Identity Management als fortwährender Prozess

Mit Sicherheit zum Ziel

Identity Management (IdM) ist eine grundsätzliche Herausforderung für nahezu jedes Unternehmen: Ohne ein gutes IdM-Konzept ist es schwer, sich am Markt zu behaupten, und fast unmöglich, Verwaltungsabläufe effizient zu steuern. Es ist ein entscheidender Erfolgsfaktor. Aber was genau ist IdM, welche Elemente sind relevant und warum ist es ein Sicherheitsthema? Dieser Artikel gibt einen Überblick über das weite Feld des IdM und erläutert, wie es sich in Bezug auf die Faktoren Mensch, Politik, Prozess und Technik einordnet.

Im Zeitalter der digitalen Kommunikation werden nicht mehr Dinge, sondern Daten und Informationen als das primäre und schützenswerte Gut angesehen. Eine digitale Identität ist allgemein gesprochen die Teilmenge der Daten und Informationen (Attribute) eines Menschen, eines Computers oder eines Internetdienstes (allgemein: einer Entität), die die Entität eindeutig unterscheidbar zu anderen macht. Die reale Entität muss nun präzise auf eine digitale Identität abgebildet werden, die anschließend nutzbar gemacht wird. Hierauf aufbauend beschreibt der Begriff Identity Management (IdM) die Erzeugung, Nutzung, Pflege und Löschung von digitalen Identitäten mitsamt der Attribute und Berechtigungen.

Der Einsatz von digitalen Identitäten erfordert vertrauenswürdige, identitätsbezogene und regelkonforme Prozesse, die unabhängig von Organisationen und Plattformen standardisiert nutzbar sind. Schlussendlich ist es ein Identity Management System (IdMS), das die entworfenen Prozesse eines IdM-Modells technisch realisiert und die praktische Nutzung der digitalen Identitäten ermöglicht.

Einordnung von IdM

Es mag überraschend erscheinen, dass für die Einführung eines IdM-Systems in einem Unternehmen nicht der Faktor Technik entscheidend ist, sondern organisatorische Faktoren wie der Mensch, die Politik und Prozesse überwiegen. So wird ein Mitarbeiter im produktiven Einsatz zwar nur den technischen Faktor nutzen, aber damit ein IdMS zufriedenstellende Erfolge erbringen kann, ist eine Gewichtung der organisatorischen Faktoren von etwa 80 Prozent (grober Erfahrungswert) erforderlich. Es gilt: Die Realisierung und Durchführung eines IdMS steht und fällt mit dem Faktor Mensch. Es muss sowohl das Konstrukt „Identity Management" als Ganzes gesehen werden, als auch der Sinn und Zweck der Umstellung kommuniziert werden, um die notwendige Akzeptanz bei den Mitarbeitern zu schaffen. Dadurch können Aufgaben in die Abteilungen delegiert und die Einführung eines IdMS auch aus den Abteilungen heraus vorangetrieben werden.

Identity Management erfordert – insbesondere bei der Realisierung – ein gewisses Umdenken hinsichtlich der Politik und Organisation eines Unternehmens. Es bedarf der Zusammenarbeit zwischen unterschiedlichen Bereichen. Ein besonders sensibler Aspekt ergibt sich aus der Tatsache, dass gewisse Verantwortungen (Rechte, Pflichten und letztendlich Macht) abgegeben und im Identity Management zentralisiert werden müssen.

In einem Unternehmen existieren unzählige Prozesse, die möglichst vollständig erfasst und in das IdMS eingepflegt werden müssen. Die Erfahrung zeigt, dass die Einführung eines IdMS treibende Kräfte zum Erfolg braucht, die sich nicht beiläufig, sondern konzentriert mit der Einführung des IdM befassen. Es muss Personal geschult werden, um die Anwender bei Problemfällen zu unterstützen.

Module, Komponenten und Funktionen

Das in Abbildung 1 gezeigte IdM-Modell stellt ein grundlegendes, allgemein gültiges und anbieterneutrales IdM-Referenzmodell dar. Es besteht grundsätzlich aus sieben Modulen, die für sich genommen nur eine beschreibende Rolle übernehmen und selbst keine Funktionalität bieten. Die Ausprägung eines Moduls sind seine Komponenten, die wiederum auf einen Pool an Funktionen zurückgreifen, mit denen die Aufgaben erfüllt werden.

