



**Setzen Sie die richtigen Sicherheitsprioritäten durch Auswahl der richtigen Identitätsmanagementlösung.**



## **Ihr Unternehmen hat Bedarf an Identitätsmanagement – was jetzt?**

Bei Unternehmen jeder Größe und Branche wächst das Bewusstsein, dass die Komplexität der IT-Sicherheitsanforderungen von heute eine zuverlässige Lösung notwendig macht. Eine Lösung, die die immer größer werdende Vielfalt an Benutzern, die Zugriff auf Ihre IT-Ressourcen benötigen, handhaben kann. Eine Lösung, die es Ihrem Unternehmen ermöglicht, Vorschriften und Audit-Anforderungen einzuhalten. Eine, die mehr Leistung bringt und dabei noch Kosten senkt.

Hier lautet die Lösung: Identitätsmanagement. Beim Identitätsmanagement kann auf Grund eines zentralisierten Kontrollverfahrens im gesamten Unternehmen die konsistente Umsetzung von Sicherheitsrichtlinien sichergestellt werden. Dabei wird in einem dezentralen Verfahren die Administration erleichtert. Eine gute Identitätsmanagementlösung überträgt den richtigen Personen bzw. Gruppen das richtige Maß an Verantwortung – unabhängig von deren Standort.

Die Entscheidung für Identitätsmanagement ist eine Sache. Aber herauszufinden, welche Identitätsmanagementlösung für Ihr Unternehmen die richtige ist, ist eine andere Sache. Es ist nicht einfach zu entscheiden, in welche Software als Erstes investiert werden soll und welcher Lieferant auf dem jeweils gewünschten Gebiet der beste ist – hier ist die richtige Wahl ein Lieferant, der Sie während des gesamten Prozesses der Implementierung Ihrer kompletten Lösung unterstützen kann.

### **Mit Unterstützung den richtigen Einstieg finden**

Indem Sie das Sicherheitsrisiko lokalisieren, dem Ihre Unternehmensprioritäten am meisten ausgesetzt sind, können Sie sich zunächst auf die Sicherheitslösungstypen konzentrieren, die sie vor genau diesen Risiken schützen. Im Laufe der Zeit können Sie dann Schritt für Schritt auch die anderen für Ihre Unternehmensziele relevanten Sicherheitsaspekte in Angriff nehmen.

Dieses Dokument soll Ihnen helfen, den Einstieg zu finden. Es beschreibt die Anforderungen, auf Grund derer sich Unternehmen am häufigsten für eine Investition in Identitätsmanagement entscheiden, und zeigt dann auf, welche Komponenten auf welche Anforderungen zugeschnitten sind. Das Dokument bietet für jede Komponente eine Bewertungsbasis, anhand derer ermittelt werden kann, ob die Lösungen des jeweiligen Lieferanten zuverlässig genug sind. Mit Hilfe dieses Leitfadens für Kunden können Sie zudem analysieren, ob Ihnen ein Lieferant die Unterstützung bieten kann, die sie benötigen, wenn Sie weitere Bereiche des Identitätsmanagements realisieren möchten.

## **Das Gesamtziel: mehr Benutzer und mehr Sicherheitsregeln zu geringeren Kosten verwalten**

Ein On Demand Unternehmen zu werden heißt, mehr Benutzern besseren Zugriff auf Ihre IT-Systeme einzuräumen. Ihre IT-Mitarbeiter müssen nicht nur den Zugriff Ihrer Mitarbeiter, sondern auch Ihrer Kunden, Ihrer Geschäftspartner und selbst unbekannter Benutzer an ungesicherten Standorten, die auf öffentliche Websites Ihres Unternehmens zugreifen, abwickeln. Und dabei geht es nicht einfach darum, jedem einzelnen Benutzer bestimmte Berechtigungen zuzuweisen. Sie müssen flexibel genug sein, Berechtigungen genauso häufig anpassen zu können, wie sich beispielsweise der Tätigkeitsbereich eines Mitarbeiters ändert.

Die Bewältigung dieses hohen Maßes an Komplexität stellt eine beträchtliche Herausforderung dar. Dies wird durch die wachsende Anzahl an Vorschriften und Audit-Anforderungen, die Sie einhalten müssen, weiter erschwert. Darüber hinaus wird die Situation noch zusätzlich durch Vorgaben zur Senkung der IT-Kosten kompliziert, die auch die IT-Konsolidierung und -Optimierung, das Outsourcing von Aufwänden, das Anbieten von mehr Kunden-Self-Service und das Automatisieren von immer mehr IT-Tasks beinhalten.

### **Diese Herausforderungen durch Implementieren von Identitätsmanagementlösungen meistern**

Unternehmen setzen Identitätsmanagementlösungen in zunehmendem Maße ein, da diese die gesamte Palette der sich heutzutage stellenden Sicherheitsanforderungen abdecken können. Das Identitätsmanagement befasst sich im Kern mit zwei Schlüsselfragen: wer sind Sie und worauf haben Sie Zugriff? Es unterstützt Sie dabei – orientiert an Ihren Geschäftsanforderungen -, der steigenden Anzahl von Benutzern Zugriff zu gewähren, die mit Ihrem IT-System in Kontakt kommen. Und dies geschieht auf eine nicht nur kosteneffiziente Weise, sondern gewährleistet auch hohe Erträge aus Investitionen.

Das Identitätsmanagement beinhaltet Funktionen für die folgenden drei Hauptbereiche:

- *Unternehmensübergreifende Synchronisierung von Identitätsdaten*
- *Verknüpfung von Benutzerkonten mit diesen Identitätsinformationen*
- *Regelbasierte Zugriffsgewährung, die Ihren Unternehmensprioritäten und -richtlinien entspricht und die den Zugriff Unbefugter auf vertrauliche und sensible Informationen verhindert*



Durch Einrichtung einer zuverlässigen Quelle für Identitätsinformationen, effiziente Handhabung von Änderungen an Informationen sowie zugehörigen Berechtigungen und effiziente Implementierung Ihrer Sicherheitsrichtlinien schaffen Sie die notwendige Basis für Zugriffsentscheidungen, Self-Service- sowie Autorisierungs- und Personalisierungsfunktionen.

