Beheer van elektronische toegang

© m7

Waarom?
Wat?
Hoe?

De elementen van identity en access management

Voor het beschermen van toegang tot informatie richten grotere organisaties steeds vaker identity en access management in: het zoveel mogelijk geautomatiseerde beheer van accounts, login-gegevens, toegangsrechten van hun gebruikers. Een gebruiker is iedereen die zich bekend moet kunnen maken aan de applicaties van de organisatie.

Waarom? (doelen)

gebruiks-vriendelijkheid

Identity en access management draagt er voor gebruikers toe bij dat zij minder wachtwoorden hoeven te onthouden, minder verschillende middelen voor authenticatie nodig hebben, zich vaak maar éen keer hoeven aan te melden voor meerdere applicaties, zelf wachtwoorden en andere gegevens kunnen beheren, wachtwoorden kunnen resetten en eventueel rechten kunnen aanvragen voor het gebruik van applicaties.

compliance

Identity en access management zorgt ervoor dat een organisatie voldoet aan wet- en regelgeving omtrent verantwoordelijkheden, vertrouwelijkheid van informatie en de privacy van gebruikers.
Het helpt ook om functiescheiding beter na te leven en geeft overzicht over toegangsrechten voor alle applicaties en diensten waarvoor dat relevant is.

veiligheid

Veiligheid betreft maatregelen tegen bedreigingen die de vertrouwelijk, integriteit en beschikbaarheid van informatie en diensten negatief beïnvloeden. Integriteit van informatie betekent dat deze niet ongeoorloofd gewijzigd kan worden. identity en access management helpt om de veiligheid te doen toenemen door te zorgen dat gebruikers alleen de informatie kunnen zien die zij mogen zien en dat deze te allen tijde beschikbaar is. Ook helpt het om het bewerken van informatie adequaat te beveiligen.

kosten-besparing

identity en access management reduceert het aantal helpdeskverzoeken gerelateerd aan wachtwoorden en inloggen, het maakt licentiebeheer veel meer inzichtelijk en faciliteert het dynamisch beheer ervan én het reduceert het aanmaken van accounts, doordat dit slechts voor iedere gebruiker eenmaal hoeft te gebeuren.

Wat? (de elementen)

provisioning

Het doorsturen van identiteitsgegevens van het ene systeem naar het andere systeem om daarmee te zorgen dat de organisatie over genormaliseerde identiteitsgegevens beschikt over alle systemen heen, d.w.z. dat wijzigingen niet tot verschillen leiden. Provisioning kan er tevens voor zorgen dat gebruikers overal dezelfde gebruikersnaam en wachtwoord kunnen gebruiken. Gebruikersnamen en wachtwoorden worden dus ook geprovisioned.

selfservice

Regelt dat gebruikers zelf hun wachtwoord kunnen wijzigen voor alle applicaties, zelf hun wachtwoord opnieuw kunnen instellen als zij het zijn vergeten, eventueel toegangsrechten kunnen aanvragen en eventueel andere identiteitsgegevens kunnen wijzigen.

life cycle management

Het bijhouden van de start en de beëindiging van een relatie tussen de organisatie en een gebruiker en zorgen dat de toegang en de toegangsrechten overeenkomen met die relatie. Het woord relatie wordt hier in brede zin gebruikt en een gebruiker kan er meerdere hebben met een organisatie. Bijvoorbeeld medewerker en klant, of gewone gebruiker en systeembeheerder. Vaak wordt gesproken over rollen. Zie daarvoor autorisatiemanagement.

authenticatie-management

sterke authenticatie

De inlogmiddelen kunnen wachtwoorden zijn, maar ook zogenaamde tokens of biometrische gegevens. Tokens zorgen ervoor dat de gebruiker naast een pincode of wachtwoord ook nog iets bij zich moet hebben om toegang te krijgen. Zoals de bankpas voor internetbankieren. Authenticatie wordt vaak geregeld via een centrale directory, bijvoorbeeld een LDAP-server of een Active Directory. Zo hoeven applicaties niet meer zelf de inloggegevens van gebruikers te bevatten en is het beheer eenvoudiger.

