

Auswertung der Online-Befragung

Identity Management Im Zeichen der digitalen Identität

Hinter dem Begriff **Identity Management (IdM)** verbergen sich verschiedene Begrifflichkeiten und Ziele. Ziel ist es, dass Änderungen von Identitäten nur einmal durchgeführt und dann auf alle anderen Systeme in der IT-Infrastruktur übertragbar sind. Dadurch werden die administrativen Kosten erheblich gesenkt. Positiver Zusatznutzen: Der Grad der Sicherheit im Rahmen des Risiko-Managements der IT-Security steigt automatisch.

Häufig in diesem Zusammenhang genannt, weil greifbar, ist das Management von Passwörtern und Zugangsberechtigungen zu IT-Systemen sowohl im Unternehmensnetzwerk als auch über das Internet. Anwender müssen sich anhand ihrer digitalen Identität – in der Regel Benutzername und Passwort – gegenüber dem IT-System ausweisen. Dadurch wird sichergestellt, dass nur Mitarbeiter mit der entsprechenden Berechtigung auf bestimmte, unternehmenskritische Applikationen zugreifen dürfen. Abhängig von der Unternehmensgröße ist die Verwaltung aller existierenden Benutzer und deren Accounts für IT-Administratoren ein enorm hoher Arbeitsaufwand. Denn diese müssen jeden Mitarbeiter einzeln im System anlegen, die dazugehörigen Zugriffsberechtigungen frei schalten und sie regelmäßig auf dem aktuellen Stand halten. So lösen beispielsweise bereits vergessene Passwörter einen umfangreichen Verwaltungsprozess aus. Software-Lösungen für das Identity Management liefern umfassende Funktionen für die Verwaltung von Benutzern und deren Zugangsdaten zu IT-Systemen. Dadurch verringern sie den zeitlichen Aufwand für die Administration deutlich.

Provisioning ist ein Unterbegriff des Identity Management, das die automatisierte Zuweisung von Berechtigungen für bestimmte IT-Anwendungen und Systeme gemäß einem definierten Benutzerprofil bezeichnet. Positionen, Status und Aufgabenbereiche der Mitarbeiter unterliegen einem ständigen Wandel. Demgemäß sind Zugangsberechtigungen und Ressourcen schnell, flexibel und unter allen Aspekten der Unternehmenssicherheit zu vergeben.

Identity Federation ist ein weiterer Unterpunkt des Identity Management. Auf der Basis von Identity Federation können Unternehmen Benutzeridentitäten und Benutzerrechte standardbasiert mit Partner-Websites austauschen und gemeinsam nutzen.

Identity Management-Systeme setzen eine Wertschöpfungskette in Gang. Die Kosten für die IT-Administration und den Help Desk (zum Beispiel vergessene Passwörter) sinken und die Produktivität der Mitarbeiter steigt. Zusätzlich verringert die erhöhte Transparenz durch zentral hinterlegte Sicherheitsregeln und automatisierte Workflows zur Vergabe, Modifikation und Löschung von User Accounts Sicherheitslücken deutlich.