Der gesamte Identitätsmanagementzyklus umfasst alle drei dieser Bereiche – wobei sie optimal aufeinander abgestimmt sind. Das heißt beispielsweise, je autoritativer Ihre Datenspeicher sind, desto sicherer können Sie sein, dass Ihre Sicherheitsrichtlinien richtig umgesetzt werden. Und durch das Einrichten von Benutzerkonten mit Vertraulichkeitseinstellungen können Sie besser gewährleisten, dass vertrauliche Informationen in Übereinstimmung mit den Wünschen des einzelnen Benutzers geschützt bleiben oder freigegeben werden.

### **Drei Ansatzpunkte für den Einstieg in das Identitätsmanagement**

Der Einstieg in die Implementierung einer Identitätsmanagementlösung und die letztendliche Realisierung der vollständigen Kontrolle über den gesamten Identitätsmanagementzyklus kann über jede der folgenden drei Hauptkategorien des Identitätsmanagements erfolgen. Sie können den Anfang machen durch:

- *Einrichtung eines autoritativen Identitätsinformationsspeichers*
- *Prüfung der Informationen über Benutzer und deren Berechtigungen oder*
- *Funktionen zur Zugriffssteuerung und kontrollierten Freigabe von Daten.*

Um den idealen Einstiegspunkt für Ihr Unternehmen zu finden, hilft es zu verstehen, was jede dieser Kategorien genau beinhaltet. Auf diese Weise können Sie ein besseres Verständnis dafür entwickeln, wie Sie mit Ihrer ersten Investition in das Identitätsmanagement den Grundstein für die Implementierung einer umfassenden Identitätsmanagementlösung legen.

- **Identitätsdaten festlegen – Benutzeridentitäten erfassen, speichern und schützen durch:**
  - *die Nutzung eines LDAP-Verzeichnisses (LDAP – Lightweight Directory Access Protocol)*
  - *die datenspeicherübergreifende Synchronisierung von Identitätsdaten, wobei jeder Datenspeicher eine Reihe von autoritativen Informationen enthält*
  - *die Möglichkeit, dass die verschiedenen Abteilungen Eigner bestimmter Benutzerdaten bleiben*
  - *Gewährleistung einer hohen Verfügbarkeit und Skalierbarkeit*

- **Benutzermanagement und Ressourcenbereitstellung (Provisioning) – Identitätsänderungen und Ressourcenzugriffsregeln durch die Bereitstellung folgender Möglichkeiten steuern :**
  - *Benutzerregistrierung und Konteneinrichtung*
  - *Benutzerselbstverwaltung (einschließlich Passwortverwaltung und Aktualisierung persönlicher Informationen)*
  - *Verwaltung von Vertraulichkeitspräferenzen der Benutzer*
  - *Benutzerprofilverwaltung*
  - *Berechtigungsverwaltung*
  - *Richtlinienverwaltung*
- **Zugriffssteuerung – Verwenden Sie Identitäten für folgende Zwecke:**
  - *Steuerung des Zugriffs auf Anwendungen, Webservices und Middleware*
  - *Implementierung einer differenzierteren Zugriffssteuerung auf UNIX® und Linux-Systemressourcen*
  - *Verwaltung der Freigabe privater und persönlicher Daten*
  - *Überwachung und Prüfung von Benutzeraktivitäten*
  - *Bereitstellung des Single-Sign-On-Verfahrens*
  - *Unterstützung integrierter und dezentraler Implementierungen*

Der folgende Abschnitt hilft Ihnen zu ermitteln, welcher dieser drei Einstiegspunkte – Festlegung von Identitätsdaten, Benutzermanagement und -Provisioning oder Zugriffssteuerung – Ihren Unternehmensanforderungen am besten gerecht wird.

### **Beginnen Sie beim Einstieg in das Identitätsmanagement mit den dringendsten Sicherheitsanforderungen**

Durch eigene Forschungen und in Zusammenarbeit mit vielen Kunden jeglicher Unternehmensgröße und Branche gesammelten Erfahrungen, konnte IBM acht Anforderungen definieren, auf Grund derer sich Unternehmen primär für die Implementierung von Identitätsmanagementlösungen entscheiden. Jeder dieser acht Anforderungen steht mindestens eine – manchmal auch mehrere – der drei Identitätsmanagementarten als mögliche Lösung gegenüber. Eine Liste mit den Anforderungen und jeweils geeigneten Einstiegspunkten finden Sie auf der nächsten Seite.

Welche dieser Anforderungen ist die für Ihre Unternehmensprioritäten relevanteste? Indem Sie ermitteln, welche Anforderung bzw. Anforderungen für Ihr Unternehmen am bedeutendsten sind, können Sie bestimmen, in welchen Bereich des Identitätsmanagements Ihr Unternehmen zuerst investieren sollte.



Anforderungen des Unternehmens:	Geeigneter Einstiegspunkt:
Kosten für Verwaltung und Unterstützung von Sicherheitsfunktionen senken	Benutzermanagement und -Provisioning
Implementierung des Single-Sign-On und einer einheitlichen Benutzerschnittstelle	Zugriffsteuerung
Senkung der Kosten für die Entwicklung adäquater Sicherheitskonzepte für branchenführende und intern erstellte Anwendungen	Zugriffsteuerung
Steuerung der Freigabe sensibler, persönlicher Daten	Privacy-Management
Einhaltung von Vorschriften und Audit-Anforderungen in einer heterogenen Umgebung (einschließlich UNIX und Linux)	Benutzermanagement und -Provisioning, Zugriffssteuerung mit Privacy-Management
Protokollierung aller Benutzer, die auf die Systeme zugreifen	Benutzermanagement und -Provisioning, Zugriffssteuerung
Verwaltung von auf mehreren Speichern verteilten Identitätsinformationen	Festlegung von Identitätsdaten
Ausbau der Sicherheit für die Implementierung von Portalen und Webservices	Zugriffssteuerung, Benutzermanagement und -Provisioning

Der folgende Abschnitt zeigt, dass es nicht nur wichtig ist, den geeigneten Einstiegspunkt zu bestimmen, sondern auch zu bedenken, wie Sie Ihre sicherheitsspezifischen Gesamtziele erreichen wollen. Der nachfolgende Teil dieses Leitfadens für Kunden soll Ihnen eine Hilfestellung bei der Auswahl des besten Anbieters für den von Ihnen bevorzugten Einstiegspunkt geben – eines Lieferanten mit dem Sie auch dann den Erfolgskurs Ihres Unternehmens beibehalten können, wenn Sie zu einem späteren Zeitpunkt weitere Sicherheitsanforderungen umsetzen möchten.


