Sichere Effektivität

Martin Grölz

Cambridge Technology Partners
Frankfurter Ring 115a
80807 München
martin.groelz@ctp.com

1 Identitätsmanagement optimiert Datenzugriff an Hochschulen

Sicherheitssteigerungen und Kosteneinsparungen sind derzeit die meistgenannten Ziele für IT-Investitionen von Unternehmen und der öffentlichen Hand. Eine Möglichkeit, die Sicherheit bei gleichzeitiger Kostenreduzierung zu steigern, bietet Identitätsmanagement. Viele Unternehmen verfolgen daher entsprechende Projekte, um das Management von Benutzerberechtigungen in einer zunehmend heterogenen IT-Landschaft zu automatisieren. Ein möglicher Lösungsansatz ist die Verwendung eines zentralen Verzeichnisdienstes (Meta Directory), über den die identitätsbezogenen Informationen in den dezentralen Benutzerverwaltungen abgeglichen werden.

Diesen Ansatz verfolgen auch mehrere Hochschulen, schließlich gibt es aufgrund der Innovationskraft und des Forschungsauftrags der Hochschulen auch dort einen verstärkten Trend zur „Heterogenisierung“ der IT-Landschaften. Knappen Kassen sorgen zudem für Personalmangel zum Betrieb der neuen Systeme und Anwendungen – eine Automatisierung der Prozesse ist daher notwendig.

Ist das Vorgehen der Industrie also übertragbar auf die Situation an den Hochschulen? Welche besonderen Anforderungen sind im Hochschulbereich zu berücksichtigen? Der Beitrag geht diesen Fragen nach und gibt aus Projekterfahrungen im Hochschulbereich heruas Hilfestellung für die Planung ähnlicher Projekte. Den Einstieg bildet eine Definition von Identitätsmanagement und eine Beschreibung des Lösungsansatzes Meta-Directory sowie der typischen Nutzentreiber für eine derartige Lösung.

1.1 Identitätsmanagement – Lösung in drei Stufen

Eine Identitätsmanagement-Lösung ermöglicht es einer Organisation, ihren Mitarbeitern, externen Mitarbeitern mit Sonderberechtigungen, Partnern und Kunden einen rollenbasierten Zugriff auf ihre Ressourcen zu gewähren, ohne Sicherheitskompromisse eingehen zu müssen. Dabei ist es unerheblich, an welchem Ort sich die Ressourcen oder die Nutzer befinden. Änderungen von Berechtigungen werden in Echtzeit an allen angeschlossenen Systemen realisiert.

Die Lösung ist kein fertig installierbares Produkt, sondern besteht aus verschiedenen Komponenten, die – je nach Organisation und Anwendungsgebiet – in unterschiedlichen Ausprägungen ein Bestandteil der Gesamtlösung werden.

Im Wesentlichen beinhaltet eine Identitätsmanagement-Lösung drei Ausbaustufen:

- Aufbau eines Zentralverzeichnisses mit allen aktuellen Identitäten
- Synchronisation mit Zielsystemen und automatisiertes Provisioning (dt: Bereitstellung)
- Personalisierung von Diensten für unterschiedliche Benutzerkategorien und Rollen

Die folgende Abbildung zeigt die generische Architektur einer Identitätsmanagement-Lösung. Die einzelnen Komponenten und ihre Bedeutung werden im nachfolgenden Text erläutert.

