# Our Digital Identity

*Die Zukunft spricht IdM*

Sponsoren: betasystems, IBM

Eine Analyse von it Research

info@it-research.net www.it-research.net

IT Research ist ein deutschsprachiges Unternehmen, das Studien, Bulletins und White Papers im Bereich der Informationstechnik erstellt. Ziel ist, auf neueste Technologien hinzuweisen, IT-Investitionen der Unternehmen noch rentabler zu machen, Fehlinvestitionen zu vermeiden und Risiken zu minimieren. Um dies zu erreichen, arbeiten wir mit einem Netzwerk von Kompetenzträgern auf den verschiedensten Gebieten der IT zusammen.

IT Research

IT Research, Ulrich Parthier, Mühlweg 2b, 82054 Sauerlach, Postfach 1128, 82050 Sauerlach
Tel.: +49 8104-6494-14, E-Mail: u.parthier@it-research.net
Internet: www.it-research.net



ISBN: 936052-28-X

# Inhaltsverzeichnis

# 1. Einführung

Identity Management, 2003 noch ein Trend-Thema, hat sich inzwischen als eines der zentralen Themen der IT etabliert und gewinnt auch in der Breite immer mehr an Aufmerksamkeit. Diese andauernde und weiter wachsende Aufmerksamkeit ist in zwei Faktoren begründet. Zum einen ist Identity Management, anders als andere Schlagwörter, kein wirklich neues Thema, sondern die Gesamtbetrachtung sowohl von seit Jahren bekannten und genutzten Technologien als auch von neuen, die Kernfunktionen erweiternden Anwendungen. Dazu gehören Verzeichnisdienste, Meta Directory-Dienste, starke Authentifizierung, Provisioning oder virtuelle Verzeichnisdienste, um nur einige zu nennen. Zum anderen wird immer deutlicher, dass sich die Erwartungen an die IT nur erfüllen lassen, wenn die Basis durch das Identity Management geschaffen wird. Sichere, womöglich unternehmensübergreifende Geschäftsprozesse lassen sich nur realisieren, wenn man die Identitäten der Nutzer dieser Prozesse kennt. Die Anforderungen im Bereich der Compliance, also der Erfüllung gesetzlicher und interner Vorschriften, sind ebenso nur dann erfüllbar, wenn man weiß, wer wann was gemacht hat und auch Richtlinien hat, mit denen gesteuert wird, wer wann was machen darf. Ohne das „wer“, also die Sicht auf die Identität von Benutzern, sind diese Themen nicht lösbar.

Dass Identity Management ein Top-Thema ist, wird auch an den Akquisitionen der letzten Jahre deutlich. Sun hat Waveset übernommen, HP unter anderem TruLogica, Netegrity hat Business Layers gekauft, um dann einige Monate später wieder von CA übernommen zu werden. BMC hat Calendra gekauft und die meisten anderen großen Anbieter im Markt wie IBM oder Microsoft haben in den letzten Jahren ebenfalls in Firmen und deren Technologien investiert, um im dynamischen Identity Management-Markt schnell reagieren zu können.

# 2. Was ist Identity Management?

Identity Management hat sich als zusammenfassender Begriff für alles, was im Zusammenhang mit digitalen Identitäten steht, etabliert. Die Sichtweise des Themas ist je nach Hersteller, Analyst oder Beratungsunternehmen etwas unterschiedlich, was allerdings vor allem an den jeweiligen Eigeninteressen liegt. Auch die Begrifflichkeiten unterscheiden sich – oft wird auch von IAM für Identity & Access Management gesprochen.

In den letzten beiden Jahren hat sich aber eine breite Sichtweise auf das Thema durchgesetzt. Identity Management umfasst Prozesse und Technologien für die Erstellung, Verwaltung und Nutzung digitaler Identitäten, die Authentifizierung, die Rechtevergabe und als Randbereich auch die Nutzung von digitalen Identitäten in Anwendungen. Dazu zählen einerseits die Basisfunktionen der Authentifizierung und Autorisierung, aber auch weitergehende Lösungen, wie sie sich im Bereich eGovernment, bei der Personalisierung von Benutzerinformationen in Portalen oder im Digital Rights Management (DRM) finden.

Durch die Vielzahl unterschiedlicher Themenfelder und dadurch, dass viele Technologien sich zumindest teilweise in ihren Einsatzbereichen überlappen, ist der Überblick über den Markt schwierig. Das Interesse der Hersteller, die Sichtweise ihren Lösungen anzupassen, trägt dazu noch weiter bei.

Wichtige Segmente des Identity Management-Markts sind Verzeichnisdienste, Meta Directory-Dienste, Access Management-Lösungen, Directory-Administration-Systeme, PKIs und andere Ansätze für die

starke Authentifizierung, Web Access Management und Systeme für die Web Service Security, Single Sign-On-Lösungen und das Provisioning. Neue Themen wie virtuelle Verzeichnisdienste gewinnen immer mehr an Gewicht. Das wichtigste Thema der nächsten Jahre wird nach unserer Ansicht aber die Identity Federation werden, die inzwischen einen Reifegrad erreicht hat, mit dem sie produktiv genutzt werden kann. Identity Federation ist die gemeinsame Nutzung von Identitätsinformationen über mehrere Anwendungen hinweg unter Verwendung definierter Standards für den Austausch dieser Daten.

## 3. Die Top-Themen im Identity Management

Auch innerhalb des Identity Managements gibt es Themen, die mehr oder weniger populär sind. Die noch vor einigen Jahren intensive Diskussion über den „richtigen" Verzeichnisdienst, damals vor allem als Microsoft versus Novell geführt, hat deutlich nachgelassen. Die Erkenntnis, dass ein Verzeichnisdienst alleine ohnehin nicht ausreichend ist, hat sich durchgesetzt. Meta Directory-Dienste spielen in der Diskussion derzeit ebenfalls eine untergeordnete Rolle, was vor allem daran liegt, dass sie sich vor allem in groß angelegten Projekten als komplex erwiesen haben. Das bedeutet allerdings keineswegs, dass diese Technologien verschwinden werden, denn für eine umfassende Identity Management-Infrastruktur werden verschiedene Ansätze benötigt.

Die meiste Aufmerksamkeit haben in den letzten beiden Jahren die Bereiche des Provisioning und des Password Managements auf sich gezogen. Inzwischen gewinnt Federation mehr und mehr an Gewicht. Die Bedeutung dieser Themen liegt primär darin begründet, dass der Business Value dabei offensichtlich ist, während andere Felder des Identity Managements die erforderliche Infrastruktur bilden. Nur sind Infrastruktur-Maßnahmen in der IT heute kaum dazu geeignet, die Budget-Freigaben zu erhalten, auch wenn sie bei einer Gesamtbetrachtung oftmals erforderlich sind, um die Wertversprechen anderer Ansätze zur Realität werden zu lassen.

### 3.1 Provisioning

Provisioning bedeutet „Bereitstellung". Beim Provisioning geht es um den Prozess der Bereitstellung von Ressourcen. Die ersten Ansätze haben auf die Einstellung neuer Mitarbeiter eingezielt, denen am ersten Arbeitstag bereits alle erforderlichen Arbeitsmittel, Zugangsberechtigungen und so weiter zur Verfügung gestellt werden sollten.

Daraus sind Ansätze entstanden, die nun generell auf alle Veränderungsprozesse rund um Mitarbeiter abheben, soweit das Identity Provisioning betrachtet wird – also die Einstellung, Jobwechsel und das Verlassen des Unternehmens. Gerade der letztgenannte Bereich, der gelegentlich auch als De-Provisioning bezeichnet wird, ist besonders wichtig, damit in einem strukturierten Prozess Geräte wie Notebooks eingezogen, Firmenwagen zurückgefordert und vor allem Zugangsberechtigungen zu internen IT-Systemen gesperrt werden.

Provisioning wird mittlerweile aber nicht mehr nur als Identity Provisioning gesehen. Es gibt Provisioning auch bei der Konfiguration von Servern und in anderen Bereichen. Provisioning kann als übergeordneter Prozess verstanden werden, mit dem die erforderlichen IT-Ressourcen, aber auch Non-IT-Assets in definierter Weise bereitgestellt respektive wieder zurückgefordert werden. Identity Provisioning ist ein wichtiger Teilbereich davon.

In den großen IT-Strategien der Key-Player wie IBM, HP und anderen spielt das Provisioning bei Schlagworten wie „On Demand“, „Agilität“ oder „Adaptive Enterprise“ eine zentrale Rolle mit dem Identity Provisioning als einem wichtigen Teilbereich. Zwischen dem Identity Management und dem Provisioning gibt es deutliche Überlappungen. Es ist aber weder richtig, Identity Management als Teil des Provisioning zu verstehen, weil zum Identity Management – wie oben ausgeführt – noch viel mehr gehört, noch ist die umgekehrte Betrachtung richtig, weil eben nicht nur Identitäten „provisioniert“ werden. Darüber hinaus sind die Bereiche auch nicht völlig zu trennen. So bestehen zwischen dem Identity Provisioning und dem Client-Management als einem weiteren Bereich der Ressourcenbereitstellung mit Softwareverteilung und Systemkonfiguration enge Zusammenhänge, auf die weiter unten noch näher eingegangen wird.

