TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Strategiepapier

So geht Identity Management heute

Das Personalsystem als Basis für automatisiertes und regelbasiertes User Lifecycle Management

Identity Management

Der Schlüssel zu mehr Effizienz und Datensicherheit innerhalb Ihrer Organisation!

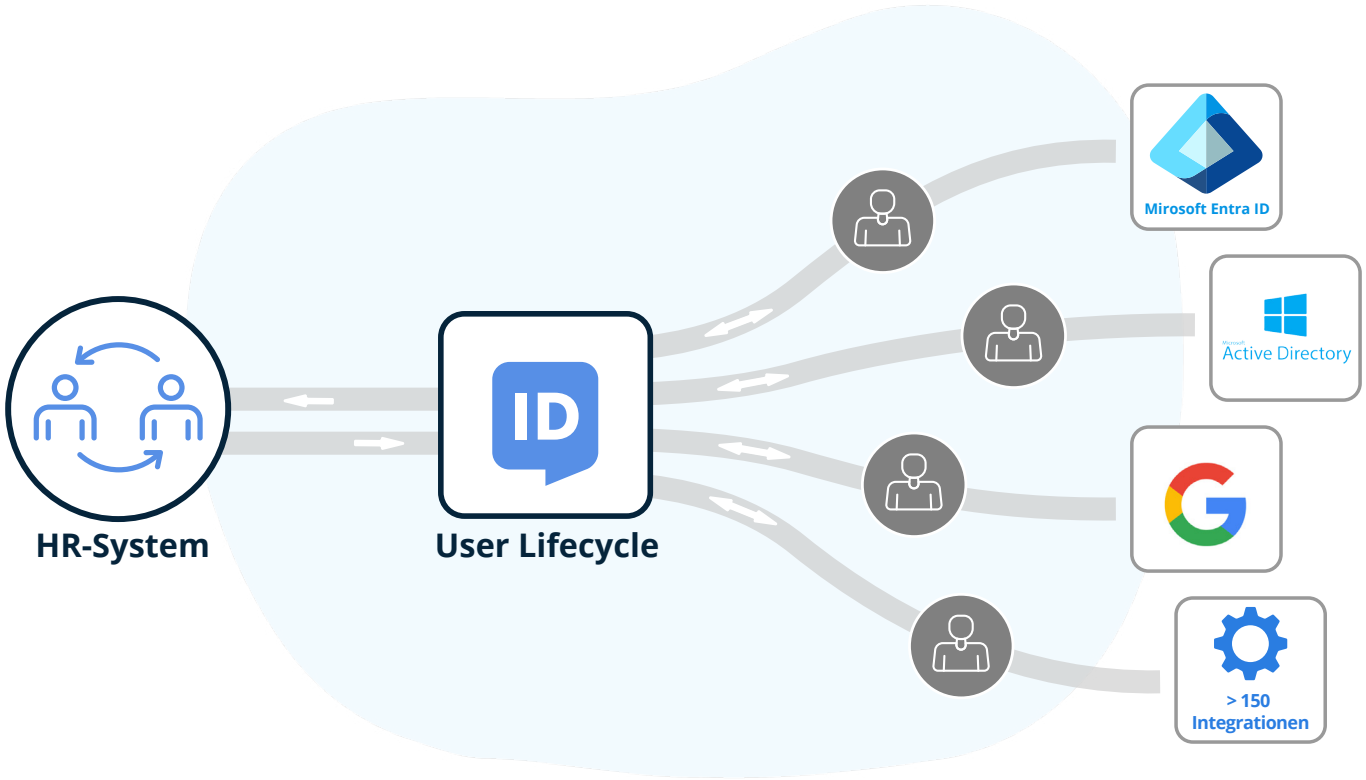
Mit der fortschreitenden Digitalisierung haben sich die Arbeitsbedingungen in den vergangenen 20 Jahren drastisch gewandelt. Ein Arbeitsplatz ist nicht gleich ein Arbeitsplatz, denn die Definition der Begrifflichkeit gleicht nicht mehr der allgegenwärtigen Definition: Die Bedeutung von „Platz“ in dem Wort „Arbeitsplatz“ ist mittlerweile variabel geworden. Mitarbeiter haben die Möglichkeit unabhängig zu sein und nicht nur im Büro, sondern auch Zuhause, im Zug, sogar am Strand - einem x beliebigigem Ort ihrer Wahl - zu arbeiten und das mit mehreren Geräten.

In unserer heutigen, digitalen Welt brauchen die Mitarbeiter zu jeder Zeit und von überall Zugang zu Ihren Daten und Systemen, die sie für Ihre Arbeit benötigen - einfach, schnell und sicher.

