DigiD is onze digitale identiteit, waarmee we gebruik kunnen maken van diensten op overheidswebsites en zorginstellingen. Met 100 miljoen DigiD-transacties per jaar is het van groot belang dat de veiligheid van deze vorm van identificeren gewaarborgd is. Maar DigiD volstaat niet meer en zal worden vervangen door eID, een algemene identiteitstool.

**tekst** Patricia van Schaik

# Toekomst van DigiD

Logius, de dienst digitale overheid en onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, eist een ICT-beveiligingsassessment van alle DigiD-koppelingen (inlogportalen) van bijvoorbeeld gemeenten, provincies en ziekenhuizen. Deze audit moet uitgevoerd worden door een Register EDP auditor, een RE. Niet slagen voor de DigiD-audit betekent afsluiting van DigiD, maar in de praktijk krijgen organisaties ruim de tijd om te verbeteren. *Jaco Koetsveld*, consultant bij LBVD, vertelt over zijn ervaringen met de DigiD-audit bij gemeenten en over de toekomst van eID.

*Hoe loopt het proces van de DigiD-audit?*
"De grote lijn is dat een aanvraag bij ons binnenkomt, waarna wij een intakegesprek met de opdrachtgever hebben om te bepalen om hoeveel koppelingen het gaat, of de opdrachtgever de beschikking heeft over Third Party Mededeling (TPM) en hoeveel richtlijnen moeten worden beoordeeld. Met andere woorden: de scope wordt bepaald.
Daarna gaat de opdrachtgever aan de slag om bewijsmateriaal aan te leveren. Dit wordt beoordeeld door de auditors, waarna een rapportage volgt die door de opdrachtgever naar Logius wordt verstuurd. Als in de rapportage alle richtlijnen op ´voldoet´ kunnen worden gezet (als voldoende beoordeeld zijn) is de opdrachtgever klaar en Logius tevreden.
Als er richtlijnen zijn die niet voldoen, omdat bijvoorbeeld de documentatie ontbreekt, niet volledig of niet actueel meer is, komt deze in de rapportage op ´voldoet niet´. In dat geval beoordeelt Logius de rapportage en vraagt dan aan de opdrachtgever om een verbeterplan en geeft een deadline om de zaken op orde te brengen. Als de opdrachtgever dat op orde heeft, volgt een herbeoordeling van de betreffende richtlijn door de auditor."

*Hoe pak je de DigiD-audit aan?*
"De DigiD-audit wordt uitgevoerd aan de hand van de richtlijnen van het Nationaal Cyber Security Center (NCSC). Het kan zijn dat organisaties een deel van de DigiD-koppeling uitbesteden. In dat geval wordt de software extern gehost en hoeven wij dus niet alle 28 richtlijnen te auditen. De hostingpartij audit hun richtlijnen en geeft ons een TPM, waarin staat dat ze voldoen. De gemeente blijft echter eindverantwoordelijk voor de DigiD-koppeling."

*Waar let je op?*
"Alle organisaties met een DigiD-koppeling moeten jaarlijks geaudit worden. Om in audittermen te spreken, er wordt dan getoetst op 'opzet en bestaan'. Werking is nog niet aan de orde."

In control zijn is het sleutelwoord in informatiebeveiligingsland en voor auditors. Daarom moeten organisaties jaarlijks de DigiD-audit laten uitvoeren. Maar, veel gemeenten zijn nog niet zo ver. In 2013 moesten ze voor het eerst de DigiD laten auditen. In 2014 hebben de organisaties een nieuwe audit laten uitvoeren, waarmee een beter beeld was gegeven hoe het ervoor staat met DigiD. In 2016 wordt met hoogstwaarschijnlijk ook getoetst op de werking van processen. Nu auditen ze alleen opzet en bestaan. Logius is hierin leidend.

*Jij denkt dus dat organisaties er nog niet klaar voor zijn?*
"Organisaties krijgen de tijd om eerst hun processen in kaart te brengen, dan hun documentatie en in een later stadium ook aan te tonen dat ze doen wat ze zeggen."

*Gaat men pas documenteren als de audit eraan komt?*
"Ja, mijn ervaring is dat het steeds weer een redelijk onbekend terrein is en een noodzakelijk kwaad. Het is geen proces maar een ad hoc activiteit. Logging bijvoorbeeld, hoe ga je daarmee om als gemeente? Daar moet eigenlijk een proces voor ingericht zijn, waarin je dagelijks de belangrijkste logs controleert, en de leidinggevende wekelijks akkoord geeft. Dit gebeurt in de praktijk nog onvoldoende. Rapportages en het periodiek opleveren ervan zijn ook vaak ondergeschoven kindjes."