Hier zeigt sich aber schon, dass Identity Provisioning kein homogener Markt ist. Wie bei „Modebegriffen“ üblich, versuchen die meisten Hersteller, sich dazu zu positionieren, so dass es heute kaum noch einen Anbieter gibt, der nicht von sich sagt, eine Provisioning-Lösung im Portfolio zu haben. Das gilt für Anbieter, die historisch aus dem Bereich der Meta Directory-Dienste kommen, ebenso wie für Hersteller aus dem Bereich des Passwort-Managements und anderer Felder des Identity Managements. Daher ist auch eine weitere Differenzierung erforderlich.

Eine Gruppe von Anbietern fokussiert auf die grafische Darstellung des Workflows, von dem aus viele verschiedene Systeme angestoßen werden können, wobei die technische Integrationstiefe zu diesen Systemen oft gering ist. Hier wird entsprechend auch auf Standards wie SPML (Service Provisioning Markup Language) gesetzt, um dann andere Systeme ansteuern zu können, die die eigentlichen Änderungen in den Zielsystemen wie das Anlegen neuer Benutzer durchführen. Generell ist aber eine Entwicklung dahin zu beobachten, dass einerseits technisch komplexere Lösungen um grafische Workflow-Tools ergänzt und andererseits die eher Workflow-orientierten Systeme nach und nach auch eine immer engere Anbindung an Zielsysteme erhalten.

Ein kritischer Punkt bei dieser Gruppe von Provisioning-Lösungen kann die Integrationstiefe sein. Das beginnt bei der Frage, wie flexibel und granular Anpassungen vorgenommen werden können und geht bis hin zum Erkennen von Änderungen in den angeschlossenen Systemen. Wenn außerhalb des Provisioning-Workflows administriert wird, kann es je nach technischem Ansatz zu Situationen kommen, in denen die Daten in den verschiedenen Systemen auseinander laufen, wenn das Provisioning-System die lokalen Änderungen nicht erkennt.

Andere Hersteller setzen stärker auf die Automatisierung von Prozessen „unter der Oberfläche“. Dabei geht es darum, auch komplexe Prozesse anstoßen zu können und eine hohe Integrationstiefe zu erreichen, aber ohne die Werkzeuge für die grafische Definition von Prozessen. Die Anbieter in diesem Marktsegment haben in der letzten Zeit verstärkt versucht, auch die grafische Komponente höher zu gewichten und dazu teilweise auch Spezialisten akquiriert, wie zuletzt der Kauf von Calendra durch BMC zeigt. Funktionen wie beispielsweise das Anstoßen von Beschaffungsprozessen für Notebooks oder Mobiltelefone und ihre Kontrolle über einen zentralen Workflow sind hier aber noch eher die Ausnahme.

Die Hersteller in diesem Bereich sind typischerweise stärker auf das interne Access Management ausgerichtet und unterstützen auch Ansätze des RBAC (Role Based Access Control), also rollenbasierende Verfahren für die Zugriffssteuerung auf interne Ressourcen, die teilweise bis hin zur Vergabe von Zugriffsberechtigungen gehen.

Bisher noch die Ausnahme sind Lösungsansätze, bei denen das Identity Provisioning um andere Provisioning-Funktionen ergänzt wird. Hier gibt es einzelne Implementierungen im Bereich des Client-Managements, mit denen die Softwareverteilung und das Provisioning integriert werden können. Alle Lösungsansätze haben die Gemeinsamkeit, dass administrative Prozess in strukturierter Form erfolgen. Das bringt Vorteile bezüglich des Aufwands, der zeitlichen Dauer und der Zuverlässigkeit, mit der diese Prozesse durchgeführt werden. Provisioning ist damit ein unverzichtbares Element in Identity Management-Strategien, auch wenn damit alleine nicht alle Herausforderungen gelöst werden können.

**Rollen, Regeln, Richtlinien**

Gerade im Zusammenhang mit dem Provisioning wird immer wieder über RBAC (Role Based Access Control) und damit auch über Rollenkonzepte diskutiert. Die Idee von RBAC ist, die Zugriffsberechtigungen in Systemen basierend auf Rollen zu vergeben, denen die Benutzer zugeordnet werden. Wenn sich die Rolle eines Benutzers ändert, ändern sich auch die Zugriffsberechtigungen. Diese Konzepte sind keineswegs neu und finden sich in ähnlicher Form eigentlich bei jedem Sicherheitskonzept – wenn Berechtigungen über Gruppen vergeben werden, ist das nichts anderes als eine spezielle Repräsentation von Gruppen.

Von Gegnern der Rollenkonzepte wird gerne ins Feld geführt, dass diese extrem aufwändig seien. Die Befürworter verweisen unter anderem auf die Standardisierung und das stringente Modell der Sicherheit, das so implementiert wird. Die Praxis zeigt, dass der Erfolg von Rollenmodellen primär davon abhängt, wie sie umgesetzt werden. Wer versucht, das gesamte Unternehmen in fein definierten Rollen abzubilden, wird scheitern. Hier ist Pragmatismus gefragt, indem man die Rollen so fein wie nötig, aber so grob wie möglich definiert. Dann sind Rollenkonzepte beherrschbar. Und in der einen oder anderen Form – sei es über Rollen, Gruppen, Kontexte oder andere Ansätze – werden solche Konzepte immer benötigt, um Sicherheit effizient steuern zu können.

Dabei stehen Rollenkonzepte immer neben Regeln, die weitere Festlegungen für den Zugriff auf die verwalteten Systeme enthalten. In der Summe ergeben sich die Richtlinien für die Zugriffssteuerung. In jedem Fall zeigt die Erfahrung, dass die verwendeten Begriffe wie Rollen für die Differenzierung von Produkten wenig geeignet sind und ein Rollenmodell auch nicht unbedingt etwas darüber aussagt, wie komplex die Implementierung ist. Denn dabei kommt es mehr auf die Projektvorgehensweise an – mit der man einfache Ansätze komplex und vermeintliche komplexe, theoretische Ansätze pragmatisch umsetzen kann.

## 3.2 Password Management

Das zweite wichtige Thema im Identity Management ist das Password Management. Auch hier gilt, dass sich hinter einem Begriff recht unterschiedliche Ansätze verbergen können. Es lassen sich im Kern drei Verfahren unterscheiden:

- Password Reset
- Password Synchronization
- Single Sign-On

In allen Fällen geht es um das Management von Kennwörtern, das aber unterschiedlich gelöst wird. Die verschiedenen Ansätze schließen sich gegenseitig nicht aus, sondern ergänzen sich teilweise sogar.

Die einfachste Lösung ist das Passsword Reset, also das Zurücksetzen von Kennwörtern. Die meisten Anbieter haben sowohl eine Web-Schnittstelle für die Anwender als auch eine Schnittstelle für den Helpdesk realisiert. Außerdem wird von verschiedenen Herstellern auch die Einbindung von Spracherkennungslösungen unterstützt, um Kennwörter auch über das Telefon zurücksetzen zu können.

Password Reset ist verhältnismäßig einfach, weil die Kennwörter in den verwalteten Systemen nur auf den gleichen Stand gebracht werden müssen. Änderungen an lokal gespeicherten Kennwörtern müssen nicht erkannt werden. Daher gibt es auch kaum einen Hersteller, der solche Verfahren nicht im Portfolio hat. Oft werden diese auch als Password Self Service bezeichnet, weil die Benutzer selbst ihre Kennwörter zurücksetzen können.

Das Nichterkennen von Kennwortänderungen in den angeschlossenen Systemen ist die größte Schwachstelle dieser Verfahren. Wenn ein Benutzer beispielsweise auf seinem Windows-Client sein Active Directory-Kennwort ändert, sollte das abgefangen werden und in Änderungen des Kennworts auch in den anderen Systemen resultieren. Ohne Synchronisation von Kennwörtern ist das Risiko hoch, dass es in verschiedenen Systemen unterschiedliche Kennwörter gibt.

Hier setzen Lösungen für die Kennwortsynchronisation an, die mit Agents auf den angeschlossenen Systemen die Kennwortänderungen erkennen. Diese werden dann an die übrigen Systeme weitergeleitet. Die Herausforderung dabei ist die Erstellung der Agents, weil sich die Schnittstellen für das Kennwortmanagement, in die sich diese einklinken können, von System zu System unterscheiden. Zudem unterstützen nicht alle Plattformen solche Schnittstellen. Deshalb werden von den Anbietern von Password Synchronization-Lösungen auch nie alle Systemplattformen unterstützt. Typischerweise werden Plattformen, bei denen keine Synchronisation erfolgen kann, über das Password Reset angebunden.

