tenfold

WHITEPAPER

Identity und Access Management Software: Anbieter & Vergleich

Einleitung

Identity- and Access Management (kurz: IAM) versetzt Unternehmen in die Lage, **Identitäten und Zugriffsrechte** auf unterschiedliche Systeme und Applikationen **zentral zu verwalten**. Für diesen Zweck kommen **unterschiedliche Software-Lösungen** zum Einsatz.

Dieses Whitepaper geht auf die beiden dominierenden Produktkategorien im Bereich **IAM-Software** ein und stellt einfache **Data-Governance-Lösungen** und komplexe **Enterprise-IAM-Lösungen** einander gegenüber.

Was ist IAM Software?

IAM Software baut auf der **digitalen Identität** des Nutzers auf. Es geht also primär um die **Authentifizierung** und **Autorisierung** des Benutzers im Netzwerk (und in der Cloud), und die Verwaltung der mit diesem Nutzer **verknüpften** Zugriffsberechtigungen innerhalb des Netzwerks und ggf. für externe Anwendungen.

Das oberste Ziel von IAM Software ist **Security**: Dadurch, dass die Zugriffsberechtigungen **zentral verwaltet** und überwacht werden, **schließt** das Unternehmen **potenzielle Sicherheitslücken**.

Welche Funktionen bietet IAM-Software?

Identity and Access Management kann grundsätzlich eine **Vielzahl von Funktionen** erfüllen, aber nicht alle Funktionen sind für jedes Unternehmen sinnvoll oder produktiv anwendbar. Daher bietet auch nicht jede IAM-Software die gleichen Funktionen. Grundsätzlich kann IAM-Software **folgende Funktionen** abbilden:

Authentifizierung

Der Endbenutzer muss belegen können, dass er derjenige ist, der er zu sein vorgibt. Dies kann über eine Kombination aus **Benutzername und Passwort** (z.B. bei der Anmeldung) erfolgen. Bei großen Enterprise-Lösungen authentifizieren sich die Benutzer häufig mit **biometrischen Daten** (z.B. Fingerabdruck), einer Keycard oder einem Token.

Autorisierung

Nach erfolgreicher Authentifizierung werden dem Benutzer bei der Autorisierung **bestimmte Rechte zugeteilt.** Die Autorisierung bestimmt, auf **welche Ressourcen** ein User im Netzwerk zugreifen kann.

Provisionierung

Die Provisionierung **erstellt**, basierend auf Workflows und Policies, **automatisiert Ressourcen** wie Benutzerkonten und Berechtigungen bzw. ordnet sie diese zu.

Single Sign On (SSO)

Die Funktion SSO sorgt dafür, dass sich Benutzer nur **einmalig authentifizieren** müssen und diese Authentifizierung anschließend für eine Vielzahl von Systemen gültig ist. Eine erneute Anmeldung ist somit nicht mehr notwendig.

Identitätsföderation

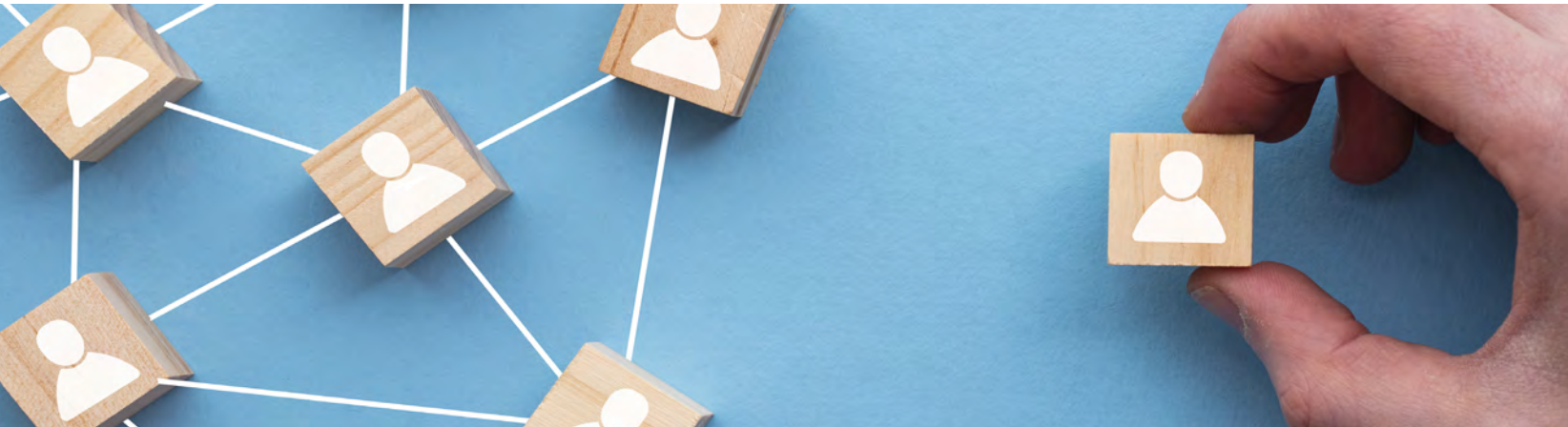
Identitätsföderation sorgt dafür, dass Parteien **Identitätsinformationen** über technische Grenzen hinweg (z.B. zwischen lokaler IT und Cloud) **austauschen** können.