federatieve authenticatie

Een speciaal onderdeel van authenticatiemanagement is federatief identity en access management, waarbij twee of meer organisaties afspraken maken over bij elkaar inloggen en daarbij vertrouwen op de authenticatievoorzieningen van de andere organisatie.

single sign-on

Zorgt ervoor dat gebruikers, nadat zij bij de eerste applicatie zijn ingelogd, voor alle of de meeste andere applicaties, dat niet nogmaals hoeven doen. Kan ook vallen onder authenticatiemanagement.

social logon

Daarnaast kunnen organisaties gebruik maken van authenticatie met behulp van sociale netwerken en cloud providers, bijvoorbeeld van facebook, Google en twitter. Dit wordt wordt veel gebruikt voor commentaar bij blogs e.d., maar ook steeds vaker voor commerciële diensten.

autorisatie-management

role provisioning

Vooraf gedefinieerde rollen (of groepen) kunnen worden geprovisioned naar applicaties en die kunnen er dan rechten aan koppelen. Dit werkt voor een hoofdverdeling van groepen (de zogenaamde basisrollen; denk aan medewerkers en externen) en voor organisatierollen en functierollen. Organisatierollen hebben bijvoorbeeld te maken hebben met afdelingen en locaties. Uiteraard kunnen nog meer rollen en groepen worden gedefinieerd, maar die zijn vaak niet via deze methode te beheren (zie identity & access governance hieronder). Die worden vaak taakgerichte rollen of business rollen genoemd.

ad hoc groepen

Naast de rollen en groepen die te maken hebben met structurele werkzaamheden is er in elke organisatie ook toegang nodig die elke gebruiker zelf kan starten en organiseren. Bijvoorbeeld voor het onderling delen van agenda's, bestanden, etc. Dit wordt meestal per applicatie geregeld, maar kan ook worden gefaciliteerd door een applicatie-overstijgende tool om groepen aan te maken en te beheren. Dat heeft tevens als voordeel dat audits eenvoudiger worden.

context en risico

Naast autorisatie op basis van rollen, kan het ook plaatsvinden op basis van de context van de gebruiker op het moment van inloggen of op basis van het risico op dat moment. Denk aan: type werkplek van een gebruiker, authenticatiemiddel (met een token krijgt een gebruiker bijvoorbeeld meer rechten), de plek in het netwerk waar de gebruiker zich bevindt (vanaf internet minder rechten dan vanaf een interne werkplek), iemand die op een zeer ongebruikelijk tijdstip zeer vertrouwelijke informatie raadpleegt. Of aan een gebruiker die dat plotseling vanuit een internetcafé doet.

identity & access governance

Role provisioning werkt niet goed voor rollen die met specifieke werktaken te maken hebben, taakgerichte rollen. Dat zijn er meestal teveel en ze zijn te specifiek om top-down (door een centrale organisatie) te kunnen vaststellen en te beheren.
Uiteraard zijn de rechten die bij taakgerichte rollen horen wel aanwezig bij organisaties, anders zouden mensen hun werk niet kunnen doen. De grote vraag is alleen of er bij het uitdelen van die rechten voldoende zorgvuldig te werk is gegaan, zodat de rechten niet veel te ruim zijn ingesteld.

Immers, daar zal niemand over klagen, in tegenstelling tot over te krap ingestelde rechten. De momenteel meest geschikte oplossing om over deze rechten iets te zeggen heet identity & access governance:

- Hiermee houd je overzicht over wie welke rechten heeft, en hoe ze eraan gekomen zijn.
- Het signaleert ook anomaliën e.d.
- Nieuwe identity en access management-tools maken het tevens mogelijk om vanuit het overzicht nieuwe (taakgerichte) rollen te definiëren en te gebruiken.
- Als laatste stap kunnen dan workflows voor aanvragen van toegang worden geautomatiseerd.