Ein Beispiel: Bei der Einpflege eines neuen Mitarbeiters stößt die Identity-Administration-Komponente die Provisionierung an und die Synchronisierung der Daten wird gestartet. Die genauen Abläufe werden durch Policies und Workflows beschrieben und durch die Module in Compliance und Audit überwacht.

Das Modul Policies und Workflows stellt das Grundmodul eines jeden IdM dar, um das herum sich alle anderen Module anordnen. Es bildet die Basis für einen geregelten Arbeitsprozess und definiert und verwaltet die einzusetzenden Vorgaben, Prozesse und Richtlinien. Im Life Cycle Management werden die notwendigen Schritte unternommen, um Identitäten und ihre Metadaten bis zur Löschung in ein IdMS zu

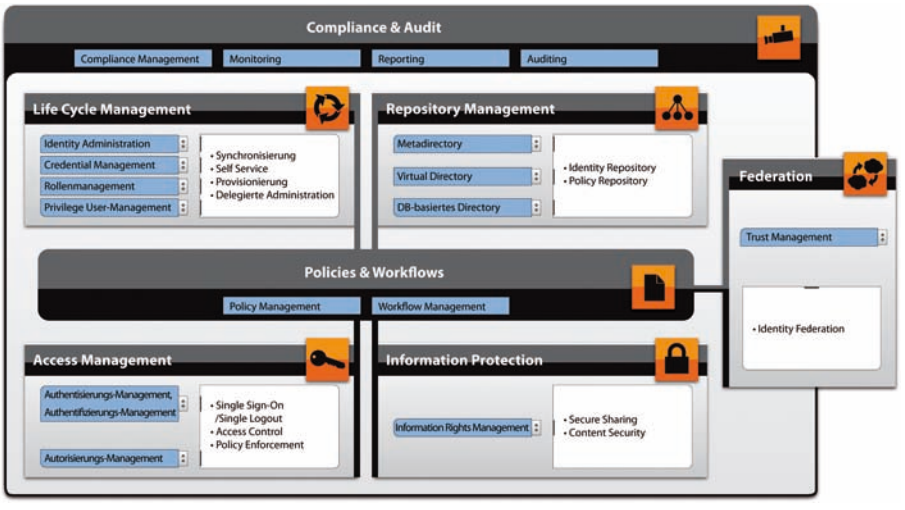


Abbildung 1: Ein grundlegendes, allgemein gültiges und anbieterneutrales IdM-Referenzmodell.

integrieren und zu verwalten. Das Modul Repository Management hat die Aufgabe, diejenigen Informationen in einem IdM zentral zu speichern und zu verwalten, die für die Identitäten in einem Netzwerk von Nutzen sein können. Das Access Management beinhaltet die Entscheidung über Zugriffsberechtigungen auf der Basis von Benutzeridentitäten, -rollen und Zugriffsrechten. Es beschreibt die notwendigen Mechanismen für den Zugriff auf ein IdMS sowie die Kontrolle und das Durchsetzen des Zugriffs. Die Technologien und Prozesse hinter dem Begriff der Information Protection gewährleisten, dass Informationen immer in ihrem angemessenen Schutzlevel gehalten und über Policies nur Personen mit entsprechenden Berechtigungen zugänglich gemacht werden. Das Modul Federation steht zum Teil außerhalb der anderen Module, um seine Funktion als „Vermittler" zwischen dem eigenen IdMS und dem anderer Organisationen herauszustellen. Es ermöglicht den gesicherten Austausch von Identitäts- bzw. Authentifizierungsinformationen zwischen mehreren IdMS basierend auf einem zuvor aufgebauten Vertrauensverhältnis. Schließlich beschreibt Compliance & Audit ein eher umfassendes Modul, da es die Prozesse aller Module überwacht und protokolliert. Unternehmen sind unter Umständen aufgefordert, gesetzliche und regulative Vorschriften einzuhalten, weshalb technische Lösungen benötigt werden, die bei der Einhaltung der Vorschriften und gegebenenfalls Erkennung und Bewertung von Risiken helfen. Das Ziel ist die Einhaltung der Rechtskonformität, also der Compliance.

