

SAP NetWeaver® IDENTITY MANAGEMENT: ZUGRIFFSRECHTE SICHER VERWALTEN

DIE IDENTITÄTSKRISE BEWÄLTIGEN

Immer mehr Unternehmen befinden sich in einer Identitätskrise. Wenn in der IT umfassende Lösungen für das Identitätsmanagement fehlen, kann die Benutzerproduktivität sinken und die Fehleranfälligkeit steigen. SAP NetWeaver® Identity Management sorgt dafür, dass digitale Identitäten konsistent, synchron und sicher verwaltet werden – plattformübergreifend, automatisiert und rollenbezogen.



In IT-Umgebungen vieler Unternehmen macht sich heute eine Identitätskrise bemerkbar: Administratoren müssen eine Vielzahl von Systemen auf aktuellem Stand halten. Datenänderungen bei Mitarbeitern benötigen nicht selten Wochen, bis sie in allen Anwendungen umgesetzt wurden. Mitarbeiter, die das Unternehmen verlassen haben, verfügen immer noch über aktive Accounts. Zudem nehmen täglich die Anrufe bei der Hotline zu, um Passwörter zurückzusetzen. Dies alles erhöht die Supportkosten und birgt hohe Gefahren in Bezug auf die Datensicherheit.

Der Kern des Problems liegt in der Komplexität heutiger IT-Umgebungen. Die IT-Abteilung ist für zahlreiche Systeme verantwortlich. Die IT-Anwendungen müssen für die täglichen Aufgaben der Mitarbeiter bereitstehen. Sie erfordern für jeden einzelnen User eigene Benutzer-IDs und Passwörter. Jeden Tag kommen neue Angestellte, Partner oder Kunden hinzu – sie alle brauchen für ihre Arbeit einen einfachen, schnellen Zugriff auf unterschiedliche Anwendungen und Systeme. Mit jedem neuen Mitarbeiter

oder System potenziert sich die Komplexität der Administrations- und Zugriffsbeziehungen. In den meisten Fällen werden die Accounts an den einzelnen Systemen manuell angelegt, verwaltet und mit Berechtigungen versehen. Doch irgendwann verliert auch der versierteste Administrator den Überblick, und spätestens dann passieren Fehler: Alte Berechtigungen bleiben bestehen, kritische Kombinationen entstehen, Datenänderungen sind fehlerhaft. Im besten Fall erfolgt ein Anruf beim Helpdesk; im schlimmsten Fall haben Unbefugte Zugriff auf Daten und verursachen Schäden.

Wenn viele der laufenden Systeme von unterschiedlichen Herstellern stammen, wird die Situation noch unübersichtlicher. Risiken steigen auch, wenn verschiedene Instanzen der gleichen Software im Einsatz sind, sei es an einem Ort oder auf mehrere Standorte verteilt. Jedes System hat seine eigenen Anforderungen an Datenqualität und -sicherheit, an Zugangsrichtlinien, Benutzerkennungen und an die Lebensdauer von Passwörtern.

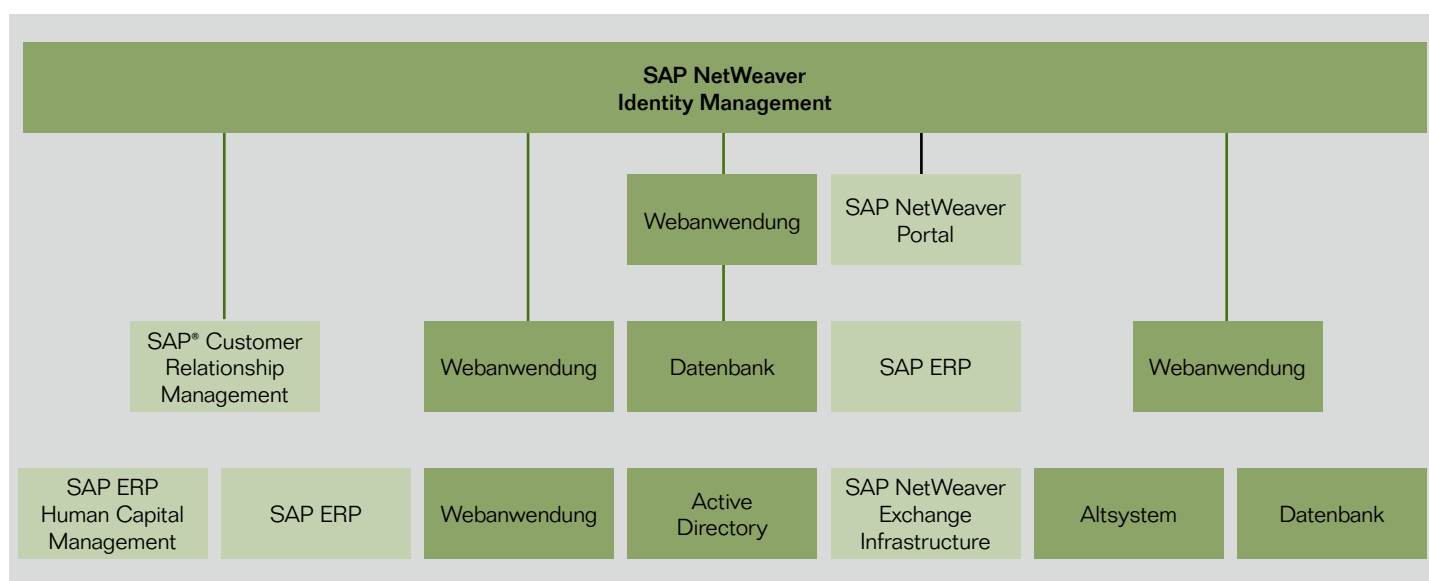
Komplexe IT-Landschaften ohne umfassendes Identitätsmanagement verursachen hohe Betriebskosten und bergen vielfältige Gefahren. Die möglichen Konsequenzen sind nicht zu unterschätzen:

- **Hohe Verwaltungs- und Supportkosten:** Fehler in den Daten führen zu häufigen Rückfragen; eine wachsende Zahl von Anrufen beim Support verursacht eine hohe Belastung. Ohnehin teure IT-Ressourcen müssen für Verwaltung und Support aufgewendet werden.
- **Unsichere Systeme:** Wenn Mitarbeiter eine andere Aufgabe übernehmen oder das Unternehmen ganz verlassen, ist der unberechtigte Zugriff auf kritische Unternehmensdaten immer eine Folge von lückenhaften oder zu langsamen Prozessen ohne Identitätsmanagement.

- **Niedrigere Benutzerproduktivität:** Es ist nicht ungewöhnlich, dass das manuelle Einrichten von Zugriffsrechten Tage oder gar Wochen dauert. Erst dann können neue Benutzer oder Mitarbeiter in einer neuen Rolle auf alle Systeme zugreifen, die sie für ihre Arbeit benötigen.
- **Externe Probleme:** Verspätet gewährte Zugriffsrechte für externe Benutzer, wie Zulieferer oder Key-Account-Kunden, können zu Verzögerungen oder sogar Ausfällen bei zentralen Geschäftsprozessen, etwa in Fertigung oder Fakturierung, führen.
- **Ungewünschte Folgen im Bereich Governance, Risk and Compliance (GRC):** Wenn gesetzliche Vorgaben auf Grund fehlerhafter oder unzureichender Daten nicht eingehalten werden, kann dies unangenehme Folgen

nach sich ziehen. Das reicht von Prüfungs- und Gerichtskosten über sinkende Aktienkurse, empfindliche Geldstrafen bis hin zu Freiheitsstrafen für Mitglieder der Unternehmensführung.

Die Ironie dabei ist: Je mehr sich die IT-Abteilung bemüht, die Informationsversorgung der Benutzer durch reibungslosen Zugriff auf neue Systeme und Services – häufig von unterschiedlichen Herstellern – zu gewährleisten, desto komplexer und teurer wird die Administration. Mehr Systeme bedeuten mehr Passwörter und eine aufwendigere Berechtigungsverwaltung. Sicherheitsmaßnahmen, wie eine regelmäßige Änderung des Passworts nach 90 Tagen, erhöhen die Anzahl der Anrufe beim Support und lösen geradezu eine Flut allgegenwärtiger gelber Klebezettel aus.



Eine effiziente und flexible Lösung für die Verwaltung von Zugriffsberechtigungen in komplexen, heterogenen Umgebungen

Die Benutzer sind frustriert, die IT-Kosten schießen in den Himmel. Teures IT-Know-how wird durch den Administrationsaufwand gebunden. Die Datenqualität ist gering, und die Unternehmen laufen Gefahr, Gesetze nicht wie gefordert einzuhalten und das Risikomanagement zu vernachlässigen.

SAP NetWeaver Identity Management

Rollenbasierte Berechtigungen einrichten und verwalten

Mit SAP NetWeaver Identity Management, einer Komponente der Technologieplattform SAP NetWeaver, steht Ihnen eine leistungsfähige Lösung für diese Probleme zur Verfügung.

SAP NetWeaver Identity Management ermöglicht es Ihnen, Ihre Berechtigungsdaten zu verwalten und über Systeme und Instanzen hinweg zu synchronisieren. Durch die Verknüpfung von Partnersystemen, Individual- und Altsystemen sowie SAP-Anwendungen werden Daten, Geschäftsprozesse,

Arbeitsabläufe und Zugriffsberechtigungen aufeinander abstimmt – automatisiert, dokumentiert, zeitnah und richtlinienkonform. Das erleichtert die Arbeit Ihrer IT-Abteilung und der Anwender. Die Gesamtverantwortlichen können sich so darauf verlassen, dass die Systeme den Sicherheitsbestimmungen und Gesetzesanforderungen entsprechen.

