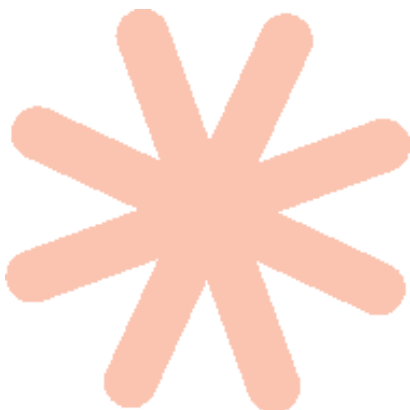


Wissen, wer wann worauf zugreift.

Warum ist ein integriertes Identitätsmanagement nötig?

Um sich in der aktuellen Wirtschaftslage effektiv im Wettbewerb behaupten zu können, eröffnen Unternehmen immer mehr Anwendern – Kunden, Mitarbeitern, Partnern und Lieferanten – den Zugang zu Informationen. Gleichzeitig müssen IT-Abteilungen mit immer weniger Ressourcen auskommen. Und was noch wichtiger ist: Sie müssen die Identitäten der Benutzer während der gesamten Nutzungsdauer effektiv verwalten können. Nun kann Identitätsmanagement so kostspielig sein, dass es die Entwicklung und Implementierung neuer geschäftlicher Initiativen behindert. Doch neue Lösungen fürs Identitätsmanagement und die Bereitstellung von Benutzerkennungen verbessern die Kosteneffizienz, beschleunigen die Marktreifung neuer Initiativen, fördern die Zufriedenheit der Endanwender und bieten ein hohes Maß an Sicherheit.

Das vorliegende Dokument beschäftigt sich mit der Frage, auf welche Personenkreise sich das Identitätsmanagement auswirkt und welche betriebswirtschaftlichen Wirkungen davon ausgehen – Bereitstellung und Verwaltung von Benutzerdaten, Fragen der Anwenderproduktivität, Anbindung an Geschäftsprozesse und Implementierung neuer geschäftlicher Initiativen. Ferner geht es um die Anforderungen, die an eine Identitätsmanagement-Lösung zu stellen sind, und um entsprechende Angebote von IBM.



Auf wen wirkt sich Identitätsmanagement aus?

Das Identitätsmanagement ist vor allem für drei Personengruppen relevant: Endanwender, Administratoren und Entwickler. Die Endanwender kommen mit dem Identitätsmanagement in Berührung, wenn sie Zugang zu Ressourcen anfordern und diese Ressourcen anschließend nutzen möchten. Die Zeit, die die Beantwortung von Benutzeranforderungen beansprucht, und die Komplexität des Vorgangs wirken sich unmittelbar auf die Zufriedenheit des Benutzers und seine Bereitschaft zur weiteren Zusammenarbeit mit dem betreffenden Unternehmen aus. Lange Verzögerungen, die durch mühsame manuelle Prozesse und Eingabefehler entstehen, sind frustrierend für den Benutzer.

Administratoren sind betroffen, wenn sie versuchen, den Zugangswünschen von Benutzern zu entsprechen, und ihnen beim Zugriff auf Ressourcen helfen. Um einem Benutzer den Zugang zu Ressourcen ermöglichen zu können, müssen sich Administratoren meist manuell um die entsprechenden Genehmigungen bemühen. Ein weiterer manueller Prozess ist die eigentliche Freigabe der gewünschten Ressourcen und das Anlegen der Benutzer-Stammdaten. Hat der Benutzer endlich Zugang, muss ihm ein Supportdienst für Rückfragen zur Verfügung stehen, damit er produktiv arbeiten kann.

Der dritte vom Identitätsmanagement tangierte Personenkreis sind die Entwickler. Bei der Erstellung neuer Geschäftsanwendungen ist es ihre Aufgabe, dafür zu sorgen, dass die richtigen Sicherheitsrichtlinien implementiert werden und die richtige Benutzergruppe Zugang zu den Ressourcen erhält. Das Schreiben von Sicherheitsprogrammen für jede neue Anwendung und die Zuordnung bestimmter Zugangsebenen zu bestimmten Benutzern sind zeitaufwändige Aufgaben.