Der (sichere) Weg zum IdMS

Ein IdMS in ein Unternehmen einzuführen, ist eine komplexe Aufgabe. Wünschenswert wäre deshalb eine definierte Vorgehensweise, an die sich die Betroffenen bei der Integration eines IdMS halten können. Aufgrund unterschiedlicher Ziele und Strukturen eines Unternehmens kann dieser Weg jedoch unterschiedlich ausfallen. Allerdings existieren in einem IdMS bestimmte Elemente, die beispielsweise nur in einer gewissen Reihenfolge auftreten können oder aus sicherheitstechnischen Aspekten zusammen einzuführen sind.

Der Identity-Management-Lebenszyklus in Abbildung 2 stellt diesen Ablauf grafisch dar. Einerseits repräsentiert er eine Anleitung zur Erstellung und fortführenden Weiterentwicklung des eigenen IdMS („Welche Aktion ist als Nächstes sinnvoll oder nötig?"). Er kann als ein Kompass angesehen werden, der nicht nur die notwendigen Schritte aufzeigt, sondern auch eine „Langzeit-Roadmap" für ein umfassendes IdMS repräsentiert. Andererseits stellt der Lebenszyklus einen Maßstab zur Bewertung der Ausgereiftheit des eigenen IdMS dar („Auf welchem Stand befindet sich mein IdMS?").

Die im IdM-Modell definierten Module eines IdMS werden in vier Abstufungen – die Reifegrade – unterteilt (Basic, Advanced, Professional und Future). Die Komponenten der Module wiederum werden entsprechend der notwendigen technischen Komplexität des Reifegrads mit fortlaufendem Levelgrad beschrieben, zum Beispiel Level 1 Self Service, Level 2 Self Service usw. Die Einteilung in Reifegrade und Level beschreibt das schrittweise Vorgehen bei der Einführung eines IdMS und ist dadurch bedingt, dass bestimmte Komponenten und Funktionen nur in Abhängigkeit voneinander eingeführt werden können oder sollten. So wird zum Beispiel deutlich, dass bei einem Basic IdMS die Umsetzung von SSO grundsätzlich nicht ratsam ist, da das Access Management noch keine starke Authentifizierung unterstützt und das Credential Management in Level 1 keine hinreichenden Konnektoren zur Verfügung stellen kann.

Wie die Bezeichnung „Lebenszyklus" und der noch nicht mit Inhalt gefüllte Reifegrad „Future IdM" andeuten, ist die vorgeschlagene Umsetzung in keinem Fall abschließend. Die Komponenten und Funktionen durchlaufen wiederholend die Prozesse der Überprüfung, Anpassung und Erneuerung. Zusätzlich können sich die Spezifikationen der einzelnen Reifegrade im Laufe der Zeit ändern, da sich zum Beispiel Verschlüsselungsstandards weiterentwickeln oder neue Techniken verwendet werden. Was heute noch ein Future IdMS ist, kann morgen schon Basic sein. Identity Management ist ein fortwährender Prozess, weshalb eine

Abbildung 2: Der Identity Management Lebenszyklus hilft bei der Integration eines IdMS

regelmäßige Prüfung vonnöten ist, um ein angemessenes Niveau des IdMS beizubehalten.

Sicherheit als Mehrwert

Durch den umfassenden Einsatz eines IdMS in einem Unternehmen bilden sich Mehrwerte in den Bereichen IT-Sicherheit, Compliance, Kostenreduktion und Benutzerfreundlichkeit. Im Folgenden seien die Mehrwerte in Bezug auf die IT-Sicherheit hervorgehoben, die sich in sechs Kategorien unterteilen lassen.

Zur ersten Kategorie gehört die Vermeidung von Fehlern durch Fehlbedienung. Beispielsweise stellt das IdMS ein komfortables Passwortmanagement zu Verfügung, welches den Nutzer, bei der Verwaltung seiner zahlreichen und ständig wechselnden Passwörter, entlastet. Eine potenzielle Schwachstelle, die vorher durch das Aufschreiben von diesen Passwörtern entstanden ist, wird somit geschlossen.

Der Einsatz starker Authentifizierungsmethoden bildet die zweite Kategorie. Bei Systemen mit sicherheitsrelevanten Daten und Informationen ist eine starke Authentifizierung unerlässlich. Hierfür kann eine sogenannte Multi-Faktor-Authentifizierung eingesetzt werden, bei der Wissen (Passwort, PIN etc.), Besitz (zum Beispiel Smart Card) und Merkmal (biometrisches Merkmal, etwa Fingerabdruck) kombiniert werden.