Schließlich gibt es noch das Feld des Single Sign-Ons. Dabei geht es nicht darum, die Kennwörter oder andere Credentials für Zielsysteme gleichzusetzen, sondern um die Speicherung der jeweils spezifischen Anmeldeinformationen für die Zielsysteme. Wenn dann ein Zugriff erfolgt, werden diese Informationen aus einem sicheren Speicher gelesen und an das Zielsystem übergeben. Das setzt im besten Fall voraus, dass die Anmeldedialogfelder analysiert werden, um die richtigen Informationen in die richtigen Felder schreiben zu können, kann im Extremfall aber auch Anpassungen der Anwendungen erforderlich machen. Der Aufwand für solche Verfahren ist relativ hoch. Der Vorteil liegt darin, dass unterschiedliche Kennwortrichtlinien einfach abgedeckt werden können und sich je nach Hersteller auch digitale Zertifikate und andere Credentials einbinden lassen.

Keiner der Ansätze ist ohne Nachteile, so dass typischerweise mit einer Kombination gearbeitet wird. So kann beispielsweise die Kennwortsynchronisation auch genutzt werden, um automatische Kennwortänderungen für Single Sign-On-Lösungen durchzuführen oder Kennwörter zunächst in die Kennwortspeicher zu schreiben.

Ein kritischer Aspekt bei allen Verfahren ist die Sicherheit. Die Gründe, die für die Einführung von Password Management-Lösungen genannt werden, sind vor allem mehr Komfort für die Anwender

und eine Entlastung des Helpdesks von den Benutzeranforderungen wegen vergessener Kennwörter. Vom Password Management versprechen sich die Unternehmen erhebliche Kosteneinsparungen.

Dabei darf aber nicht übersehen werden, dass durch konsequente Vereinheitlichung von Kennwörtern oder ein zentrales Kennwort für den Credential-Speicher bei Single Sign-On-Systemen auch das Risiko steigt. Wenn ein Angreifer an dieses Kennwort kommt, hat er Zugang zu allen Systemen. Dem steht entgegen, dass Benutzer nach Einführung von Password Management-Lösungen typischerweise nicht mehr mit Standard-Kennwörtern arbeiten und die Chance, dass sie sich ein Kennwort merken, sehr viel höher ist als die Wahrscheinlichkeit, dass viele Kennwörter gemerkt und nicht auf der Schreibtischunterlage oder an anderen unsicheren Stellen aufgeschrieben werden.

Dennoch ist die Einführung von Password Management-Lösungen nur ein erster Schritt, dem konsequenterweise die Einführung von Verfahren für die starke Authentifizierung folgen muss. Das kann die Nutzung von Smartcards mit digitalen Zertifikaten sein, das kann aber auch die zusätzliche Verwendung biometrischer Verfahren sein.

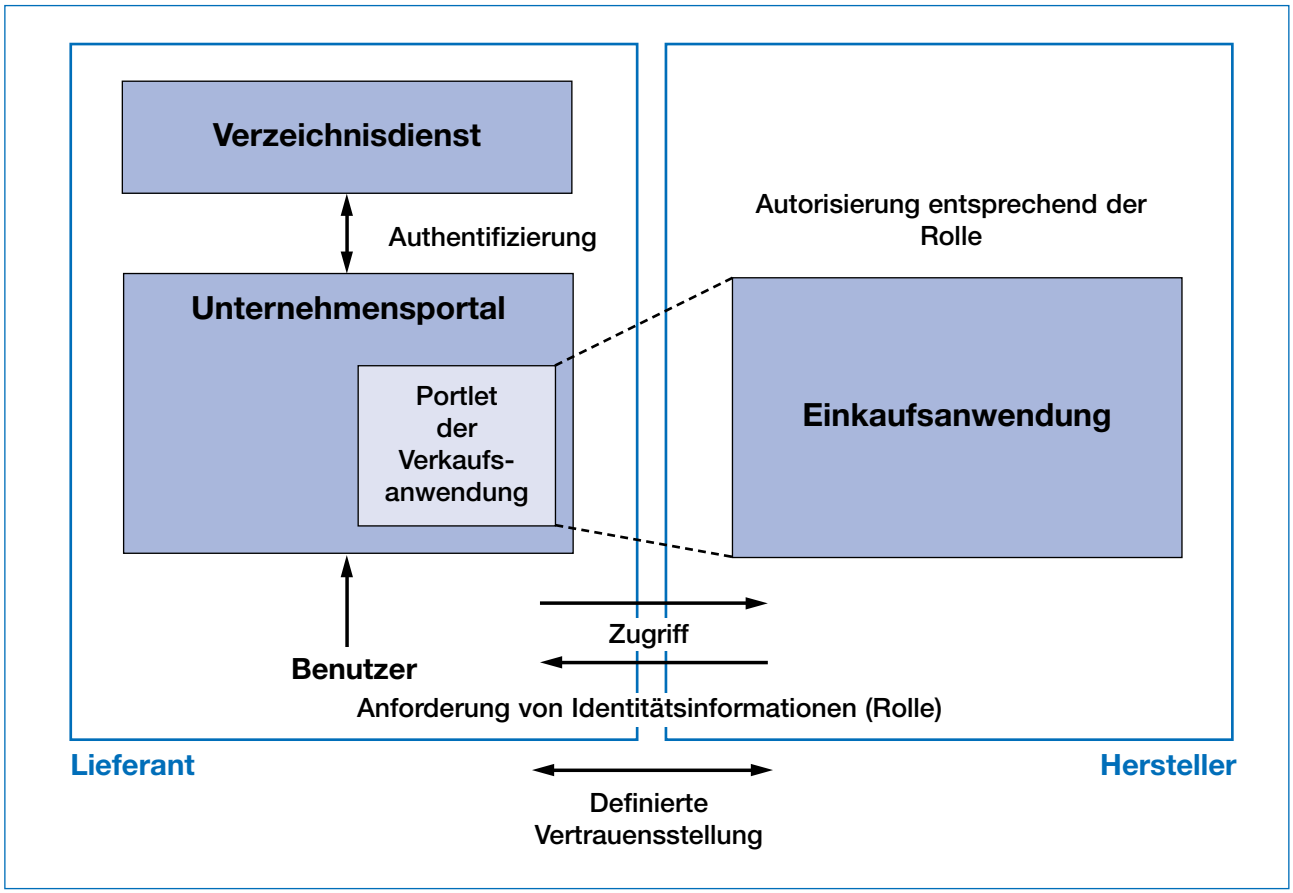
Zu berücksichtigen ist darüber hinaus, dass die Verwaltung von Kennwörtern für verschiedene Systeme auch voraussetzt, dass es eine einheitliche Sicht auf die Identität der Benutzer in diesen Systemen gibt. Diese kann dadurch hergestellt werden, dass die Nutzer zu Beginn ihre verschiedenen Benutzernamen und Kennwörter erst in diesem System eintragen. Mehr Sinn macht es aber, wenn die Benutzernamen vereinheitlicht werden – ein Prozess, der auch für das Provisioning fast unverzichtbar ist. Die Praxiserfahrungen in diesem Zusammenhang zeigen, dass die Datenqualität in Verzeichnissen meist sehr viel schlechter als befürchtet ist.

Gerade diese erforderliche Vereinheitlichung von Identitäten in den angeschlossenen Verzeichnissen macht auch deutlich, dass man einzelne Ansätze des Identity Managements nicht isoliert betrachten kann. Sowohl Provisioning als auch Password Management können interessante Ansatzpunkte für Identity Management-Projekte sein. Sie sind geeignet, schnell erste Erfolge zu zeigen. Dauerhafter Nutzen wird aber nur erzielt, wenn diese Verfahren im Kontext einer Identity Management-Gesamtstrategie stehen.

### 3.3 Federation

In ihrem Trend-Report nennen die Analysten von Kuppinger Cole + Partner (www.kuppingercole.de) die Identity Federation als das Top-Thema 2005 im Identity Management – weniger, weil es bereits in großer Zahl Projekte und Implementierungen geben wird als vielmehr, weil sie erwarten, dass dieses Thema die Diskussionen im Identity Management zunehmend dominieren wird. Für diese Einschätzung spricht, dass sich mit Hilfe der Identity Federation viele Business-Probleme einfacher oder überhaupt erst lösen lassen. Um den (potenziellen) Wert der Identity Federation zu verstehen, muss man sich zunächst mit dem Verfahren auseinandersetzen.

Die Grundidee der Federation ist die gemeinsame Nutzung von Identitätsinformationen über verschiedene Systeme hinweg. Wenn ein Benutzer auf das Portal in seinem Unternehmen zugreift, wird er dort gegen einen Verzeichnisdienst authentifiziert. In diesem sind Identitätsinformationen zu dem Benutzer gespeichert. Es ist nun denkbar, dass er in diesem Portal auf eine Anwendung der (externen) Betriebskrankenkasse zugreift und mit dieser Arbeit. Im Federation-Konzept vertraut diese An-




**Identity Federation erlaubt die einfache, unternehmensübergreifende Kopplung von Systemen.**

wendung dem Portal respektive dessen Verzeichnisdienst bezüglich der Authentifizierung. Sie fordert bei Bedarf weitere Informationen zu dem Benutzer an – das könnten die Mitarbeiternummer, das Geburtsdatum oder andere Informationen sein, die vielleicht sogar aus dem HR-System gelesen werden müssen. Die Anwendung der Krankenkasse muss diese Informationen nicht mehr selbst verwalten, was die Integration zwischen zwei oder mehr Anwendungen vereinfacht.