Zur Stichprobe

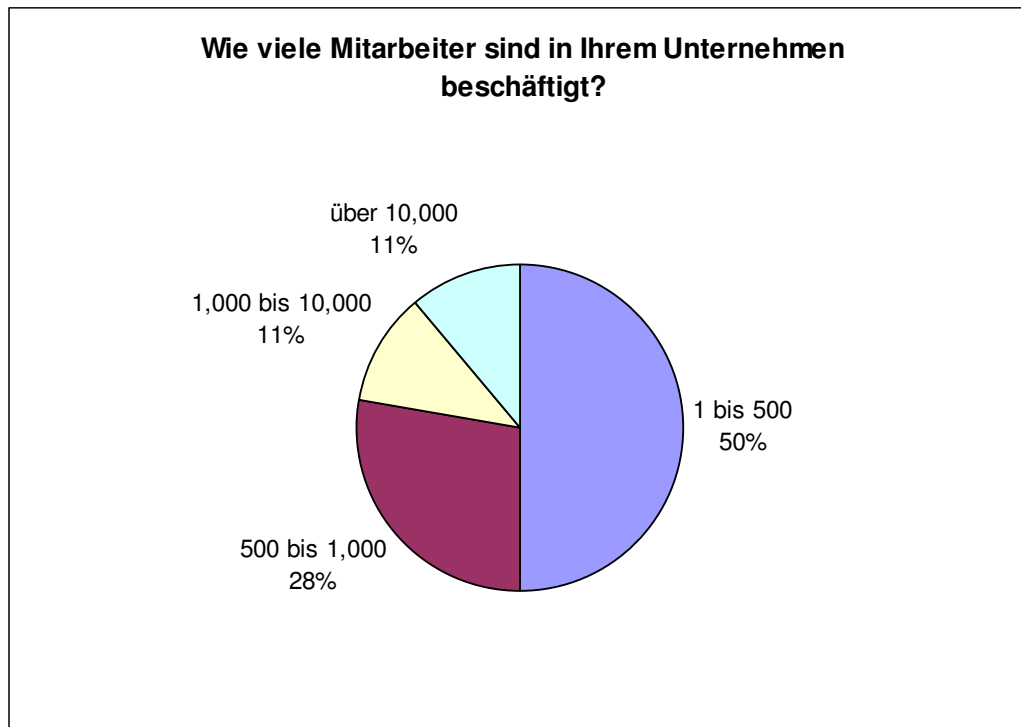
Benutzerkennungen und Passwörter gehören zum Alltag. Viele Unternehmen beschäftigen sich damit, die Verwaltung der Zugangsberechtigungen zu vereinfachen. Um ihre Wünsche und Vorgehensweisen zu erforschen, haben wir im Zeitraum vom 1.1. bis 20.2.2004 eine Online-Erhebung zu diesem Thema durchgeführt.

Um die Interessenten nicht durch zu viele Fragen zeitlich zu belasten, wurde die Anzahl auf 27 Fragen beschränkt. Gleichzeitig wurde keine Eingabeerzwingung programmiert, um die Abbruchrate gering zu halten. Bei einem Teil der Fragen waren Mehrfachnennungen möglich.

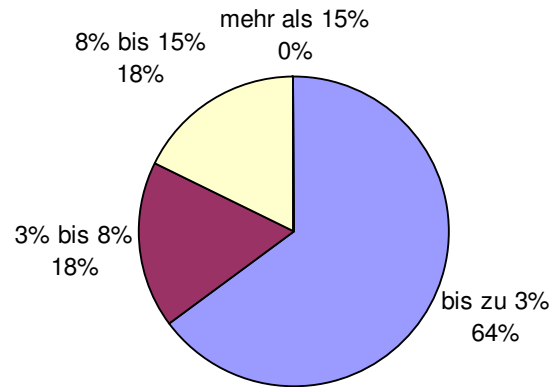
Das bedeutet auch, dass bei einem - wenn auch geringen Teil der Fragen - Antworten von den Anwendern übersprungen werden konnten.

Auf der Basis von 102 Antworten ergaben sich die nachfolgend in Diagrammen dargestellten Antworten. Die wichtigsten Ergebnisse haben wir in diesem Dokument zusammengefasst.

Profil der Teilnehmer an der Umfrage



Wie viel Prozent des IT-Budgets geben Sie in 2004 für IdM aus?



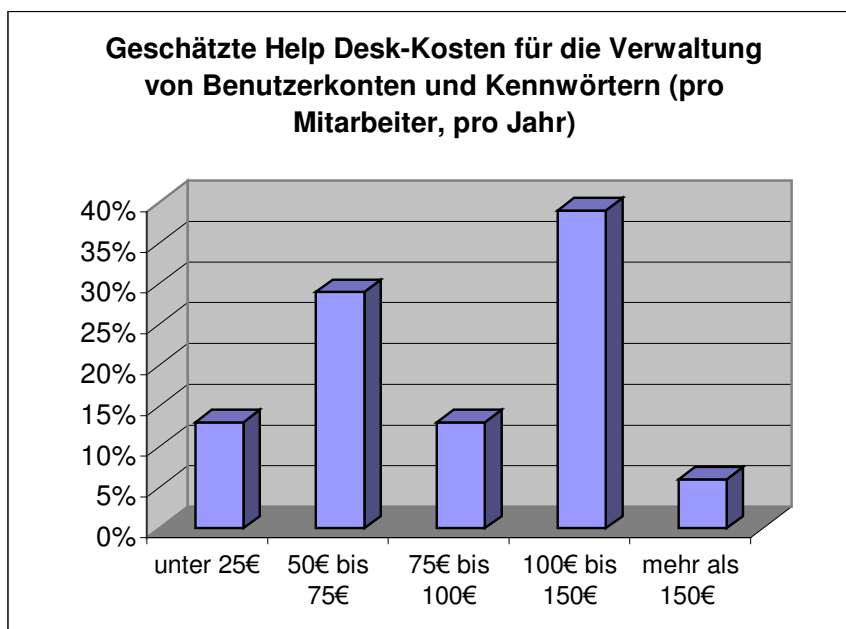
Von den 22% der Unternehmen mit mehr als 1000 Mitarbeitern geben Zweidrittel bis zu 3% ihres IT-Budgets für IdM aus und etwa Eindrittel zwischen 3% und 8%.

