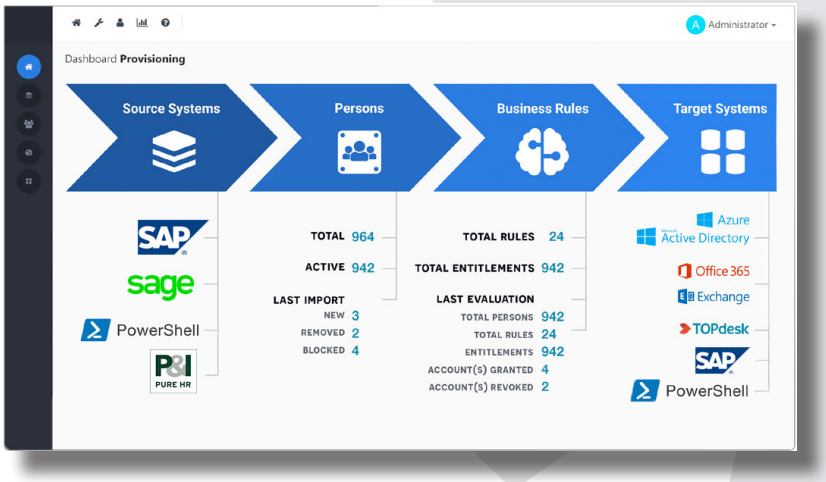
HelloID

Provisioning

manuell vs. automatisiert



Jede IT-Abteilung stößt beim User Lifecycle Management irgendwann an ihre Grenzen. Unaufhörlich müssen User-Konten erstellt, geändert und gelöscht werden. Gleiches gilt für die zugehörigen Berechtigungen auf unterschiedlichste Anwendungen in einer hybriden IT-Umgebung – und zwar ohne lange Verzögerungen. Die IT hat 2 Möglichkeiten diesen Prozess namens User Provisioning zu bewältigen: manuell oder über eine automatisierte Provisioning-Lösung.

Manuell

Manuelles Provisioning geschieht oft ad hoc und unstrukturiert. Die Personalabteilung sendet per Ticket oder E-Mail eine Anfrage für ein neues Benutzerkonto an die IT-Abteilung. Ein IT-Administrator vergibt die benötigten Berechtigungen für

- Active-Directory- oder Azure-Konten
- E-Mail-Accounts
- Netzwerkordner und Dateifreigaben
- Gruppenmitgliedschaften, -berechtigungen
- Software-Lizenzen (Office 365, SAP etc.)

Bei Beförderungen, Versetzungen, Projektmitarbeit , Kündigungen usw. müssen Konten und Rechte angepasst bzw. unbedingt zeitnah entzogen werden. Darüber hinaus soll die IT für zyklische Audits Berechtigungen inventarisieren und bzgl. Compliance-Vorgaben überprüfen.

Für IT-Teams, die ohnehin mit Ausfällen, bug-fixes und Remote-Support beschäftigt sind – ganz zu schweigen von Innovationen – bedeutet das nie endende, vermeidbare Routinearbeit.

Jeder manuelle Änderungsprozess stellt außerdem eine potenzielle Fehlerquelle dar: wenn die Personalabteilung versäumt, einen Austritt an die IT zu kommunizieren oder die IT aufgrund fehlender Infos nicht alle relevanten Berechtigungen erteilt.

Solche Versäumnisse sind keine Seltenheit und für alle Beteiligten frustrierend, weil Mitarbeiter ohne korrekte Zugänge unproduktiv sind und der HR- und IT-Abteilung doppelte Arbeit entsteht. Noch schädlichere Auswirkungen und ein enormes Compliance- und Sicherheitsrisiko birgt die übersprungene De-Provisionierung: eine schleichende Anhäufung von User-Rechten und nie entzogener Zugriff für ehemalige Mitarbeiter.

Automatisiert

Eine automatisierte Provisioning-Lösung (heutzutage aufgrund der Zukunftsfähigkeit in der Regel ein IDaaS-Tool) löst all diese Probleme. Sie gewährt, ändert und widerruft Berechtigungen automatisch auf Grundlage der Änderungen im Personalsystem. Manuelle Eingriffe durch die IT werden so weit wie möglich vermieden.

Der Provisioning-Prozess

1. Die Provisioning-Lösung wird mit einem Quellsystem verbunden, typischerweise das HR-System. Generell kann aber jedes System, sogar eine CSV-Datei genutzt werden.

