Bernd Hohgräfe

IT-INSTRUMENTE

Identity Management: Prozessintegration als Schlüssel zum Erfolg

Hochschulinterne Prozesse deutlich optimieren

Die zunehmende Privatisierung von Hochschulaufgaben wird das Verhältnis zwischen den Studierenden und ihrer Bildungseinrichtung tiefgreifend verändern. Wenn sie immer mehr als „Kunden" betrachtet werden, entwickelt sich der Einschreibe- bzw. Rückmeldevorgang dementsprechend zur Bestellung einer von der Hochschule zu erbringenden kostenpflichtigen Leistung. Die „zahlende Kundschaft" erwartet dann einen entsprechenden Gegenwert. Nicht nur im Hinblick auf die Qualität der Lehre, sondern auch auf die schnelle Bereitstellung der für ihr Studium notwendigen Infrastruktur: Studierendenausweis, Benutzerkonten, Zugangsberechtigungen, Bibliotheks- und Mediennutzung sowie entsprechende Support- und Service Level. Identity Management kann hier einen deutlichen Beitrag zur Optimierung der entsprechenden hochschulinternen Prozesse im Hinblick auf Zeit und Kosten leisten.

Die Hochschule der Zukunft kann sich auf erprobte IT-Konzepte und -Instrumente stützen.

Foto: Archiv

Identity Management ist eine notwendige Voraussetzung für jede Art von E-Business – auch im universitären Umfeld. Diese These mag auf den ersten Blick überraschen, erklärt sich aber im aktuellen Kontext zunehmender Privatisierung der Hochschulen. Denn wenn der Studierende zum zahlenden Kunden wird, steigen die Ansprüche an die für das Entgelt erwartete Leistung. In den USA ist eine solche Erwartungshaltung der Studierenden – nicht zuletzt aufgrund der hohen Kosten eines Studiums – bereits üblich und sie wird sich auch in Deutschland mit der Einführung von Studiengebühren verbreiten. Vor diesem Hintergrund gewinnt das Thema „Identity Management" in diesem Umfeld zunehmend an Bedeutung.

Vom Meta Directory zum Identity Management

„Eine Menge von Prozessen und eine unterstützende Infrastruktur für das Anlegen, die Pflege und die Nutzung digitaler Identitäten" – so definiert die Burton Group Identity Management. Es handelt sich dabei um die konsequente Weiterentwicklung jener Lösungen, die vor vielen Jahren zuerst als Verzeichnisdienst (Directory Service) eingeführt wurden. Während ein Verzeichnisdienst anfänglich als reines Auskunftssystem für Identitäten der angeschlossenen Systeme diente und damit eine eher passive Funktion hatte, entstand schon bald die Notwendigkeit, die in jeder Organisation existierenden verschiedenen Verzeichnisse und Datenbanken miteinander abzugleichen.

Reine Meta Directory-Lösungen stellen die Konsistenz und Aktualität der personenbezogenen Daten in allen angeschlossenen Systemen sicher. Dabei gleichen sie jedoch nur einzelne Attribute ab, ohne aktiv Einträge anzulegen. Bei den angeschlossenen Systemen handelt es sich typischerweise um Datenhaltung und Benutzerverwaltung von Betriebssystemen, Mailservern, Telekommunikationsanlagen, Portallösungen und verschiedenen Applikationen, wie Abbildung 1 zeigt.