Geschäftliche Konsequenzen des Identitätsmanagement-Zyklus.

Der Identitätsmanagement-Zyklus besteht aus einer Reihe von Einzelschritten. In der Regel gehören zu jedem Einzelschritt manuelle Arbeitsgänge, mit denen das Unternehmen den gegebenen Sicherheitserfordernissen Rechnung trägt. Meist wird jeder Schritt von den verschiedenen Mitarbeitergruppen unterschiedlich gehandhabt – eine Tatsache, die zu Differenzen in der Auslegung und Umsetzung von Sicherheitsvorschriften führen kann.

Schritt 1: Bereitstellung und Verwaltung von Benutzerkennungen.

Der Zugang zu Ressourcen kann von Mitarbeitern, Kunden oder Partnern erbeten werden. Die IT-Administratoren definieren in Zusammenarbeit mit den Geschäftsbereichen Kategorien von Anwendern, die jeweils bestimmte IT-Ressourcen – Betriebssystemserver, Portale und Anwendungen – benutzen dürfen. Um jedem Anwender rasch Zugang zu den benötigten Ressourcen verschaffen

und ein produktives Arbeiten gewährleisten zu können, müssen die IT-Administratoren die Genehmigungs- und Bereitstellungsvorgänge unternehmensweit koordinieren und für die Einhaltung der Sicherheitsregeln des Unternehmens sorgen. Die Notwendigkeit, auf manuellem Wege Genehmigungen einzuholen, Ressourcen freizugeben und mehrere Benutzerkonten für jeden Anwender anzulegen, führt nicht selten dazu, dass neue Benutzer lange auf ihre Zugangsfreigabe warten müssen. Durch den Einsatz von Identitätsmanagement-Technologie lassen sich solche Verzögerungen wie auch die damit zusammenhängenden Administrationskosten erheblich reduzieren.

Typischer manueller Prozess

Anlegen einer Benutzer-Änderungsanforderung.

Prüfung der Benutzerrolle und der Richtlinien (im Kontext der Datenschutzvorschriften und der Benutzerpräferenzen).

Weiterleitung der Genehmigungsanforderung an die zuständige Stelle.

Administrator legt Benutzerkonten an, aktualisiert und löscht sie. Die Benutzerstammdaten mit Angabe der Gruppen- und Rollenzugehörigkeit wird erstellt.

Der Administrator gewährt, aktualisiert und widerruft Zugriffsrechte und verwaltet Vertraulichkeitspräferenzen. Er definiert, welche IT-Ressourcen für welchen Benutzer auf welcher Zugriffsebene zugänglich sind.

Bereitstellung der eigentlichen IT-Ressourcen für jeden Benutzer, wobei das Benutzerkonto (Stammdaten) die Zugriffsrechte ressourcenspezifisch vorgibt und diese nach Ressourcen gesondert verwaltet werden.

Vorteile eines automatischen Prozesses

Dank Benutzerselbstverwaltung können Anwender selbst rund um die Uhr Änderungsanforderungen generieren.

Rollenorientiertes Policy Management sorgt für konsistente Anwendung von Regeln und Vorschriften.

Workflow-Funktionalität beschleunigt Weiterleitung; bestimmte Genehmigungsverfahren können automatisch abgewickelt werden.

Ein einziger Administrationsvorgang für die automatische Erstellung, Aktualisierung und Löschung von Benutzerkonten.

Zugriffsrechte werden gemäß der Rolle des Benutzers und seinen persönlichen Vertraulichkeitspräferenzen automatisch erteilt.

Automatische Erstellung, Aktualisierung und Tilgung von Benutzerkonten und Vertraulichkeitspräferenzen für die einzelnen IT-Ressourcen.



