Het beveiligen en toegankelijk maken van gegevens in de cloud behoren topprioriteiten te zijn. Maar de maatregelen die worden getroffen, zegt Rob van der Staaij, vallen tegen. Er moet volgens hem meer werk worden gemaakt van het inrichten van identity & access-management in cloudomgevingen.

door: ROB VAN DER STAAIJ **beeld:** ISTOCKPHOTO

TOEGANGSCONTROLE IN DE CLOUD MOET BETER

Identity as a service kan behulpzaam zijn bij inrichten identity & accessmanagement

Cloudcomputing begint steeds meer deel uit te maken van de bedrijfsvoering en de IT-infrastructuur van organisaties, ondanks een aantal onzekerheden dat dit met zich meebrengt. Zo mogen er vraagtekens worden gezet bij de beveiliging van gegevens. Cybercriminaliteit en 'insider threat' zijn voorbeelden van bedreigingen waarvan ook cloudcomputing niet is gevrijwaard.
Identiteitenbeheer en toegangscontrole, bekend onder de noemer 'identity & access'-management (IAM), behoren tot de belangrijkste maatregelen die zowel organisaties als cloudproviders moeten nemen om gegevens in de cloud te beveiligen en toegankelijk te maken. Maar juist op dit terrein blijkt de volwassenheid van de maatregelen zich nogal eens op een (veel) lager niveau te bevinden dan we zouden mogen verwachten, zoals een inventarisatie van de belangrijkste services en technieken uit het betreffende domein laat zien.

Authenticatie

Authenticatie is een conditio sine qua non voor cloudapplicaties. Zonder authenticatie krijg je geen toegang tot welke clouddienst dan ook, of dit nu Salesforce is of Gmail. De meest eenvoudige vorm van authenticatie bestaat uit het invoeren van een combinatie van gebruikersnaam en wachtwoord. Welnu, deze wijze van authenticeren is meteen verreweg de meest gebruikte in cloudomgevingen. Gebruikt iemand tien cloudapplicaties, dan is het met deze methode ook tien keer nodig om accountgegevens in te voeren. Tegelijkertijd is deze manier van authenticeren de minst veilige. Het overgrote deel van de gevallen waarbij cloudapplicaties worden gehackt, is te wijten aan het kraken of stelen van wachtwoorden.
Met web-accessmanagement kan het authenticatieproces al een stuk efficiënter worden ingericht. Deze bekende service uit het IAM-domein, die al heel wat langer opgeld doet dan het fenomeen cloudcomputing, bestaat uit een verzameling services variërend van sessiemanagement tot single sign-on. Om die laatste gaat het hier, want met single sign-on kan iemand door zich slechts eenmaal te authenticeren toegang kijgen tot alle benodigde applicaties. Om te voorkomen dat het achterhalen van het wachtwoord de deur tot alle cloudapplicaties wagenwijd openzet, is het toepassen van een tweede authenticatiefactor, bijvoorbeeld in de vorm van een smartcard of digitale sleutel, hier altijd nodig. Web-accessmanagement wordt zowel door organisaties zelf als door cloudproviders ingezet om de toegang tot cloudapplicaties in te richten. Indien toegepast binnen de organisatie, verschilt een cloudapplicatie voor de eindgebruiker niet van de overige bedrijfsapplicaties die op dezelfde manier worden ontsloten. Federated identity biedt eveneens single sign-on, maar werkt over de grenzen van organisaties heen. Hierbij treedt één partij op als identityprovider. Meestal is dit de klantorganisatie zelf (of een organisatie binnen dezelfde branche of keten), maar het kan ook een partij zijn die namens de klantorganisatie optreedt. Een gebruiker authenticeert zich bij de identityprovider – met behulp van bijvoorbeeld Active Directory – en krijgt vervolgens toegang tot de applicaties van de cloudprovider zonder zich daar opnieuw te hoeven authenticeren. Dankzij cloudcomputing vertoont federated identity de laatste tijd een forse groei, na jaren van stagnatie.