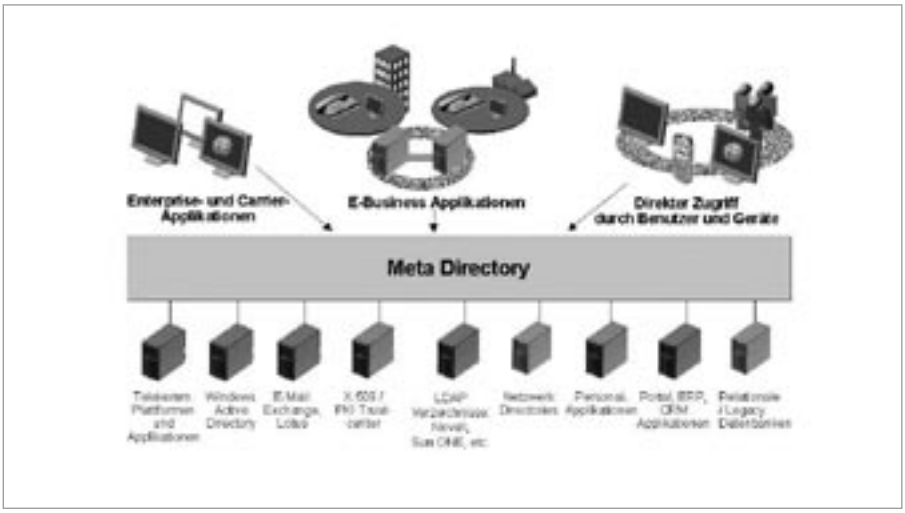

Abb. 1: Ein Meta Directory dient als Informationsdrehscheibe.

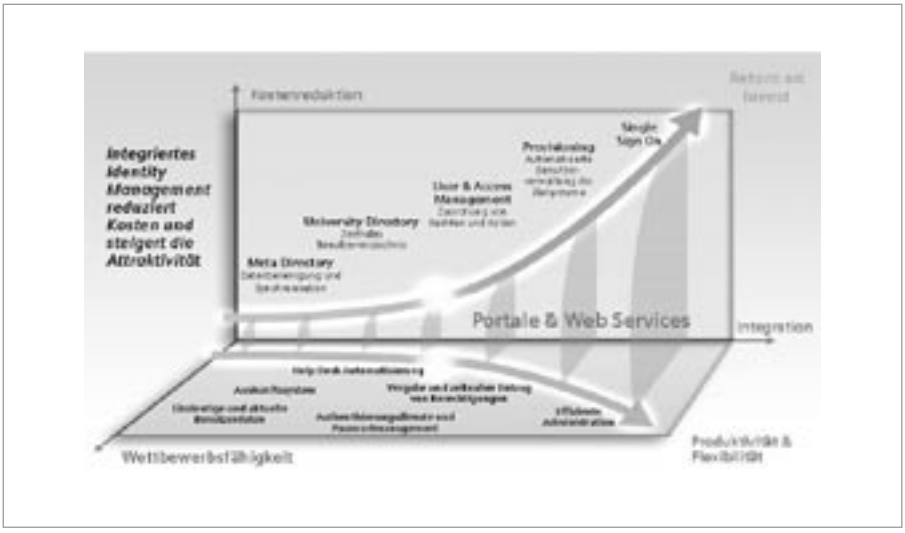

Abb. 2: Eine Identity Management-Lösung hat viele Nutzendimensionen.

Bei einer solchen Meta Directory-Lösung wird die Benutzerverwaltung weiterhin von den einzelnen Systemen beziehungsweise Applikationen übernommen. Demgegenüber erfolgt bei einer Identity Management-Lösung die **Benutzerverwaltung** zentral für alle angeschlossenen Systeme, wobei eines dieser Systeme durchaus die Quelle für einen neuen Benutzer sein kann, im Hochschulbereich also etwa das Hochschul-Informations-System HIS. Im Rahmen der Benutzerverwaltung werden für einzelne Benutzer(-gruppen) dann die notwendigen Berechtigungen vergeben. Jeder Berechtigung sind entsprechende Benutzerkonten und **Gruppenzugehörigkeiten** in den angeschlossenen Zielsystemen sowie eventuell notwendige Geräte (Assets) zugeordnet. Das automatisierte Anlegen und Löschen dieser Benutzerkonten, die Zuordnung zu den korrekten Gruppen in den jeweiligen Zielsystemen sowie die Auslösung von Bestellvorgängen wird als Provisionierung (Provisioning) bezeichnet. Den erhöhten Nutzen eines integrierten Identity Managements gegenüber einem „einfachen“ Meta Directory veranschaulicht Abbildung 2.

