

// Identity Management by doubleSlash

Sichere und flexible Verwaltung von Benutzerdaten



Informationsströme lassen sich grundlegend verbessern, wenn digitales Wissen mit Identitäten verknüpft wird. Das Identity Management rückt in den Mittelpunkt jeder Unternehmenssoftware.

1

2

3

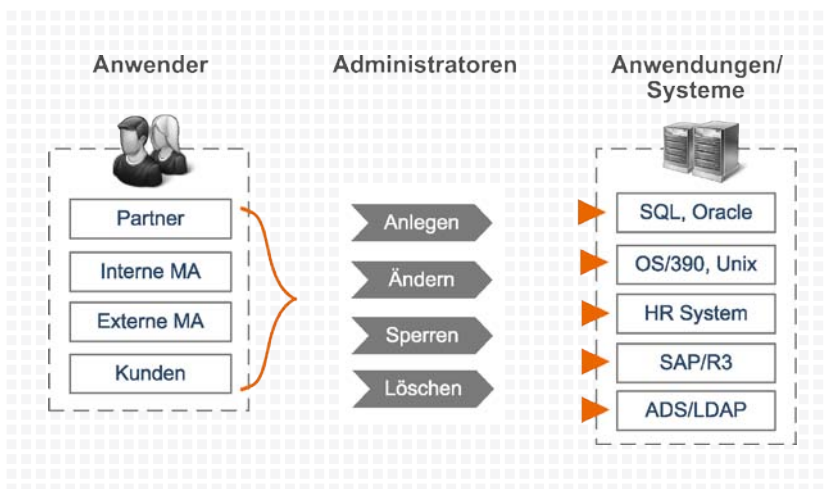
4

5

An die Sicherheitsinfrastruktur von Unternehmen werden immer höhere Anforderungen gestellt. Trotz gewachsener heterogener Systemlandschaften werden Flexibilität und eine einheitliche, zentrale Verwaltung der Benutzerdaten gefordert. Berechtigungen von Kunden, Geschäftspartnern und Mitarbeitern sollen kontrolliert werden können.

Es bedarf einer durchdachten Identity Management Infrastruktur, mit der künftige Anforderungen von Fachabteilungen schnell realisierbar sind.

Die Verwaltung digitaler Identitäten ist die Voraussetzung, um Zugriffsschutz und personalisierte Anwendungen realisieren zu können. Die Frage ist also nicht, ob Identity Management stattfindet, sondern wie sicher und effizient Administrationsvorgänge gestaltet werden können.



Welche Chancen bietet Identity Management?

Wird Identity Management als gelebte Strategie verstanden, ergeben sich Chancen in den Teilbereichen:

- **Access Management** – Definition von Zugriffsberechtigungen und Realisierung von Zugriffsschutz.
- **Auditing** – Revisionssichere, automatische Dokumentation aller Aktionen zur Gewährleistung von Compliance.

- **User Management** – Verwalten von verteilten Benutzerdaten in heterogenen Systemlandschaften.
- **User Provisioning** – Verwalten der Lebenszyklen digitaler Identitäten.
- **Single Sign-On** – Einmaliges Anmelden über alle Webanwendungen hinweg.
- **Identity Federation** – Austausch und lose Verknüpfung von Identitätsdaten für flexiblere Geschäftsbeziehungen und Unternehmensstrukturen.

1. Access Management – Zugriffsschutz auf wichtige Daten

Ein vorausschauendes Access Management unterstützt Sie maßgeblich dabei, dass Ihre Anwender nur auf relevante Daten zugreifen dürfen. Standards wie z. B. RBAC (Role Based Access Control) ermöglichen eine größtenteils automatisierte Rechteverwaltung auf Grundlage der vorher definierten Regeln. Rechte, Rollen, Gruppen und Profile müssen strukturiert, definiert und modelliert werden. Dabei hilft doubleSlash.