Eine enorme Herausforderung für die IT-Abteilung und für das Management. Für die IT-Abteilung ist die manuelle Verwaltung der Useraccounts, Zugänge und deren Berechtigungen organisatorisch extrem aufwendig, technisch komplex und anfällig für Fehler. Das Management ist sich darüber im Klaren: eine fehlerhaft gepflegte Zugangs- und Berechtigungsstruktur kann zu unnötigen Kosten, negativen IT-Audits, Reputationsschäden, Verlust von Daten, -Umsatz und -Kunden sowie unzufriedenen Mitarbeiter führen.

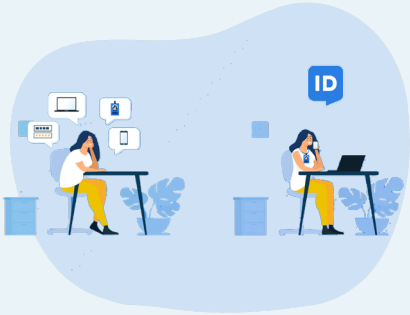
Zudem bieten die Daten in Ihrem Personalsystem eine perfekte Grundlage für eine automatisierte, regelbasierte und fehlerfreie Benutzerverwaltung. Entlasten Sie Ihre IT und erhöhen Sie zeitgleich die Datensicherheit in Ihrem Netzwerk! Wie das bei Ihnen im Unternehmen funktionieren wird und was wichtig zu erfahren ist, lesen Sie in diesem Magazin.

So geht Identity Management heute!



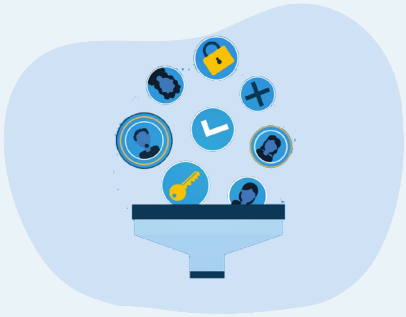
Identity & Access Management startet in der Personalabteilung

Manuell vs. Automatisiert



Ein perfekter erster Arbeitstag

5 Gründe für automatisiertes Offboarding



Intelligentes Role Mining: ein Booster für die rollenbasierte Zugriffskontrolle

Identity- und Access-Management startet in der Personal-abteilung

Das Personalmanagement spielt in vielen Unternehmen eine zunehmend wichtige Rolle. Und das ist auch völlig nachvollziehbar, schließlich sind Menschen ihr wichtigster Erfolgsfaktor. Daher werden inzwischen erhebliche Investitionen in die Personalstrategie und die Professionalisierung von Personalprozessen und -systemen getätigt.

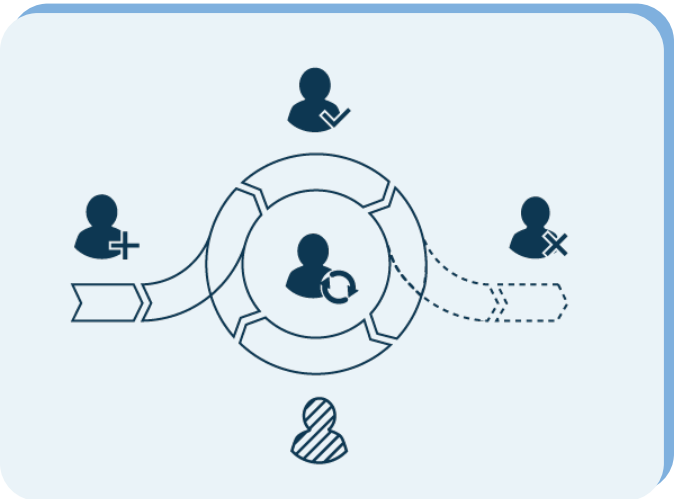
Ein schöner Nebeneffekt davon ist die Ausweitung dieser Professionalisierung der HR auch auf andere Geschäftsprozesse. So können Sie beispielsweise ein modernes HR-System als Ausgangspunkt für die Automatisierung Ihres Identity- und Access-Managements nutzen und damit Ihren gesamten IT-Betrieb benutzerfreundlicher, effizienter und sicherer gestalten. Wir zeigen Ihnen, wie das geht!

Die Bedeutung eines automatisierten Identity- und Access Managements

Viele Arbeitnehmer sind fast immer online und nutzen täglich Dutzende Anwendungen – das gilt nicht mehr nur für reine „Bildschirmarbeiter“. Heutzutage haben auch der Lagerarbeiter, der Pfleger am Krankenbett oder der Fahrer hinter dem Steuer direkten Zugriff auf ihre Anwendungen und Daten. Gerade bei diesen Usern ist die Benutzerfreundlichkeit entscheidend. Sie müssen in der Lage sein, ihre Arbeit mit einem Klick oder einer Wischbewegung zu erledigen. Gleichzeitig darf das nicht auf Kosten der Sicherheit und der Privatsphäre passieren. Mitarbeitende sollten nur auf die Daten zugreifen, die sie tatsächlich für ihre Arbeit benötigen. Außerdem kommt es darauf an, wann, wo und über welches Gerät jemand Zugang beantragt. Deshalb muss jeder Mitarbeiter unbedingt sein eigenes Benutzerkonto haben.