Allerdings gibt es einige wichtige Anforderungen für dieses Modell. Zum einen müssen die Identitäten bei den verschiedenen Anwendungen aufeinander abgebildet werden. Das geschieht häufig dadurch, dass nur Informationen zu einer Rolle an das andere System übergeben werden. So könnten sich beispielsweise Mitarbeiter im Support eines IT-Dienstleisters bei diesem anmelden und dann auf Systeme eines Kunden zugreifen, wobei sie automatisch über die Rolleninformationen einer bestimmten Gruppe zugeordnet werden. Wenn ein neuer Mitarbeiter beim IT-Dienstleister eingestellt wird, muss diesem nur dort die Rollenzugehörigkeit zugeordnet werden. Beim Kunden ist aber keine Administration erforderlich.

Neben dieser Zuordnung spielt das Vertrauensverhältnis zwischen den Partnern die entscheidende Rolle. Bei einer Identity Federation über interne Anwendungen hinweg lässt sich das meist recht leicht herstellen. Beim Zusammenspiel mit externen Partnern muss es zunächst genau definiert werden. Hilfreich sind dabei bestehende vertragliche Regelungen beispielsweise über den Austausch von Informationen zwischen einem Arbeitgeber und einer Krankenkasse.

Um den Aufbau dieser Vertrauensverhältnisse auch in offenen Strukturen zu vereinfachen, hat Sun schon vor einigen Jahren die Liberty Alliance ins Leben gerufen. Diese hat mittlerweile mehrere Hundert Unternehmen als Mitglieder und Standards definiert, die als Basis für die Identity Federation dienen können. Prozesse, die sich über mehrere Anwendungen in einem Unternehmen oder über Unternehmensgrenzen hinweg erstrecken, lassen sich auf diese Weise sehr viel einfacher als bisher realisieren.

### 3.4 Weitere Einsatzfelder

Das bedeutet aber keineswegs, dass es beim Identity Management nur um Provisioning, Password Management und zukünftig Federation geht. Verzeichnisdienste sind das Fundament. Und es gibt genug Fälle, in denen eine Synchronisation von Verzeichnisinformationen mit Hilfe von Meta Directory-Diensten die beste Lösung ist, statt mit einer losen Kopplung über Federation oder nur mit Hilfe von Provisioning-Workflows zu arbeiten. Virtuelle Verzeichnisdienste helfen beim Zugriff auf Informationen aus verschiedenen Verzeichnissen, Web Access Management ist für den relativ einfachen Schutz von Web-Anwendungen bei externen Zugriffen ein interessanter Ansatz. Daher müssen die verschiedenen Ansätze auch immer im Kontext einer Gesamtstrategie für das Identity Management betrachtet werden, auch wenn man sich bei der Einführung zunächst auf wenige Punkte fokussiert, die beispielsweise einen besonders hohen Business Value versprechen.

## 4. Die Treiber des Identity Managements

Die Identity Management-Analysten von Kuppinger Cole + Partner (www.kuppingercole.de) haben sechs Business-Treiber für das Identity Management identifiziert:

- Umsetzung von Geschäftsprozessen
- Compliance
- Neue Anwendungen wie Digital Rights Management, eGovernment und andere
- Kostenoptimierung
- Sicherheit
- „Ease of use“ durch weniger Benutzerkonten und Kennwörter

Auf die neuen Anwendungen wurde bereits kurz eingegangen, der „Ease of use“ ist weitgehend selbsterklärend. Die anderen Aspekte sind aber eine nähere Betrachtung wert, weil sich daran auch zeigt, dass sich die Treiber für das Identity Management geändert haben. Der Blickwinkel ist nicht mehr nur Administration und Sicherheit, sondern vom Wandel der IT geprägt, die nun in der Lage sein muss, Geschäftsprozesse effizient umzusetzen. Die schon erwähnten Schlagworte wie On-Demand-IT, Agilität oder Adaptiveness stehen dafür. IT ist mehr denn je ein Dienstleister, der dafür zu sorgen hat, dass das Business optimal funktioniert und die Business-Anforderungen schnell, effizient und sicher umgesetzt werden können.

### 4.1 Geschäftsprozesse optimieren

Das kann aber ohne Identity Management nicht gelingen. Geschäftsprozesse können nur sicher gestaltet werden, wenn es einen einheitlichen Blick auf Identitäten gibt. Ob dazu mit einer losen Kopp-

lung wie bei der Identity Federation oder mit einer engen Kopplung durch Meta Directory-Dienste oder gemeinsam genutzte Verzeichnisdienste gearbeitet wird, lässt sich nur im Einzelfall entscheiden. Der oft zu findende Ansatz, einfach eine weitere Sicherheitsschicht bei der Umsetzung eines Geschäftsprozess zu realisieren, führt aber in jedem Fall nur zu Sicherheitsinseln, die auf Dauer nicht mehr beherrschbar sind.

Auch die Effizienz der Umsetzung von Geschäftsprozessen hängt direkt am Identity Management. Wenn eigene Sicherheitsschichten durch ein eigenes Benutzermanagement für jede Anwendung, mit der ein Geschäftsprozess umgesetzt wird, realisiert werden, ist der Implementierungsaufwand hoch. Zudem steigt der Administrationsaufwand kontinuierlich an. In der Konsequenz entstehen auch dadurch Sicherheitsprobleme. Die Compliance-Anforderungen, auf die nachher noch eingegangen wird, lassen sich auf diese Weise nicht erfüllen.

### Lose Kopplung – enge Kopplung

Ein interessantes Thema in diesem Zusammenhang ist die Frage nach der Kopplung von Identitätsinformationen in verschiedenen Systemen. Hier gibt es mittlerweile eine beachtliche Bandbreite. Das Spektrum reicht von einem gemeinsamen Verzeichnisdienst für verschiedene Anwendungen über Meta Directory-Dienste, das Provisioning und virtuelle Verzeichnisdienste bis hin zur Identity Federation als der losesten Form der Kopplung solcher Informationen.

Keiner dieser Ansätze ist frei von Nachteilen. Für eine enge Kopplung spricht, dass die Informationen gesichert den gleichen Stand haben und nicht, wie beispielsweise bei der Federation, während der Verarbeitung auf verschiedene Systeme zugegriffen wird. Dafür steigt aber auch die Komplexität, wie sich an den Datenstrukturen von Verzeichnissen zeigt, in die viele Anwendungen Daten schreiben und wie auch an manchem Meta Directory-Projekt bereits deutlich geworden ist. Provisioning als ein Mittelweg bietet das Risiko, dass Daten lokal verändert werden, so dass es zu Inkonsistenzen kommt. Virtuelle Verzeichnisdienste sind ohnehin eher auf Abfragen als Änderungen ausgelegt. Letztlich gilt es, in einer Identity Management-Strategie die richtige Auswahl zwischen den verschiedenen Ansätzen zu treffen. Diese wird in hohem Maße auch von der „Hoheit“ über die Informationen geprägt – je einheitlicher diese ist, desto eher lässt sich eine enge Kopplung realisieren.


**Für die Integration von Identitätsinformationen gibt es verschiedene Ansätze. In Projekten gilt es, den adäquaten Weg zu wählen.**

### 4.2 Compliance

Während in den USA Compliance mittlerweile das Top-Thema auch für die IT ist, spielt es im deutschsprachigen Raum noch keine so große Rolle. Das liegt vor allem daran, dass es in den USA einige prominente Fälle wie Enron und Worldcom gab, die das Thema in die Schlagzeilen brachten. Die Politik hat darauf mit weiteren Regelungen wie dem Sarbanes-Oxley-Act (SOX) reagiert.

Die Bedeutung darf aber auch im europäischen Raum nicht unterschätzt werden. SOX wirkt sich auch auf Unternehmen mit Rechnungslegung in den USA aus, also beispielsweise solche, die in den USA an einer Börse gelistet sind. Andere, branchenspezifische Regelungen wie HIPAA sind für Unternehmen dieser Branchen wichtig, wenn sie in den USA Geschäfte tätigen wollen. Darüber hinaus gibt es auch in Europa viele Vorschriften, von den Risiko-Management-Regelungen in AG und GmbhG über die Datenschutzregelungen bis hin zu Basel II.

Compliance bedeutet nun, dass Unternehmen sich an diese Regelungen, ebenso wie an Standards beispielsweise für die Corporate Governance halten. Das bedeutet vor allem, dass es klare Prozesse gibt, mit denen festgelegt wird, wer was im Unternehmen machen darf. Provisioning und die dadurch definierten Workflows ist ein wichtiger Ansatz dafür. Es bedeutet aber auch die Fähigkeit nachvollziehen zu können, wer wann was getan hat – also das Auditing. Beides funktioniert nur, wenn die Frage des „wer“ geklärt ist. Wenn ein Benutzer in jedem System unterschiedliche Benutzerkennungen hat, wird die Analyse seines Handelns sehr schwierig. Compliance ist dann kaum noch zu erreichen. Identity Management ist daher eine Grundvoraussetzung für Compliance.