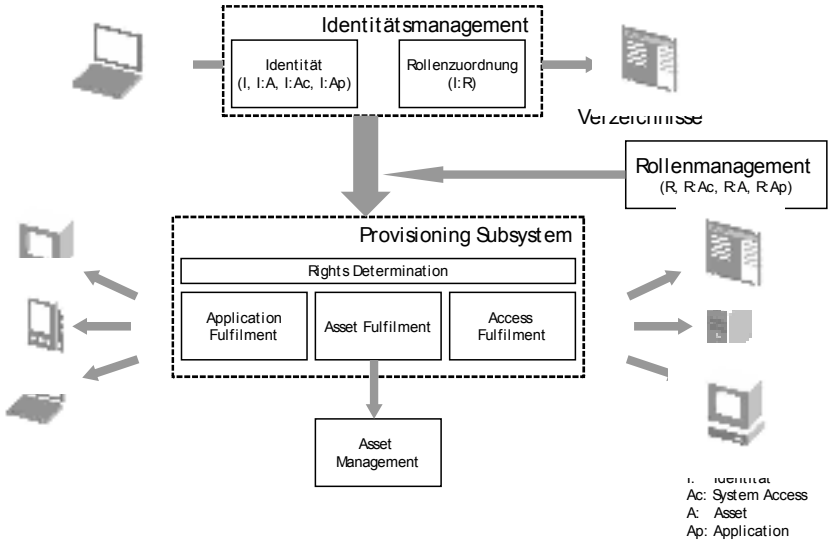

Abbildung 1: Generische Architektur Identitätsmanagement

1.1.1 Übergeordnetes Verzeichnis verwaltet Daten

Der zentrale Bestandteil der Lösung ist die Komponente Identitätsmanagement. Bei dieser Komponente handelt es sich um einen zentralen Datenspeicher zur Ablage der aus den angeschlossenen Anwendungen konsolidierten Benutzerinformationen. Diese Komponente wird oft auch als Meta Directory bezeichnet, also als ein übergeordnetes Verzeichnis. Neben der ausschließlich passiven Konsolidierung von Benutzerinformationen kann das Meta Directory aber auch zur zentralen Verwaltung von dezentralen Benutzerinformationen und -berechtigungen dienen. Hierzu können den verwalteten Benutzern Berechtigungen direkt oder über Rollen zugewiesen werden.

1.1.2 Automatisierter Datenabgleich

Das Provisioning Subsystem verbindet das Meta Directory mit den Anwendungen zum Abgleich der relevanten Daten. Der Abgleich kann dabei bi-direktional erfolgen, also sowohl Datentransfer aus den dezentralen Anwendungen in das Meta Directory als auch viceversa. Durch diese Komponente erreicht der Lösungsansatz für das Identitätsmanagement eine hochgradige Flexibilität. Zudem können komplexe Geschäftsprozesse abgebildet werden: Organisationen können für jedes einzelne Datenfeld eines Benutzers entscheiden, ob dieses durch das Meta Directory zur Verfügung gestellt oder aus einer dezentralen Anwendung bereitgestellt wird und das Meta Directory lediglich die Verteilung an die weiteren angeschlossenen Systeme übernimmt.

Über das Provisioning Subsystem werden Benutzer automatisiert im angeschlossen System angelegt oder aktualisiert (eProvisioning). Die Automation dieses Prozesses ermöglicht zum Beispiel bei neu eingestellten Mitarbeitern die Bereitstellung sämtlicher erforderlicher Berechtigungen binnen weniger Stunden (“Zero Day Start“). Von hoher Sicherheitsrelevanz ist das zeitnahe Entfernen von Berechtigungen (“De-Provisioning“ oder „Last Day Stop“), das ebenfalls durch das Provisioning Subsystem für alle angeschlossenen Systeme automatisiert erfolgen kann.

Über die Fulfilment Agents kann das Provisioning Subsystem zusätzlich beliebige Prozesse in den dezentralen Anwendungen anstoßen. Abbildung 1 zeigt beispielhaft die Anbindung an eine Softwareverteilung, so dass für jeden Anwender alle Anwendungen automatisiert installiert und deinstalliert werden können. Ein vergleichbares Szenario ist durch die Anbindung eines Asset Managements für Arbeitsgeräte wie Laptops oder Mobiltelefone denkbar. Die Informationen über die zur Verfügung gestellten Berechtigungen, die installierten Anwendungen und die ausgehändigten Arbeitsgeräte werden hierbei stets zentral im Meta-Directory dokumentiert.