Mehrwert durch den Einsatz von Rollen

Berechtigungen werden dabei zunehmend nicht mehr direkt, sondern indirekt über Rollen vergeben. Dieses so genannte „Role Based Access Management“ (RBAM) ist inzwischen standardisiert und hat zwei wesentliche Vorteile: Zum einen kann einer Rolle eine Vielzahl einzelner Berechtigungen zugeordnet sein, sodass Benutzern beim Anlegen statt vieler einzelner Berechtigungen nur noch eine einzige Rolle zugewiesen werden muss. Zum anderen können die einer Rolle zugeordneten Berechtigungen bei Bedarf einfach angepasst werden und gelten damit automatisch für alle Inhaber dieser Rolle.

Rollen lassen sich darüber hinaus auch automatisiert aufgrund von so genannten „Policies“ vergeben. Dabei können Personen, die eine bestimmte Rolle innehaben, in Abhängigkeit von bestimmten Parametern – wie beispielsweise Funktion, Fachbereich und Standort – unterschiedliche Berechtigungen zugeordnet werden. So ergeben sich etwa für einen Dekan je nach Fachbereich unterschiedliche spezifische **Berechtigungen**. Damit wird die Benutzerverwaltung deutlich vereinfacht und beschleunigt.

Ein Studierender kann innerhalb einer Hochschule durchaus mehreren Rollen gleichzeitig zugeordnet sein, zum Beispiel als Studierender, studentische Hilfskraft und Mitglied in der studentischen Selbstverwaltung. Im Zeitverlauf können einzelne Rollen hinzukommen oder entfallen.

So kann ihm bei der Exmatrikulation automatisch die Rolle „Studierender“ entzogen und die Rolle „Alumnus“ zugewiesen werden. Es ist denkbar, dass er dann (einen Teil seiner) Benutzerkonten und seine E-Mail-Adresse behält, aber seine Berechtigungen entsprechend angepasst werden. Dabei ist insbesondere die Bedeutung des automatisierten Entzugs von Rollen und/oder Berechtigungen unter Sicherheitsaspekten nicht hoch genug einzuschätzen, denn auf diese Weise können Sicherheitsrisiken durch unberechtigten Zugriff ehemaliger Studierender vermieden werden.

Dipl.-Ing., Eur Ing Bernd Hohgräfe ist Leiter des Center of Competence Identity and Access Management bei Siemens Communication Consulting, Essen.

◆ **Access Management als sinnvolle Ergänzung:**
Wenn Benutzer, Rollen und Berechtigungen an der Hochschule erst einmal zentral verwaltet und vergeben werden, ist es sinnvoll, auch den Zugang zu bzw. Zugriff auf Ressourcen zentral zu überwachen. Ressourcen können dabei Arbeitsplatzrechner, Betriebssysteme, Portale, Applikationen, Datenbestände und Datenbanken sein. Hier sind die folgenden Aspekte von Bedeutung:

◆ **Authentifizierung:**
Benutzer müssen eindeutig identifizierbar sein, und elektronische Identitäten müssen sicher und zweifelsfrei validiert werden. Dies ist die Voraussetzung für die korrekte Autorisierung. Hier können neben Log-in und Passwort auch Chipkarten oder biometrische Verfahren zum Einsatz kommen, um eine möglichst starke Authentifizierung zu erreichen.

◆ **Autorisierung:**
Zugriffe auf geschützte Ressourcen müssen gemäß der Sicherheitsrichtlinie (Rollen- und Berechtigungskonzept) überprüft werden, damit es nur berechtigte Zugriffe gibt. Die Rechtmäßigkeit eines Zugriffs kann dabei von weiteren Parametern wie Zugriffsort und -zeit abhängen.

◆ **Auditing:**
Alle Aktivitäten im Zusammenhang mit Benutzerzugriffen müssen gespeichert, überwacht und für regulative Anforderungen greifbar sein. Dies ist insbesondere für alle finanziellen und prüfungsbezogenen Transaktionen unabdingbar, um auch später noch entsprechende Nachweise erbringen zu können.

