

## Erschwingliche IDM-Lösungen – Sicherheit für alle

Ich habe  
eine Idee!

Mitarbeiter kommen, Mitarbeiter gehen, und für jeden muss gesorgt werden. Nicht nur, um ihren Arbeitsplatz zu behalten, sondern auch, um das Recht auf Zugang zu allen notwendigen Informationssystemen (IS) zu haben und dieses Recht auch zu verlieren, wenn sie das Unternehmen verlassen. Deshalb gibt es Identitätsmanagement nicht nur für große Unternehmen, sondern auch für kleine und mittelständische Betriebe.



### FALLSTUDIE

## IDM Eigenschaften

IDM ist eine schnelle, flexible und kostengünstige Lösung, die viele Probleme in Unternehmen jeder Größe beseitigt. Warum sollten also nicht auch kleinere Unternehmen von technologischen Fortschritten profitieren, die sich bisher nur große Konzerne leisten konnten?

**Es ist da. Ein neuer Mitarbeiter hat gerade das Gebäude betreten. Was ist mit ihm?** Um ordnungsgemäß arbeiten zu können, muss die lokale IT-Abteilung ihm den nötigen Zugang zu den Informationssystemen gewähren. Solche Aufgaben werden in der Regel über interne Vorschriften abgewickelt, in der Regel ein zeitaufwändiges System von Anträgen und Genehmigungsverfahren, bei dem der Administrator des Informationssystems auf der Empfängerseite steht, um sicherzustellen, dass die erforderlichen Einstellungen vorgenommen werden.

Mit ähnlichen Problemen, jedoch umgekehrter Natur, haben auch Unternehmen zu kämpfen, wenn ihre Mitarbeiter sie verlassen. Darüber hinaus besteht ein erhebliches Sicherheitsrisiko bei ihrer Verlassung. Oft wissen die zuständigen Personen, die die entsprechenden Genehmigungen widerrufen oder besser noch aufheben sollten, nichts von der Abweichung. Es besteht auch das Risiko, dass sich die Position eines Mitarbeiters ändert. Hier gibt es oft einen kumulativen Zugriff, da dem Mitarbeiter neue Berechtigungen zugewiesen werden, die ursprünglichen Berechtigungen aber bestehen bleiben.

Sicherheitsaudits, denen sich Unternehmen regelmäßig unterziehen sollten, sind ein grundlegender Schutz vor solchen Problemen. In der Tat sollte ein Teil des Audits der Verwaltung der Nutzer von Informationssystemen gewidmet sein. Eine typische Frage, die ein Wirtschaftsprüfer stellt, lautet: „Wer darf auf welche Informationssysteme zugreifen und wer hat dies genehmigt?“. Die Erstellung und Verteidigung der entsprechenden Berichte ist jedoch oft ein „Albtraum“ für die verantwortlichen IT-Manager, ganz zu schweigen davon, dass das Unternehmen möglicherweise nicht aus den Prüfungsergebnissen lernt.

## Die Magie von IDM

Identitätsmanagement (IDM) ist ein Informationssystem, das den Identitätslebenszyklus jedes Benutzers verwaltet und eine effektive Verwaltung der Zugriffsrechte sicherstellt. IDM ist mit dem HR-System verknüpft, von dem es Informationen über alle Änderungen der Mitarbeiterdaten erhält (Änderung der Position, des Nachnamens, Eintritt eines Mitarbeiters, Austritt...). Auf der anderen Seite ist das IDM in die einzelnen Informationssysteme integriert und verwaltet die IS-Benutzer automatisch auf der Grundlage der im IDM definierten Regeln.

### ERBRACHTE LEISTUNGEN



## Wer bietet IDM an

Inzwischen gibt es eine Reihe von IDM-Lösungen auf dem Markt, nämlich die auf kommerziellen Produkten von Softwareunternehmen wie Oracle, Microsoft, IBM, Novell oder CA basieren, sowie auf Open-Source-Lösungen wie OpenIDM, Apache Syncope, midPoint oder OpenIAM.