1.1.3 Gruppierung mittels Rollenmanagement

Eine zentrale Bedeutung für die weitgehende Automatisierung der Verwaltung von Berechtigungssystemen spielen Rollenkonzepte und das Management von Rollen. Unter Rollen versteht man hierbei eine Gruppierung von unterschiedlichen Berechtigungen für Anwendungen, Gebäude oder sonstige Arbeitsmittel. Durch eine sinnvolle Gruppierung dieser Berechtigungen nach Aufgabengebieten können die Berechtigungen standardisiert und die Aufwände reduziert werden. Bei Einsatz eines Rollenkonzeptes wird im Meta Directory lediglich die Rolle zugeordnet. Das Provisioning Subsystem trennt die zugeordnete Rolle in die dahinter gruppierten Berechtigungen auf, basierend auf den vom Rollenmanagement zur Verfügung gestellten Rollenbeschreibungen.

1.2 Vorteile von Identitätsmanagement

Identitätsmanagement ist für eine Organisation am besten geeignet, wenn eine große Anzahl von Identitäten (Benutzer-Kategorien und Rollen) mit häufigem Änderungsbedarf gepflegt werden muss. Derartige Organisationen können durch Identitätsmanagement erhebliche Effizienzgewinne und Sicherheitsvorteile realisieren.

Die Anzahl an unterschiedlichen „Identitäten“, die eine Organisation definieren und pflegen muss, hängt u.a. von folgenden Kriterien ab:

- der Anzahl der Benutzer-Kategorien (Angestellte jeder Art, externe Mitarbeiter, Partner, Kunden, etc.).
- der Anzahl der funktionalen Rollen (Assistent, Verkäufer, Fahrer, Techniker, Manager, Hausmeister, IT-Administrator, Mitarbeiter der Personalabteilung, etc.).
- der Häufigkeit des Personal- und Rollenwechsels durch Anstellungen, Kündigungen oder Änderungen des Aufgabenbereiches.

Für jede Identität müssen Berechtigungsregeln für den Zugriff auf alle Ressourcen definiert und gepflegt werden, z.B.:

- Benutzerberechtigung im Netzwerk (Benutzerkennung/Kennwort für Email, Zugriffsrechte im Intranet, Lese- und Schreibrechte auf Home-Verzeichnis und zentrale Datenablagen, Benutzungsrechte für Ressourcen wie Drucker).
- Benutzerberechtigung für jede zugelassene Benutzeranwendung (evtl. einschließlich sämtlicher Benutzerkennungen und Kennworte).
- Ausweiskarte, Eintrittskarte und/oder Schlüssel, evtl. eine weitere Karte für das Zeiterfassungssystem.
- Telefonnummer und aktueller Eintrag im Telefonbuch.

1.2.1 Reduktion der administrativen Kosten

In Organisationen mit einer Großzahl von Identitäten und einem signifikanten Personalwechsel entsteht ein hoher Aufwand im IT-Bereich für die manuelle Pflege der Identitäten. Für den amerikanischen Markt gibt es eine Reihe von Studien, die die Einsparpotenziale durch Identitätsmanagement belegen. Auch wenn die den Studien zugrunde liegenden Statistiken nur zur Orientierung verwendet werden können, zeigen die Ergebnisse ein erhebliches Potenzial für die Reduzierung von IT-Aufwänden auf.

META Group Research [1] schätzt, dass Firmen mit Umsätzen über 500 Millionen Dollar etwa 35 Prozent ihres gesamten IT-Budgets allein für das Benutzermanagement und die Pflege von Benutzerdaten, Zugriffsberechtigungen und Autorisierungen, aufwenden.

Auch AMR Research [2] ist der Ansicht, dass diese Aufwände bei 20 Prozenz bis 40 Prozent des gesamten IT-Budgets liegen. Der Marktbeobachter weist ferner darauf hin, dass die Anrufe, die im Zusammenhang mit Benutzerkennungen beim Help-Desk auflaufen, durch effektives Identitätsmanagement um 60 bis 90 Prozent reduziert werden können.