Schritt 2: Benutzer greift auf die Ressourcen zu.

Ein weiterer erheblicher Kostenfaktor sind das Management und die Unterstützung berechtigter Ressourcennutzer. Zu diesem Aufgabenkreis gehören die Verwaltung mehrerer Benutzerkennungen pro Benutzer, die ressourcenübergreifende Kontrolle der Einhaltung von Sicherheitsregeln, die Gewährung des Zugriffs und die Umsetzung von Protokollierungsvorschriften. Sicherheitsregeln ändern sich selten nennenswert; dafür aber die Beziehungen zwischen Anwendern und den Regeln, beispielsweise dann, wenn ein Neukunde den Status eines Stammkunden zugewiesen bekommt. Solche Veränderungen müssen in der gesamten e-business Infrastruktur des Unternehmens berücksichtigt werden.

Bestehen für jeden Benutzer mehrere Benutzerkonten, kommt es entsprechend häufig zu Anfragen bezüglich vergessener Passwörter oder sonstiger administrativer Details. Nimmt man an, dass ein durchschnittlicher Anruf beim Support 20 EUR kostet und jeder Benutzer dreimal jährlich den Support anruft, entstehen hier beachtliche Kosten. Durch die Nutzung von Identitätsmanagement-Technologie kann auch hier die Anwenderproduktivität erheblich gesteigert und der Supportkostenaufwand entsprechend reduziert werden.

Typischer manueller bzw. anwendungsspezifischer Prozess

Der Benutzer muss sich bei jeder Ressource gesondert anmelden, meist mit unterschiedlichen Benutzerkennungen und Passwörtern.

Die Benutzerrolle, einschlägige Sicherheitsregeln, Datenschutzvorschriften und Vertraulichkeitspräferenzen werden anwendungsspezifisch abgefragt.

Benutzerzugriff wird anwendungsabhängig gewährt oder verweigert.

Zu Prüf- und Berichterstattungszwecken werden Protokolldateien gepflegt.

Vorteile eines automatischen Prozesses

Mit einem einzigen Anmeldeprozess, dem 'Single Sign-on', kann der Benutzer auf alle benötigten Ressourcen zugreifen. (Mit sog. 'Federated Identities' – der gemeinsamen Nutzung von Benutzerauthentifizierungsdaten und Benutzerattributen durch auf Vertrauensbasis kooperierende Web-Service-Anwendungen – ist auch eine unternehmensübergreifende Anmeldung bei Web-Services möglich.)

Zugangsanforderungen werden anhand der Benutzerpräferenzen sowie in Hinblick auf die geschäftliche Legitimität automatisch überprüft.

Der Zugang wird automatisch und konsistent für alle Ressourcen verwaltet, ohne dass Anwendungen modifiziert werden müssen.

Die Daten für Protokollierung und Berichterstattung werden automatisch generiert.

Schritt 3: Implementierung neuer Geschäftsinitiativen.

Nicht selten möchte ein Unternehmen neue Dienstleistungen anbieten oder neue Geschäftsinitiativen verwirklichen, um sich Wettbewerbsvorteile zu sichern und die Kundenloyalität zu fördern. In der Regel ist es die Aufgabe der Anwendungsentwickler des jeweiligen Unternehmensbereiches, neue Dienste zu erstellen und die jeweiligen Zugangsebenen für Benutzer durch Anlegen eines Sicherheitsmodells für die betreffende Anwendung bzw. das Portal umzusetzen. In vielen Fällen werden dabei Benutzerlisten und Zugriffsrechte neu angelegt, die bereits an anderer Stelle existieren. Dies bringt zusätzliche betriebswirtschaftliche Probleme mit sich: höhere Kosten der Anwendungsentwicklung, längere Implementierungszyklen und höhere Gesamtkosten (Total Cost of Ownership, TCO).