Da Compliance-Anforderungen aber vor allem von der Geschäftsführung und aus dem Controlling kommen, ist es auch einer der wichtigsten Ansatzpunkte, um an Budgets für Identity Management-Projekte zu gelangen.

### 4.3 Sicherheit

Compliance hat einiges mit Sicherheit zu tun, wobei das Thema Sicherheit insgesamt noch breiter ist. In seiner Rolle als Business-Treiber für das Identity Management ist Sicherheit immer noch von Bedeutung, wobei es heute um deutlich mehr als nur die Erfüllung von Sicherheitsanforderungen geht. Schon die Anforderung, Benutzerkonten von ehemaligen Mitarbeitern zuverlässig zu löschen, zeigt die Bedeutung der Sicherheit. Auch die Anforderungen im Bereich des Web Access Managements illustrieren die Sicherheitsanforderungen. Insgesamt gilt aber, dass viele Anforderungen im Bereich der Sicherheit mehr und mehr über das übergeordnete Thema Compliance argumentiert werden – Sicherheit als Mittel zum Zweck.

### 4.4 Kosten

Selbst wenn man ROI-Rechnungen skeptisch gegenüber steht, werden diese doch von vielen Unternehmen für jedes Projekt gefordert. Zudem steht die IT auch weiterhin unter Kostendruck und muss ihre Effizienz verbessern. Identity Management bietet hier einige interessante Ansätze wie das Provisioning und das Kennwort-Management. Gerade das Provisioning mit definierten und automatisierten Prozessen kann die Produktivität der IT deutlich erhöhen.

Wie aber schon im Zusammenhang mit diesen Themen ausgeführt wurde, ist eine Gesamtbetrachtung wichtig. Und diese umfasst beim Provisioning eben auch die Frage nach der Bereinigung von Identitätsdaten und ergänzenden Ansätzen wie der Synchronisation über Meta Directory-Dienste für Teile der Informationen, ebenso wie sich beim Password-Management zwangsläufig die Frage nach der (teuren) starken Authentifizierung stellt. Bei einer Gesamtbetrachtung mag Identity Management daher doch nicht ganz so günstig sein. Man muss aber das Potenzial für die Optimierung von Geschäftsprozessen und das Thema Compliance gegenüber stellen – Identity Management ist nur zum Teil Lösung und zum anderen Teil eben eine zwingende Infrastrukturmaßnahme, auch wenn sie auf andere Ebene, beispielsweise durch konkrete Federation-Projekte und die dadurch umgesetzten Geschäftsprozesse, argumentiert und finanziert wird.

### Teilbereiche des Identity Management

Identity Management ist ein komplexes Feld mit vielen Teilelementen. Die Einführung einzelner Lösungen wie des Provisioning setzen immer auch andere Technologien wie das Kennwort-Management voraus. Ein Gesamtmodell des Identity Management kann in die Basisfunktionen

- Infrastruktur: Verzeichnisse, Meta Directory-Dienste, PKIs
- Management-Funktionen: Reporting/Auditing, Workflow-Tools
- Kennwortmanagement: Kennwortsynchronisation, sichere Speicherung von Credentials und die darauf aufbauenden Anwendungen
- Single Sign-On und Credential-Verwaltung
- Provisioning mit User Provisioning, Resource Provisioning, Employee Self Service und Richtlinien-Management
- Profile Management
- Privacy Management
- Web Access Management mit Web Single Sign-On und Zugriffssteuerung
- Web Services Management mit unternehmensübergreifender Identitätsbereitstellung, Trustbrokering und unternehmensübergreifender Identitätszuordnung
- Identity Federation mit der gemeinsamen Nutzung von Identitätsinformationen über Anwendungen hinweg

gegliedert werden. Das Provisioning ist dabei der prozessorientierte Teil des Identity Managements, bei dem es um die Erstellung und Optimierung von Prozessen innerhalb des Identity Managements und darüber hinaus geht, wobei auch Federation durch eine starke Prozessorientierung geprägt ist.

Die Vielzahl der Funktionen macht bereits klar, dass es keine einzelne Software gibt, mit der alle Funktionen abgedeckt werden können. Es gibt aber inzwischen eine Reihe von Anbietern, die heute für alle wichtigen Bereiche des Identity Managements Software-Lösungen haben. Diese überschneiden sich teilweise sogar. So können im Falle von Novell beispielsweise Benutzerinformationen zwischen dem Active Directory und dem eDirectory sowohl über das Novell Account Management 3.0 als auch mit Hilfe von DirXML synchronisiert werden. Auch bei IBM und anderen gibt es solche Überlappungen im Produktportfolio.

## 5. Strategien für das Identity Management

Da die verschiedenen Teile des Identity Managements eng zusammenhängen, ist eine Identity Management-Strategie unverzichtbar. Diese sollte folgende Eckpunkte umfassen:

- Die Definition der Zielsetzungen für die Identity Management-Projekte, wobei die oben genannten Treiber eine zentrale Rolle spielen.
- Eine klare Zuordnung der Gesamtverantwortlichkeit für das Thema Identity Management im Unternehmen.
- Die Definition von Grundanforderungen an Identity Management-Systeme wie beispielsweise die Audit-Fähigkeit und die Anforderungen an die Authentifizierung.
- Die Festlegung der „Hoheit“ über Identitätsdaten in verschiedenen Verzeichnissen und Anwendungen, also insbesondere die Frage nach dem führenden System, aus dem Änderungen in andere Systeme übernommen werden. Dazu gehört die Analyse der relevanten Identitätsdaten von Mitarbeitern, Partnern, Kunden und so weiter und darauf basierend die Definition der Kernprozesse und -zuständigkeiten für die Erstellung, Änderung und Löschung von Identitäten.
- Die Festlegung einer Reihenfolge für die Einführung von Identity Management-Technologien.
- Die Festlegung der Anbieter, die im Zusammenhang mit dem Identity Management zum Einsatz kommen.

Dabei ist zu beachten, dass keineswegs eine Komplettstrategie für das gesamte Unternehmen entstehen muss. Viele Aspekte lassen sich besser auf Bereichsebene lösen, soweit das Zusammenspiel mit anderen Unternehmensbereichen geklärt ist. So kann in kleineren Strukturen mit Synchronisationstechnologien gearbeitet werden, während die Kopplung über Bereichsgrenzen hinweg besser mit Hilfe der Identity Federation funktioniert. Das Identity Management ist zu kritisch für die Fähigkeit zur Umsetzung von Geschäftsprozessen ebenso wie für die Compliance, als dass man es nur in Form taktischer Projekte betreiben kann. Diese sind ein idealer Ausgangspunkt, machen aber noch keine Strategie.

## 6. Die Key-Player im Markt

Durch die Vielzahl von Akquisitionen in den letzten Jahren hat sich auch die Marktsituation im Identity Management-Markt verändert. Es gibt heute eine Reihe von Key-Playern, die über ein recht beachtliches Portfolio verweisen können. Zu nennen sind hier CA, Evidian, HP, IBM, Microsoft, Novell, Siemens/Oblix und Sun. Fast alle Unternehmen haben in den letzten Jahren Firmen zugekauft oder mit ihren eigenen Ressourcen die Entwicklung eines umfassenden Portfolios vorangetrieben.

CA ist ähnlich wie IBM ein Unternehmen, das sich mit Teilgebieten, die heute dem Identity Management zugerechnet werden, schon sehr lange beschäftigt. Produkte wie Top Secret und ACF2 stehen dafür. Mittlerweile hat CA ein sehr breites Portfolio, mit dem wesentliche Bereiche des Identity Managements abgedeckt werden.

Evidian, eine Bull-Tochter, ist dagegen eher ein unbekannter Riese, der im europäischen Markt aber auf viele Referenzen verweisen kann. Die Stärke liegt hier in einem sehr gut integrierten, weil selbst entwickelten Produktportfolio, das ebenfalls zu den interessantesten Angeboten am Markt zählt.

HP hat mit der Akquisition von Teilen von Baltimore sowie von TruLogica, durch Investments in Web Service Management und unlängst angekündigte Federation-Lösungen mittlerweile auch ein sehr breites Portfolio aufgebaut und sich damit ebenfalls in die Liga der Key-Player vorgeschoben.

In dieser befindet sich IBM schon länger. IBM war eines der ersten Unternehmen, das die Relevanz des Themas erkannt und entsprechende Zukäufe getätigt hat. Mit seinem Portfolio von Verzeichnisdiensten über das Access Management bis hin zu Provisioning und Host-Security hat auch IBM ein sehr umfassendes Portfolio zu bieten.