Autorisatie

Over autorisatiebeheer in cloudomgevingen kunnen we betrekkelijk kort zijn. Autorisaties worden nog altijd per applicatie beheerd. Geen enkele cloudprovider biedt de mogelijkheid om autorisaties op centrale wijze, dus buiten de applicaties om, in te richten. Niet zo verwonderlijk, want het op deze wijze inrichten en beheren van autorisaties is überhaupt een zelfzaamheid. Steeds meer organisaties passen wel 'role-based access control' (RBAC) in een of andere vorm toe voor het bundelen van autorisaties tot rollen of profielen, maar de autorisaties worden uiteindelijk gewoon afgehandeld binnen de afzonderlijke cloudapplicaties.
Het aanmaken, wijzigen en ongedaan maken van gebruikersaccounts is bij uitstek een taak die geautomatiseerd zou moeten worden uitgevoerd. Dat kan uitstekend met behulp van user provisioning, een van de IAM-services waar veel organisaties de laatste jaren flink in hebben geïnvesteerd. Een aantal IAM-leveranciers levert connectoren die speciaal voor cloudomgevingen zijn aangepast. In cloudomgevingen vormt user provisioning echter een ondergeschikte methode voor het beheren van accountinformatie, want het handmatig beheren ervan is hier nog altijd de standaard. Evenmin erg vooruitstrevend is de batchmethode die ook veelvuldig wordt gehanteerd. Hierbij wordt een lijst met gebruikersaccounts, bijvoorbeeld in de vorm van een CSV-bestand of Excelsheet, aan de cloudprovider overhandigd met het verzoek om deze in de cloudapplicatie te verwerken. Andere methoden, zoals directory-synchronisatie of instant provisioning – het aanmaken van accountinformatie op het moment van inloggen – zijn nog minder gebruikelijk.
Willen organisaties iets weten over het gebruik van clouddiensten – bijvoorbeeld wie op welk tijdstip toegang heeft gehad tot bepaalde cloudgegevens – dan zijn zij hiervoor meestal afhankelijk van de cloudprovider. Die moet de gegevens vervolgens per applicatie opvragen, want een geïntegreerde audit- en rapportagefunctionaliteit is een zeldzaamheid binnen cloudomgevingen. Die lacune kan ook nog eens leiden tot te veel betalen, want ongebruikte licenties kunnen zo eveneens aan het zicht worden onttrokken. Ook toezichthouders stellen in de context van cloudomgevingen in toenemende mate deficiënties vast. Wat cloudproviders voor dit doel beschikbaar zouden moeten stellen zijn API's en webservices waarmee organisaties zelf de benodigde gegevens kunnen opvragen. Zulke interfaces worden nog maar mondjesmaat toegepast.

Identity as a service

In de markt zijn verschillende partijen actief die identity & accessmanagement als service aanbieden, ook wel bekend als Identity as a service (IDaaS). Wanneer we de verschillende IDaaS-providers beschouwen, dan kunnen ruwweg drie varianten worden onderscheiden. Er zijn partijen die begonnen zijn als identityprovider in federatieve omgevingen en hun diensten en klantenkring gaandeweg hebben uitgebreid. Daarnaast zijn er IDaaS-providers die de gehele IAM-omgeving van – meestal grote – organisaties overnemen en het beheer daarvan voor hun rekening nemen. Ten slotte zijn er IDaaS-providers die als pure play-providers kunnen worden gekarakteriseerd en zich helemaal hebben toegespitst op het leveren van authenticatiediensten. Organisaties (en vaak ook hun klanten) kunnen op deze wijze de toegang regelen tot zowel cloudapplicaties als de eigen applicaties. Er is overigens veel beweging in de IDaaS-markt waarin leveranciers elkaar overnemen en diensten minder scherp af te bakenen zijn. IDaaS kan organisaties helpen om identity & accessmanagement in de cloud in te richten. Een absolute voorwaarde is dan wel dat de IDaaS-provider overtuigend kan aantonen dat de gegevens van de klant bij hem in veilige handen zijn, want het gaat hier om gegevens waarmee op de meest directe wijze identiteitsfraude en cybercrime kunnen worden gepleegd. Klanten moeten de IDaaS-provider daarom gedetailleerd vragen naar de in gebruik zijnde IAM-methoden en -technieken en overige beveiligingsmechanismen. Kortom, veel organisaties hebben jaren werk geïnvesteerd in het op orde krijgen van identity & accessmanagement binnen de eigen IT-infrastructuur. Deze inspanningen mogen niet teniet worden gedaan door de beweging naar de cloud. Er moet daarom meer werk worden gemaakt van het naar behoren inrichten van IAM in cloudomgevingen. Identity as a service kan daarbij behulpzaam zijn, maar dan moet de IDaaS-provider kunnen aantonen over de nodige expertise en de juiste hulpmiddelen te beschikken. «