Darüber hinaus bergen diese Effizienzmängel auch Sicherheitsrisiken. Werden Sicherheitsregeln innerhalb eines Unternehmens von verschiedenen Personengruppen manuell implementiert, ergeben sich fast zwangsläufig Diskrepanzen zwischen den einzelnen Anwendungen, Portalen und Servern sowie Lücken in der Regulierung. So kann es beispielsweise mehrere Tage dauern, bis die Zugriffsrechte eines ausgeschiedenen Mitarbeiters aus allen Systemen, Ressourcen und Anwendungen gelöscht worden sind. Bestimmte Aspekte des Identitätsmanagements senken den Aufwand der Anwendungsentwicklung und beschleunigen die Implementierung.



Typischer manueller Prozess

Entwicklung anwendungsspezifischer Geschäftslogik.

Entwicklung der Security-Funktionalität für die neue Initiative.

Test und Implementierung der neuen Initiative.

Erstellen gesonderter Geschäftsprozesse für Genehmigungsverfahren.

Bereitstellung des Benutzerzugangs zur neuen Initiative.

Vorteile eines automatischen Prozesses

Entwicklung anwendungsspezifischer Geschäftslogik ohne Security-Funktionalität.

Nutzung der vorhandenen Sicherheits- und Vertraulichkeitsinfrastruktur; eine gesonderte Programmierung von Sicherheitsfunktionen für jede Initiative ist unnötig.

Die Konsistenz der Security-Implementierung wurde bereits getestet.

Workflow-Integration in vorhandene Systeme beschleunigt Genehmigungsverfahren und beseitigt Redundanzen.

Automatische Zugangsbereitstellung in Abhängigkeit von der definierten Benutzerrolle.

Integriertes Identitätsmanagement.

Viele Softwareprodukte zielen nur auf einzelne Aspekte des Identitätsmanagements bzw. auf die Optimierung eines einzelnen manuellen Prozesses ab. Wer eine Identitätsmanagement-Lösung implementieren will, sollte bereits bei der Planung bedenken, wie sich die einzelnen Identitätsmanagement-Funktionen in das Gesamtsystem einfügen, und welches Wertschöpfungspotenzial die Integration dieser Funktionen birgt. Das nachstehende Schema illustriert die verschiedenen Funktionsbereiche einer Identitätsmanagement-Lösung.

Bei der Entwicklung eines umfassenden Identitätsmanagement-Plans empfiehlt es sich, diese Funktionsbereiche bestimmten Ebenen zuzuordnen. Ein Identitätsmanagement-Schema besteht aus den vier Ebenen Identity Federation*, Identity Lifecycle Management, Identity Control und Identity Foundation. Je höher die Ebene, desto größer das Wertschöpfungspotenzial für das Unternehmen. Um einen optimalen Return-on-Investment zu erzielen, sollte eine Identitätsmanagement-Lösung implementiert werden, die alle diese Ebenen und Funktionsbereiche integriert.



* Die gemeinsame Nutzung von Benutzerauthentifizierungs- und Benutzerattributinformationen durch mehrere Web-Service-Anwendungen.

Identitätsmanagement-Schema

Identity Federation

- *Unternehmensübergreifende Bereitstellung der Benutzerkennungen*
- *Trustbrokering*
- *Unternehmensübergreifende Identitätszuordnung*

Identity Lifecycle Management

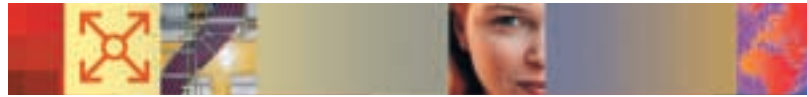
- *Benutzerregistrierung u. Kennungsdatenbereitstellung*
- *Benutzerprofil-Management*
- *Benutzerselbstverwaltung*
- *Verwaltung von Authentizitätsnachweisen*
- *Verwaltung von Benutzer-Vertraulichkeitspräferenzen*
- *Policy Management*

Identity Control

- *Zugriffssteuerung und Single Sign-on für Anwendungen und Middleware*
- *Zugriffssteuerung für persönliche Daten*
- *Überwachung und Protokollierung von Benutzeraktivitäten*

Identity Foundation

- *Verzeichnisse und Metaverzeichnis*
- *Berichterstattung*
- *Workflow*
- *Web-Technologie*



Die Ebene 'Identity Foundation'.