Digitale Identitäten als Herausforderung

Welche Probleme und Herausforderungen im Umgang mit digitalen Identitäten standen im letzten Jahr in Ihrem Unternehmen/Ihrer Organisation im Vordergrund beziehungsweise haben die höchsten Kosten verursacht? Folgende Punkte standen zur Auswahl und wurden wie folgt beantwortet (Mehrfachnennungen waren möglich):

Das Management/Zurücksetzen von Kennwörtern der Anwender	50%
Die Administration von Informationen in verschiedenen Verzeichnisdiensten	50%
Berechtigungsmanagement unübersichtlich	47%
Berechtigungsmanagement zu aufwändig	41%
Zu viele verschiedene Konten pro Benutzer	31%
Änderungen der Sicherheitseinstellungen beim Wechsel von Mitarbeitern im Unternehmen dauern zu lange	28%
Zugriffsberechtigungen von Mitarbeitern sind nicht nachvollziehbar	28%
Bereitstellen aller IT-Ressourcen für neue Mitarbeiter ist zu aufwändig	12%
Identity Theft, also Missbrauch digitaler Identitäten durch interne oder externe Personen	6%

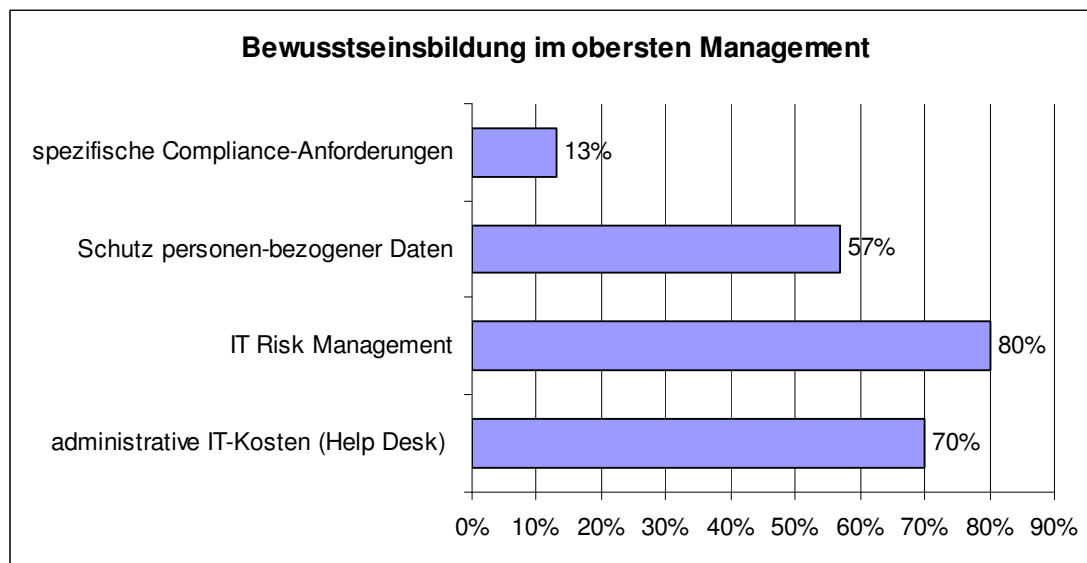
Rund die Hälfte der Befragten gab an, dass sich der Aufwand für die Verwaltung der Benutzerberechtigungen im vergangenen Jahr im Vergleich zu den Vorjahren erhöht hat. Wie viel Geld der Administrationsaufwand tatsächlich verschlingt, können 6% der Befragten genau beziffern. Rund 70% hingegen gaben an, dass der Aufwand für das Identity Management nur sehr ungenau zu beziffern sei. Die Mitarbeiter am Help Desk müssen sich mit dem Management von Benutzerkonten und Passwörtern auseinandersetzen. So schätzen rund 40% der befragten Unternehmen, die Help Desk-Kosten pro Mitarbeiter und Jahr auf 100 € bis 150 €.