**Wählen Sie eine Lösung – und einen Lösungsanbieter – der Ihre langfristigen Sicherheitsbedürfnisse erfüllen kann**

Infolge der Komplexität der heutigen Sicherheitsanforderungen entscheiden sich die meisten Unternehmen dafür, eine Gesamtarchitektur einzurichten und diese dann schrittweise zu implementieren. Jedes Unternehmen geht taktisch vor und implementiert eine Lösung in einem Bereich. Aber Unternehmen, die den Überblick darüber verlieren, wie sich die ursprüngliche Lösung in das Gesamtsicherheitskonzept des Unternehmens einfügen sollte, laufen Gefahr, dass sich die Investition nur als Übergangslösung entpuppt – und ein langfristiges Return-on-Investment damit ausgeschlossen bleibt.

Lesen Sie hier, wie Sie Ihre langfristig ausgelegte Lösung bereits beim Einstieg in das Identitätsmanagement strategisch planen:

- *Möglicherweise kristallisieren sich mehrere der in diesem Dokument aufgeführten Identitätsmanagementkomponenten als Möglichkeiten heraus. Wählen Sie jedoch einen Lösungsanbieter, der Sie durch den gesamten Prozess begleiten kann.*
- *Die kosteneffektivsten Lösungen arbeiten mit Komponenten, die sich in Ihrem gesamten IT-System wieder verwenden lassen. Wählen Sie Lösungen mit einer End-to-End-Funktionalität.*
- *Neue Komponenten sollten sich leicht in bereits bestehende integrieren lassen. Vermeiden Sie Lösungen, die unweigerlich in doppelten Funktionen, mehreren Lernkurven und komplexen Integrationen münden werden.*

Egal welcher Einstiegspunkt in das Identitätsmanagement für Ihr Unternehmen der geeignetste ist, ist es von größter Wichtigkeit, einen Anbieter auszuwählen, der Ihnen bei der Implementierung von Identitätsmanagementlösungen als langfristiger Partner zur Seite stehen kann.



In den folgenden Abschnitten bietet dieser Leitfaden für jeden der Einstiegspunkte Checklisten, mit deren Hilfe Sie Lieferanten und ihre Produkte bewerten können. Beachten Sie bei der Auswahl einer Lösung, die sich für ihre bevorzugte Anforderung am besten eignet, dass ein Anbieter die gesamte Bandbreite Ihrer Identitätsmanagementlösung unterstützen kann.

### **Implementieren Sie eine Lösung zur Festlegung von Identitätsdaten, bei der Benutzerinformationen zu wertvollen Unternehmensressourcen werden**

Mit der zunehmenden Anzahl von Benutzern, die Zugriff auf Ihre Systeme benötigen, wächst auch die Anzahl der Speicherplätze an denen Informationen zu diesen Benutzern abgelegt sind. So ist in Ihrer Personalabteilung möglicherweise ein aktueller Bestand an Mitarbeiterdaten erfasst. Ihre Vertriebsmitarbeiter wiederum sammeln möglicherweise maßgebliche Informationen über potenzielle Kunden. Und in anderen Datenbanken könnten sich aktuelle Informationen über Kunden und Geschäftspartner befinden.

Um ein Sicherheitskonzept konsistent im gesamten Unternehmen umsetzen zu können, müssen Sie eine hocheffiziente Möglichkeit zur Synchronisierung dieser Benutzerinformationen finden. Wenn sich der Name eines Mitarbeiters ändert, sollte diese Änderung sowohl in der Datenbank der Personalabteilung als auch in allen anderen Datenbanken, die Ihren Kunden Informationen über Ihr Unternehmen bereitstellen, einfließen. Wenn ein potenzieller Kunde oder Geschäftspartner zu einem aktiven Kunden wird, sollte diese Statusänderung gleichzeitig in allen Informationsspeichern registriert werden.

Eine Identitätsintegrationslösung synchronisiert Daten unternehmensweit. Sie ermöglicht es Ihnen alle Daten immer auf dem aktuellsten Stand zu halten und dabei gleichzeitig die Kosten für ein manuelles Aktualisieren der Daten zu senken. Mit einer guten Identitätsintegrationslösung können Sie Regeln festlegen, die vorgeben, welche Gruppen und Einzelpersonen zum Ändern welcher Datenfelder berechtigt sind. Die Lösung sorgt dann dafür, dass die von autorisierten Personen vorgenommenen Änderungen auch in alle anderen Datenbanken einfließen, die dieselben Daten enthalten und nutzen.

Einige der primären Vorzüge der Identitätsintegration:

- *Speicherübergreifende Synchronisierung von Daten*
- *Reduzierung der Anzahl von Personen, die mit der Pflege derselben Daten beschäftigt sind*
- *Möglichkeit der Migration von Daten in neue Anwendungen*

Das heißt, mithilfe der Identitätsintegration lassen sich die Kosten für den Aufbau eines autoritativen Informationsspeichers senken. Durch Verwendung dieses Speichers ermöglichen Sie es den Mitarbeitern Ihres Unternehmens maximalen Nutzen aus Ihren Systemen zu ziehen und Ihren Kunden und Partnern exzellenten Service zu bieten.

Eine gute Identitätsintegrationslösung sollte die folgenden Kriterien erfüllen:

- *Arbeitet mit einer dezentralen Architektur, damit lokale Gruppen die Daten, mit denen Sie am meisten vertraut sind, mit den Tools verwalten können, mit denen Sie am produktivsten sind*
- *Stellt eine Anbindung an Datenspeicher in Ihrem Unternehmen bereit*
- *Kann auf vordefinierte Ereignisse reagieren und ermöglicht damit die automatisierte Aktualisierung Ihrer Identitätsspeicher in Echtzeit*
- *Kann rasch implementiert werden und bei einer Erweiterung besteht nur eine minimale Abhängigkeit von zentralen Datenspeichern*
- *Stellt eine zentrale „Metaansicht“ aller derjenigen Verzeichnisse bzw. Datenbanken bereit, die Ihren Anforderungen am besten gerecht werden – ohne sich auf die proprietären Datenspeicher eines bestimmten Lieferanten festlegen lassen zu müssen*
- *Kann auf jeder beliebigen Betriebssystemplattform eingesetzt werden und damit maximale Flexibilität ermöglichen*
- *Nutzt wieder verwendbare Anbindungen und Komponenten*
- *Erlaubt die Integration einer großen Vielfalt an Datentypen, inklusive Kennwortdaten*