Diese Ebene definiert die technischen Komponenten, die für den Aufbau von in die e-business Infrastruktur integrierten Lösungen benötigt werden. Dies sind folgende Hauptkomponenten:

- *Verzeichnis-Infrastruktur – eine offene, standardkonforme Verzeichnis-Infrastruktur ermöglicht die Anbindung eines beliebigen Benutzerverzeichnisses und die Konsolidierung von Daten aus mehreren Verzeichnissen.*
- *Metaverzeichnisfunktion – zuständig für die 'Übersetzung' und Distribution von Daten zwischen Endpunkt-Repositoryen.*
- *Workflow – Automatisierung der Anforderungsverarbeitung und Anbindung an vorhandene Geschäftssysteme.*
- *Berichterstattung – Berichte über dienstrelevante Ereignisse, Prüfprotokollberichte, Leistungsberichte und Benutzerdatenberichte.*
- *Web-Technologie – vereinfacht Interaktion zwischen Komponenten und durch Firewalls hindurch unter Verwendung von Standardprotokollen wie SSL, XML, HTTPS, LDAP und Web Services.*

Die Ebene 'Identity Control'.

Zu dieser Ebene gehören Dienste, die die unternehmensweite Umsetzung der Zugangs- und Vertraulichkeitsvorschriften verwalten und kontrollieren. Zwei für e-business besonders wichtige technische Komponenten sind die Unterstützung für weitgehend alle Formen der Benutzerauthentifizierung sowie die Steuerung des Zugriffs auf alle oder fast alle Arten von Ressourcen durch authentifizierte Benutzer.

- *Zugriffssteuerung und Single Sign-on für Anwendungen und Middleware – unterstützt werden Dienste wie Web Single Sign-on, verteilte internetgestützte Administration, zentrale Autorisierung und Schutz von Anwendungs- und Betriebssystem-Ressourcen.*

- *Zugriffssteuerung für persönliche Daten – Wahrung des Kundenvertrauens und der Markenintegrität durch Datenschutz und Einhaltung der fünf Schritte des Vertraulichkeitsmanagements.*
- *Überwachung und Protokollierung der Benutzeraktivitäten – Echtzeitüberwachung von Ereignissen zur Erkennung möglicher Missbräuche und Angriffe.*

Die Ebene 'Identity Lifecycle Management'.

Auf dieser Ebene geht es um die Vereinfachung der benutzerseitigen Handhabung, die Bereitstellung von Benutzeridentitätsdaten und die Verwaltung von Zugriffsregeln über Altsysteme sowie über e-business Anwendungen und -systeme hinweg.

- *Benutzerregistrierung und Bereitstellung der Benutzerkennungen – Verwaltung der Benutzerkennendaten von der Erstellung bis zur endgültigen Konfiguration in den Zielressourcen; Automatisierung der Validierung; Genehmigung und Erstellung von Benutzerdaten auf der Grundlage von unternehmensinternen Vorschriften.*
- *Benutzerselbstverwaltung – verringert die Kosten der Verwaltung von Benutzer-Anforderungen und verbessert den Service für Benutzer.*
- *Verwaltung von Benutzer-Vertraulichkeitspräferenzen – Verwaltung von Benutzerdaten, die Rückschlüsse auf die Identität des Benutzers erlauben, sowie von Präferenzen des Benutzers laut Vertraulichkeitsvereinbarung.*
- *Verwaltung der Benutzerprofile – Verwaltung der Attribute, die zur Definition von Benutzern dienen.*
- *Verwaltung von Authentizitätsnachweisen – jedes Benutzerprofil enthält Informationen über Authentizitätsnachweise, die dem Benutzer die Anmeldung bei bestimmten Ressourcen gestatten.*
- *Policy Management – Verwaltung der Benutzer-Zugriffsrechte und der Regeln für den Ressourcenzugriff.*



Die Ebene 'Identity Federation'.