◆ **Accounting:**
Abrechnungsrelevante Daten müssen benutzerbezogen gespeichert und für Abrechnungszwecke verfügbar sein. Der Grad der Erfassung hängt davon ab, ob und wie IT-Leistungen an der Hochschule verrechnet werden. Identity und Access Management schaffen hier die Voraussetzung für zukünftige nutzungsbezogene Verrechnungsmodelle.

Verwaltungsprozesse für Studierende und Verwaltung

Die heutigen Prozesse im Hochschulbereich sind historisch gewachsen und orientieren sich vielfach noch an papierbasierten Abläufen. So ist es nach wie vor üblich, dass ein Studienanfänger sich zuerst im Studierendensekretariat immatrikuliert, dann in der Bibliothek einen Benutzerausweis beantragt und diesen später abholen muss. Danach erhält er im Hochschulrechenzentrum ein Benutzerkonto, und im weiteren Verlauf seines Studiums muss er zur Belegung von Veranstaltungen sowie Anmeldung zu Prüfungen immer wieder persönlich in der Verwaltung erscheinen. Dies erfordert mehrfache manuelle und redundante Datenerfassung und einen hohen, wenngleich verteilten Administrationsaufwand. Mangelnde Transparenz bei den vergebenen Berechtigungen ist die Folge. Und auch für den Studierenden hat dieses Vorgehen spürbare Nach-

Stichwörter
Hochschulen
Universitäten
Meta Directory
Identity Management
Access Management
Automatisierte Benutzerverwaltung
Berechtigungsvergabe
Administrationsprozesse

Abb. 3: Optimierte Administrationsprozesse vereinfachen Verwaltung und Provisionierung.

teile, da er verschiedene Verwaltungsstellen aufsuchen und mehrfach Wartezeiten in Kauf nehmen muss.

Dass es anders gehen kann, zeigen Beispiele aus der Wirtschaft, die zunehmend auch in modernen Verwaltungen eingeführt werden. Das Beispiel der Immatrikulation könnte damit folgendermaßen und wie in Abbildung 3 dargestellt ablaufen:

1. Der Studienanfänger immatrikuliert sich im Studierendensekretariat, wo er mit seinen Stammdaten im Hochschul-Informations-System (HIS) erfasst wird. Über die Verbindung zum Identity-Management-System wird in der Folge automatisch ein Verzeichniseintrag generiert. Falls sich im Laufe des Studiums Veränderungen ergeben, werden seine Stammdaten stets hier an zentraler Stelle aktualisiert.

2. Im nächsten Schritt werden ihm in der rollenbasierten Benutzerverwaltung auf Grund seiner Stammdaten (Standort, Fachbereich etc.) entsprechende Rollen zugewiesen. Dies kann ganz oder teilweise automatisiert – einschließlich entsprechender Freigabe- und Genehmigungsverfahren – und auch dezentral in den einzelnen Fachbereichen geschehen.

3. Danach werden vom Identity-Management-System im Hochschulrechenzentrum automatisch ein persönliches Benutzerkonto angelegt und eine E-Mail-Adresse vergeben. Die Berechtigungen seines Benutzerkontos hängen dabei von den dem Studierenden zugewiesenen Rollen ab. Diese Informationen werden in der Benutzerverwaltung synchronisiert und stehen damit allen angeschlossenen Systemen zur Verfügung.

4. Auch im Ausleihsystem der Universitätsbibliothek wird automatisch ein Benutzerkonto mit entsprechenden Konditionen angelegt – abhängig von der Rolle des Studierenden, beispielsweise für Gasthörer kostenpflichtig. Die Bestätigung wird an seine aus Schritt 3 bekannte E-Mail-Adresse verschickt.

5. Dann wird im Prüfungsamt automatisch ein Konto für die individuellen Leistungspunkte angelegt. Der erste Kontoauszug wird ebenfalls an die aus Schritt 3 bekannte E-Mail-Adresse verschickt.

6. Abhängig von den zugewiesenen Rollen kann der Studierende nun das Hochschul-Portal nutzen, online Veranstaltungen belegen, sich zu Prüfungen anmelden und Ergebnisse einsehen.