2. Auditing – Reporting, Compliance und Billing

Ein intelligentes Auditing ermöglicht, dass Ihre Anwendungen den Anforderungen von Betriebsrat, Revision und staatlichen Behörden bezüglich Datenschutz und Privatsphäre gerecht werden.

- **Reporting** – Durch die Auditing-Funktionalität des Identity Management Systems wird es möglich, Auskunft geben zu können, warum und wann bestimmte Rechte vergeben, wann sie wieder entzogen und welche Zugriffe und Aktionen durch den Benutzer getätigt wurden.
- **Compliance** – Damit wird die Grundlage gelegt, dass Ihre Anwendungen den Anforderungen von Betriebsrat, Datenschutz und staatlichen Behörden gerecht werden.
- **Billing** – Beim Auditing ist zusätzlich möglich, Zugriffe und ausgeführte Aktionen automatisiert zu Kostenstellen zuzuordnen und in Rechnung zu stellen.

3. User Management – Wer ist eigentlich wer?

Kunden, Mitarbeiter und Geschäftspartner müssen heute in vielen Anwendungen ihre persönlichen Daten hinterlegen.

Ob in einem Zeiterfassungssystem, einer Lieferantendatenbank oder einem Reportingsystem – überall werden neben den eigentlichen Benutzerdaten weitere Daten gepflegt. Hierzu gehören Rechnungsdaten, Adressen, Anschriften, persönliche Daten, Profile, Organigramme, Abteilungsbezeichnungen usw.. Mit einem User-Management erhalten Sie die geordnete Übersicht auf alle Benutzerdaten.

4. User Provisioning – damit Veränderungen einfacher werden

Neue Mitarbeiter beginnen ihre Tätigkeit, andere ändern den Standort, wiederum andere verlassen das Unternehmen. Organisatorische Veränderungen sind üblich!

User Provisioning hilft Ihnen, die Anwender der IT-Infrastruktur automatisiert umzuorganisieren. Möglichst schnell werden sie mit allen notwendigen Zugängen ausgestattet. Kennworte müssen nicht mehr von Spezialisten geändert werden. Benutzer werden automatisch in den notwendigen Systemen angelegt. Umgekehrt sorgt Deprovisioning dafür, dass die angelegten Benutzerkonten und Berechtigungen wieder zur rechten Zeit automatisiert gelöscht bzw. entzogen werden.

Gerade wenn Sie viel mit zeitlich befristetem Projektpersonal arbeiten, erleichtert User Provisioning die Organisation der IT-Infrastruktur. Das Projektpersonal benötigt zwar Zugang zu IT-Systemen, dieser Zugang soll jedoch nur projektspezifisch sein und einem festgelegten Zugangsprofil entsprechen.

5. Single Sign-On – ein sicheres Passwort für alle Anwendungen

Die Vielzahl der Passwörter verführt Benutzer dazu, diese zu notieren oder einfache Passwörter zu wählen. Während Letzteres durch Passwortregeln zu umgehen ist, ist Ersteres nur durch die Reduktion der Passwörter oder den Einsatz alternativer Authentifizierungsverfahren in den Griff zu bekommen. Sowohl

Single Sign-On (SSO), als auch starke Authentifizierungsverfahren können Helpdesk-Kosten enorm reduzieren. Single Sign-On bietet Effizienzsteigerung für IT-Abteilungen durch Entlastung von Routineaufgaben, wie dem Rücksetzen von Passwörtern. Bei vergessenen Passwörtern entfallen somit lange Wartezeiten des Benutzers.

Single Sign-On ermöglicht es, dass nur noch ein Login für alle angeschlossenen Anwendungen erforderlich wird. Neben der höheren Benutzerfreundlichkeit wird damit auch die Sicherheit erhöht, da Benutzer eher auf Passwortzettel verzichten, wenn Sie sich nur noch ein Passwort merken müssen. Wir zeigen Ihnen, wie Sie die Anzahl an Passwörtern sukzessive reduzieren und zu einem einfachen SSO-System kommen.