1.2.2 Erhöhte Produktivität

Eine überforderte Hotline- und/oder IT-Abteilung kann zeitnahe Unterstützung nicht leisten, so dass Wartezeiten und mangelhaftes Problemmanagement die Leistungsfähigkeit der gesamten Organisation betreffen und beeinträchtigen. Ohne die – durch Identitätsmanagement ermöglichte – automatische Bereitstellung von Zugriffsberechtigungen auf die

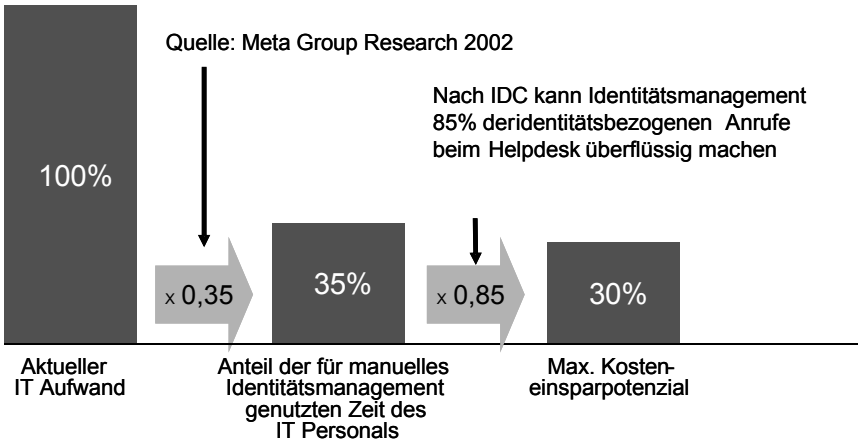

Abbildung 2: Kosteneinsparpotenzial durch automatisiertes Identitätsmanagement, Quelle: META Group Research 2002

benötigten Systeme und Anwendungen vergehen mitunter Wochen, bis ein neuer Mitarbeiter produktiv zum Einsatz kommt.

Ein Identitätsmanagement-Projekt hat zudem weitere Produktivitätsgewinne im Bereich „Single-Sign-On“ (SSO) zur Folge. Single-Sign-On, zu deutsch „einmalige Anmeldung“, ermöglicht es Benutzern, die Vielzahl der täglich zu verwendenden Passwörter zu reduzieren und verringert dadurch gleichzeitig die Anfragen beim Helpdesk, die aus vergessenen Passwörtern resultieren.

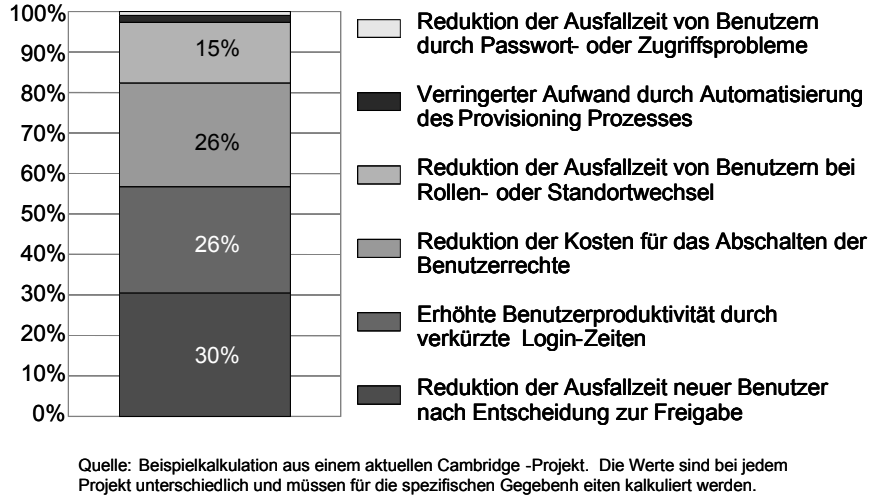

Abbildung 3: Produktivitätssteigerung durch Identitätsmanagement

1.2.3 Gesteigerte Sicherheit durch automatisierte Autorisierung

Ein überfordertes und nicht optimal gepflegtes Berechtigungssystem führt unmittelbar zu Sicherheitslücken und Datenschutzproblemen, die von den Benutzern unbewusst oder bewusst missbraucht werden. Rich Mogull [3], Senior Analyst bei GartnerGroup erläutert: "Nicht *hacking* verursacht die schlimmsten Einbrüche in die Sicherheitssysteme eines Großunternehmens. Es ist häufig die Arbeit eines Angestellten des Unternehmens, die den meisten Schaden verursacht." Richard Hunter, [4] Vice President und „Director of Research" bei Gartner Group, quantifiziert das Problem: "Gartner schätzt, dass über 70 Prozent der nicht autorisierten Zugriffe auf Informationssysteme sowie 95 Prozent der Einbrüche, die zu signifikanten Verlusten führen, von Angestellten verursacht worden sind."