Dr. Rob van der Staaij is adviseur bij Atos Consulting (rob.vanderstaaij@atos.net).

STANDAARDEN EN SPECIFICATIES

In tegenstelling tot de matige volwassenheid van identity & accessmanagement in cloudomgevingen, zijn er genoeg standaarden en specificaties beschikbaar die het werk meer dan goed aankunnen. Sommige daarvan zijn er al enige tijd, maar er zijn ook recente en veelbelovende standaarden.

- **SAML (Security Assertion Markup Language):** een absolute winnaar op het gebied van authenticatie en single sign-on. Wordt in meer dan negentig procent van de implementaties van federated identity toegepast.
- **WS-Federation:** kan beschouwd worden als de Microsoft-variant van SAML. Heeft buiten Microsoft-omgevingen geen voet aan de grond gekregen. Ook Microsoft is hiervan doordrongen geraakt, want inmiddels is ondersteuning voor SAML ingebouwd.
- **XACML (eXtended Access Control Markup Language):** standaard voor het centraal inrichten en regelen van autorisaties, buiten de applicaties om. Nu nog niet toegepast in cloudomgevingen, maar dat zal zeker veranderen.
- **OpenID:** standaard waarmee gebruikers zelf een identityprovider kunnen kiezen om zich te authenticeren. Bestaat al een tijdje, maar begint nu eindelijk momentum te krijgen, omdat het tegenwoordig gecombineerd kan worden met OAuth (gezamenlijk OpenID Connect geheten).
- **OAuth (Open Authorization):** standaard waarmee op maat gesneden toegang tot informatie verleend kan worden aan derden zonder dat daarbij authenticatie-informatie (zoals een wachtwoord) prijsgegeven hoeft te worden. Wordt ondersteund door klinkende namen zoals Google, Twitter, Facebook, Salesforce, Microsoft en PayPal.
- **SPML (Service Provisioning Markup Language):** keurige standaard voor user provisioning, het centraal en geautomatiseerd beheren van gebruikersaccounts. Heeft echter geen enkele voet aan de grond gekregen in cloudomgevingen, wat het ergste doet vrezen voor deze standaard.
- **SCIM (Simple Cloud Identity Management):** veelbelovende standaard voor het beheren van identiteiten in cloudomgevingen. Veelbelovend omdat het, zoals de naam al aangeeft, eenvoudig van opzet is, maar vooral omdat het een initiatief is van partijen als Google, Ping Identity, VMware en Salesforce.

Voor reacties en nieuwe bijdragen van IT-experts:
Henk Ester,
070 3780397
h.ester@sdu.nl

IDentity.Next '12
20-21 november The Hague

The program with top experts, professionals and industry stakeholders aims to discuss the world around Digital Identity and best practices. The overall theme of 2012: Making (y)our business with digital identity.

For more information about the theme and pogram:
www.identitynext.eu