2. Mehrere Zielsysteme, in denen Benutzer Berechtigungen benötigen, werden an die Provisioning-Lösung angebunden: z. B. Active Directory, Salesforce, Office 365, SAP etc.

3. Im nächsten, wichtigsten Schritt werden Business Rules entwickelt. Diese Logik bestimmt, wie die importierten Personaldaten kombiniert und verarbeitet werden soll: Welches Attribut im Quellsystem gewährt welche Berechtigung im Zielsystem?

4. Einmal konfiguriert, überwacht die Provisioning-Lösung das Quellsystem und modifiziert automatisch alle Zielsystemkonten entsprechend.

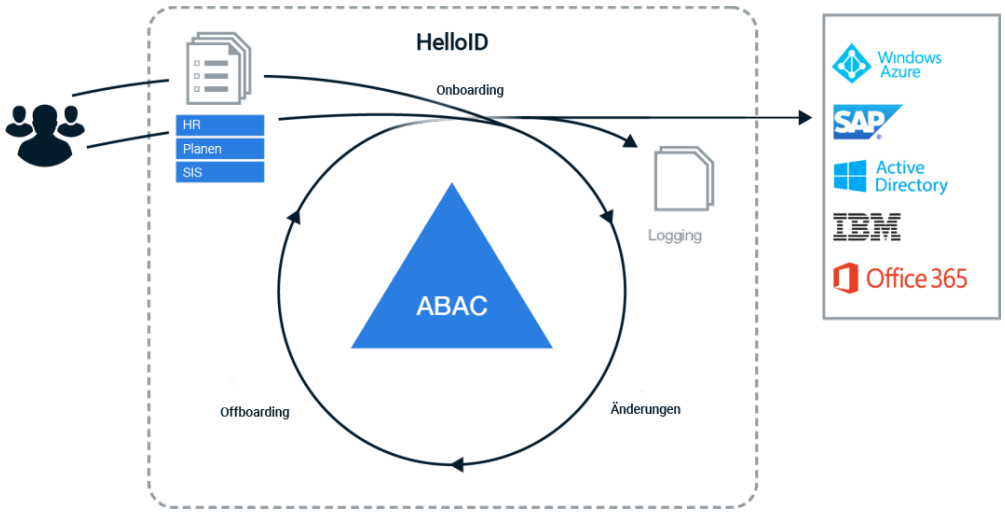
Flexibilität ist hierbei oberstes Gebot. Viele Unternehmen verwenden eine große Anzahl von Legacy- und/oder proprietären Quell- und Zielsystemen. Daher unterstützt jede gute Provisioning-Lösung die Entwicklung benutzerdefinierter Konnektoren und das Mapping komplexer Attribute.

Starten Sie sofort

Mit einer Out-of-the-Box IDaaS-Lösung für User Provisioning brauchen Sie nur wenige Stunden mit einem geschulten Consultant, der die Provisioning-Software mit Ihren Quell- und Zielsystemen verknüpft, egal ob On-Premise oder schon in der Cloud. Attribute Mapping und Rollendefinition können selbst von der IT-Abteilung eingepflegt und nach Bedarf angepasst werden.

Die Produktivsetzung kann im Anschluss an die Einrichtung phasenweise erfolgen. Denken Sie zum Beispiel an ein Go-Live pro Abteilung oder Bereich unter Verwendung der bis dahin fertiggestellten Business Rules. Sie müssen nicht befürchten, dass Ihre Mitarbeiter durch die Produktivsetzung ihre Arbeit nicht mehr ausführen können. Eher wird die IT-Abteilung sofort eine Entlastung spüren und sich noch besser um die folgenden Schritte kümmern können.

Im Vergleich zu manuellem Provisioning sind automatisierte Lösungen schnell, effizient, fehlerfrei und kostengünstig. Sie befreien das IT-Personal von Routinearbeiten, schaffen Zeit für wirkungsvollere Projekte. Da alle Änderungen auf Basis eines unternehmenspezifischen Regelwerks automatisch vergeben werden, geschieht Provisioning immer nachvollziehbar, transparent und vollständig. Kein User wird vergessen, die IT kann jederzeit sagen, wer warum welche Rechte hat. Durch phasenweise Implementation sind die Vorteile von automatisiertem Provisioning sofort spürbar:



Business Rules entwickeln

Die Entwicklung von Business Rules, einem regelbasierten Zugriffsmodell für die Organisation, ist der wichtigste Schritt zur erfolgreichen Einführung von automatisiertem Provisioning und verdient eine genauere Betrachtung. Das Ziel ist die Entwicklung einer „Matrix“, die alle Business Roles im Unternehmen auf entsprechende Zugriffsrechte abbildet. Auf diese Weise können Berechtigungen auf strukturierte Weise bestimmt und vergeben werden.