Über die Immatrikulation hinaus gibt es weitere Beispiele für automatisierbare Prozesse im universitären Alltag, von denen hier nur eine Auswahl aufgeführt ist:

- Bezahlung von Studiengebühren, Kopieraufträgen und Mensaessen,
- Rückmeldung für ein Semester und die entsprechenden Wahlfächer,
- Online-Reservierung von Büchern,
- elektronische Signatur und Abgabe von Semesterarbeiten,

keywords
universities
meta directory
identity management
access management
automated user administration
administration processes

- Online-Anmeldung zu Prüfungen und Abfrage von Ergebnissen,
- Fernzugriff auf zentral gespeicherte Vorlesungsunterlagen,
- verschlüsselter Datenaustausch bei externen Studienarbeiten.

Identity und Access Management als organisatorische Angelegenheit

Allen Anwendungen gemeinsam ist, dass die erforderliche Technik und die benötigten Produkte zur Umsetzung bereits zur Verfügung stehen. So sind elektronische Geldbörsen – in Form der Geldkarte oder als Fahrausweis mit integriertem Chip für den Öffentlichen Personennahverkehr – bereits im Einsatz. In großen Unternehmen wie etwa der Siemens AG erfolgt die Ausleihe von Medien bereits elektronisch, Verpflichtungserklärungen werden digital signiert, Belegschaftsaktien online bestellt und Gehaltsabrechnungen elektronisch verschlüsselt verteilt. Vom Arbeitsplatz beim Kunden oder zu Hause greifen Mitarbeiter über ein „Virtual Private Network" auf das Siemens-Intranet zu.

Die Herausforderung besteht nun im universitären Umfeld darin, diese Prozesse im Gesamtzusammenhang zu sehen und Synergien bezüglich der bereitzustellenden Infrastruktur zu erkennen. Identity und Access Management sind dabei **Infrastrukturkomponenten**, die sich um so eher amortisieren, je mehr Anwendungen und Prozesse sie nutzen. Ihr Einsatz ist heute weniger eine technische als vielmehr eine organisatorische Frage.

Als Beispiel für eine solche Infrastruktur sei hier stellvertretend die Architektur der Siemens Identity und Access Management-Lösung beschrieben, die Abbildung 4 zeigt. Als gemeinsame Datenablage für Identitäts- und Konfigurationsdaten wird der bewährte, X.500 und LDAP konforme Directory Server HiPath DirX verwendet. Er dient als zentrale Informationsdrehscheibe für die anderen Komponenten der Produktfamilie HiPath DirX Solutions:

- DirXmetahub führt Benutzerdaten aus einer Vielzahl von Verzeichnissen und Datenbanken zusammen und bereinigt sie.
- DirXmetaRole automatisiert die Verwaltung von Benutzern und die rollenbasierte Vergabe von Benutzerkonten und Berechtigungen in den angeschlossenen Systemen.
- DirX Identity als Nachfolger integriert beide Komponenten unter einer gemeinsamen Webbasierten Oberfläche mit Genehmigungs-Workflows und User-Self-Service Diensten.
- DirX Access ermöglicht den Zugang zu einer Vielzahl von Anwendungen durch einmalige Anmeldung (Single Sign On).

Ergänzend können zur sicheren Identifizierung von Anwendern Chipkartenlösungen eingesetzt werden.

Qualitative und quantitative Vorteile

Identity und Access Management-Lösungen müssen über die Verwaltung von Benutzerkonten für lokale menschliche Nutzer hinaus noch zwei weitere Gruppen von Benutzern abbilden:

Abb. 4: Module des Siemens Identity und Access Managements bilden eine integrierte Lösung.

summary

In view of the increasing privatisation of university tasks in Germany, identity and access management can make a clear contribution to optimise the internal processes of universities. The transformation of former paper-based administration processes into electronic operations generates positive effects on time and costs for both, the students and the university administrations. The required technology is already available. Current projects show that these solutions can be and have to be adapted to the individual needs and intentions of each institution.