Microsoft ist im Vergleich mit den anderen Key-Playern ein Exot, weil es neben dem Active Directory und anderen im Windows Server 2003 integrierten Komponenten sowie den MIIS 2003 keine wesentlichen Identity Management-Produkte im Portfolio gibt. Durch das Active Directory und die Bedeutung der .NET-Strategie in Verbindung mit Federation-Konzepten ist das Unternehmen als Anbieter aber dennoch zu beachten.

Novell ist vielleicht der meist unterschätzte Player in diesem Markt, was auch daran liegen mag, dass das Unternehmen mehr über andere Themen redet. Basierend auf dem eDirectory und dem Meta Directory-Dienst NSure Identity Manager gibt es aber viele weitere Lösungen bis hin zum Single Sign-On.

Siemens ist durch das Venture Capital-Investment in Oblix indirekt zu einem Komplettanbieter geworden. Die Produktpaletten der beiden Unternehmen ergänzen sich. Darüber hinaus ist Siemens einer der wenigen Anbieter, der auch eigene Smartcard-Lösungen im Portfolio hat und damit im Bereich der starken Authentifizierung glänzen kann.

Sun ist mit der Akquisition von Waveset, einer Rückbesinnung auf die Stärken im Identity Management und mit seiner führenden Rolle bei der Identity Federation ebenfalls einer der Key-Player im Identity Management-Markt.

## 7. Die Spezialisten – „Best of Breed“

Eine „Zwitterstellung“ in der Marktbetrachtung nimmt BMC ein. Trotz der Akquisition von Calendra kann man BMC nicht als Komplettanbieter bezeichnen. Wesentliche Elemente wie das Web Access Management fehlen noch. Auf der anderen Seite hat BMC aber für sein Kerngeschäft des Business Service Management ein abgerundetes Portfolio.

Daneben gibt es eine Vielzahl von Spezialisten in den verschiedenen Segmenten des Identity Managements. Zu nennen sind hier – ohne Anspruch auf Vollständigkeit – folgende Firmen:

- Beta Systems ist einer der etablierten deutschen Anbieter im Identity Management-Markt. Basierend auf der langjährigen Kompetenz insbesondere im Mainframe-Umfeld umfasst das Produktportfolio mittlerweile die Unterstützung aller wesentlichen Systemumgebungen mit einem besonderen Schwerpunkt auf rollenbasierenden Provisioning-Konzepten.

- Maxware ist ein norwegischer Anbieter, der aus dem Bereich der Meta Directory-Dienste kommt, mittlerweile aber auch Provisioning und Virtuelle Verzeichnisdienste im Portfolio hat.

- OSM ist ein Spezialist für das Provisioning im UNIX- und Linux-Umfeld und damit oftmals eine wichtige Ergänzung für andere Produkte.

- M-Tech ist einer der Password Synchronisations-Spezialisten am Markt, erweitert sein Portfolio aber verstärkt in Richtung auf Provisioning und Compliance-Lösungen.

- Völcker Informatik, ein Unternehmen aus Berlin, ist der Spezialist für die Integration von Provisioning und Client-Management.

- Blockade ist ähnlich wie OSM ein Spezialist für Password-Synchronisation mit besonderen Stärken im Bereich der Mainframe-Anbindung.

- RSA hat sich über sein klassisches Themenfeld der Authentifizierung und von Verschlüsselungslösungen hinaus mittlerweile in den Bereich des Provisioning bewegt.

- Entrust ist als klassischer PKI-Anbieter inzwischen dabei, sich in Richtung auf End-to-End-Security insbesondere im Mail-Bereich zu bewegen.

- Octet String und Radiant Logic sind Spezialisten für virtuelle Verzeichnisdienste.

Zählt man die Anbieter von starken Authentifizierungslösungen und anderen Bereichen mit dazu, gibt es insgesamt derzeit aber sicher deutlich über 100 Hersteller rund um das Identity Management – genug Auswahl also für die richtige Lösung.

## 8. Best of Breed oder alles aus einer Hand?

Identity Management ist, wie weiter oben aufgezeigt, ein ausgesprochen breites Feld. Bei der Auswahl von Identity Management-Lösungen steht man vor der Frage, ob man eine Ein-Hersteller-Strategie oder eher eine Best-of-Breed-Strategie verfolgen sollte. Im Bereich des Identity Managements gibt es keinen Anbieter, der wirklich Komplettanbieter ist, auch wenn die Key-Player mittlerweile über ein recht umfassendes Portfolio verfügen.

Diese Tatsache macht schon deutlich, dass eine Ein-Hersteller-Strategie schwierig ist. Jeder Anbieter hat in dem einen oder anderen Bereich entweder relativ schwache Produkte oder schlicht keine eigenen Lösungen. Eine Ein-Hersteller-Strategie hätte also in jedem Fall die Konsequenz, dass man vor allem funktionale Einschränkungen in Kauf nehmen muss. Auf der anderen Seite befindet sich das Identity Management auch heute noch in einer Frühphase der Entwicklung – eine allumfassende Identity Management-Lösung kann man heute noch nicht implementieren, so dass man ohnehin schrittweise an die Projekte heran muss und bei den größeren Herstellern hoffen könnte, dass diese in der Zwischenzeit ihr Portfolio weiter komplettieren.

Bei einer Best-of-Breed-Strategie wird man mit einem anderen Problem konfrontiert. Abgesehen von den „hauseigenen“ Consultants von Herstellern wie IBM oder Novell gibt es am Markt immer noch

## Produkt oder Projekt?

Wenn man auf Hersteller im Identity Management mit der Bitte um eine Evaluationsversion ihrer Software zugeht, gibt es deutliche Unterschiede. Es gibt einerseits immer mehr Anbieter, die solche Versionen auch zum Download anbieten oder bereitwillig CDs versenden. Andere Hersteller reagieren aber eher verschreckt und stellen die Software allenfalls unter Betreuung eigener Consultants zur Verfügung.

Dahinter stehen mehrere offensichtliche Probleme des Identity Management und der Angebote in diesem Bereich. Einerseits haben viele Anbieter kein fertiges Produkt, sondern setzen Identity Management-Lösungen heute noch in Projekten um. Dabei wird zwar auf einen oft recht umfassenden Kern zurückgegriffen, der aber immer ergänzt werden muss.

Der zweite Problemkreis ist, dass die Produkte oft sehr komplex sind, was teilweise in der Natur der Sache liegt – die Kennwortsynchronisation ist beispielsweise ebenso wenig trivial wie die Anbindung von Host-Systemen. Die Erfahrung mit Tests durch Kunden oder auch Zeitschriften, in denen dann kleinere Hürden zu einer insgesamt negativen Kritik geführt haben, führen hier bei manchem Anbieter zu einer spürbaren Zurückhaltung, seine Software einfach so herauszugeben.

Es stellt sich aber auch die Frage, ob es überhaupt möglich ist, ein solch komplexes Thema wie das Identity Management mit einer Anwendung zu adressieren. Die Antwort ist recht einfach: Es gibt zwar für Teilbereiche wie das Provisioning, das Kennwort-Management oder Meta Directory-Dienste Software-Produkte. Es gibt aber heute und wohl auch in absehbarer Zeit keine Komplettlösung, die das volle Spektrum des Identity Managements abdecken kann. Wohl gibt es aber einige Hersteller wie Sun, Siemens/Oblix, CA, Evidian, IBM und Novell, die zumindest die meisten Teilbereiche mit eigenen Produkten adressieren.

Aber auch von diesen Herstellern gibt es kein „Plug and Play“-Paket für das Identity Management oder auch nur das Provisioning oder andere Teilbereiche. Zu unterschiedlich sind die Anforderungen der Kunden und zu komplex die Details heterogener Umgebungen. Das beginnt schon bei der Frage, welche Attribute von einem zentralen Verzeichnis aus an welche anderen Verzeichnisse provisioniert werden und wie man spezifische Attribute, die nur in einzelnen untergeordneten Verzeichnissen benötigt werden, verwaltet. Nicht ohne Grund macht IBM wesentliche Teile seines Umsatzes mit den IBM Global Services. Und nicht ohne Grund ist Novell mit Cambridge Technology Partners zusammen gegangen, um neben den Produkten auch die Beratung und Implementierung anbieten zu können. Auch die anderen genannten Anbieter haben viele eigene Consultants und wickeln mit diesen oder Partnern die Projekte ab.

Auf der anderen Seite darf Identity Management nicht primär als Projekt-Geschäft gesehen werden. Die Anpassung ist erforderlich. Je mehr Elemente der Lösung aber über Produkte geliefert werden, desto schneller und günstiger ist potenziell die Umsetzung. Es lohnt sich in jedem Fall, hier die verschiedenen Anbieter genau zu vergleichen. Denn bei einigen drängt sich der Eindruck doch auf, dass sie zunächst das Label Identity Management oder User Provisioning für sich reklamiert haben, ohne dass die Produktbasis heute wirklich gegeben ist.