IdM – Einschätzung und Umsetzung

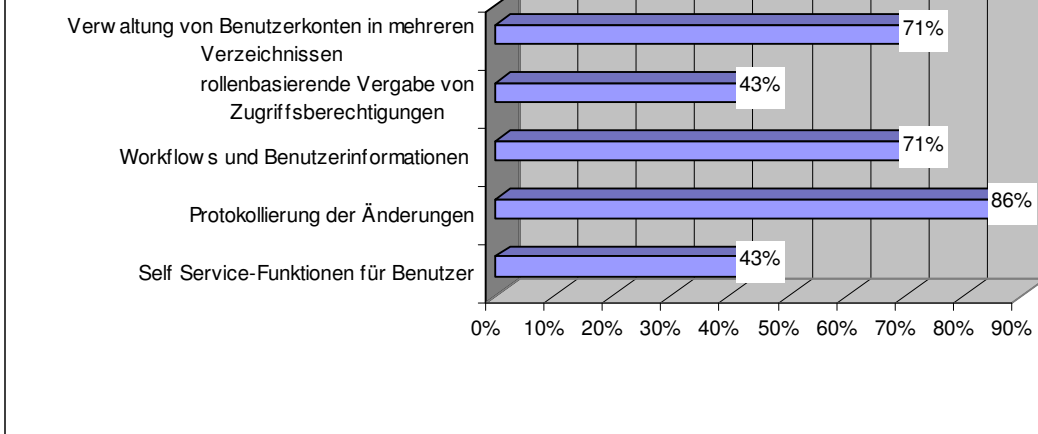
In etwa der Hälfte der Unternehmen gibt es eine definierte Strategie für das IdM. Knapp 60% der Unternehmen mit definierter Strategie setzen diese auch durchgängig um.

Häufig mangelt es gerade im obersten Management am Bewusstsein für Schwachstellen in der Informationstechnik. Was allerdings IdM betrifft, scheint die Führungsschicht bereits sensibilisiert zu sein. Von den Personen, die die Umfrage ausgefüllt haben, gaben rund 70% an, dass ihr oberstes Management über administrative IT-Kosten, insbesondere Help Desk-Kosten durch Benutzer- und Kennwortmanagement, und das IT Risk Management (gesicherter und kontrollierter Zugang zu sensiblen Unternehmensdaten und IT-Assets wie Source Codes) Bescheid weiß.



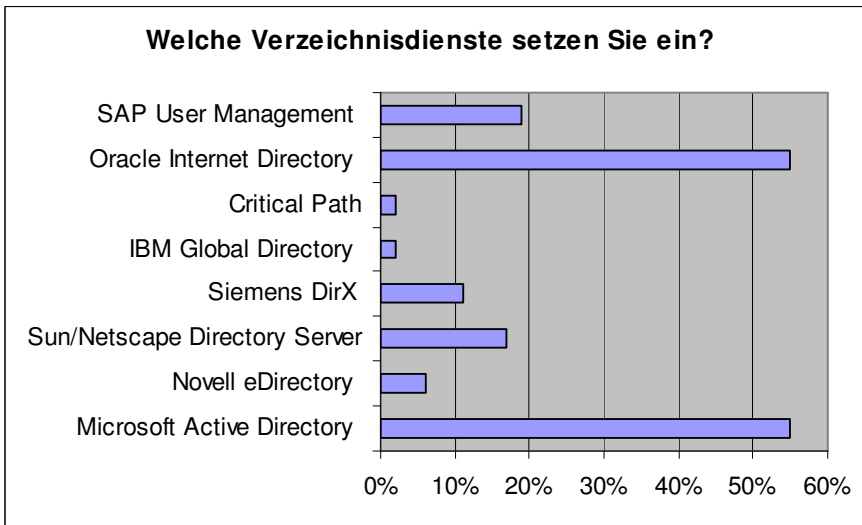
In fast allen befragten Unternehmen können Mitarbeiter ihre Kennwörter selbst ändern. Die Mehrheit der Mitarbeiter nutzt derartige Self-Service-Funktionen um Kennwörter zurückzusetzen oder Benutzerprofile zu aktualisieren. Ein Viertel der befragten Unternehmen setzt bereits Software für das User- oder Resource Provisioning ein.