## Identitätsmanagement

Jeder Wechsel eines Mitarbeiters erfordert eine Änderung der Einstellungen der Benutzerdaten in den Informationssystemen des Unternehmens. Spezialisierte Software sorgt für eine effiziente Verwaltung der IDM-Agenda, die Folgendes umfasst:

- automatische Weiterleitung von Änderungen an Benutzerkonten im IS,
- Gewährleistung der Konsistenz der Benutzerkonten im gesamten IS,
- Aufzeichnung aller Änderungen und durchgeführten Aktionen (Audit),
- Formalisierung und Automatisierung von IDM-Prozessen,
- zentrale Registrierung aller Benutzerkonten im IS,
- Selbstbedienungssystem für grundlegende IDM-Aufgaben (Passwortänderung, Beantragung/Genehmigung von Zugangsberechtigungen).

Zusätzlich zu den automatischen Aktionen bietet IDM die Möglichkeit, Zugriff auf der Grundlage genehmigter Anfragen zu gewähren. Der Genehmigungsprozess aktiviert die Erstellung der Anfrage und die einzelnen Genehmigenden werden aus der Organisationsstruktur des Unternehmens abgeleitet.

IDM bietet eine zentrale, einheitliche Aufzeichnung aller Zugriffsberechtigungen für alle Informationssysteme des Unternehmens. Um die Konsistenz der Informationen im IDM und im integrierten IS zu gewährleisten, ist eine Rücksynchronisierung der Benutzerberechtigungen erforderlich. Dieser Prozess wird „Reconciliation“, genannt und ermöglicht es, unbefugte Änderungen von Benutzerberechtigungen zu erkennen, die außerhalb der IDM-Lösung vorgenommen wurden.

Dank der „Reconciliation“, sind alle Anwendungskonten mit bestimmten Benutzern verknüpft, so dass alle ihre Aktivitäten schnell und eindeutig identifizierbar sind und eine persönliche Verantwortlichkeit besteht.

Natürlich verfügt IDM auch über eine Auditing-Funktion, die die Registrierung und anschließende Nachvollziehbarkeit von Änderungen in Benutzerdatensätzen gewährleistet.

IDM ermöglicht die Verwendung geeigneter Unternehmensrollen (z.B. Personalverantwortlicher, Buchhalter, Vertriebsmitarbeiter) und abstrahiert damit von spezifischen Anwendungsrollen von Informationssystemen (z.B. write\_erp\_saldo, statement\_history\_bank). Der Grund dafür ist, dass die Verwendung einzelner Anwendungsrollen für professionelle (nicht-IT) Abteilungen nicht intuitiv ist und ihre Arbeitsleistung unnötig erschwert. Auf der anderen Seite ist die Verwendung von klaren benannten Unternehmensrollen – wie es in IDM der Fall ist – wird eine erhebliche Vereinfachung bei allen notwendigen Aufgaben erreicht. Darüber hinaus sind Unternehmensrollen ein effektives Instrument, um die Anhäufung von Berechtigungen zu minimieren, wenn ein Mitarbeiter auf eine andere Position wechselt.

Das Beste an all dem ist, dass es sich nicht um eine Technologie handelt, die aufgrund ihrer Robustheit oder ihrer Kosten nur für große Unternehmen erschwinglich ist. Tatsächlich lässt es sich auch für kleine und mittlere Unternehmen schnell und kostengünstig auf jeder Plattform aufbauen. Viele Kunden, insbesondere im Segment der kleineren Unternehmen, sind besorgt über die finanzielle Komplexität von IDM-Lösungen. Sie sind dann überrascht, dass die Investition nicht in die Millionen geht sondern Hunderttausende. Schließlich muss jedes Unternehmen Arbeitnehmerrechte und -ansprüche verwalten, unabhängig davon, ob es hundert, tausend oder zehntausend Mitarbeiter beschäftigt.