Kein Hersteller kann heute „Plug-and-play“-Lösungen für das Identity Management und das Provisioning liefern, die ohne erheblichen zusätzlichen Projektaufwand genutzt werden können. Dazu sind die Anforderungen aus heterogenen Umgebungen noch zu komplex und der Markt noch zu jung. Dennoch sollte bei der Auswahl von Herstellern darauf geachtet werden, dass diese über echte Produkte verfügen und in diesem Bereich über das Powerpoint-Niveau hinausgekommen sind.

wenige Unternehmen, die auf die technische Umsetzung von Identity Management- und Provisioning-Lösungen spezialisiert sind. Die Zahl der Beratungsunternehmen, die das Feld des Identity Managements für sich entdecken, steigt zwar stark an. Die wenigsten dieser Anbieter haben aber eine langjährige Erfahrung mit diesen Themen, so dass man ihre Kompetenzen genau prüfen sollte. Diese haben dabei in der Regel wiederum nur einige oder wenige Produkte im Portfolio. Die Konsequenz daraus ist, dass eine Integration verschiedener Lösungen für das Identity Management aufwendiger wird.

Eine dritte Möglichkeit besteht darin, sich zunächst auf Kernthemen des Identity Managements zu fokussieren wie Meta Directory-Dienste und das Provisioning und dort jeweils einen der führenden Anbieter auszuwählen. Damit können einerseits optimale Funktionen in den verschiedenen Bereichen genutzt und andererseits die Integrationsprobleme minimiert werden. Um diese herum können dann Best-of-Breed-Lösungen für andere Themenbereiche eingesetzt werden. Da das Thema Identity Management, schon durch den noch entwicklungsfähigen Reifegrad des Marktes und der Produkte, sich ohnehin über Zeiträume von einigen Jahren in Unternehmen entwickeln wird, lassen sich auf diese Weise heute bereits konkrete Lösungen umsetzen, ohne sich bereits in eine Ecke zu drängen.

Bei der Auswahl der Hersteller gilt es, einerseits deren Vision für das Thema und andererseits die wirtschaftliche Stärke und Zuverlässigkeit einzubeziehen. Die Sourcing-Entscheidungen für das Identity Management und das Provisioning unterscheiden sich hier nicht von solchen Entscheidungen in anderen Feldern der IT.

# 9. Fallbeispiel & Lösungsspektrum

## 9.1 Schnelle Amortisation – Kosten und Nutzen von Identity Management

Identity Management-Lösungen (IdM-Lösungen) verwalten digitale Benutzer wie Mitarbeiter, Geschäftspartner und Kunden. Sie automatisieren bis zu 80% der Routinetätigkeiten zur Administration von Benutzerrechten und -konten, bieten höhere Datensicherheit und können für geforderte Risikoeinschätzungen wie beispielsweise Basel II herangezogen werden. Damit sich solche Lösungen schnell amortisieren, bedarf es einer effizienten Kosten-Nutzen-Analyse. Speziell dafür hat Beta Systems Software AG, Berlin, eine stringente Methodik entwickelt.

Die effiziente Verwaltung digitaler Identitäten und eine unternehmensweit einheitliche IT-Sicherheit ermöglichen das reibungsfreie Funktionieren eines Unternehmens. Hierzu zählen das Passwort-Management, Antragsverfahren für Zugriffsberechtigungen sowie spezielle Administrationskonzepte in allen denkbaren verteilten IT-Systemen vom Mainframe bis hin zu Windows, Unix und Linux. Sicherheits- und Datenschutzrichtlinien sind unternehmensweit durchzusetzen und verschiedene Benutzerprofile in Datenbanken und Verzeichnissen zu pflegen. So steigt mit der Anzahl der zu verwaltenden Identitäten der Bedarf an einem effizienten Management.

IdM-Lösungen bieten intelligente Administrationswerkzeuge, mit denen sie zahlreiche Aufgaben automatisieren. Routinetätigkeiten wie das Einrichten neuer Benutzerkonten, die Zuweisung von Ressourcen, aber auch Änderungen von Berechtigungen und Benutzerkonten sowie das Löschen dieser lassen sich effizienter gestalten. Werden Neueinträge und Änderungen zum Arbeitsplatz von Personaldatensystemen etwa aus SAP R/3 abgegriffen und von Provisioning-Systemen zentral verwaltet, ergeben sich hohe Automationseffekte.

Das lässt sich bewerten: Jeder manuelle Administrationsvorgang zu einer Benutzeridentität dauert pro System zwischen fünf und zwanzig Minuten. Die Einsparung errechnet sich aus den Kosten für einen Administrator. Ähnliche Einspareffekte bietet die Automation des Antragsverfahrens für Identitäten und Ressourcen. Die übrigen nicht automatisierbaren Tätigkeiten lassen sich meist über ein integriertes elektronisches Genehmigungsverfahren zentral steuern und verwalten. Nach der elektronischen Genehmigung erfolgt die Zuordnung für alle angebundenen Systeme automatisch auf der Basis von Zugriffsregeln oder für fachlich gruppierte Berechtigungen.

### Kosten sparen

Die rollenbasierte Administration vereinfacht die Antragstellung sowie die restlichen manuellen Administrationsvorgänge. In Rollen wie „Berater“ oder „Sachbearbeiter“ sind Berechtigungen gebündelt. Anstelle vieler Einzelberechtigungen wird den Anwendern einfach eine entsprechende Rolle zugewiesen. Features wie das Zurücksetzen von Passwörtern durch den User, oder die Passwort-Synchronisation reduzieren die Help-Desk-Anfragen um bis zu 70%. Einsparungen ergeben sich aus der Anzahl der reduzierten Calls, die mit den Kosten des Help-Desk-Calls multipliziert werden.

IdM-Systeme optimieren das Erstellen regelmäßiger Reports und Ad-hoc-Berichte für die Revision. Der Einsatz eines zentralen plattformübergreifenden Reporting-Tools minimiert den Arbeitsaufwand um 50 bis 80 %, da das Sammeln und manuelle Konsolidieren von Einzelreports entfällt.

Durch eine zeitnahe Rechtevergabe stellen IdM-Systeme dem Nutzer Systeme schnell zur Verfügung. Die daraus resultierende Produktivitätssteigerung kann aber von internen Mitarbeitern kaum eindeutig nachvollzogen werden. Konkreter sind die Kosten für einen Subunternehmer zu berechnen, der durch fehlende Berechtigungen einige Tage nicht arbeiten kann.

Eine korrekte Rechtevergabe, die konsequente Rechteverwaltung und eine regelmäßige Revision wahren die Vertraulichkeit von Daten und gewährleisten Sicherheit. Über den „Single Point of Control“ eines IdM-Systems können aktuelle Ressourcenzuordnungen von Usern direkt ermittelt und unerwünschte Berechtigungskorrelationen erkannt, geändert und gelöscht werden.

**Investitionskosten**

Kosten fallen für die Anschaffung, Einführung und den Betrieb einer IdM-Lösung an. Dank des modularen Aufbaus kann nach der Anzahl der eingesetzten Module oder der zu verwaltenden Benutzer lizenziert werden. Zu den Kosten im laufenden Betrieb zählen Wartung und Upgrade der benötigten Hard- und Software sowie die Pflege der Rollen und deren Anpassung an organisatorische Veränderungen.

Bei einer Gegenüberstellung von Kosten und Nutzen für einen bestimmten Zeitraum von 3 Jahren wird der Return on Investment (ROI) sichtbar. Der Break-Even ist mit der richtigen Strategie schon nach 12 bis 15 Monaten erreichbar, wenn in 3 bis 6 Monaten die wichtigsten Zielsysteme mit rund 90 Prozent der Benutzer integriert werden.

## 9.2 Die RWTH Aachen setzt beim Identitätsmanagement auf den IBM Tivoli Identity Manager

Der April naht und mit ihm der Beginn des Sommersemesters an der Rheinisch-Westfälischen Technischen Hochschule (RWTH) in Aachen. Was für ungefähr 5000 Erstsemestler der Eintritt in einen weiteren Lebensabschnitt ist, bedeutete früher für die Administratoren des Rechen- und Kommunikationszentrum sehr viel Arbeit: Sie mussten den neuen Studenten den Zugang zu etlichen Dienstleistungen der Hochschule bereitstellen, die gewünschten Ressourcen frei schalten und die neuen Benutzer-Stammdaten per Hand eingeben. Hinzu kam die Unterscheidung verschiedener Personengruppen wie Studenten, Institutsgäste oder Dozenten und das Löschen ehemaliger Nutzer. All diese Aufgaben machten die Verwaltung von Benutzern zu einer immer vertrackteren Aufgabe. Dennoch können die IT-Mitarbeiter dem Semesterbeginn in Zukunft gelassener entgegensehen – die meiste Arbeit nimmt ihnen ab sofort der Tivoli Identity Manager von IBM ab.