Um derartige Probleme zu vermeiden, müssen die Berechtigungen aller Benutzerkategorien und Rollen so definiert werden, dass der Zugriff auf Ressourcen nur gemäß systematischer Geschäftsregeln freigegeben werden kann. Durch eine zentrale Dokumentation muss sichergestellt werden, dass jederzeit ein zuverlässiger Überblick darüber besteht, wer über welche Berechtigungen verfügt sowie wann er sie durch wen erhalten hat. Sicherheitseinbrüche werden aber nicht nur von den Angestellten und anderen berechtigten Nutzern verursacht, sondern auch von aus der Organisation ausgeschiedenen oder gekündigten Mitarbeitern, die durch fehlende Sicherheitskontrolle ihre Berechtigungen behalten haben. Eine Befragung der META Group [1] ergab, dass durchschnittlich nur 73 Prozent der ausgeschiedenen Mitarbeiter ihre Zugriffsrechte verlieren. 27 Prozent der ehemaligen Mitarbeiter behalten dagegen auf Dauer ein unautorisiertes Zugriffsrecht. Externer unautorisierter Zugriff auf die sensiblen Unternehmenssysteme ist damit jederzeit möglich. Cambridge-Kunden bestätigen diese alarmierende Tatsache:

- „Zwischen 3000 und 5000 noch funktionsfähige Zutrittskarten sind innerhalb eines Jahres nicht zurückgegeben worden."
- „Einer unserer ehemaligen Angestellten war sechs Monate lang nicht bei der Bank angestellt. Als er wieder eingestellt wurde, funktionierten seine Benutzerkennung und sein Passwort aber immer noch."

Viele Organisationen interessieren sich für Identitätsmanagement-Lösungen, da dadurch wie erwähnt Effizienzgewinne und Sicherheitsvorteile ermöglicht werden. Nach der erfolgreichen Einführung einer solchen Lösung ist jedoch noch wesentlich mehr gewonnen worden, nämlich die Flexibilität, Identitäten und Ressourcenzuordnungen schnell und „schmerzlos" zu ändern und auf neue Anforderungen anzupassen. Am besten zeigt sich diese Flexibilität bei Akquisitionen, Fusionen oder Umstrukturierungen. In diesen Fällen müssen erhebliche Änderungen der bestehenden Geschäftsprozesse durchgeführt werden. Identitätsmanagement sichert eine systematische und rollenbasierte Berechtigungskontrolle für alle Benutzergruppen einschließlich der Partner und Kunden. Dadurch können Autorisierungsregeln erheblich einfacher eingehalten werden.

Gesetzliche Änderungen können ebenfalls dazu führen, dass ausgewählte Aufgaben nur von speziell dazu berechtigten oder zugelassenen Mitarbeitern durchgeführt werden kön-

nen, und dass die Einhaltung solcher Anforderungen schriftlich bewiesen werden muss. Das Bundesdatenschutzgesetz[1] (BDSG) verfügt beispielsweise im Paragraph 9:

- „ Öffentliche und nicht öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten."