Welche Funktionen nutzen Sie in Provisioning-Systemen?



Diejenigen Unternehmen, die noch keine Software für das User- oder Resource Provisioning einsetzen (rund Dreiviertel), verwenden mehrere Verzeichnisse. Dabei kommen bei Zweidrittel der Unternehmen sechs bis 25 verschiedene Directories zum Einsatz.

Welche Verzeichnisdienste setzen Sie ein?



Das Oracle Internet Directory und das Microsoft Active Directory führen mit jeweils rund 55% die Liste der Verzeichnisdienste an.

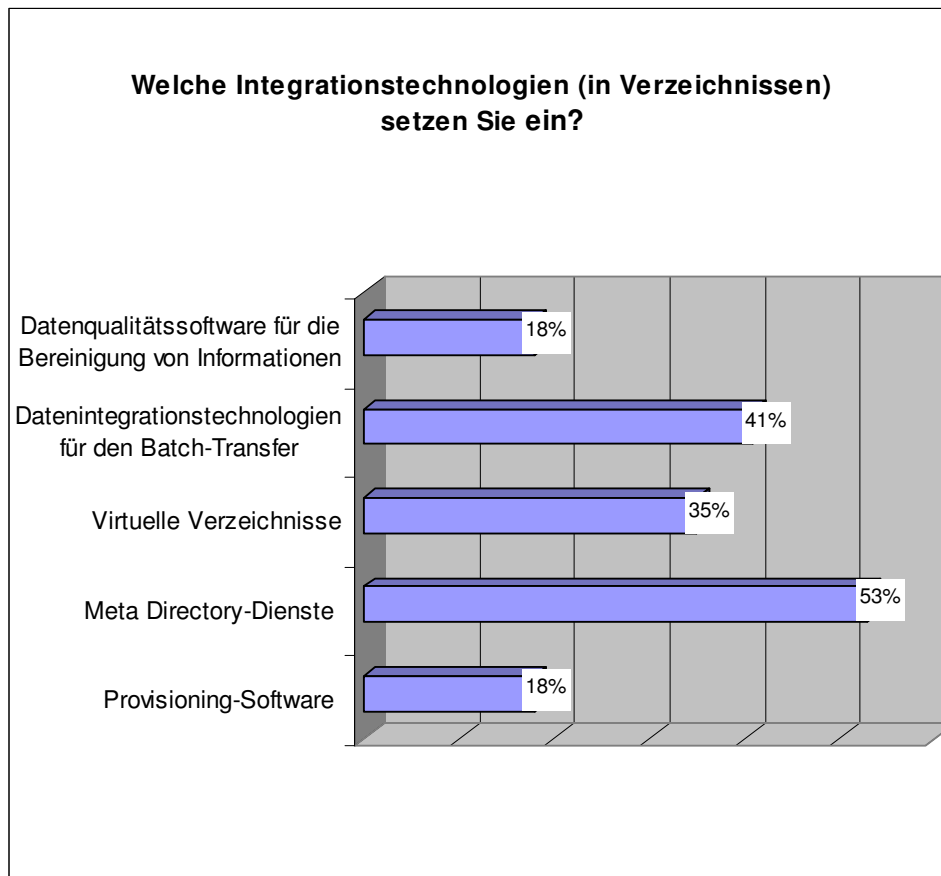
Wer wird in den Verzeichnissen geführt?

Die Anzahl der internen Benutzer, die mit den Verzeichnissen verwaltet werden, hängt eng zusammen mit der gesamten Anzahl an Mitarbeitern des Unternehmens.