Nun kann es sich keine Hochschule leisten, Identity und/oder Access Management um ihrer selbst willen einzuführen, sondern dies geschieht immer im Hinblick auf die damit verbundenen qualitativen und quantitativen Vorteile sowie den Nutzen für die Beteiligten. Für die Studierenden sind dies beispielsweise die Einführung von Self-Service-Diensten, der freie Zugriff auf Veranstaltungsunterlagen, die Online-Belegung von Veranstaltungen und die Einsicht in Prüfungsergebnisse.

- „Maschinelle Nutzer", so genannte Funktions-Accounts, die in der Praxis von Anwendungsprogrammen zu vielfältigen Zwecken genutzt werden. Der Zugriff erfolgt heute in der Regel über Web Services.
- „Entfernte Benutzer", etwa Studierende anderer Hochschulen. Statt diese User zusätzlich (und redundant) lokal zu pflegen, kommt hier das Konzept der „Federated Identity" zum Einsatz: Ihnen werden – aufgrund einer vorab vereinbarten Vertrauensbeziehung mit ihren Organisationen – entsprechende lokale Berechtigungen eingeräumt, ohne dass diese Benutzer lokal verwaltet werden.

Beide Konzepte – Web Services und Federated Identity – sind noch relativ neu und daher noch nicht weit verbreitet. Allerdings gilt auch hier, dass die zur Umsetzung erforderliche Technik und die benötigten Produkte bereits zur Verfügung stehen.

Nun kann es sich keine Hochschule leisten, Identity und/oder Access Management um ihrer selbst willen einzuführen, sondern dies geschieht immer im Hinblick auf die damit verbundenen qualitativen und quantitativen Vorteile sowie den Nutzen für die Beteiligten. Für die Studierenden sind dies beispielsweise die Einführung von **Self-Service-Diensten**, der freie Zugriff auf Veranstaltungsunterlagen, die **Online-Belegung von Veranstaltungen** und die Einsicht in Prüfungsergebnisse. Administratoren und Verwaltung profitieren unter anderem von der Vermeidung redundanter Datenerfassung, der Transparenz vergebener Berechtigungen, der systemgestützten Administration und der leichteren Integration neuer Dienste.

Die Hochschule insgesamt kann damit ihre Prozesse optimieren, standardisieren und dementsprechend günstiger realisieren. Dies gilt umso mehr, als nicht nur Personen, sondern auch Objekte wie Ressourcen (zum Beispiel Hörsäle) und Assets (Fahrzeuge, Arbeitsplatzrechner etc.) zunehmend mit einer Identität versehen und in Identity-Management-Systemen verwaltet werden können.

Projekte und Erfahrungen

An einer Reihe von Hochschulen und Universitäten in Deutschland sind inzwischen Projekte im Umfeld Identity und Access Management begonnen worden. Dabei kommen Produkte verschiedener Hersteller oder unterschiedliche Open Source Softwares (openLDAP) zum Einsatz. Der Schwerpunkt dieser Projekte liegt bisher im Bereich Meta Directory und Identity Management, was sich auch aus den Anforderungen und Zielen der Projekte ableitet. Unter den Anforderungen, die zur Etablierung eines Identity-Management-Projektes führten, finden sich zum Beispiel:

- Optimierung der Administration und Kosteneinsparungen,
- automatisierte Benutzerverwaltung über bestehende Systemgrenzen hinaus,
- Berechtigungsvergabe durch die Fachbereiche ohne detaillierte IT-Kenntnisse,
- einheitliche Benutzerverwaltung für verschiedene Benutzergruppen (Studierende, Lehrende, Wissenschaftliche Mitarbeiter, Verwaltungsmitarbeiter und externe Mitarbeiter),
- Prozessoptimierung im Hinblick auf eine zukünftig stärkere Integration der Telekommunikation in die IT-Umgebung durch Voice over IP.

