Identity & Access Management beginnt mit der Personalabteilung

Ein neuer Mitarbeiter - ein neuer Personalbogen, der ausgefüllt wird. Diese Formulare enthalten die meisten Informationen, die für die Erstellung und Verwaltung eines neuen Benutzerkontos benötigt werden. Diese Formulare erfassen unter anderem personenbezogene Daten wie Vertragsbeginn und -ende, Position, dessen Vorgesetzter und die Abteilung. Identity-Management-Prozesse können vollständig automatisiert werden, indem diese Personaldaten mit dem Rest des Netzwerks verknüpft werden. Mit einem Klick kann Ihre IT-Abteilung einige der aufwändigsten Aufgaben der Benutzerkontenverwaltung einsparen.

Zunehmend werden in Unternehmen Richtlinien und Prozeduren eingeführt, die die Personalsysteme automatisch als die zentrale Datenquelle für Identity and Access Management Prozesse positionieren. Die Personalabteilung besitzt qualitativ hochwertige und aktuelle Daten, die ein Unternehmen optimal für weitere Identity and Access Management Prozesse verwenden kann. Alle anderen verknüpften Systeme können ihre Daten mit der zentralen Personalverwaltung synchronisieren - die perfekte Grundlage für ein professionelles Identity- und Access-Management.

Durch eine Vielzahl von zertifizierten Partnern verbindet sich die IAM-Lösung von Tools4ever mit allen gängigen Personalsystemen. Dazu gehören unter anderem SAGE, P&I LOGA, ADP und SAP HCM/ HR. IAM erkennt jede Änderung im Personalsystem automatisch und synchronisiert die notwendigen Änderungen mit Ihrem Netzwerk. Die Datenerfassung von IAM und die entsprechenden Prozesse erfolgen wie folgt:

Personalveränderung	Prozess in IAM
Onboarding/ User-Provisioning	IAM erstellt eine Mitarbeiter-Identität, das Benutzerkonto im AD, das E-Mail-Postfach und das Homeverzeichnis eines neuen Mitarbeiters nach dem Access Governance (AG)- Modell. IAM erstellt die Benutzerkonten und Zugriffsrechte in Downstream-Systemen (z.B. SAGE, P&I LOGA, ADP und SAP). IAM bietet mehr als 150 Schnittstellen.
Updates/Reprovisioning	Wenn IAM Änderungen an der Identität eines Mitarbeiters erkennt, synchronisiert es die Updates, um anschließend die Zugangsrechte entsprechend anzupassen. Das Access Governance-Modell wird automatisch herangezogen, um die konfigurierten Berechtigungen für eine bestimmte Rolle hinzuzufügen und zu entfernen.
Deaktivierung/Offboarding	Nach Beendigung wird das Benutzerkonten phasenweise deaktiviert und in eine andere OE verschoben.
Namensänderung (z.B. Heirat/ Scheidung)	IAM passt den Benutzernamen und die E-Mail-Adresse automatisch an.

DER SICHERE LINK ZWISCHEN PERSONALABTEILUNG UND IAM

Neuer Mitarbeiter direkt produktiv

Durch die Anbindung des Personalsystems an die Benutzerkonten im Netzwerk werden Änderungen sofort und fehlerfrei umgesetzt. Das Konto wird am ersten Arbeitstag eines Mitarbeiters angelegt und der Mitarbeiter kann sofort mit der Arbeit beginnen. IAM wird standardmäßig mit einem Berechtigungsmanagementmodell (Access Goverance/RBAC ausgeliefert, so dass ein Mitarbeiter bei seinem Eintritt in das Unternehmen sofort die richtigen Berechtigungen erhält, die zu seiner Funktion gehören.

Bidirektionale Übermittlung

Neben dem Auslesen von Informationen aus dem Personalsystem können auch regelmäßig Informationen zurückgemeldet werden, wie z.B. die von IAM generierte E-Mail-Adresse des Mitarbeiters oder eine Telefonnummer.

Sicherheit / Auditing

Updates/Reprovisioning: Einer der wichtigsten Gründe mit einer Identity- und Access Management-Lösung im Rahmen der Compliance zu arbeiten, ist die Vermeidung von gewachsenen Berechtigungsstrukturen. Dank detaillierter Berichte über die bestehenden bzw. zu vielen Berechtigungen lässt sich die gewachsene Berechtigungsstruktur für kommende Audits einfacher überblicken. So erkennen Sie in wenigen Klicks, welcher Benutzer mehr Rechte und Ressourcen als unbedingt erforderlich besitzt. Das Ergebnis sind z.B. niedrigere Lizenzenkosten. Mit der Nutzung von User-Provisioning (automatisiertes On- und Offboarding verhindert IAM, dass Benutzer mehr Zugriffsrechte besitzen, als unbedingt erforderlich, indem Berechtigungen basierend auf dem konfigurierten AG-Modell hinzugefügt und entfernt werden.

Beendingung des Arbeitsverhältnisses: IT-Abteilungen werden oft später oder erst gar nicht informiert, wenn Mitarbeiter das Unternehmen verlassen. Die aktiven Benutzerkonten des Ex-Mitarbeiters führen so zu potentiellen unberechtigten Zugriffen. Eine Nicht-Deaktivierung führt dazu, dass ehemalige Mitarbeiter noch lange Zeit nach ihrem Austritt, Zugriff auf Unternehmensinformationen haben. Zudem werden oft teure Lizenzen reserviert für Mitarbeiter, die schon längst ausgeschieden sind.

Return on Investment (ROI)

In vielen Unternehmen dauert das Anlegen, Ändern und Löschen von Benutzerkonten mindestens 30 Minuten, teilweise sogar bis zu mehreren Stunden. Durch die Implementierung von IAM sinkt der Aufwand für den Systemadministrator und/oder Help-Desk Mitarbeiter auf Null. In einem Unternehmen mit 1.000 Mitarbeitern kann dies schnell zu einer erheblichen Entlastung der IT Abteilung führen. Zusätzlich wird durch die Automatisierung die Fehlerquote reduziert.

Bieten Sie dem Unternehmen erweiterte Funktionen an

Im Personalsystem stehen viele Informationen zur Verfügung, die Prozesse in einem Unternehmen verbessern können. Beispielsweise ist es, durch die Verbindung zwischen Arbeitnehmern und Managern im Personalsystem möglich, einen Vorgesetzten per E-Mail über ein neu angelegtes Benutzerkonto mit den genauen Angaben des betreffenden Mitarbeiters zu informieren. Dies ermöglicht eine Verknüpfung zwischen dem Vorgesetzten und dem neuen Mitarbeiter, die im Personalsystem hinterlegt ist. Umgekehrt kann im Falle eines Austritts auch wieder automatisch eine E-Mail an den Vorgesetzten des Mitarbeiters weitergeleitet werden.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Tools4ever Informatik GmbH
Hauptstraße 145-147
51465 Bergisch Gladbach
+49 2202 2859 200
sales@tools4ever.de