Die Anzahl an Partnern, Lieferanten oder Kunden, die in die Verzeichnisse aufgenommen werden, weist keinerlei Relation zur Anzahl der Mitarbeiter auf. Nahezu alle Unternehmen verwalten externe Benutzer in ihren Directories. Bei einigen Unternehmen beträgt die Anzahl an externen Benutzern ein Vielfaches der eigenen Mitarbeiterzahl.

Meta Directories – Lastesel oder Vorreiter?

Gut die Hälfte der befragten Unternehmen setzt Metadirectories ein, dicht gefolgt von Datenintegrationstechnologien für den Batch-Transfer von Verzeichnisdaten.



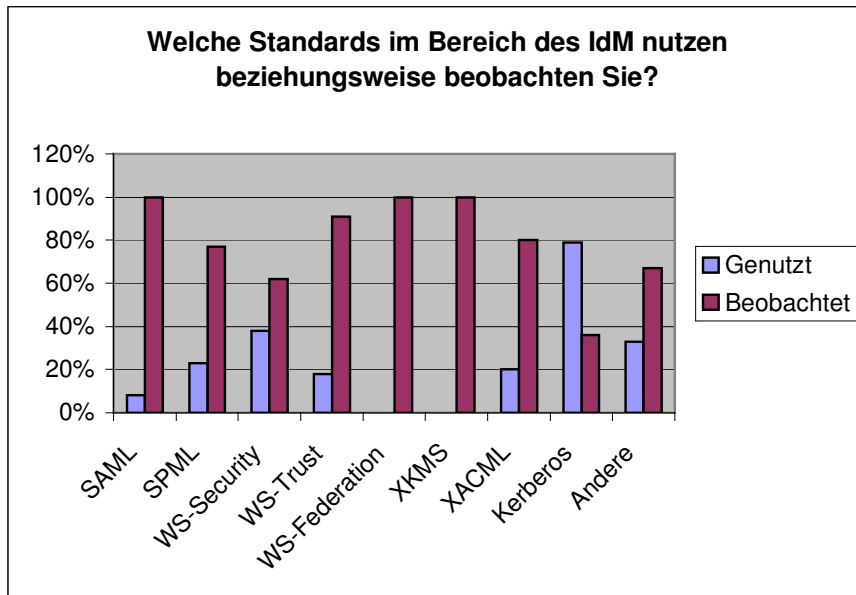
IdM: heute und morgen

Zur Authentifizierung von Anwendern sind Benutzername und Passwort ein Muss. Digitale Zertifikate und Token-Verfahren setzt fast die Hälfte aller befragten Unternehmen ein:

Benutzername und Passwort	100%
Digitale Zertifikate	50%
Token-Verfahren	47%
Biometrische Verfahren	3%

Seit Jahren bewährt sich Kerberos (in der griechischen Mythologie der dreiköpfige Wachhund an den Pforten zur Unterwelt) als offener Standard für die Authentifikation von Clients und Servern in Netzwerken. Durch Kerberos werden in offenen Netzwerken insbesondere Angriffe durch passives „Sniffing“ unterbunden, aber auch „Spoofing“, „Dictionary Attacks“, „Replay“ und andere Angriffe erschwert.

WS-Security gewinnt an Bedeutung als Standard für Web Services. Er umfasst das Signieren und Verschlüsseln von SOAP-Nachrichten, sowie das Anhängen von Security Credentials an SOAP-Nachrichten.