1.3 Identitätsmanagement im Hochschulbereich

Auch wenn eine Hochschule nicht in jeder Hinsicht mit einem Industrieunternehmen vergleichbar ist, sind einige Grundannahmen durchaus übertragbar. Unabhängig von der weiteren Entwicklung in der deutschen Hochschulpolitik werden die finanziellen Mittel für die Aufrechterhaltung des Forschungs- und Lehrbetriebes knapp bleiben. Daran können auch punktuelle Investitionen nichts verändern. Der Druck, Kosten zu sparen, ist auf jeden Fall gegeben. Weitere Argumente, die für das automatisierte Identitätsmanagement sprechen, gelten im Hochschulbereich eher noch verstärkt:

- Wo sonst gibt es eine dermaßen hohe Fluktuation an Identitäten, die Semester für Semester neu zu erfassen und mit unterschiedlichen Berechtigungen auszurüsten sind?
- Wo sonst findet sich ein dermaßen hohes Innovationsinteresse, so dass jedes denkbare System auch irgendwo eingesetzt wird?
- Wo ist andererseits so wenig zentrale Organisation vorhanden, dass eine verlässliche Entscheidung über Bestehenlassen oder Entziehen einmal erteilter Berechtigungen für die Administratoren der einzelnen Anwendungen kaum möglich ist und entsprechende Prozesse bestenfalls über Laufzettel gelöst werden können?

Der Bedarf an entsprechenden Lösungen zeigt sich nicht zuletzt an dem hohen Interesse an Identitätsmanagement in den Kreisen der Rechenzentren und der Hochschulverwaltungen. Im Rahmen des ZKI wurde ein eigener Arbeitskreis eingerichtet, der sich ausschließlich mit der Thematik Meta-Directorys und Identitätsmanagement befasst.[2]

1.3.1 Identitätsquellen an Hochschulen

In vielen Unternehmen kann davon ausgegangen werden, dass aus den Daten der Personalverwaltung ein überwiegend vollständiges Zentralverzeichnis aller Mitarbeiter aufgestellt werden kann. Dagegen wird an den Hochschulen die zahlenstärkste Benutzergruppe gar nicht durch die Personalverwaltung erfasst. Die Verwaltung der Studierenden erfolgt unabhängig von der der Mitarbeiterschaft. Weitere Nutzergruppen für Hochschulressourcen sind externe Mitarbeiter und Gastdozenten ohne Anstellungsvertrag, Gasthörer oder auch

[1] In der entsprechenden Anlage zu BDSG §9 findet sich eine Aufzählung von Maßnahmen, die sich auf die Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle von Daten beziehen.

[2] ZKI-AK Meta-Directory, Informationen unter http://gaia.zam.fh-koeln.de/zki-ak/

Bürger, die nur bestimmte Dienstleistungen, z.B. Rechnerpools, nutzen wollen. Das bedeutet, dass schon der erste Schritt zum Identitätsmanagement, nämlich der Aufbau eines aktuellen Zentralverzeichnisses sehr komplex ist. Hinzu kommt, dass es sich bei den Nutzern keineswegs um Gruppen ohne Überschneidungen handelt. Viele Studierende üben zusätzlich zu ihrem Studium eine Aushilfstätigkeit an der Universität aus und werden dort über die Personalverwaltung erfasst. Je nach Gruppenzugehörigkeit gibt es aber mitunter starke Unterscheidungen bei der weiteren Berechtigungsvergabe. Auch wenn der eigentliche Nutzen aus dem Identitätsmanagement erst durch das Anschließen der weiteren Zielsysteme und die Automatisierung von bisherigen Laufzettelprozessen gezogen werden kann, sollten beim Design des Zentralverzeichnisses keine Kompromisse eingegangen werden. Entsprechend einfacher wird das spätere Anbinden weiterer Zielsysteme.

1.3.2 Synergiepotentiale im Hochschulbereich

Ein Vorteil ist die weite Verbreitung der HIS-Software[3] für die verschiedenen Verwaltungsaufgaben im Hochschulbereich. Ergänzt durch Informationsaustausch in Gremien wie dem erwähnten ZKI-Arbeitskreis können Hochschulen, die sich neu mit dem Thema auseinandersetzen, an den Erfahrungen und Ergebnissen der anderen Hochschulen partizipieren.

Interessant und hilfreich sind vor allem die grundsätzlichen Architekturüberlegungen und Design-Entscheidungen. Der verbleibende Anpassungsbedarf an die lokalen Gegebenheiten sollte jedoch nicht unterschätzt werden. So ist zum Beispiel die Nutzung einzelner Datenfelder innerhalb der HIS-Anwendungen und auch die definierten Prozesse zwischen den Abteilungen von Hochschule zu Hochschule so unterschiedlich, dass zumindest große Teile der Geschäftslogik für die Datensynchronisation an jeder Hochschule neu implementiert werden müssen.

