stelde dat Logius geen mededelingen doet over de stand van zaken. Dat sluit aan bij onze eerdere ervaringen van oktober 2013. Ook toen kregen we geen officiële reactie op onze constatering dat de respons op de opdracht van Logius erg laag was.

De eisen van Logius zijn tot stand gekomen onder grote druk van de 2e Kamer. Onze volksvertegenwoordigers willen het gebruik van DigiD veiliger te maken. Dat is een prima streven. Het lijkt echter dat nog niet alle publieke organisaties daarvan doordrongen zijn. Sommige organisaties (alleen de publieke sector mag DigiD gebruiken) zijn andere, minder veilige authenticatiemethoden gaan gebruiken. Dat is apart: Logius wil het veiliger maken en roept onbedoeld onveilig gedrag op.

Juist daarom zou het goed zijn wanneer Logius meer openheid van zaken zou geven. Interessant is om te weten hoeveel en welke organisaties gestopt zijn met DigiD. Ook is belangrijk om te weten welke publieke organisaties gebruik zouden moeten maken van DigiD maar dat nog niet doen. Zo valt het geringe aantal ziekenhuizen op dat gebruik maakt van DigiD. Dat geldt ook voor de veelgeplaagde sector woningbouwverenigingen die wel het BurgerServiceNummer krijgen i.v.m. de inkomensafhankelijke huur maar nog geen DigiD hanteren bij de woningtoewijzing. Eigenaardig want DigiD is toch het identificatiemiddel van de burger bij de overheid.

Informatieveiligheid is een precair onderwerp. Recente onthullingen over de activiteiten van veiligheidsdiensten en verwante partijen geven een ontluisterend beeld van onze (publieke) informatieveiligheid. Burgers en bedrijven die gebruik maken van publieke gegevens, mogen ervan uit gaan, dat de overheid die gegevens veilig beheert.

In het afgelopen jaar hebben wij een afnemers van DigiD ondersteund bij het voorbereiden en uitvoeren van het assessment op hun gegevensbeveiliging. Bij vrijwel alle organisaties heeft dat geleid tot aanzienlijke ingrepen in zowel de hardware en de software die wordt gebruikt. Ook de procedures rond het gebruik van informatiesystemen is daarbij vaak aanzienlijk aangepast. Het eisenpakket dat Logius hanteert m.b.t. webapplicaties is ons inziens uiterst zinvol en noodzakelijk. Bij de meeste organisaties, die wij hebben geaudit of begeleid, is de informatieveiligheid zowel technisch als organisatorisch aanzienlijk verbeterd. De meetlat van Logius ligt niet erg hoog: Logius heeft slechts 28 van de 59 door het Nationaal Cyber Security Centrum (NCSC) vastgelegde beveiligingsrichtlijnen voor webapplicaties verplicht gesteld voor 2013 en heeft laten weten de eisen in 2014 niet te verzwaren.

De zwakste schakel bepaalt uiteindelijk de sterkte van de totale keten. Als burger of bedrijf moet u op uw hoede zijn voor organisaties die uw vertrouwelijke gegevens gebruiken. Identiteitsfraude wordt een steeds groter probleem en juist daarom moeten publieke organisaties echt werk maken van de gegevensbeveiliging. Uit een recent onderzoek in opdracht van het Ministerie van Binnenlandse Zaken blijkt dat ca. 5% van de Nederlandse bevolking op een of andere manier met identiteitsfraude te maken heeft gehad. En dat percentage groeit, naarmate de technische mogelijkheden toenemen. (zie : http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/05/23/omvang-van-identiteitsfraude-en-maatschappelijke-schade-in-nederland.html

Daarom zouden we juist meer van DigiD gebruik moeten maken om onze eigen identiteit te beschermen en gegevensveiligheid te bevorderen. Zo bezien is het omzeilen van de eisen van Logius en het NCSC door alternatieve inlog- en authenticatiemethoden te gebruiken, een bedenkelijke zaak. Het is niet DigiD dat het probleem vormt maar de webapplicatie, de infrastructuur en vooral de mensen erachter.

Uit onze eigen analyse blijkt dat maar een beperkt deel van alle afnemers van DigiD het assessment heeft uitgevoerd. Van de 55 organisaties waarvan wij weten dat ze het assessment hebben uitgevoerd, heeft zo'n 80 % het assessment met succes heeft afgerond, 15% heeft het niet gehaald en uitstel gevraagd en gekregen van Logius en 5% is (tijdelijk) gestopt met het digitale loket en is aan het migreren naar een andere DigiD veilige omgeving.

Een aantal informatieleveranciers en samenwerkingsverbanden van gemeenten bleken hun zaken niet op orde te hebben. Een flinke groep organisaties heeft afgezien van verder gebruik van DigiD. Zo onttrekken deze organisaties zich aan de waarneming. De burgers en bedrijven die met deze organisaties zaken doen lopen risico. Wij schatten dat de laatste groep minimaal 50 tot 100 afnemers van DigiD groot is, op een totaal van ruim 600.

Wij denken dat als onze vermoedens kloppen de missie van Logius vooralsnog is mislukt. Informatie-veiligheid in de publieke sector heeft niet die prioriteit die je zou mogen verwachten. En daarmee lopen wij als burger en bedrijven het risico van privacy- en identiteitsmisbruik. In dit verband is het aandoenlijk om bij vrijwel iedere website een cookie waarschuwing gepresenteerd te krijgen: een nutteloze maatregel. De vertrouwelijkheid van uw gegevens wordt veel meer bedreigd door de gebrekkige opslag en beveiliging van gegevens waaronder diezelfde sessiecookies. Daarvoor krijgt u geen waarschuwing.

Het zou goed zijn wanneer Logius de actuele feiten rond het DigiD assessment publiek maakt en de organisaties die zijn gestopt met DigiD benoemt, evenals wie uitstel heeft gekregen. Dan zien we wat er aan de hand is en kunnen concrete maatregelen worden genomen. De overheid, politiek en ambtelijk apparaat, zouden Logius moeten helpen om door te pakken op de ingeslagen weg. Wat nu gebeurt lijkt een halfslachtige polderoplossing: eerst harde eisen stellen en dan uiteindelijk toch ongewenst gedrag gedogen omdat er teveel zwakke broeders blijken te zijn. Zwakke heelmeesters maken stinkende wonden en houden hier grote veiligheidsrisico's in stand. En daarvan worden wij als burgers en bedrijven in dit land mogelijk het slachtoffer.

De gemeenten, waterschappen, belastingorganisaties, zorginstellingen, leveranciers, samenwerkingsverbanden en al die organisaties die informatieveiligheid wel serieus nemen verdienen waardering. Daarom begrijpen wij niet waarom hun prestaties niet wereldkundig worden gemaakt. Dat zou voor de twijfelaars en achterblijvers een stimulans kunnen zijn en voor ons als burgers en bedrijven een geruststelling.

De schrijvers

René IJpelaar is als IT auditor werkzaam bij het bureau BKBO en is verantwoordelijk voor de uitvoering van een groot aantal DigiD assessments in het kader van gegevensbeveiliging bij gemeenten, belastingorganisaties, leveranciers, ziekenhuizen, etc.

Herman Timmermans is werkzaam bij TASCLINX BV en is o.a. actief bij de ontwikkeling en uitwerking van informatiebeleid bij organisaties in de private en publieke sector. In het afgelopen jaar is hij betrokken geweest bij de voorbereiding en uitvoering van DigiD assessments bij middelgrote organisaties.