Auf dieser Ebene findet der Austausch von Identitätsinformationen zwischen kooperierenden Unternehmen statt, der eine gemeinsame Nutzung von Authentifizierungsdaten und -attributen durch Web-Service-Anwendungen auf Vertrauensbasis ermöglicht.

- *Unternehmensübergreifende Bereitstellung oder Benutzerkennungen – automatische Anerkennung der Anmeldung von Benutzern anderer Unternehmen und Gewährung des Zugangs zu Standarddiensten.*
- *Unternehmensübergreifende Identitätszuordnung – Erstellung und Management der 'Übersetzung' von Authentizitätsnachweisen und Kennungen im unternehmensübergreifenden Austausch; Benutzertypen sind 'Anonym' und 'Nicht-Anonym'.*
- *Trustbrokering – Handhabung der Laufzeitmerkmale, die einen sicheren, zuverlässigen Benutzerdatenaustausch zwischen zwei Unternehmen ermöglichen.*

Die Funktionen dieser Ebenen leisten auch einen Beitrag zur Umsetzung des 'Autonomic Computing'-Konzepts. Auf der Ebene 'Identity Foundation' ermöglicht die Kombination von Metaverzeichnis und Berichterstattung die Erkennung von Ereignissen und Veränderungen innerhalb der Umgebung und deren automatische Meldung nach Maßgabe der im Workflow definierten Geschäftsregeln. Auf der Ebene 'Identity Control' kann die automatische Durchsetzung von Zugriffs- und Vertraulichkeitsregeln anhand von Überwachungsfunktionen stattfinden, die das Benutzerverhalten



erfassen. Auf der Ebene 'Identity Lifecycle Management' entsteht ein geschlossener Regelkreis im Sinne des Autonomic Computing durch die Kombination der dynamischen Bereitstellung von Benutzerkennungen, der Benutzerselbstverwaltung und des automatischen Abgleichs von Identitätsprofiländerungen zwischen lokalen Systemen und Anwendungen einerseits und der zentralen Administration andererseits.

Eine sich selbst schützende Umgebung hat das Ziel, zu einer bestimmten Zeit an bestimmte Benutzer je nach deren Rolle und den geltenden Regeln spezifische Informationen bereitzustellen. Eine zum Selbstschutz fähige IT-Umgebung erkennt feindselige Verhaltensmuster und unbefugtes Eindringen (Intrusion) unmittelbar und trifft autonom Maßnahmen zum Schutz vor unbefugten Zu- und Eingriffen, Viren- und Denial-of-Service-Angriffen. Selbstschutzfunktionen schaffen die Voraussetzungen für eine konsequente Umsetzung von Sicherheits- und Datenschutzregeln; sie tragen zur Senkung der Administrationskosten im Security-Bereich bei, und sie steigern letztlich die Mitarbeiterproduktivität und die Kundenzufriedenheit.



Kriterien zur Wahl des Identitätsmanagement-Anbieters.