Identity & access governance vaak genoemd samen met Identity & Access Intelligence dat business intelligence-achtige dashboards verschaft, maar dan voor toegangsrechten.

cloud access management

Met de opkomst van cloud diensten en social media hebben gebruikers niet alleen meer door de organisatie uitgegeven accounts, maar ook externe accounts, los van de organisatie, terwijl ze diensten die daar bij horen wel gebruiken voor activiteiten die bij de organisatie horen. Om deze trend te kunnen beteugelen is het nodig om voldoende soortgelijke diensten te beschikbaar te stellen, ook in de cloud, waarvoor het access management goed kan worden geregeld. De authenticatie wordt dan geregeld met federatief identity en access management.

device management

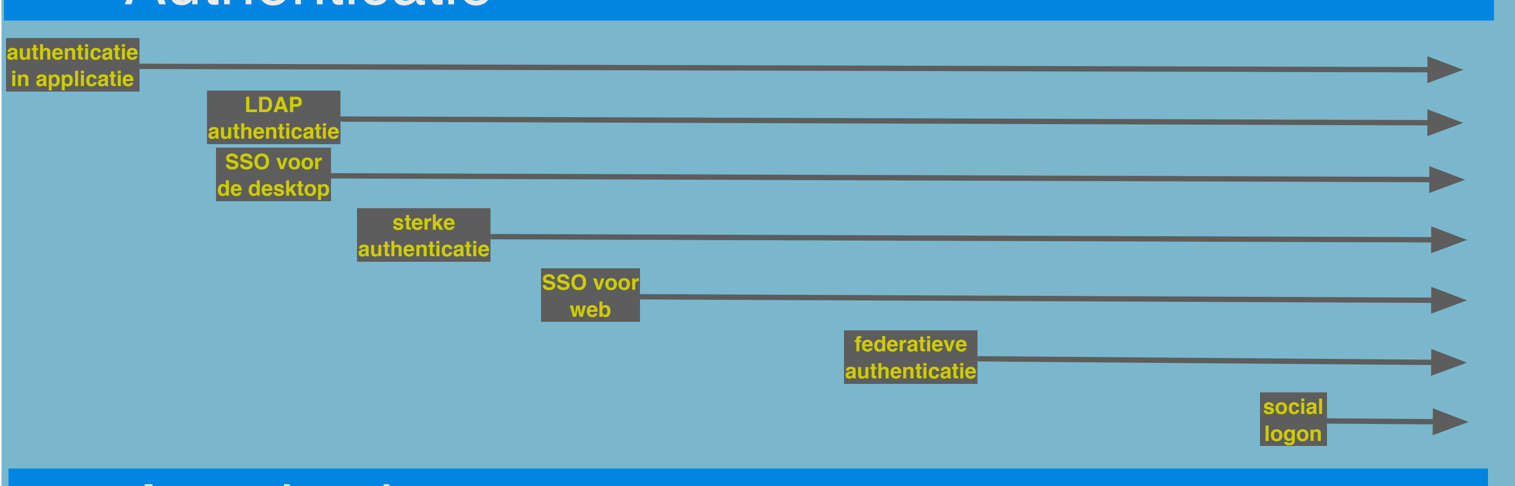
Vreemde eend in de bijt, want het gaat niet direct om rechtenbeheer voor gebruikers, maar om beheer van een device. Er komen steeds meer eigen devices van gebruikers in een organisatie die voor het werk worden gebruikt. Die kunnen vaak eenvoudig door anderen worden misbruikt (denk aan diefstal, verlies, etc.). Dus is het zaak de devices die toegang bieden goed te beveiligen. Er zijn meerdere tools om dit te doen (voor een geheel device, of het deel ervan dat voor werk wordt gebruikt).
Het beheer van devices en de apps erop is zeker van belang als een app op het device voor sterke authenticatie wordt gebruikt.
Daarnaast kunnen devices ook worden gebruikt als een extra stap voor autenticatie/autorisatie, omdat de kenmerken van een device kunnen worden herkend. Dan is het zaak dat een device kan worden verwijderd als het is verloren of gestolen.