Zudem verfolgen die beteiligten Hochschulen und Universitäten mit der Einführung eines Identity Management-Systems unter anderem die nachstehenden Ziele:

- Novellierung von Verwaltungsprozessen,
- Reduzierung der Anzahl der verwendeten Anmeldeformulare,
- zentrale Benutzerverwaltung für Mitarbeiter und Studierende,
- Vereinheitlichung der Namensgebung (Benutzerkonto, E-Mail-Adresse etc.),
- Verbesserung der Konsistenz, Aktualität und Qualität der Benutzerdaten,
- Abgleich der personenbezogenen Daten zwischen Mail- und Telefonsystemen, Personaldatenbanken, Directory Servern, SAP-Kostenstellen und Auskunftssystem,
- automatische Erstellung von Benutzerzertifikaten.

Selbstverständlich variieren Anforderungen und Ziele von Hochschule zu Hochschule. Dabei spielen die Zahl der Studierenden, die Anzahl und Heterogenität der eingesetzten Systeme, die bisherigen oder geplanten Prozesse, die finanzielle Ausstattung und nicht zuletzt auch die Innovationsfreudigkeit der beteiligten Organe eine große Rolle. Wie der Erfahrungsbericht einer großen Universität in Norddeutschland bestätigt (siehe Abbildung 5), ist eine Identity-Management-Lösung immer auch eine **hochschulindividuelle Lösung**, die zunächst sorgfältige Planung und intensive Zusammenarbeit aller internen und externen Partner erfordert, dann aber auch positive Aspekte für alle Beteiligten mit sich bringt. Aus den bisherigen Rückmeldungen aus laufenden Hochschulprojekten lässt sich jedenfalls entnehmen, dass sich die meisten erfreulich positiv entwickeln und sie damit ihren Beitrag zur Optimierung und Kundenorientierung der hochschulinternen Prozesse leisten.

- Die Einführung von Identity und Access Management erfordert mehr organisatorischen als technischen Aufwand.
- Die aktive Mitarbeit aller beteiligten Einrichtungen und Personen ist notwendig (positive Aspekte für alle Beteiligten).
- Ein Bewusstsein für das gemeinsame Projekt sollte hergestellt werden.
- Quell-Datenbestände (HIS-SOS, HIS-SVA) müssen vorher überarbeitet werden.
- Während der Realisierung ist das Feinkonzept laufend fortzuschreiben.
- Die Inanspruchnahme von Consultants der Hersteller ist effektiv und empfehlenswert (gezielte Konzepterarbeitung und effektive Umsetzung durch Erfahrung und Systemkenntnisse).
- Identity Management ist nicht „von der Stange“ zu haben, sondern ist entsprechend der Prozesse in der Hochschule ein sehr individuelles System.

Abb. 5: Erfahrungen einer Universität in Norddeutschland mit der Einführung von Identity und Access Management.

Fazit

Vor dem Hintergrund einer zunehmenden Privatisierung von Hochschulaufgaben kann mit Identity und Access Management ein deutlicher Beitrag zur Optimierung der entsprechenden hochschulinternen Prozesse geleistet werden. Wenn papierbasierte Verwaltungsabläufe in automatisierte elektronische Prozesse umgewandelt werden, treten Zeit- und Kosteneffekte ein, von denen sowohl Studierende als auch Hochschulverwaltungen profitieren. Die dafür erforderliche Technik steht bereits zur Verfügung. Aktuelle Projekte an einer Reihe von Hochschulen und Universitäten zeigen, dass entsprechende Lösungen individuell an die Anforderungen und Ziele der jeweiligen Einrichtung angepasst werden können und müssen.

Literatur:

Windley, Ph., Digital Identity, 1. Aufl., Sebastopol (CA) 2005.

von Knop, J./Havercamp, W./Jessen, E. (Hrsg.), Heute schon das Morgen sehen, 19. DFN-Arbeitstagung über Kommunikationsnetze, Düsseldorf 2005.

Fumy, W./Sauerbrey J. (Eds.), Enterprise Security, IT Security Solutions, Concepts, Practical Experiences, Technologies, Dezember 2005.

Kontakt:

Bernd Hohgräfe
Siemens Communication Consulting
Kruppstraße 16
45128 Essen
Tel.: +49 (0)2 01/8 16-33 49
E-Mail: bernd.hohgraefe@siemens.com