1.3.3 Organisatorische Fragen und Projektmanagement

Die hochschulweite Einführung von Identitätsmanagement erfordert darüber hinaus in vielen Fällen die Anpassung von Prozessen – speziell im Personalbereich, die Festlegung von Datenhoheiten und technischen Schnittstellen. Wie bei allen komplexen Projekten ist deshalb ein schrittweises und fokussiertes Vorgehen erforderlich, sowie die Unterstützung durch das Management, in diesem Fall also durch die Hochschulleitung, zwingend.

Die Verwaltung von Identitäten als reine Infrastruktur-Aufgabe findet jedoch nur schwer das Interesse der Hochschulleitung. Entscheidend ist es deshalb, die Implementierung in ein Portfolio konkreter Initiativen zu strukturieren, die jeweils für sich allein bereits direkten und messbaren Nutzen erzeugen. Typische Beispiele für solche Initiativen sind hochschulweite und tagesaktuelle elektronische Telefonbücher (sog. White Pages), weitgehende automatisierte Versorgung mit Zugangsrechten (Provisioning), Aufbau zentraler

[3] HISSOS-GX für die Studierendenverwaltung, HISSVA-GX für die Mitarbeiterverwaltung, HISFSV-GX für die Finanz- und Sachmittelverwaltung

Verzeichnisse für Authentisierung und Autorisierung. Nur für solche konkreten Initiativen kann ein Nutzen identifiziert und damit auch das benötigte Projektbudget bewilligt werden.

Weiterhin ist für die erfolgreiche Umsetzung eine funktionierende technische und vor allem organisatorische Management-Infrastruktur mit definierten Richtlinien, Prozessen und Werkzeugen notwendig. Durch die Fokussierung auf konkrete Initiativen wird es möglich, den Ausbau der Infrastruktur gemäß den Anforderungen der umzusetzenden Initiativen zu priorisieren. Nicht alle technischen Schnittstellen sind im ersten Schritt erforderlich, ebenso werden beispielsweise nicht alle Attribute eines Mitarbeiters in gleichermaßen hoher Qualität für eine Telefonbuch-Anwendung benötigt. Der direkte Bezug zu dem Nutzen der Initiative hilft nicht nur bei der Budgetierung. Er schafft auch eine Basis, um Konsens über erforderliche Prozessänderungen und Änderungen von Datenhoheiten zu erreichen.

1.3.4 Externer Rat ist gefragt

In Anerkennung der organisatorischen Komplexität eines Identitätsmanagement-Projektes vertrauen viele Unternehmen auf die Unterstützung durch externe Berater. Bei einem derartigen Projekt sollte zunächst eine Phaseneinteilung des Projektes vorgenommen werden, um den Umfang überschaubar zu halten. Anschließend wird in der Industrie der erreichbare Nutzen der einzelnen Initiativen zu quantifiziert und während des Projektverlaufs der Erfolg gemessen. Die Unterstützung ist eine Partnerschaft auf Zeit, von der erwartet wird, dass nach Abschluss des Projektes keine Abhängigkeit vom Berater besteht.