Authenticatie- en autorisatie-management in de tijd

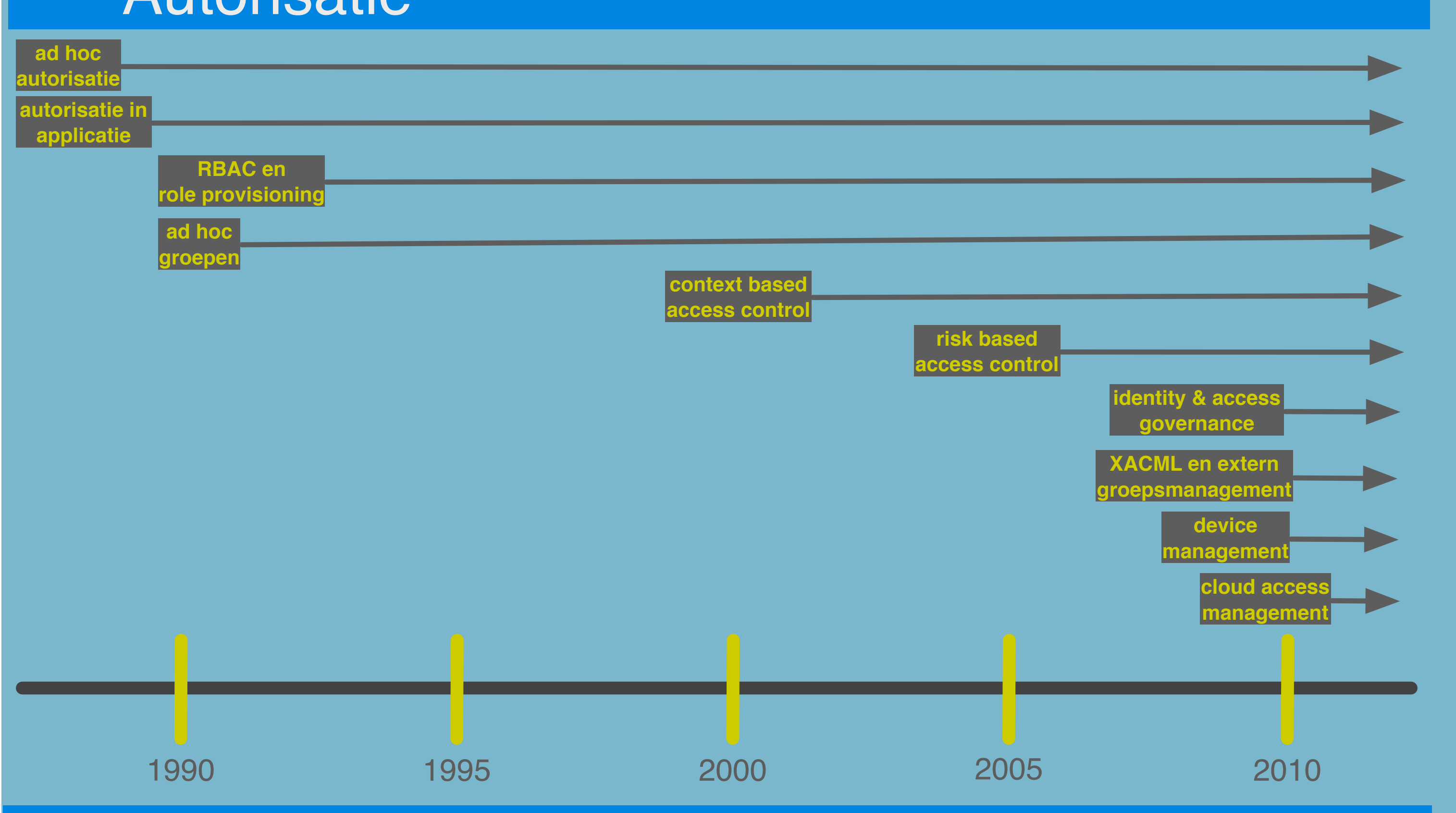
De ideeën over authenticatie en het beheer van autorisaties zijn in de loop der jaren een aantal keren gewijzigd en aangevuld. Voor de jaren 90 van de vorige eeuw bestond er eigenlijk alleen maar authenticatie met gebruikersnaam en wachtwoord en werden autorisaties voor iedere individuele gebruiker ad hoc uitgedeeld. Beide vonden plaats binnen de applicaties zelf. In de jaren 90 kwamen er oplossingen voor authenticatie buiten de applicatie met LDAP (zodat gebruikers overal hetzelfde wachtwoord hadden) en single sign-on voor de desktop met Kerberos. Later werd single sign-on mogelijk voor webapplicaties (met cookies) en tegenwoordig kunnen single sign-on voor de desktop en voor het web worden gecombineerd.