Die dritte Kategorie beinhaltet die Kontrolle von Systemen und Netzzugängen. Ein umfassend eingesetztes IdMS stellt sicher, dass alle aktivierten Zugänge in Benutzung und auch autorisiert sind, während verwaiste und nicht autorisierte Zugänge geblockt oder gelöscht werden.

Die Automatisierung und Nachvollziehbarkeit stellen zwei weitere Kategorien der Sicherheitsmehrwerte dar. Allgemein müssen potenziell kritische Aktionen nicht mehr manuell und auf Abruf getätigt werden, sondern laufen im Normalfall automatisch, basierend auf definierten Regeln und Workflows, ab. Die Nachvollziehbarkeit aller Aktionen innerhalb eines IdMS erfüllt Anforderungen, die sowohl intern (beispielsweise muss zu jeder Zeit erkennbar sein, welcher Nutzer aus welchem Grund welche Aktion getätigt hat) als auch extern (ein Unternehmen ist gegebenenfalls dazu aufgefordert, gesetzliche und regulative Vorschriften einzuhalten und umzusetzen) relevant sind.

Die letzte Kategorie beschreibt die durchgängige Dokumentensicherheit, die ein IdMS gewährleisten muss. Es bietet Grundlagen für die Rechtsverbindlichkeit von Dokumenten und setzt eine Reglementierung des Zugriffs auf Dokumente durch.

Die angesprochenen Punkte können zusammengefasst auch als Sicherheitsrichtlinien eines Unternehmens angesehen werden, wobei das IdMS die Möglichkeiten bietet, diese selbstständig umzusetzen und die Mitarbeiter weitestgehend zu entlasten.

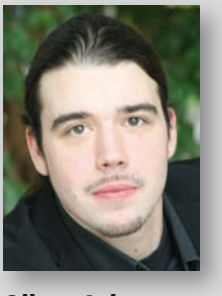
Fazit und Ausblick

Identity Management ist ein sehr lebendiges Thema, dessen Realisierung ein gutes IdM-Konzept verlangt und eine schrittweise Vorgehensweise nahelegt. Nach der erfolgreichen Integration ist die Arbeit jedoch nicht getan. Identity Management ist ein fortwährender Prozess, weshalb eine regelmäßige Überprüfung, Anpassung und Erneuerung zwingend erforderlich ist. Ziel ist es, das IdM-System stets auf einem angemessenen Niveau beizubehalten, um sowohl die Sicherheit als auch die Mehrwerte Kostenreduktion, Benutzerfreundlichkeit und Gewährleistung von Compliance voll auszuschöpfen.

Darüber hinaus ist Identity Management offen für weitere Techniken und Ideen. So lassen sich viele interessante aktuelle, aber auch zukünftige Technologien mit IdM verbinden. Durch den Einsatz von Trusted Computing beispielsweise stützt sich ein IdMS auf hardwarebasierte Sicherheit. Mittelpunkt dieser Idee ist das Trusted Platform Module (TPM), das als vertrauenswürdiger Sicherheits-Anker fungiert und potenziell manipulierbare Software hardwarebasiert absichert. Aber auch die Einbindung von mobilen Endgeräten wie Notebooks oder Smartphones ist im IdM-Kontext denkbar und auch sicher realisierbar. Bei Technologien wie Network Access Control (NAC) kann mittels Regeln und Policies beschrieben werden, wie ein IT-System ein Netzwerk sicher betreten kann.
Es ist offensichtlich, dass die professionelle Verwaltung von Identitäten kein „Ding der Unmöglichkeit" ist. Den zahlreichen Problemstellungen beim Identity Management muss nur auf die richtige Art und Weise begegnet werden. Von Bedeutung ist das Wissen, dass ein Identity Management System kein Tool ist, das einmal gekauft und installiert wird und anschließend jahrelang funktioniert. Ein IdMS ist ein komplexes System sowohl technischer als auch organisatorischer Faktoren, das einer fortwährenden Pflege bedarf, um zufriedenstellende Erfolge zu bieten. ■

Prof. Dr. Norbert Pohlmann
ist Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen
(www.internet-sicherheit.de)

B.Sc. Sebastian Feld
ist wissenschaftlicher Mitarbeiter des Instituts für Internet-Sicherheit im Forschungsschwerpunkt Identity Management



Oliver Achten
ist Mitarbeiter des Instituts für Internet-Sicherheit im Forschungsbereich Identity Management