### **Implementieren Sie bei globalen Unternehmensanwendungen eine Verzeichnisinfrastruktur, die rund um die Uhr Hochleistung verspricht**

Um umfassende Identitätsmanagementlösungen einsetzen zu können, muss Ihre Infrastruktur Identitätsdaten für eine wachsende Anzahl von Anwendungen mit Verzeichnisunterstützung handhaben können. Dies ist mit der Infrastruktur einer stark genutzten Autobahn vergleichbar. Je umfangreicher und zuverlässiger das Strassennetzwerk ist, desto höher ist die Wertschöpfung aus allen darauf verkehrenden Fahrzeugen. Analog dazu folgt: Je umfassender und zuverlässiger die Infrastruktur Ihrer Identitätsdaten, desto größer ist die Wertschöpfung, die aus allen Identitätsmanagement- und Unternehmensanwendungen, die diese Daten nutzen, erzielt werden kann.



On Demand Unternehmen benötigen für ihre Identitätsdaten eine offene, zuverlässige und skalierbare Daten-Engine:

- *Offen – Ihre Daten-Engine sollte auf allen gängigen Plattformen ausführbar sein. Um als Softwareplattform für Ihr gesamtes Unternehmen fungieren zu können, muss das Verzeichnis einer großen Anzahl der Anwendungen, die für Ihr Unternehmen wichtig sind, eine dynamische, ausbaufähige Unterstützung bieten.*
- *Zuverlässig – Um globale Anwendungen unterstützen zu können, sind Unternehmen zunehmend gezwungen, eine rund um die Uhr verfügbare Verzeichnisinfrastruktur aufzubauen. Eine erweiterte Replikationsfunktionalität – einschließlich einer Multi-Master-Fähigkeit – stellt eine hohe Verfügbarkeit und rasche Bereitstellung von Content, auf den häufig zugegriffen wird, weltweit an jedem beliebigen Ort zur Verfügung.*
- *Skalierbar – Auf Grund des kontinuierlichen Wachstums und der Konsolidierung Ihrer Verzeichnisse benötigen Sie eine sichere relationale Datenbank – nicht nur einen proprietären Datenspeicher. Fordern Sie eine leistungsstarke Daten-Engine, die große Gruppen – bis hin zu mehreren Hunderttausend Benutzern – unterstützen und auch bei wachsenden Verzeichnisdimensionen eine Leistungsfähigkeit auf gleich bleibend hohem Niveau gewährleisten kann.*

Um eine Verzeichnisinfrastrukturlösung zu ermitteln, die diese drei Standards erfüllt, suchen Sie nach einer Lösung mit den folgenden Merkmalen:

- *Zertifiziert von der Open Group als LDAP Version 3-konform*
- *Unterstützt führende Plattformen einschließlich Microsoft® Windows®, Linux, IBM AIX, Sun Solaris und HP-UX*
- *Bietet eine starke Linux-Lösung, da viele Unternehmen ihre Verzeichnisse auf diese kosteneffektive, leistungsstarke Plattform konsolidieren*
- *Ermöglicht die Realisierung einer für globale Unternehmensanwendungen erforderlichen Verfügbarkeit rund um die Uhr mittels erweiterter Replikations- und Multi-Mastering-Funktionalitäten – einschl. Unterstützung zahlreicher Verzeichnis-Masterkopien und der Fähigkeit der Replikation verschiedener Verzeichniszweige für verschiedene Master*
- *Wurde in einer Vielzahl unterschiedlicher Kundenanwendungen rund um die Welt implementiert*
- *Verwendet eine relationale Datenbank mit hohen Sicherheitsstandards – anstelle eines proprietären Datenspeichers – und gewährleistet damit exzellente Skalierbarkeit, Zuverlässigkeit und Leistungsfähigkeit*

### **Sichern Sie sich einen kosteneffektiven Aufbau konsistenter Sicherheitskonzepte durch Implementierung einer Lösung für Benutzermanagement und -Provisioning**

Ohne ein System für ein unternehmensweites Sicherheitsmanagement kann sich Ihr Unternehmen zahlreichen Herausforderungen ausgesetzt sehen. Berechtigungen werden möglicherweise an Konten von Personen erteilt, die keinen Zugriff mehr benötigen, da sie aus dem Unternehmen ausgeschieden sind oder eine andere Tätigkeit übernommen haben. Ihre IT-Mitarbeiter müssen vielleicht übermäßig viel Zeit für das fallweise Erteilen und Beschränken von Benutzerberechtigungen aufwenden – was Ressourcen bindet, die für andere Projekte mit mehr Geschäftswertpotenzial nicht mehr zur Verfügung stehen. Oder Ihr Unternehmen findet möglicherweise das Erfassen der Informationen, die Sie zur Einhaltung von Sicherheitsaudits benötigen, zu kosten- und zeitaufwändig.

Mit Lösungen für Benutzer-Provisioning und -Management kann Ihr Unternehmen konsistente Sicherheitsstandards aufstellen und gleichzeitig die Kosten für die Verwaltung von Sicherheitsfunktionen senken. Diese Lösungen automatisieren das Einrichten und Löschen von Benutzerkonten. Wenn beispielsweise ein neuer Mitarbeiter hinzukommt oder sich der Status eines Mitarbeiters ändert, müssen die Zugriffsberechtigungen des Mitarbeiters korrekt zugewiesen bzw. neu zugewiesen werden. Eine Lösung für Benutzer-Provisioning und -Management legt durch Anwendung von Regeln fest, welche Benutzergruppen über welche Berechtigungen verfügen sollen, um den Zugriff für jeden Mitarbeiter automatisch einzurichten. Die Automatisierung sorgt dafür, dass die Kosten für das Ausführen von Routineaufgaben durch IT-Mitarbeiter sinken und Sicherheitskonzepte einheitlich umgesetzt werden.