Autorisatie heeft van oudsher altijd in de applicatie plaatsgevonden. Sinds enige tijd is er de technische standaard XACML (eXtensible Access Control Markup Language), waarmee autorisatie buiten de applicatie kan komen te liggen. XACML is geschikt voor cloud-applicaties. Geschikt voor RBAC (Role Based Access Control, Context Based Access Control, Risk Based Access Control. Men spreekt dan wel van ABAC (Attribute Based Access Control) als verzamelnaam voor alle vormen van Access Control.
Bij RBAC wordt aan een rol een verzameling rechten gekoppeld en rollen worden weer aan personen toegekend. Werkt goed met een beperkt aantal rollen, vooral als deze eenduidig zijn gedefinieerd en niet snel wijzigen. Voorbeelden: basisrollen (belangrijkste hoofdgroepen gebruikers), functierollen, organisatierollen (afdeling, locatie). Voor meer taakgerichte rollen is RBAC lastiger, omdat die vaak sneller veranderen, bijvoorbeeld al bij een kleine reorganisatie. Dan werkt identity & access governance veel beter.

Authenticatie

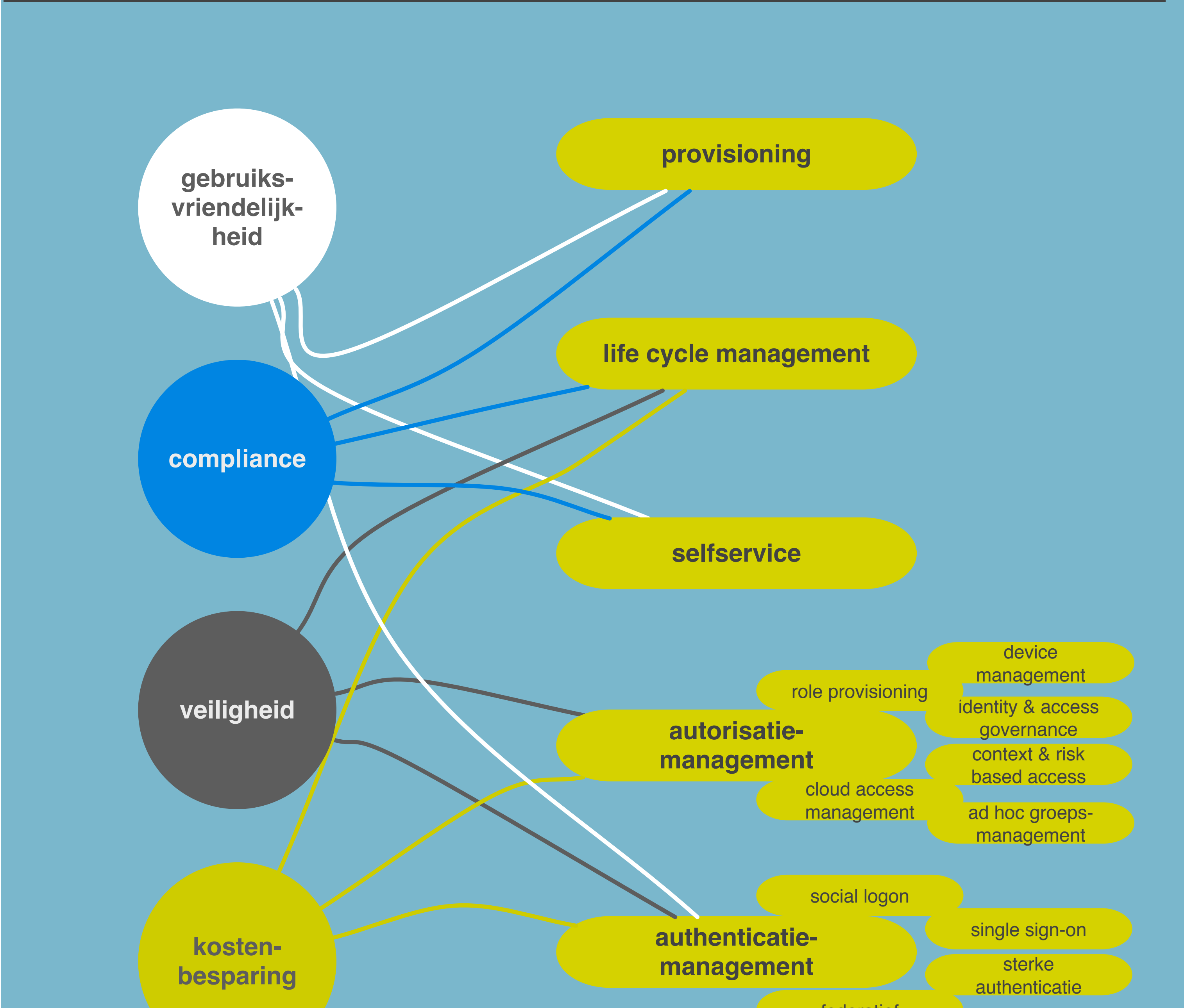


Autorisatie



Samenhang tussen doelen en elementen

Doelen | Elementen



identity en access management op het internet

De voordelen van IAM kunnen worden uitgebreid over de grenzen van de eigen organisatie heen. Dit houdt in dat de gebruikersnaam en het wachtwoord (en eventueel sterkere vormen van authenticatie), die binnen de organisatie worden gebruikt, ook daarbuiten gebruikt kunnen worden. We spreken dan over federatief identity & access management. In zo'n federatie spelen drie partijen een rol:

- de organisatie, die de identiteit en het authenticatiemiddel van de gebruiker verstrekt en beheert (identity provider, IdP);
- de dienstaanbieder (service provider, SP), die niet langer zelf accounts hoeft uit te geven, maar erop vertrouwt dat de organisatie uit de vorige regel de gebruikers adequaat authenticeert en de juiste gegevens van hen doorgeeft;
- de federatie operator, die zorgt voor de techniek en afspraken om de federatie goed te laten werken.