Die Wahl einer Security-Lösung mit hoch integrierten Funktionen ist außerordentlich wichtig. Bei der Auswahl einer Identitätsmanagement-Lösung für Ihr Unternehmen spielen auch Kriterien eine Rolle, die über rein technologische Erwägungen hinausgehen, so zum Beispiel die Qualität der Kundenbetreuung des Anbieters, seine globale Präsenz und der Grad der Integration, den die Lösung bietet. Entscheidende Auswahlkriterien sind:

- *Entspricht das Security-Konzept des Anbieters Ihrem eigenen?*
- *Unterstützt die Technologie des Anbieters Ihre geschäftlichen Ziele?*
- *Ist das Angebot eine Komplett- oder eine Teillösung?*
- *Berechnet der Anbieter jede Komponente bzw. jedes Produkt gesondert (z. B. wird Workflow-Funktionalität als Zusatzoption verkauft?) oder handelt es sich um ein Komplettangebot mit einem eindeutigen Endpreis?*
- *Sind die Produkte des Anbieters so weitgehend integriert, dass ein nahtloses Ineinandergreifen der Funktionsbereiche gewährleistet ist?*
- *Wie gut ist die Kundenbetreuung des Anbieters?*
- *Wie gut ist der Anbieter weltweit vertreten?*
- *Wie sehen Sie die Stabilität und langfristige Marktpräsenz des Anbieters im heutigen wirtschaftlichen Umfeld?*
- *Kann der Anbieter Produkte liefern, die strategisch konzipiert und technisch ausgereift sind?*
- *Unterstützt der Anbieter offene Standards?*

Die Identitätsmanagement-Lösung von IBM.

IBM bietet eine der sehr wenigen integrierten Identitätsmanagement-Lösungen an, die die Funktionsbereiche Benutzermanagement, Bereitstellung von Benutzerkennungen, Zugriffssteuerung und Vertraulichkeitsmanagement umfassen. Die Identitätsmanagement-Lösung von IBM hilft Ihrem Unternehmen, folgende Ziele zu erreichen:

- *Rasche Online-Einsatzbereitschaft und Produktivität von Benutzern, Systemen und Anwendungen*
- *Geringere Kosten dank Merkmalen wie zentralisiertes Management, delegierte Administration und Benutzerselbstverwaltung*
- *Optimale Investitionserträge durch Anbindung an vorhandene Geschäftsanwendungen und rasche Implementierung neuer Geschäftsinitiativen*

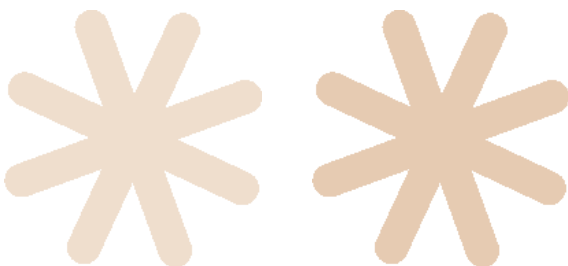
Die Identitätsmanagement-Lösung setzt sich aus drei integrierten Security-Produkten zusammen: IBM Tivoli Identity Manager, IBM Tivoli Access Manager for e-business und IBM Tivoli Privacy Manager for e-business.

Die IBM Tivoli Security-Lösung ermöglicht zudem die konsistente, automatische Umsetzung von Zugriffssteuerungs- und Vertraulichkeitsregeln, trägt zur Senkung der Kosten der Sicherheitsadministration bei und verhilft Ihrem Unternehmen durch die Vorteile einer umfassenden, integrierten Lösung zu produktiveren Mitarbeitern und zufriedeneren Kunden.

Diese integrierte Lösung zeichnet sich außerdem durch folgende wichtige Merkmale aus:

- *Sie verwirklicht die fünf Schritte des Vertraulichkeitsmanagements: Definition von Vertraulichkeitsregeln, Implementierung der Vertraulichkeitsregeln, Erfassung der Benutzerzustimmung zu den Regeln, Überwachung des Zugriffs und Umsetzung der Zugriffsregeln sowie Generierung von revisionssicheren Zugriffsprotokollberichten.*
- *Bildung einer sich selbst schützenden Umgebung durch:*
 - *Verhinderung unbefugter Zugriffe durch einen einzigen, zentralen Security-Policy-Server zur Durchsetzung eines Sicherheits-Managements, das verschiedene Dateitypen, Anwendungsserver, Geräte und Protokolle umfasst*
 - *Passwort- und Benutzer-Integrität durch Web Single Sign-on*
 - *Robuste Protokollierungs- und Informationserfassungstools zur Erkennung potenzieller und bereits eingetretener Probleme*
- *Bildung einer sich selbst optimierenden Umgebung durch:*
 - *Load-Balancing und automatische Abbildung von Web Object Spaces*
 - *Hoch verfügbare und skalierbare, auf offenen Standards beruhende Architektur*
- *Automatisierung des Workflow und der Administration der Benutzerdaten durch leistungsfähige Benutzermanagement-Funktionen*

Die IBM Security-Lösung unterstützt offene Standards – ein Faktor, der die Implementierung beschleunigen und die Kosten reduzieren kann. Darüber hinaus ist die Anbindung an weitere IBM Kerntechnologien gewährleistet, beispielsweise an IBM WebSphere Application Server, WebSphere MQ, IBM Directory Server und Lotus Domino. Die Sicherheitsinfrastruktur kann UNIX®- und Linux-Umgebungen einbeziehen.



Fazit.

Die Verwaltung von Benutzeridentitätsdaten während ihres gesamten Nutzungszyklus ist häufig ein kritischer Faktor für den wirtschaftlichen Erfolg eines Unternehmens. Mit der exponentiellen Zunahme der Benutzer gewinnt sie noch an Bedeutung. Das Identitätsmanagement hat Auswirkungen auf Benutzer, Administratoren und Entwickler. Bisher werden die zahlreichen Verwaltungsaufgaben während des Identitätsmanagement-Zyklus in der Regel manuell ausgeführt. Da oft jeder Schritt von den verschiedenen Mitarbeitergruppen eines Unternehmens unterschiedlich gehandhabt wird, sind Differenzen in der Auslegung und Umsetzung von Sicherheitsvorschriften keine Seltenheit.

Herausforderungen im Zusammenhang mit dem Identitätsmanagement können weitreichende betriebswirtschaftliche Auswirkungen haben. Manuelle Prozesse sind häufig die Ursache hoher Benutzeradministrations- und Bereitstellungskosten, ganz zu schweigen von den Sicherheits- und Ausfallrisiken. Die Nichtbeachtung von Vertraulichkeitspräferenzen der Benutzer kann das Markenimage und das Vertrauen der Kunden beeinträchtigen und die Wettbewerbsposition des Unternehmens in Mitleidenschaft ziehen.

Unternehmen, die eine Identitätsmanagement-Lösung implementieren möchten, sollten nach einer integrierten Lösung Ausschau halten, die eine rasche Wertschöpfung sowie Wettbewerbsvorteile durch gesteigerte Kosteneffizienz und eine frühere Marktreifung neuer Initiativen erwarten lässt. Eine solche Lösung verspricht eine positive Wirkung auf die Kundenzufriedenheit und verschafft dem Unternehmen ein hohes Maß an Sicherheit.

Weitere Informationen.

Weitere Informationen zu IBM Identitätsmanagement-Lösungen und integrierten Lösungen von IBM erhalten Sie von Ihrem IBM Vertriebsbeauftragten oder im Internet unter:

ibm.com/de/software/sysmgmt

ibm.com/tivoli





IBM Deutschland GmbH
70548 Stuttgart
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Bändliweg 21, Postfach
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:

ibm.com

ibm.com/de/software/sysmgmt

ibm.com/tivoli

IBM, das IBM Logo, das e-Logo, Tivoli, Lotus, Domino und WebSphere sind Marken oder eingetragene Marken der International Business Machines Corporation in den USA und/oder anderen Ländern.

UNIX ist eine Marke von The Open Group in den USA und anderen Ländern.

Marken anderer Unternehmen/Hersteller werden anerkannt.

© Copyright IBM Corporation 2003
Alle Rechte vorbehalten.