Da Lösungen für Benutzer-Provisioning und -Management Zugriffsberechtigungen nach einem zentralen und organisierten Prinzip verwalten, verschaffen diese Lösungen unternehmensweit einen klaren Überblick darüber, wer welche Berechtigungen hat. Dank dieses Überblicks können Sie die Zugriffe aller autorisierten Benutzer genau nachvollziehen, und Ihnen Zugriffsberechtigungen nur in dem Umfang erteilen, der Ihren Geschäftsprioritäten und -anforderungen entspricht. Lösungen für Benutzer-Provisioning und -Management erfassen darüber hinaus zu Prüfzwecken genauestens alle Änderungen an Zugriffsberechtigungen – und ermöglichen so Einsparungen an Arbeitszeit und Aufwand für die Einhaltung von Audit-Anforderungen.



Diese Lösungen lassen sich außerdem in Privacy-Management-Lösungen integrieren und helfen Ihrem Unternehmen damit Vorschriften einzuhalten und im ganzen Unternehmen verteilte vertrauliche Informationen zu schützen.

Stellen Sie sicher, dass die von Ihnen ausgewählte Lösung für Benutzer-Provisioning und -Management die folgenden Merkmale aufweist:

- *Verwaltet verteilte Benutzergruppen und kann Benutzern mehrere Funktionen zuweisen*
- *Ermöglicht proaktives Umsetzen von Sicherheitsrichtlinien – eine Automatisierung basierend auf Funktionen und Regeln*
- *Dehnt die Sicherheitsautomatisierung auf Geschäftspartner aus*
- *Leitet Zugriffsanforderungen über Autorisierungsprozesse weiter und leitet diese, wenn keine prompte Aktion erfolgt, an alternative höhere Genehmigungsebenen weiter*
- *Bietet eine bidirektionale, sichere und bandbreiten-effiziente Schnittstelle zu Systemen, die Sie in Ihrem gesamten Unternehmen einsetzen bzw. möglicherweise zu einem zukünftigen Zeitpunkt einführen werden*
- *Ist skalierbar und passt sich damit an Änderungen in Ihrem Unternehmen an*
- *Weist nur wenige Installationsabhängigkeiten auf.*
- *Spiegelt, repliziert und partitioniert Daten, um eine maximale Datenintegrität und -verfügbarkeit zu gewährleisten*
- *Umfasst alle erforderlichen Softwarekomponenten, einschließlich gegebenenfalls erforderliche Datenbanken, LDAP-, Web- und Anwendungsserver*

#### **Wählen Sie eine Zugriffssteuerungslösung, die Ihre Sicherheitslücken auf ein Minimum reduziert und benutzerfreundlich ist**

Da Sie Ihren Kunden und Partnern Zugang zu immer mehr Anwendungen anbieten, benötigt eine zunehmende Anzahl von Benutzern Zugriff auf Ihre Systeme. Um maximalen Wert aus diesen Anwendungen schöpfen zu können, müssen diese benutzerfreundlich sein. Damit mehr Zeit für die Entwicklung von Anwendungen bleibt, den Geschäftswert erhöhen, muss der Zeitaufwand reduziert werden, den IT-Mitarbeiter für die Verwaltung bestehender Anwendungen benötigen.

Mit Zugriffssteuerungslösungen lassen sich die Nutzbarkeit und Sicherheit Ihrer kunden- und partnerorientierten Anwendungen verbessern. Dadurch dass die Single-Sign-On-Funktionalität nicht nur Ihren Mitarbeitern, sondern auch Ihren Partnern und Lieferanten zur Verfügung steht, reduzieren Zugriffssteuerungslösungen eine Reihe kennwortabhängiger Probleme auf ein Minimum:

- *Verwechslung bei Mehrfachzugriffskennwörtern*
- *Sicherheitsrisiko durch schriftliches Notieren von Kennwörtern*
- *Ausfallzeiten für Endbenutzer, wenn deren Zugang zu Konten blockiert ist*
- *Zeitaufwand, den IT-Mitarbeiter für die Verwaltung von Passwörtern benötigen*

Die Zugriffssteuerung bietet zudem eine stabile Grundlage für die Personalisierung von Content, wodurch das Benutzererlebnis bezüglich Qualität und Effizienz verbessert wird.

Durch das Herausheben der sicherheitsspezifischen Entwicklung aus dem Prozess der Anwendungsentwicklung versetzen Zugriffssteuerungslösungen Ihre IT-Mitarbeiter in die Lage, sich voll auf Kernaktivitäten zu konzentrieren. Wenn Entwickler bei jeder Anwendung gesondert Sicherheitsvorsorge treffen müssen, bedingt dies hohe Entwicklungskosten und eine niedrigere Sicherheitskonsistenz innerhalb Ihres Unternehmens. Bei einer zentralen Zugriffssteuerungslösung können Ihre Entwickler das Sicherheitsmanagement einfach der Lösung überlassen – und auf diese Weise einen hohen Sicherheitsstandard bei minimalen Kosten erzielen.

Darüber hinaus ermöglichen Zugriffssteuerungslösungen die Konsolidierung verschiedener Zugriffssteuerungs- und Autorisierungslösungen, schließen Sicherheitslücken in Betriebssystemen und prüfen Zugriffs- und Datenschutzanforderungen.

Die Zugriffssteuerungslösung, auf die Ihre Wahl fällt, sollte:

- *Verschiedene Authentifizierungsverfahren und Zugriffsgeräte unterstützen (Desktops, PDAs, Mobiltelefone usw.) – es sollte mit genau so vielen verschiedenen Protokollen arbeiten, wie Ihre Benutzer für den Zugriff auf Ihr System nutzen*
- *Umfassende Integrierbarkeit in Identitätsserver, Anwendungen, Middleware, Betriebssysteme und Plattformen bieten*





- *Eine richtlinienbasierte Sicherheitsinfrastruktur implementieren zur einfacheren Verwaltung und Anpassung des Sicherheitskonzepts entsprechend den Unternehmensregeln und Geschäftszielen*
- *Durch Stellvertreterverwaltungs-, Self-Care- und Selbstregistrierungsfunktionen den Verwaltungsaufwand verringern*
- *Offene Standards einschließlich Webservices nutzen, um sowohl jetzt als auch später maximale Interoperabilität zu gewährleisten*
- *Nahtlose Abwicklung einer großen Anzahl an – erwarteten wie unerwarteten – Aktivitäten bei gleich bleibender Leistungsfähigkeit bzw. Verfügbarkeit bieten*
- *Zugriffsanforderungsdaten nutzen, um Schwachstellen zu lokalisieren und proaktive Sicherheitsverbesserungen zu ermöglichen*
- *Mehr Sicherheit für alle gängigen Plattformen einschließlich Mainframes und Anwendungen, die auf Mainframes ausgeführt werden, bieten*
- *Maximale Interoperabilität – inklusive Single-Sign-On – mit Ihrer bestehenden Desktopinfrastruktur sowie anderen Sicherheitsumgebungen und führenden e-business Anwendungen ermöglichen*