Als zentrale Einrichtung bietet das Rechen- und Kommunikationszentrum (RZ) der RWTH Aachen Ressourcen und Dienstleistungen für Institute, Angehörige und Studierende der Hochschule an. Zu den Hauptaufgaben gehören die Planung, der Betrieb und die Bereitstellung von zentralen Daten-, Rechen-, Visualisierungs- und Kommunikationsanlagen und der darauf aufbauenden Dienste, deren Anschaffung und Betrieb durch einzelne Institute entweder unerschwinglich oder nicht sinnvoll wäre, sowie die Beratung und Unterstützung bei der Nutzung. Außerdem betreibt das RZ die Hochleistungsrechner und das Hochschulkernnetzes der Universität.

## Ein Kommen und Gehen

Doch die meiste Arbeit macht die digitale Verwaltung der vielen verschiedenen Anwender: Mit 30.800 Vertretern bilden dabei natürlich die Studenten die Hauptgruppe, die mit Eintritt, Wechseln und Studienfortschritten bis hin zur Exmatrikulation auch den größten Verwaltungsaufwand verursachen. Daneben gibt es außerdem die wissenschaftlichen Mitarbeiter und Professoren, Institutsgäste, ehemalige RWTH-Absolventen (Alumni) und sogar Angehörige anderer NRW-Hochschulen, die im Rahmen des Ressourcenverbundes Nordrhein-Westfalens (RV-NRW) eng mit dem Rechenzentrum zusammenarbeiten. Jahrelang mussten die Administratoren all diesen verschiedenen User-Typen – die übrigens innerhalb der RWTH nicht einheitlich erfasst sind – maßgeschneiderte Zugänge zum Hochschulnetz einrichten.

Eine zusätzliche Herausforderung für die IT-Mitarbeiter bestand in der Ausweitung des digitalen Angebotes wie etwa neue Lehr- und Lernformen à la High End-Simulationen, die Einrichtung des Virtual Reality Centers Aachen, die Bibliotheksverwaltung inklusive elektronischer Medien oder die verteilte, Web-basierte Abwicklung verschiedener Verwaltungsabläufe wie etwa der Hörsaalbelegung, die Einrichtung von Bestellportalen oder dem virtuellen Prüfungsamt. Die fehlende einheitliche Datenbasis führte häufig zu Mehrfachregistrierungen einer Person, zeitlichen Verzögerungen beim Löschen von digitalen Karteileichen oder bei der Erstbereitstellung von Diensten für Neuzugänge.

## Dienste auf Knopfdruck

Im Rahmen eines übergreifenden Vertrages zwischen Nordrhein-Westfalen und IBM Tivoli wurde Anfang 2003 allen beteiligten Hochschulen der IBM Tivoli Identity Manager (ITIM) vorgestellt. „Damit war zum ersten Mal eine sowohl technisch ausgefeilte wie auch bezahlbare Lösung für uns in Sicht," so Dr.-Ing. Klaus Brühl aus dem Bereich Rechen- und Datendienste des RZ. Die Hochschulen Aachen und Bonn ergriffen als Erste die Chance und richteten mit der Unterstützung von IBM Testinstallationen ein. Dem großen Ziel, allen unterschiedlichen Personengruppen definierte Dienste „auf Knopfdruck" zur Verfügung zu stellen beziehungsweise ohne zusätzliche Identitätsprüfung elektronisch anfordern zu können, kommt der ITIM in der Version 4.5.1 bereits sehr nahe. Auch das automatische Löschen einer Person, sobald sie nicht mehr einer der berechtigten Gruppen angehört, leistet die Software. Die Erfassung der Personen und die Verantwortlichkeit bleibt bei der dafür zuständigen Stelle, das heißt es werden lediglich die Personendaten (wie Name, Matrikel- oder Personalnummer) importiert. Die Rollenzuteilung von zum Beispiel Studierenden bestimmt das Zugangsprofil und erschließt sich aus der Datenquelle, also der Studentendatenbank der Hochschulverwaltung, oder wird gegebenfalls in Sonderfällen manuell zugewiesen.

## IBM Tivoli Identity Manager im Einsatz

Nach erfolgreicher Testinstallation richtet der IBM Tivoli Identity Manager seit Juli 2004 automatisch Zugänge für die verfügbaren Dienste an. Spezielle Genehmigungsprozesse stellen dabei sicher, dass der Nutzer, sei es nun ein Student, Auszubildender oder Landesnutzer des Ressourcenverbundes nur Zugang zu den Systemen erhält, die er für seinen Alltag braucht. Studenten werden beispielsweise automatisch für das hauseigene Mailsystem RWTH-Mail, das WLAN oder den Online-Studienplaner CAMPUS-Office freigeschaltet. Außerdem können sie sich über ihr ITIM-Passwort selbst auch Zugang zu weiteren Anwendungen verschaffen und auch die Passworte für alle Dienste zentral

im ITIM pflegen. Bei 42.589 Anwendern, die über das Identitätsmanagement zugreifen, kam es allerdings im Zuge der Einrichtung zu kleineren organisatorischen Problemen: „Eine Herausforderung bestand darin, unsere Organisationsstrukturen in ITIM möglichst ‚ITIM-konform' abzubilden," so Dr. Brühl. Zeit kostete es vor allem auch, interne Verfahrensabläufe zu vereinfachen, was für heftige Diskussionen unter den Beteiligten sorgte.

Dass das Konzept allerdings sehr gut funktioniert, bestätigte der Leiter des Rechen- und Kommunikationszentrums, Prof. Christian Bischof: „Wir haben im Herbst mit Microsoft einen Vertrag abgeschlossen, der es den Studierenden der RWTH erlaubt, PC-Betriebssysteme und diverse Programmiertools von einem Server im RZ auf die eigenen PCs herunter zu laden. Den Zugang dazu können sich die Studierenden über das Web im ITIM selbst frei schalten. Die bei solchen Gelegenheiten üblichen Menschenschlangen beim Ausfüllen von Anträgen im Rechenzentrum gab es diesmal allerdings nicht."

Die Arbeit am Identitätsmanagement der RWTH ist noch nicht beendet: Da noch nicht alle Dienste mit ITIM verwaltet beziehungsweise alle Personengruppen in der Hochschule erfasst werden, wird gegenwärtig an einem ausführlichen „Feinkonzept" für die Einbindung weiterer Stellen gearbeitet.

**Über Tivoli Software von IBM**

Mit der Tivoli Software von IBM können IT-Unternehmen, ihr Total Costs of Ownership (TCO) reduzieren und das Serviceniveau der IT-Infrastruktur verbessern. Die System-Management Software Tivoli bietet traditionellen Unternehmen und e-business Unternehmen Support in den Bereichen Sicherheits- und Speicher-Management und System Automatisierung. Unterstützt durch IBM Services, Support und Forschung gehört Tivoli zu den fünf wichtigsten IBM Software Group Marken - DB2, Lotus, Rational, Tivoli und WebSphere.

## 10. Profil: Die Sponsoren

Die Beta Systems Software AG (Prime Standard: BSS) ist ein führender Anbieter von hochleistungsfähigen und intelligenten Lösungen für die Verwaltung von Massendaten. Beta Systems liefert Software, welche es Unternehmen ermöglicht, ihre Prozesse im Rahmen der Datensicherung, des Dokumentenmanagement und des Betriebs von Rechenzentren einfacher und effizienter zu gestalten. Das Unternehmen ist spezialisiert auf die Automatisierung und Optimierung großvolumiger Datenverarbeitungsprozesse seiner Kunden und konzentriert sich dabei auf kostenminimierende und intelligente Handhabung, Speicherung und Verteilung von Informationen und Dokumenten. Beta Systems' Kunden sind typischerweise große Organisationen und Unternehmen aus dem Industrie-, Finanz-, Telekommunikations-, Energieversorgungs-, Dienstleistungs- und öffentlichen Bereich, deren Datenverarbeitung bisher einen hohen Aufwand an Zeit, Geld und weiteren Ressourcen erforderte. Die von Beta Systems entwickelten Lösungen sind offen in ihrer Architektur und erzeugen eine Informations-Infrastruktur, welche die bisherige Komplexität des Informationsmanagements erheblich reduziert. Die Produkte von Beta Systems werden weltweit über eigene Tochtergesellschaften sowie Partnerunternehmen vertrieben. Das Unternehmen ist seit 1997 börsennotiert und hat 994 Mitarbeiter weltweit (Stand 30. September 2004).

Beta Systems Software AG
Alt-Moabit 90d
10559 Berlin
Tel.: (030) 726 118 - 674
Fax: (030) 726 118 – 852

www.betasystems.com

IBM ist der weltweit größte Anbieter von Informationstechnologie (Hardware, Software und Services). Das Unternehmen beschäftigt weltweit rund 340.000 Mitarbeiter und ist in 170 Ländern aktiv. IBM bietet seinen Kunden die komplette Produktpalette an fortschrittlicher Informationstechnologie an: Von der Hardware, Software über Dienstleistungen und komplexen Anwendungslösungen bis hin zu Outsourcingprojekten und Weiterbildungsangeboten. Mit der Strategie des On Demand Business rüstet IBM seine Kunden für künftige Herausforderungen und sich schnell verändernde Marktanforderungen.

www.ibm.com/de