Self-Service

Über eine Self-Service-Funktion kann der Benutzer bestimmte Services selbstständig anfordern. Er kann z.B. **Berechtigungen**, das Ändern von Benutzerdaten oder das **Zurücksetzen des Passwortes** beantragen.

Data Ownership

Unter Data Ownership versteht man die Möglichkeit, für Ressourcen **verantwortliche Manager/ Administratoren** zu definieren, die über den Zugriff entscheiden können.



Workflows

Workflows innerhalb eines IAM steuern die Abläufe. In der Regel unterscheidet man zwischen **Workflows zur Genehmigung** und **Workflows zur Provisionierung**. Ersteres bedeutet, dass ein Verantwortlicher (**Data Owner**) den Zugriff auf bestimmte Daten erlaubt. Letzteres bedeutet, dass **technische Abläufe** in Gang gesetzt werden, um eine **bestimmte Ressource** bereitzustellen.

Rollensystem

Viele IAM-Systeme arbeiten mit einem **rollenbasierten Zugriffssystem**. Dieses sorgt dafür, dass Benutzer ihre Standard-Berechtigungen erhalten. Die Rollen sorgen gleichzeitig dafür, dass Benutzer Berechtigungen **wieder verlieren**, wenn sie sie nicht mehr benötigen. Grundlage für das Rollensystem ist u.a. die **Unternehmensstruktur**.

User Lifecycle Management

User Lifecycle Management bedeutet, dass die Berechtigungen eines Benutzers über dessen gesamten **Lebenszyklus** (vom Eintritt ins Unternehmen bis zum Ausscheiden) automatisiert überwacht und **verwaltet werden**.

IAM Software Lösungen im Vergleich

Grundsätzlich sehen wir im Bereich IAM Software **zwei dominierende Produktkategorien**, die jeweils auf unterschiedliche Zielgruppen ausgerichtet sind:

(1) einfache **Data-Governance-Lösungen**
(2) komplexe, auf Großkonzerne ausgerichtete **Enterprise-Lösungen/IAM-Suites**

(1) Data Governance Software

Bei Data-Governance-Software liegt der Fokus auf **unorganisierten Daten**. Diese Lösungen bringen also **vorübergehend** Ordnung in Ihre Fileserver und helfen bei der Automatisierung bestimmter Tätigkeiten. Allerdings stoßen sie bei der **Standardisierung und Automatisierung** von Workflows an ihre Grenzen.

Dies führt vor allem im Rahmen des User Lifecycle Managements zu Problemen, weil z.B. die Neuanlage eines Benutzers und die damit verbundene Vergabe von Berechtigungen **ebenso zeitaufwändig** ist, als wenn Sie sämtliche Schritte direkt in den jeweiligen Systemen (z.B. im Active Directory) durchführen würden.

Data-Governance-Lösungen fehlt es an Komplexität
Nehmen wir an, ein Unternehmen im **Midmarket-Segment** entscheidet sich für eine **Data-Governance-Lösung**, um z.B. Berechtigungsschwierigkeiten auf Netzwerkfreigaben zu lösen. Folgendes passiert: Die Software bringt **kurzfristig Ordnung** in die Fileserver, allerdings hält diese Ordnung nicht lange an, weil sie lediglich die Symptome, **nicht aber das Grundproblem** der dezentralen Berechtigungsvergabe beseitigt.

Das liegt daran, dass Data-Governance-Lösungen für mittelständische Unternehmen **nicht komplex genug** sind. Sie sind nicht der Lage **Prozesse, Policies und Rollen** so abzubilden, dass es tatsächlich zu einer **nachhaltigen Verbesserung** kommt.

(2) Enterprise-Lösungen/IAM Suiten

Enterprise-Lösungen bzw. **IAM-Suiten** sind auf die komplizierten **Strukturen von Großkonzernen** ausgelegt und können theoretisch unendlich viele Funktionen abbilden. Während Enterprise-Organisationen diese komplexen IAM-Suiten tatsächlich benötigen, um die Vielfalt ihrer Prozesse und Workflows abbilden zu können, sind diese Produkte für kleine und/oder mittelständische Unternehmen in der Regel NICHT geeignet.