#### **Eine Zugriffssteuerungslösung für UNIX- und Linux-spezifische Sicherheitsanforderungen herausfiltern**

Bei UNIX- und Linux-Umgebungen stellen sich durch die Kontrolle der Super-User- und Root-Konten ganz spezielle Anforderungen an die Zugriffssteuerung. Das primäre Sicherheitsrisiko, dem Unternehmen ausgesetzt sind, liegt in einem Fehlverhalten durch interne Benutzer und Mitarbeiter. Super-User-Konten sind ganz besonders missbrauchsgefährdet, da die Zugriffsberechtigungen für diese Konten traditionell keiner Kontrolle unterliegen und außerdem keine Möglichkeit besteht, die Aktionen der Personen, die mit diesen Konten arbeiten, zu prüfen.

Eine Zugriffssteuerungslösung für Ihre UNIX- und Linux-Systeme bietet Ihnen die Möglichkeit, die Anwendungen, Dateien und Daten auf diesen Betriebsplattformen und auch die Plattformen selbst zu sichern. Sie wendet dieselben Unternehmensrichtlinien an, die Sie zur Steuerung der Zugriffe in Ihrem gesamten Unternehmen verwenden, und erzeugt ein ausgereiftes Prüfprotokoll für eine mögliche Rückverfolgbarkeit Ihrer Systemadministratoren. Für Ihre unternehmenskritischen Anwendungen, die sich auf UNIX- und Linux-Systemen befinden – und insbesondere auch für Unternehmen in sicherheitssensiblen und stark regulierten Branchen – ist eine auf diese Umgebungen zugeschnittene Zugriffssteuerungslösung von zentraler Bedeutung, wenn eine End-to-End-Sicherheitsrichtlinie implementiert werden soll.

Eine hochkarätige Zugriffssteuerungslösung für Ihre UNIX- und Linux-Umgebungen sollte die folgenden Merkmale aufweisen:

- *Kombiniert umfassenden Schutz vor unbefugten Zugriffen – Firewall auf Host-Basis, Anwendungs- und Plattformschutz, Benutzer-Tracking und -steuerung – mit zuverlässigen Auditing- und Einhaltungsprüffunktionen*
- *Setzt bewährte, aber anpassbare Richtlinien ein, mittels derer Unternehmen rasch eine wirkungsvolle Sicherheitsinfrastruktur aufbauen können*
- *Ermöglicht eine zentrale Zugriffsverwaltung und führt Prüfungen über eine große Anzahl von UNIX- und Linux-Servern hinweg aus*
- *Stellt umfangreiche Auditing-Funktionen und ausführliche Berichte bereit, die Sie Regulierungsbehörden sowie externen und Unternehmens-Prüfern vorlegen können*
- *Liefert Sicherheits- und Auditing-Funktionen der Mainframe-Klasse in einem benutzerfreundlichen Lightweight-Produkt*
- *Integriert seine grafische Oberfläche und Richtlinien-datenbank in alle Sicherheitsanwendungen für Ihre UNIX- und Linux-Systeme, Webanwendungen und IBM WebSphere MQ-Installationen*
- *Verursacht kaum Overhead (weniger als 1 %), hält die Sicherheit während Systemsicherungen aufrecht und bildet ein hochskalierbares System*

#### **Wählen Sie eine Lösung, die die Sicherheit Ihrer IBM WebSphere Business Integration-Umgebung erweitert**

Unternehmen, die zur Verarbeitung persönlicher Daten und anderer sensibler Datenarten WebSphere MQ einsetzen, möchten häufig die nativen Sicherheitsservices von WebSphere MQ erweitern und so einen End-to-End-Schutz von Nachrichtendaten erreichen. Bei zunehmender Verknüpfung von immer mehr Geschäftsbereichsanwendungen mittels WebSphere MQ suchen diese Unternehmen nach einem Weg, sowohl Datenschutz- als auch Zugriffssteuerungsrichtlinien systemübergreifend im gesamten Unternehmen zentral zu verwalten.

Durch eine erweiterte Sicherheitslösung für WebSphere MQ sind diese Unternehmen in der Lage, die Integrität und Vertraulichkeit von Nachrichten nicht nur während der Übertragung von System zu System, sondern auch dann zu gewährleisten, wenn sie sich unter der Kontrolle von WebSphere MQ selbst befinden. Darüber hinaus kann eine auf diese Weise erweiterte Sicherheitslösung durch Anwenden von Unternehmensrichtlinien das gewünschte Maß an Vertraulichkeit und Integrität für jede Transaktion bieten.



Bei der Analyse erweiterter Sicherheitslösungen für Ihre WebSphere MQ-Umgebung sollten Sie darauf achten, dass die Lösung die folgenden Merkmale aufweist:

- *Hilft, die Sicherheit bei wichtigen WebSphere MQ-Transaktionen zu verstärken, ohne WebSphere MQ-Anwendungen modifizieren oder rekompilieren zu müssen*
- *Ermöglicht die strikte Wahrung der Datenintegrität und -vertraulichkeit anhand von Prüffunktionen auf Nachrichtenebene, um die Einhaltung der definierten Sicherheitsrichtlinien zu gewährleisten*
- *Ermöglicht niedrigere Verwaltungskosten durch die zentrale Verwaltung der Zugriffssteuerungs- und Datenschutzrichtlinien über Mainframe- und verteilte Server hinweg*
- *Stellt unternehmensweite Verwaltung von Sicherheitsrichtlinien für WebSphere MQ zur Verfügung. Dies umfasst Nachrichtenintegrität und -vertraulichkeit, Sicherheitsauditverfahren und Warteschlangen-Zugriffskontrollgenehmigungen von einem webbasierten Verwaltungstool*
- *Ist kompatibel mit anderen Mitgliedern der IBM WebSphere Business Integration-Produktfamilie, einschließlich IBM WebSphere MQ Workflow sowie IBM WebSphere Business Integration Message Broker und IBM WebSphere Business Integration Event Broker*