Am häufigsten wird die RBAC- oder ABAC-Methodik (Role-Based Access Control | Attribute-Based Access Control) verwendet. Hierfür werden im ersten Schritt grundlegende Business Roles und Verantwortlichkeiten identifiziert. Für die meisten Organisationen bietet sich dafür der Pyramiden-Ansatz an.

1. Zunächst werden an oberster Stufe der Pyramide die Rechte definiert, die jeder Mitarbeiter der Organisation (evtl. aufgeteilt nach Standort) benötigt: z. B. Anmeldung über das Active Directory, Zugriff auf Intranet, Office-Suite, E-Mail-Client, gemeinsames Netzwerkverzeichnis.

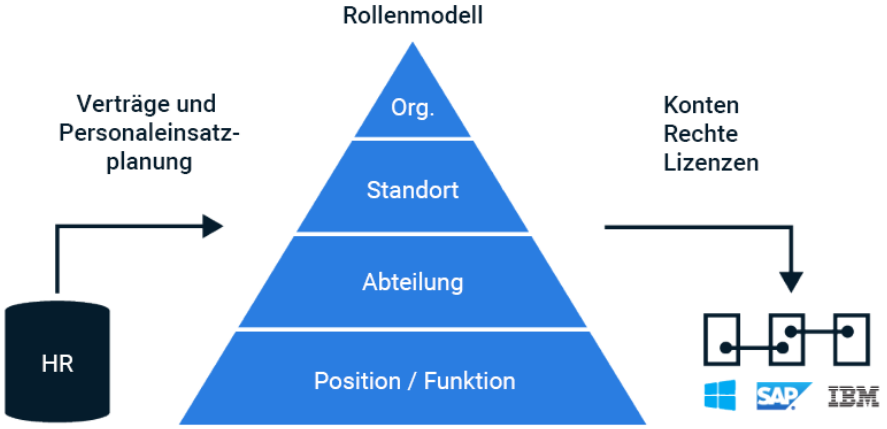
2. An folgender Stufe der Berechtigungspyramide steht die Abteilungszugehörigkeit. Hier werden beispielsweise Zugriff auf Abteilungslaufwerke oder Nutzungsrechte des ERP-Systems für die Buchhaltung festgelegt. Für die Radiologie-Abteilung eines Krankenhauses kann hier definiert werden, dass Zugriff auf Patientenakten oder ein Zugangschip für die entsprechenden Räume benötigt wird.

3. Je nach Position/Funktion des Mitarbeiters innerhalb der Abteilung werden die Berechtigungen genauer definiert und erweitert. Zum Beispiel kann der Abteilungsleiter weitreichende Genehmigungsrechte innerhalb des ERP-Systems innehaben, während dem Sachbearbeiter automatisch nur Bearbeitungsrechte auf Rechnungsebene gewährt werden.

4. Schließlich werden diese Rollen je nach Bedarf übereinandergelegt. Eine Krankenschwester in der chirurgischen Abteilung erhält beispielsweise sowohl die Rolle „Krankenschwester“ als auch die Rolle „Chirurgie“ und wird mit beiden Berechtigungssätzen ausgestattet.

Auf diese Weise wird die RBAC-Matrix fortschreitend pyramidenförmig aufgebaut und phasenweise, z. B. pro Abteilung unter Verwendung der bis dahin fertiggestellten Business Rules produktiv gesetzt. Das schafft sofort eine Entlastung für die IT-Abteilung.

In den meisten Organisationen kann 80 % der RBAC-Matrix mit den 50 wichtigsten Rollenkombinationen definiert werden. Dies ist ein einmaliger Einrichtungsaufwand, der sich über die gesamte Lebensdauer der Provisioning-Lösung auszahlt. Die verbleibenden 20 % an Detailberechtigungen werden von den Managern vor Ort individuell festgelegt. Um die IT weiter zu entlasten, können hierfür Workflows und Self-Service genutzt werden. An diesem Punkt funktioniert die automatisierte Provisioning-Lösung auf Basis von Business Rules optimal.



Tools4ever.de
sales@tools4ever.de
Tel. +49 2202 2859-200