Wenn Sie diese Konten für Hunderte oder gar Tausende von Mitarbeitern verwalten müssen – mit unterschiedlichen Zugriffsrechten und Einstellungen für jeden Mitarbeiter – wird Ihnen schnell klar, dass Identity- und Access-Management ein komplizierter Prozess ist. Das Letzte, was wir wollen, ist, dass Identity und Access-Management zu einem neuen Engpass in Ihrer IT-Landschaft wird. Es sollte stattdessen die Digitalisierung vereinfachen und sie nicht noch komplexer machen. tisch verarbeiten. Und wir können sie and das Active Directory sowie möglichst viele andere Geschäftsanwendungen weitergeben – ohne jegliche manuelle Arbeit.“

Was läge also näher, als diesen Prozess so weit wie möglich zu automatisieren und das HR-System als Quelle zu nutzen? Ewout van Rootselaar vom Marktführer Tools4ever erklärt: „Das HR-System dient ja dazu, Mitarbeiter zu registrieren, ihre Versetzungen zu verfolgen und auch ihr Ausscheiden zu erfassen. Durch die Verknüpfung des HR-Systems mit unserer Identity- und Access-Management-Plattform können wir nun die Daten von neuen und ausscheidenden Mitarbeitern sowie Versetzungen vollautomatisch verarbeiten. Und wir können sie and das Active Directory sowie möglichst viele andere Geschäftsanwendungen weitergeben – ohne jegliche manuelle Arbeit.“

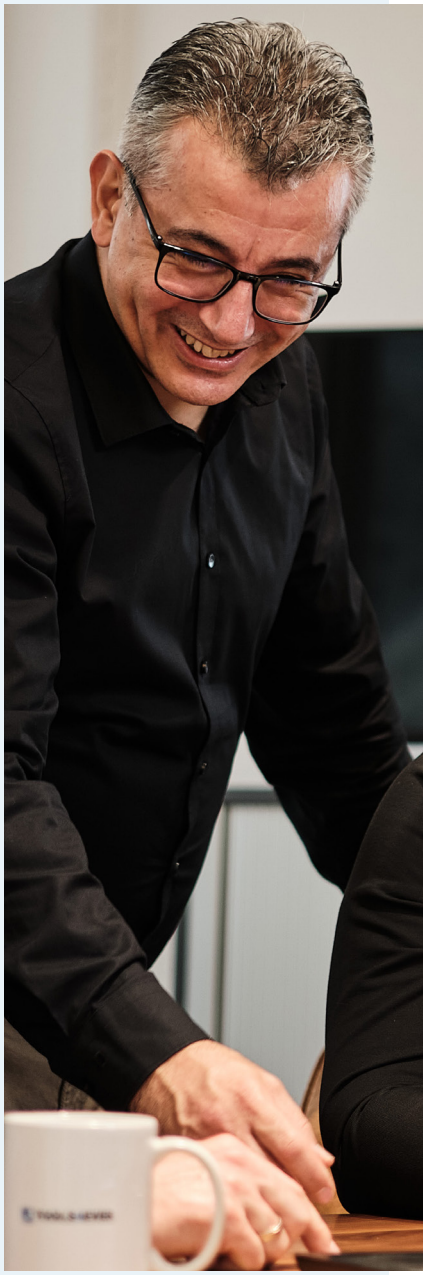


Neue Rolle für das HR-System

Dies erfordert natürlich eine neue Sicht auf die HR-Organisation. Traditionell ist der Aufgabenbereich der Personalabteilung auf die eigenen Mitarbeiter mit unbefristeten Arbeitsverträgen beschränkt. Sie ist oft noch nicht für flexible Einstellungen zuständig.

Gleichzeitig greifen die Unternehmen immer häufiger auf diese flexiblen Mitarbeiter zurück – von Interim-Managern und Fachkräften bis hin zu Gastronomiepersonal und anderen Zeitarbeitskräften. Auch Einrichtungen des Gesundheitswesens sind oft auf zahlreiche Freiwillige angewiesen. Durch die Einbeziehung dieser Mitarbeiter in den HR-Prozess professionalisieren Sie nicht nur die Personalverwaltung dieser immer wichtiger werdenden Mitarbeitergruppe. Sie können sie dann auch vollautomatisch mit einem eigenen Benutzerkonto ausstatten. Gerade bei dieser Gruppe mit ihren vielen Veränderungen und der hohen Fluktuation ist es wichtig, dass ihre Konten effizient, fehlerfrei und sicher geführt werden.