#### **Freigabe sensibler Informationen mit einer Privacy-Management-Lösung steuern**

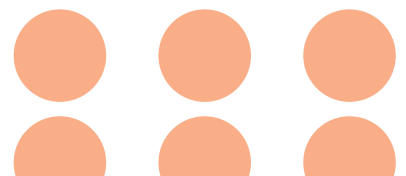
Unternehmen suchen zunehmend nach effizienten Methoden zur Einhaltung der steigenden Anzahl an Datenschutzvorschriften und Forderungen der Verbraucher nach mehr Datenschutz. Die schiere Dimension dieser Aufgabe kann unüberwindbar erscheinen, da ohne ein automatisiertes, zentrales Verfahren zur Verwaltung privater Informationen die Datenschutzrichtlinien in jeder einzelnen Anwendung codiert und im gesamten Unternehmen manuell implementiert werden müssen.

So müssen beispielsweise in Unternehmen, die zur Identifikation ihrer Benutzer eindeutige Kenndaten verwenden, wie z. B. die in den USA übliche Sozialversicherungsnummer oder in anderen Ländern die Steuernummer, diese Daten vor einer möglichen Einsichtnahme durch unbefugte Mitarbeiter geschützt werden. Aber in den meisten Fällen sind die Kosten, die anfallen, um Anwendungen und Datenbanken so umzuprogrammieren, dass bestimmte sensible Daten nicht verwendet werden, viel zu hoch. Das Umcodieren von bestehenden Anwendungen hat zudem einen weiteren Nachteil. Denn bei einer weiteren Richtlinienänderung muss dieser Prozess möglicherweise erneut durchgeführt werden. Hier schafft eine Infrastrukturlösung Abhilfe – eine Lösung, die eine intelligente Verwaltung von Daten in Übereinstimmung mit den Richtlinien und Benutzerpräferenzen ohne Abhängigkeit von einzelnen Anwendungen erlaubt.

Eine optimale automatisierte und zentrale Privacy-Management-Lösung ermöglicht es Ihnen, Datenschutzrichtlinien in Übereinstimmung mit den Vertraulichkeitspräferenzen der einzelnen Benutzer umzusetzen – und dies über alle datenschutzrelevanten Anwendungen und Datenbanken innerhalb Ihres Unternehmens hinweg. Das Automatisieren des Datenschutzmanagements hilft die Kosten für die Implementierung und für das Anpassen Ihrer Datenschutzrichtlinien so gering wie möglich zu halten. Die Zentralisierung ermöglicht zudem die unternehmensweite konsistente Anwendung Ihrer Datenschutzrichtlinien und vereinfacht die automatische Generierung von Prüfberichten.

Bei dem derzeitigen Marktangebot ist es schwierig eine einzige Lösung zu finden, die den gesamten Umfang an Datenschutzmanagement-Funktionen umfasst, der erforderlich ist, um sowohl den heutigen Datenschutzerfordernungen Rechnung zu tragen, als auch für zukünftige gerüstet zu sein. Halten Sie nach einer Privacy-Management-Lösung Ausschau, die die folgenden Merkmale aufweist:

- *Reduziert den Umfang, in dem Ihre bestehenden Anwendungen umprogrammiert bzw. neu implementiert werden müssen, um Datenschutz- und Vertraulichkeitsvorschriften zu erfüllen*
- *Generiert verschiedene Berichtstypen, die als Nachweis für die Einhaltung von Unternehmensrichtlinien herangezogen werden können*
- *Gibt sensible und persönliche Daten innerhalb Ihres Unternehmens nur für die richtigen Personen und nur aus den richtigen Unternehmensgründen frei*
- *Bindet die Vertraulichkeitspräferenzen einer Einzelperson ein und berücksichtigt diese bei der Bewilligung von Datenanforderungen*
- *Hilft die Vorschriften einzuhalten, ohne die Produktivität zu beeinträchtigen, Geschäftsprozesse unnötig zu komplizieren, Kosten zu erhöhen oder Ihren Wettbewerbsvorteil zu schmälern*
- *Erfüllt die gängigen Datenschutzmanagement-Standards wie Unterstützung für P3P (Plattform for Privacy Preferences)*
- *Bietet eine benutzerfreundliche Verwaltungskonsolle, die Richtlinien in Englisch (oder in anderen natürlichen Sprachen) verwaltet und es auch Benutzern ohne IT-Fachkenntnisse erlaubt, Richtlinien festzulegen und zu verwalten*



### **IBM Sicherheitssoftware gewährleistet ein hohes Maß an Integrationsfähigkeit und kann so Ihre langfristigen Sicherheitsstrategien unterstützen**

Wenn Sie damit beginnen, sich näher mit Lieferanten für den von Ihnen bevorzugten Einstiegspunkt in das Identitätsmanagement zu beschäftigen, werden Sie feststellen, dass IBM Ihnen nicht nur in diesem Bereich eine branchenführende Lösung anbieten kann, sondern sämtliche Sicherheitslösungen von IBM eine unübertroffene Flexibilität und Integrationsfähigkeit bieten. Und was bedeutet das für Sie? Für Sie bedeutet dies, dann, wenn Sie bereit sind, weitere Bereiche des Identitätsmanagements zu implementieren, mit IBM einen Lieferanten zur Seite zu haben, der Ihre langfristigen Sicherheitsziele am besten unterstützen kann.

Die führende Rolle von IBM auf dem Gebiet der Integration manifestiert sich jedoch nicht nur in der nahtlosen Weise, in der Lösungen von IBM zusammenarbeiten. Sie sind zudem aus wieder verwendbaren Komponenten aufgebaut. Wenn Sie eine neue Lösung implementieren, die die zu Grunde liegende Funktionalität mit einer bereits installierten Lösung gemeinsam nutzen kann, ist es nicht notwendig, zwei Instanzen derselben Komponente auszuführen. IBM hilft dabei, den Softwarespeicherbedarf Ihrer integrierten Lösung zu minimieren und damit die Effizienz zu maximieren. Dies ist besonders wichtig, wenn Sie Ihren Mitarbeitern Anwendungen mit hoher Nutzbarkeit und Ihren Kunden exzellenten und schnellen Service bieten möchten.