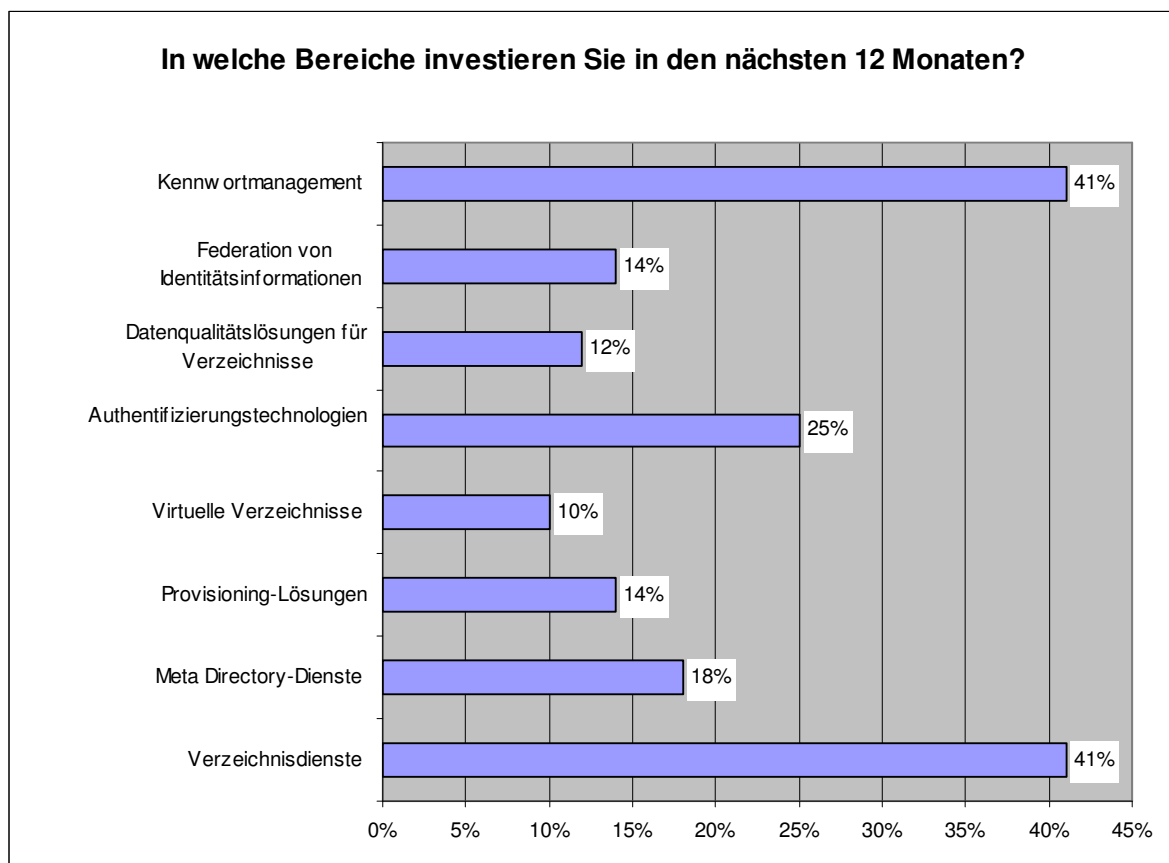
Mit großem Interesse beobachten viele der Befragten die offenen OASIS (Organization for the Advancement of Structured Information Standards)-Spezifikationen SAML (Security Assertion Markup Language) und SPML (Service Provisioning Markup Language), die XML (Extended Markup Language)-basierte Frameworks für den Austausch und die Administration von Benutzerzugriffsrechten und Ressourceninformationen in heterogenen Umgebungen definieren. WS-Trust hingegen ist eine IBM-eigene Spezifikation für die Sicherheit von Web Services.

IBM und Microsoft sind federführend bei der Definition der WS Federation Language. Diese Spezifikation soll standardisieren wie Unternehmen Kennungen von Benutzern und IT-Systemen über verschiedene Authentifizierungssysteme und Unternehmensgrenzen hinweg gemeinsam nutzen können.

Das World Wide Web Consortium (W3C) definiert die XML Key Management Specification (XKMS). Diese umfasst die beiden Teile XML Key Information Service Specification (X-KISS) und XML Key Registration Service Specification (X-KRSS).

OASIS verabschiedete die eXtensible Access Control Markup Language (XACML) als offenen Standard. XACML ist eine XML-basierte Sprache zur Zugangskontrolle. XACML beschreibt die Sprachrohre beider Seiten, derjenigen, die Zugang wünscht, und der antwortenden Seite. Die Policy Language bestimmt, wer, was zu einem bestimmten Zeitpunkt machen darf. Die Response Language prüft, ob eine bestimmte Anforderung erlaubt wird und liefert die Antworten auf Anfragen der Policy Language.

Bei der Frage nach den Investitionen in den nächsten zwölf Monaten waren drei Nennungen erlaubt. Kennwort-Management und Verzeichnisdienste gehören zu den Bereichen des IdM, in die am häufigsten investiert wird. Rund ein Viertel der Befragten plant für Authentifizierungstechnologien Geld auszugeben.



Diese Umfrage wurde gesponsert von



SIEMENS