Enterprise-Projekte können Jahre dauern
Komplizierte IAM-Suiten sind **nicht darauf ausgelegt**, auf Basis von Best Practices **innerhalb kurzer Zeit in Betrieb** genommen zu werden.

In den meisten Fällen bestehen sie aus **mehreren Einzelprodukten**, deren vollständige **Inbetriebnahme** häufig die zeitlichen, administrativen und finanziellen **Ressourcen** sprengt, die der IT eines mittelständischen Unternehmens zur Verfügung stehen. Häufig bleibt von der geplanten Funktionalität am Ende nur ein Bruchteil übrig, weil Teile der Lösung aufgrund fehlender Ressourcen niemals fertig implementiert wurden.

Die richtige IAM Software wählen

Sie sollten Ihre Identity and Access Management Software nicht nach dem Hersteller auswählen, sondern danach, ob die Software **für den Einsatz in Ihrem Unternehmen** geeignet ist.

Insbesondere für **mittelständische Unternehmen** ist es wichtig, den **Funktionsumfang der IAM-Lösung** genau zu prüfen und sicherzustellen, dass die Software innerhalb eines **angemessenen** zeitlichen (und finanziellen) **Rahmens** implementiert und effektiv genutzt werden kann.

IAM Software für den Mittelstand

In den meisten mittelständischen Unternehmen haben wir es zu **90 Prozent mit standardisierbaren Vorgängen** zu tun, die automatisiert über IAM abgebildet werden können. Alle paar Wochen gesellt sich noch ein **Spezialvorgang** hinzu, der nicht standardisierbar ist **(10 Prozent)**.
Da sich die Anschaffung eines komplexen Enterprise-IAM allein wegen der wenigen Spezialvorgänge nicht rechnet, brauchen mittelständische Unternehmen eine Software, die die Standard-Vorgänge in **kürzester Zeit** und **out-of-the-Box** implementiert und für die wenigen Spezialvorgänge Erweiterungen bietet. Wir sprechen in diesem Zusammenhang auch von **Top down vs. Bottom up.**

Bottom up vs. top down

Identity and Access Management Software für den Mittelstand sollte grundsätzlich nach dem Prinzip **bottom up** funktionieren. Das bedeutet, dass mit dem Standardumfang zunächst die Funktionalitäten für die wichtigsten und am **häufigsten durchgeführten Prozesse** (die berühmten 90 Prozent) zur Verfügung stehen müssen.

Wenn die Möglichkeiten des Standardumfangs erschöpft sind, bestimmte wichtige, nicht änderbare Workflows darin aber nicht abbildbar sind, sollte die Software die **Möglichkeit der Erweiterung** bieten: von unten nach oben.

IAM Software Vergleich – Fazit

Data-Governance-Lösungen befassen sich mit Berechtigungen auf unorganisierten Daten, bieten jedoch k**eine Funktionen für die nachhaltige Verbesserung** von Strukturen und Prozessen.

IAM-Lösungen für Großkonzerne sind **strukturell** wiederum **so komplex**, dass die Implementierung **mehrere Jahre** in Anspruch nehmen kann, die laufende Wartung **entsprechend aufwändig** ist, und jede noch so kleine Anpassung oder Änderung in den Einstellungen **externes Expertenwissen** voraussetzt.

Die Lösung ist eine IAM-Software, die ähnlich schnell implementiert ist wie Data-Governance-Lösungen, aber dem Unternehmen trotzdem jede Funktionalität bieten kann, die die jeweilige Organisationsstruktur erfordert. Diese Lösung heißt tenfold.

tenfold – Vordenker im midmarket-Segment

tenfold ist Next Generation Access Management. Unsere IAM-Software "tenfold" ist speziell an die Bedürfnisse von **mittelständischen Organisationen** angepasst und wir legen besonderen Wert darauf, dass ALLE tenfold-Nutzer, vom IT-Admin bis zur HR-Fachkraft, **effizient** mit der Software arbeiten können. tenfold bietet Ihnen **alle Funktionen** in EINEM Produkt. Das hat folgende Vorteile:

- Ihre Mitarbeiter benötigen nur **eine einzige Schulung**.
- Eine S**ynchronisierung der Daten** zwischen unterschiedlichen Produkten ist **nicht erforderlich**, wodurch wir zusätzliche Fehlerquellen vermeiden.
- Alle Daten sind überall **verfügbar und stets aktuell**.
- Die Benutzeroberfläche und sämtliche Begrifflichkeiten sind **einheitlich.**
- Sie müssen lediglich die Infrastruktur **für *einen* Application Server** zur Verfügung stellen.