Wenn Sie sich für IBM entscheiden, haben Sie einen Partner, in dessen Stabilität und Bestandsfestigkeit Sie vollstes Vertrauen haben können. Denn IBM wird auch noch in vielen Jahren bzw. Jahrzehnten für Sie mit führenden Lösungen da sein, die das Sicherheitsmanagement vereinfachen, egal wie komplex dieses geworden ist.

### **Wagen Sie den Schritt in das Identitätsmanagement – mit ausgezeichneten Sicherheitslösungen von IBM**

IBM kann Ihnen für jede Phase des Identitätsverwaltungszyklus Software anbieten, die mit allen Kriterien einer hervorragenden Lösung aufwarten kann:

*IBM Directory Integrator und IBM Directory Server zur Festlegung von Identitätsdaten:*

- *IBM Directory Integrator bietet bei heterogenen Identitätsdatenquellen eine Synchronisierung in Echtzeit, ermöglicht Ihnen den Aufbau einer autoritativen und immer auf dem aktuellen Stand gehaltenen Identitätsdaten-Infrastruktur und hilft maximalen Nutzen aus bestehenden Investitionen in Verzeichnisprodukte zu ziehen*
- *IBM Directory Server stellt eine leistungsstarke LDAP-Identitätsinfrastruktur bereit, die die Basis für die Implementierung umfassender Identitätsmanagementanwendungen und erweiterte Softwarearchitekturen bildet*

*IBM Tivoli Identity Manager für Benutzermanagement und -Provisioning – Ermöglicht eine zentral koordinierte Erzeugung von Benutzerkonten, die Automatisierung des Genehmigungsprozesses, die Bereitstellung von Ressourcen und die Generierung von Prüfprotokollen. Mit dem IBM Tivoli Identity Manager lassen sich Benutzer, Systeme und Anwendungen schnell online bringen, so dass Sie leichter eine betriebliche Effizienz erreichen, Kosten senken und die Investitionsrendite steigern können.*





*IBM Tivoli Access Manager-Software für Zugriffssteuerung*  
– Stellt eine konsistente identitätsbasierte Steuerung von einer einzigen Verwaltungskonsole aus zur Verfügung und erlaubt so eine Single-Policy-Zugriffsverwaltung über ein breites Spektrum an Ressourcen. Die IBM Tivoli Access Manager-Produktfamilie umfasst:

- *IBM Tivoli Access Manager for e-business: Stellt End-to-End-Sicherheit einschließlich einer Single-Sign-On-Funktion, Autorisierung auf URL- und Anwendungsebene, dezentraler Verwaltung auf Webbasis und richtliniengesteuerter Sicherheit bereit.*
- *IBM Tivoli Access Manager for Operating Systems: Schützt einzelne Anwendungs- und Betriebssystemressourcen durch Aufstellen von Regeln, die den Zugriff auf alle UNIX- und Linux-Konten einschließlich der Super-User- und Root-Konten optimieren.*
- *IBM Tivoli Access Manager for Business Integration: Verbessert die nativen Sicherheitservices von WebSphere MQ durch die Bereitstellung von End-to-End-Integrität, Datenschutz bei Nachrichtendaten und einer zentralen Verwaltung der Datenschutz- und Zugriffssteuerungsrichtlinien.*

*IBM Tivoli Privacy Manager for e-business für Freigabesteuerung* – nutzt Tivoli Identity Manager und Tivoli Access Manager-Software zur Implementierung und Umsetzung von Datenschutzrichtlinien, zur Sicherung persönlicher Daten, und zum Schutz des Verbrauchervertrauens und der Markenintegrität.





### Weitere Informationen

Wenn Sie mehr darüber erfahren möchten, welche Identitätsmanagementlösung die richtige Einstiegsmöglichkeit für Ihr Unternehmen ist, und herausfinden möchten, welche Vorteile die IBM Sicherheitsmanagementsoftware Ihrem Unternehmen bringen kann, wenden Sie sich an Ihren IBM Vertriebsbeauftragten oder IBM Business Partner – oder besuchen Sie uns unter:

**ibm.com**/tivoli/solutions/security

Um eine Übersicht darüber zu erhalten, wie Identitätsmanagement ein kosteneffektives Sicherheits-Framework um Ihr Unternehmen errichten kann, lesen Sie die IBM Info für Führungskräfte zum Identitätsmanagement:

<ftp://software.ibm.com/software/tivoli/whitepapers/wp-idm.pdf>

IBM stellt Ihnen darüber hinaus ausführliche Leitfäden für Kunden zur Verfügung, die Sie bei Ihren Überlegungen zu Lösungen für Benutzer-Provisioning und -Management sowie Zugriffssteuerungslösungen zu Rate ziehen können:

<ftp://software.ibm.com/software/tivoli/buyers-guides/bg-ident-mgmt.pdf>

<ftp://software.ibm.com/software/tivoli/buyers-guides/bg-access-mgt.pdf>

### Tivoli-Software von IBM

Als integraler Bestandteil der umfassenden IBM Infrastrukturlösung unterstützt Tivoli IT Infrastrukturmanagement Software konventionelle Unternehmen, angehende On Demand Unternehmen sowie Internet-Unternehmen weltweit bei der Optimierung ihrer bestehenden aber auch zukünftigen Technologieinvestitionen. Gestützt auf erstklassige IBM Services, Support und Forschung stellt die Tivoli Software eine nahtlos integrierte und flexible Infrastrukturmanagementlösung zur Verfügung, die Mitarbeiter, Geschäftspartner und Kunden auf der Basis einer zuverlässigen Sicherheitslösung miteinander verbindet.

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

IBM, das IBM Logo, das e-Logo, ibm.com, AIX, Tivoli and Tivoli Enterprise Console und WebSphere sind eingetragene Marken der IBM Corporation. On Demand Business und das On Demand Business Logo sind Marken der IBM Corporation in den USA und/oder anderen Ländern.

Microsoft, Windows, Windows NT und das Windows Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

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

Weitere Unternehmens-, Produkt- und Servicennamen können Marken anderer Hersteller sein.

Hergestellt in den USA  
02-04

Alle Rechte vorbehalten

Gedruckt in den USA auf umweltfreundlichem Papier mit 10% Altpapieranteil.

© Copyright IBM Corporation 2004  
Alle Rechte vorbehalten.