- *De opzet:* Bij de opzet wordt beoordeeld of een ontwerp van een maatregel aanwezig is, bijvoorbeeld binnen een beleidstuk, een (project)plan of procedurele documentatie.
- *Het bestaan:* Bij het bestaan wordt beoordeeld of de opzet vertaald is naar procedures, activiteiten en concrete maatregelen en/of gedrag in de praktijk, bijvoorbeeld in de vorm van rapportages, wijzigingsregistraties, testdocumentatie, logs.
- *De werking:* Bij de werking wordt beoordeeld of de maatregelen feitelijk voor een vastgestelde periode zijn uitgevoerd. Afhankelijk van de gekozen norm kan dat variëren van een aantal weken tot een jaar. Hierbij wordt gekeken of rapportages ook periodiek worden opgeleverd, afgetekend, etc.

*Hoeveel tijd nemen de audits in beslag?*
"Als ze hun zaakjes op orde hebben zijn ze relatief snel klaar. Als er weer opnieuw gekeken moet worden naar de eigen documentatie en processen kan het wel eens een uitdaging zijn."

*Waarom gaat dit zo?*
"Het gevoel dat bij veel organisaties leeft is: weer een audit, weer die zooi opleveren. Het is een noodzakelijk kwaad. Mijn ervaring is dat sommige gemeenten bijna murw zijn geslagen door het aantal audits dat ze moeten afleggen op verschillende gebieden. Het doel is toe te werken naar de digitale overheid in 2017, wat betekent dat de burger altijd digitaal bij elke overheidsorganisatie documenten kan aanvragen. Dit is heftig voor gemeenten, want het hangt samen met de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Wat je ziet bij al die audits, is dat ze allemaal teruggrijpen naar de BIG. Ook de normen die in de DigiD-audit gevraagd worden, zijn eigenlijk het eerste hoofdstuk van de BIG. Er is dus overlap, en dit is een bewuste keuze om de implementatie van de BIG tezamen met andere zaken te regelen."

*Wat gaat er goed bij gemeenten?*
"Gemeenten gaan steeds meer waarde hechten aan digitale veiligheid in het algemeen en daardoor ook van hun DigiD-koppeling. Gemeenten zijn goed bezig, ze begrijpen waarom ze eraan moeten voldoen dus ze zorgen zo goed mogelijk dat het er is. Het besef is gaan leven dat ze het doen voor de veiligheid van de burger en het dus niet alleen een noodzakelijk kwaad is."

*Jaco Koetsveld: " De huidige DigiD volstaat niet meer."*

*Hoe ziet de toekomst van DigiD eruit?*
"De huidige DigiD volstaat niet meer. Hij is beschikbaar op een laag (gebruikersnaam en wachtwoord) en middel (gebruikersnaam en wachtwoord met SMS-authenticatie) betrouwbaarheidsniveau en dat is niet voldoende. Daarom gaat eID DigiD vervangen, is DigiD niet meer nodig, en zal het auditproces veranderen. Met de komst van eID, wordt het gebruik nog breder. eID is een algemene identiteitstool, waarmee je bijvoorbeeld ook kunt webwinkelen. Maar vanuit het oogpunt van informatiebeveiliging maken we ons ook zorgen, bijvoorbeeld over big data. Uit de 'Visiebrief digitale overheid 2017' van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, komt naar voren dat de overheid veel waarde hecht aan de privacy van burgers en bedrijven. Verder wordt er aandacht geschonken aan acceptatie van eID. Ik kijk met gezonde nieuwsgierigheid en beroepsinteresse uit naar de komst van de opvolger van DigiD, met toch de nodige scepsis als het gaat om de borging van onze privacy. Maar met eID wordt de digitale wereld hopelijk weer een stukje leefbaarder."■

**Patricia van Schaik is consultant**

## 2017

- De DigiD-audit is redelijk nieuw, want pas sinds 2013 verplicht. Met oog op de BIG moeten bedrijven en burgers eind 2017 alle zaken die ze met overheid doen digitaal gaan afhandelen (uit: Visiebrief digitale overheid 2017).
- De DigiD-audit is in het leven geroepen naar aanleiding van Lektober en de DDoS-aanvallen op DigiD, om te borgen dat dit niet meer voor kon komen.
- Leestip: 'De Cirkel' van Dave Eggers. Een boek over het leven met 1 online identiteit, en de consequenties die dat heeft voor privacy, geheimen en de maatschappij.