Ter illustratie van de voordelen van federatief werken nemen we het geval dat een organisatie een applicatie uit de cloud afneemt voor haar gebruikers. We vergelijken voor dit geval het werken met en zonder federatie in onderstaande tabel aan de hand van de eerder genoemde elementen.

	Standaard	Federatief
gebruiksvriendelijkheid	extra gebruikersnaam en wachtwoord extra keer inloggen	vertrouwde gebruikersnaam en wachtwoord single-sign-on (SSO, één keer inloggen)
compliance	profiel van gebruiker wordt door dienstaanbieder uitgevraagd	organisatie bepaalt welke gegevens van gebruikers nodig zijn, dus betere privacy bescherming
veiligheid	nieuw inlogscherm en dus risico op phishing	vertrouwde inlogscherm of zelfs geen inlog bij SSO
kostenbesparing	oplopende licentiekosten door ontbreken beheer levenscyclus	automatische (de)provisioning door beheer levenscyclus, dus altijd het juiste aantal licenties

Federatief identity & access management wordt sinds ongeveer tien jaar in de praktijk toegepast. Voorbeelden zijn de federaties in het onderwijs, de openbare-bibliotheeksector, de overheid (DigiD, eHerkenning), de gezondheidszorg (nog in wording, maar denk hierbij aan het Landelijk Schakelpunt) en het bedrijfsleven (bijvoorbeeld bij ketensamenwerking in de maakindustrie: assemblage en toeleveranciers). In het tijdperk van cloud computing is dit onderwerp actueler dan ooit.

Social logon

Social login is het uitbesteden van de authenticatie van de gebruiker op een website aan een social media netwerk (Facebook, LinkedIn, Google, Hyves, enz.). Het voordeel is meer gemak voor de gebruiker, want hij heeft minder accounts nodig. Vele organisaties worstelen met de vragen: wat kan ik met social login? wat moet ik met social login?

Als uw organisatie IAM op orde heeft, dan zou social login een waardevolle aanvulling kunnen zijn. De voordelen (gebruiksgemak) moeten dan wel zorgvuldig tegen de risico's (laat u wel de juiste gebruiker toe?) worden afgezet. Een ander voorbeeld is het gebruik van social login niet zozeer voor de eigen gebruikers binnen uw organisatie, maar juist voor de gasten. In dat geval krijgt uw gast geen apart account van uw organisatie, maar na een gedegen registratieproces gebruikt uw gast zijn social media account.