6. Identity Federation – digitale Identitäten im Verbund

Der einzelne Anwender muss sich täglich wiederholt bei verschiedenen Sicherheitsdomänen anmelden. Das ist nicht nur aufwendig und anfällig für Fehler, sondern unterbricht auch den Arbeitsfluss. Mit Identity Federation besteht die Möglichkeit, standardbasierte Benutzeridentitäten und Zugriffsberechtigungen mit Ihren Geschäftspartnern auszutauschen. So können Sie beispielsweise aus Ihrer internen Web-Anwendung heraus sicher und ohne erneute Authentifizierung auf die Systeme Ihrer Lieferanten und Händler zugreifen.

Eine Identity Infrastruktur wird nicht von heute auf morgen föderationsfähig, auch wenn Fertigprodukte auf den ersten Blick oft diesen Eindruck erwecken. Als Technologie die hilft, den Time-to-Market zu verbessern, Transaktionskosten zu reduzieren und damit neue Geschäfte ermöglicht, ist Identity Federation vielversprechend. Unternehmen profitieren davon, ihre Identity Management Architektur in Einzelschritten mit eigenem Mehrwert für Federation zu rüsten, um zukünftigen Entwicklungen gewachsen zu sein. Unter Umständen genügt für Ihr Unternehmen vorerst, die Infrastruktur durch sanfte Migration anzupassen, sodass diese sich später leicht um Federation-Schnittstellen erweitern lässt. Hierbei stehen wir Ihnen gerne mit Rat und Tat zur Seite!

Identity Management aus der Praxis

Aufgrund der hohen Individualität verschiedener Systemlandschaften ist Identity Management kein Thema, das mit einem Fertigprodukt abgedeckt werden könnte – auch wenn Hersteller dies gern anders darstellen. Wir betrachten Identity Management als ein strategisch-fachlich getriebenes Vorgehen und nicht als fertiges „Out of the Box“ Produkt. Eine zukunftsweisende Strategie kommt nicht ohne genaue Analyse der individuellen Problematik und entsprechender Lösungskonzeption aus. Häufig besteht die Lösung in einer flexiblen zukunftssicheren Architektur oder in einfachen organisatorischen Maßnahmen. Aus diesem Grund setzt doubleSlash nicht auf Produktlösungen Dritter, sondern auf solide Softwarekomponenten aus dem eigenen Haus, welche sich in der Praxis mehrfach bewährt haben.

Vor allem durch technische Standards wie WS-Federation, SAML, SPML und XACML gewährleisten wir Kunden größtmögliche Unabhängigkeit vom Hersteller. Als Softwareintegrator ist doubleSlash gerade bei neuen Entwicklungen darauf spezialisiert, vorhandene Identitätssilos reibungslos anzubinden. Dabei stellt sich immer wieder die Frage, ob Identity Management Benutzerdaten zentral konsolidieren oder dezentral virtualisieren sollte. doubleSlash setzt beide Strategien kombiniert ein. Wo eine Konsolidierung aus organisatorischen Gründen nicht möglich oder wünschenswert ist, kann durch Synchronisation die Datenkonsistenz und durch Virtualisierung die einheitliche Administration gewährleistet werden. Virtualisierung nutzen wir zur nahtlosen und unmerklichen Migration von Datenpools. Dies ist ein entscheidender Vorteil, wenn es darum geht ein Identity Management ohne für die Benutzer spürbare Baustellenbelastungen einzuführen.

Das gelingt umso besser, wenn ein Identity Management in Kombination mit einem operativen Mehrwert eingeführt wird. Mit unserer Softwarelösung Identity Manager schaffen wir die gesunde Basis zur sukzessiven Integration fachlicher Webanwendungen. So funktioniert Identity Management aus der Praxis für die Praxis. Überzeugen Sie sich!

Kontakt

Sprechen Sie mit uns über unsere Projekte und Ihre Ideen! Oder besuchen Sie uns in Friedrichshafen.



Oliver Belikan
Tel.: +49 7541 70078-0
info@doubleSlash.de
www.doubleSlash.de



Referenzen, die für sich sprechen