Verantwortliche in Finanzwesen und IT, CFOs und CIOs stellen mit SAP NetWeaver Identity Management einen wesentlichen Teil des unternehmensweiten Risiko- und Identitätsmanagements sicher. IT-Abteilungen erhöhen durch diese Architektur die System- und Datensicherheit deutlich. Mitarbeiter können, mit den notwendigen Berechtigungen versehen, ihre täglichen Aufgaben um ein Vielfaches besser bewältigen.



Zusammenfassung

SAP NetWeaver Identity Management ermöglicht die zentrale Verwaltung und Provisionierung personenbezogener Daten und User- und Rolleninformationen in heterogenen IT-Umgebungen mit SAP- und Nicht-SAP-Anwendungen.

Herausforderungen

- Datenredundanz und -qualität: Eine Vielzahl von Systemen bergen eine Fülle redundanter Benutzerdaten, die oft fehlerhaft sind und jeweils einzeln administriert werden müssen
- Benutzerproduktivität: Manuelles Einrichten von Zugriffsrechten für neue Benutzer dauert oft sehr lange und ist fehleranfällig
- Sicherheit: Unberechtigte Zugriffe auf Unternehmensdaten durch Verzögerungen beim Einrichten beziehungsweise Löschen von Zugriffsrechten (zum Beispiel beim Austritt aus einem Unternehmen, bei Rollenänderungen)
- Verwaltungs- und Supportkosten: Je nach Unternehmen beziehen sich bis zu 50 Prozent der Anrufe beim IT-Support auf Probleme mit Passwörtern und der Zugangsberechtigung

Unternehmensprozesse und Softwarefunktionen

- Ihnen stehen integrierte Verwaltungswerkzeuge zur Verfügung, wie zum Beispiel eine leistungsstarke Datensynchronisierungs- und Selfservice-Schnittstelle. So lassen sich Zeit und Verwaltungskosten einsparen sowie eine kontinuierliche Benutzerproduktivität sicherstellen. SAP NetWeaver Identity Management hilft Ihnen, die Zugangsberechtigungen jedes einzelnen Benutzers in heterogenen Umgebungen rollenbasiert einzurichten. So vereinfachen Sie Ihre Administrationsarbeiten und verhindern unrechtmäßige Zugriffe auf Informationen.
- Unterstützen Sie den reibungslosen Ablauf von Geschäftsprozessen in Systemen mit der Enterprise Service-Oriented Architecture (Enterprise SOA).
- Ergänzen Sie die bereits vorhandenen Technologien für Benutzermanagement und -verwaltung in SAP Business Suite und SAP NetWeaver.

Hauptnutzen

- Zentrales Management von Benutzerdaten auch in heterogenen IT-Umgebungen
- Entlastung von Administration und Support
- Höhere Benutzerproduktivität durch zeitnahe und automatisierte Einrichtung der Zugangsberechtigungen
- Verlässliche Einhaltung von Vorschriften im Bereich Governance, Risk and Compliance (GRC)
- Sicherer Schutz vor unberechtigten Zugriffen auf kritische Unternehmensdaten

Weitere Informationen

Wenn Sie mehr darüber erfahren möchten, wie Sie mit SAP eine umfassende, integrierte Identity-Management-Lösung umsetzen können, wenden Sie sich an Ihren SAP-Berater, oder besuchen Sie uns im Internet unter www.sap.de/idm.

50 088 170 (08/06)

© 2008 SAP AG.

Alle Rechte vorbehalten. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign und weitere im Text erwähnte SAP-Produkte und -Dienstleistungen sowie die entsprechenden Logos sind Marken oder eingetragene Marken der SAP AG in Deutschland und anderen Ländern weltweit. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen. Die Angaben im Text sind unverbindlich und dienen lediglich zu Informationszwecken. Produkte können länderspezifische Unterschiede aufweisen.

In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden. Die vorliegenden Angaben werden von SAP AG und ihren Konzernunternehmen („SAP-Konzern“) bereitgestellt und dienen ausschließlich Informationszwecken. Der SAP-Konzern übernimmt keinerlei Haftung oder Garantie für Fehler oder Unvollständigkeiten in dieser Publikation. Der SAP-Konzern steht lediglich für Produkte und Dienstleistungen nach der Maßgabe ein, die in der Vereinbarung über die jeweiligen Produkte und Dienstleistungen ausdrücklich geregelt ist. Aus den in dieser Publikation enthaltenen Informationen ergibt sich keine weiterführende Haftung.