Auch an Hochschulen ist externer Rat hilfreich. Oftmals ist es für einen externen Berater leichter, einerseits abteilungs- und bereichsübergreifende Zusammenarbeit zu organisieren, andererseits in der Nutzenbetrachtung und Priorisierung von persönlichen Präferenzen unabhängig zu bleiben. Die externe Unterstützung sollte daher prinzipiell in die Projektplanung einbezogen werden. Neben der technischen und fachlichen Kompetenz ist immer auch die persönliche Kompetenz des Beraters ein entscheidender Faktor für den Erfolg eines Projektes. Wichtig für die Hochschulen ist auch die Bereitschaft des Beraters, sich in der Vorgehensweise an die jeweiligen Bedürfnisse der Hochschule anzupassen. In der Industrie ist es oftmals Hauptzielvorgabe, ein Projekt so schnell wie möglich abzuschließen. Für eine Universität kann es andere Kriterien geben, so zum Beispiel der größtmögliche Knowhow-Transfer an die eigenen Mitarbeiter durch die Einbindung von Hochschulmitarbeitern in das Projekt, um die zukünftige Abhängigkeit von externer Beratung und damit weitere Kosten zu minimieren. Cambridge hat in seinen Projekten im Hochschulbereich gute Erfahrungen gemacht mit einer Kombination aus Projektmanagementunterstützung, Beisteuerung von Analyse- und Designergebnissen sowie Technologie-Training und anschließendem Coaching der Projektmitarbeiter während der Entwicklung. Durch den Einsatz des Coaches auf mehreren Projekten kann der Abruf je nach Bedarf an der Hochschule gesteuert werden.

Um Vertrauen in die Lösung aufzubauen, können kleine Workshops, die Zwischenergebnisse für eine Projektinitiative liefern, einen sinnvollen Einstieg bilden. Das IT-Beratungsunternehmen Cambridge Technology Partners veranstaltet zum Beispiel sowohl strategi-

sche Workshops, die die weitere Projektplanung erleichtern, als auch technische Workshops, die die Möglichkeiten der Lösung in einer abgeschlossenen Umgebung aufzeigen.

1.4 Resümee

Identitätsmanagement ist ein Thema, das aufgrund seines Beitrags zur Steigerung der IT-Sicherheit und der enormen Automatisierungspotentiale nicht nur für Unternehmen, sondern auch für Hochschulen interessant ist. Ein in der Praxis verbreiteter erfolgreicher Ansatz ist der Einsatz eines Meta Directorys als zentrales Element des Identitätsmanagements. Zwischen den Hochschulen gibt es einen regen Informationsaustausch und die Möglichkeit von den Erfahrungen an anderen Einrichtungen zu profitieren. Der größtmögliche Nutzen eines Identitätsmanagement-Projektes lässt sich am besten durch eine genaue Festlegung der Projektziele und der dazu notwendigen Initiativen, sowie durch eine starke Projektorganisation erreichen. Dazu ist eine externe Unterstützung in aller Regel hilfreich. Hochschulen richten besondere Anforderungen an Berater hinsichtlich der Erfahrung mit den fachlichen Besonderheiten in der Hochschulorganisation und eines effizienten Knowhow-Transfers in die eigene Einrichtung.

1.5 Über Cambridge Technology Partners

Cambridge Technology Partners, eine Tochter der Novell Inc., ist ein weltweit tätiges IT-Beratungsunternehmen – führend bei der Entwicklung und Umsetzung von IT-Strategien in den Bereichen CRM und Business Integration sowie der damit verbundenen Optimierung der Marketing-, Vertriebs- und Service-Prozesse. Im Fokus steht die Interaktion mit Kunden, Partnern, Lieferanten und Mitarbeitern – unabhängig vom Kommunikationskanal. Zur signifikanten Senkung der IT-Kosten erarbeitet Cambridge zudem maßgeschneiderte Konzepte für den Einsatz von Linux.

Das Angebot von Cambridge umfasst die Integration von Anwendungen für Customer Relationship Management, den Bereich Business Integration mit Identitätsmanagement, Enterprise Application Integration und Web Services, die Erarbeitung individueller IT-Strategien sowie Inbetriebnahme und Support der Lösungen.

Das IT-Beratungsunternehmen analysiert die Schwerpunktthemen zudem regelmäßig in fundierten branchenspezifischen und -übergreifenden Studien und leitet individuelle Empfehlungen ab.

Cambridge im Internet: http://www.cambridge-germany.com

Literatur

[1] Chris King: „The Value of Identity Management“. META Group Research, 2002

[2] Bob Parker: „Five High-Value Infrastructure Projects for the 2003 Budget“. AMR Reseach, Inc., September 2002

[3] Rich Mogull: „Danger within“. Gartner Group, Februar 2002

[4] Richard Hunter: „Enterprises and Employees: The growth of distrust“. Gartner Group, 2002