Der Business Case



“Indem wir so viele Mitarbeiter wie möglich im HR-System registrieren, und dieses mit der Identity- und Access-Management-Plattform verbinden, können wir die Verwaltung der Benutzerkonten oft vollständig automatisieren.” Was bedeutet das für die IT und die Organisation? Ewout van Rootselaar von Tools4ever gibt einen Überblick:

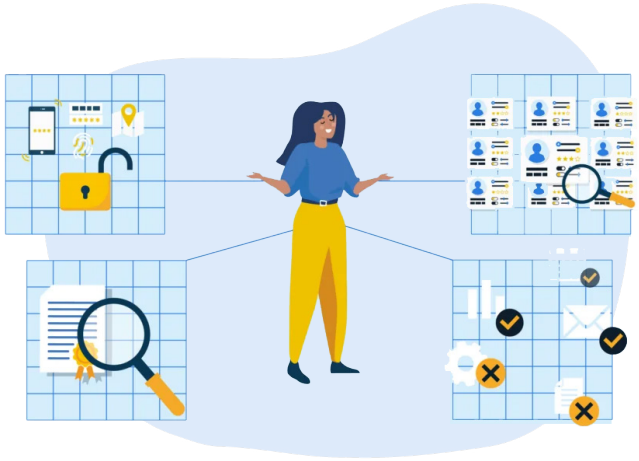
„In vielen Unternehmen dauert das Anlegen, Ändern und Löschen von Benutzerkonten mindestens 30 Minuten ‚pro Ticket‘. Durch die Verknüpfung des HR-Systems mit unserer Identitätsmanagement-Plattform ist der Aufwand für den Systemadministrator und/oder Helpdesk-Mitarbeiter praktisch gleich Null. Unserer Erfahrung nach lohnt sich der Einsatz eines Identity- und Access- Management-Tools für Unternehmen mit 200 Mitarbeitern oder mehr.

Und das betrifft nur die reinen Effizienzvorteile. Darüber hinaus können Sie oft enorme Einsparungen bei Ihren Lizenzkosten erzielen. Unternehmen vergeben häufig schnell neue Lizenzen an ihre Mitarbeiter, wenn beispielsweise jemand eine Anwendung für eine bestimmte Aufgabe oder ein Projekt benötigt. Die Lizenzen werden nur selten entzogen, wenn der Arbeitnehmer sie nicht mehr benötigt. Diese ständige Anhäufung von Lizenzen und Zugängen führt oft unbemerkt zu enormen Kosten. Durch die automatische Verwaltung der Konten und der damit verbundenen Zugänge können Sie enorme Einsparungen erzielen.

Auf diese Weise sind sie auch automatisch mit den bestehenden strengen Datenschutzvorschriften konform. Indem Sie die Konten und Zugänge einer Person automatisch und regelbasiert verwalten, garantieren Sie, dass Mitarbeiter nur Zugriff auf Daten haben, die sie auch wirklich für Ihre Arbeit bruchen. Außerdem verringern Sie die Gefahr, dass ehemalige Mitarbeiter unbefugten Zugriff auf persönliche Kunden- oder Mitarbeiterdaten erhalten. Die Bedeutung dieses Themas ist enorm. Im Falle eines Datenlecks kann die deutsche Datenschutzbehörde Geldstrafen von bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes verhängen. Ganz zu schweigen von der möglichen Rufschädigung und weiteren Schadensersatzforderungen.

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.



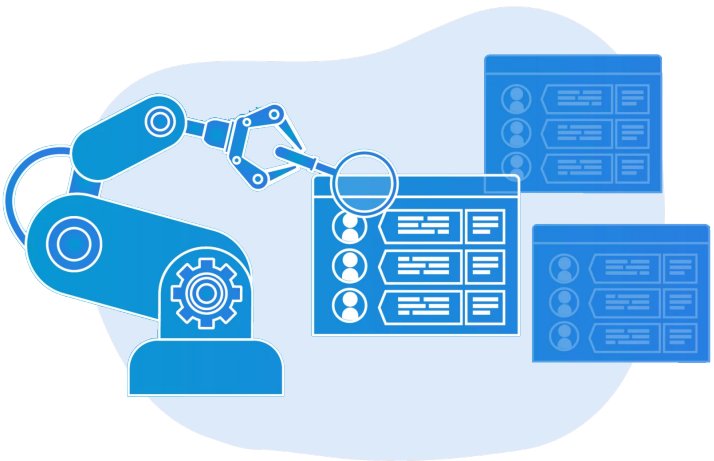
Manuell

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 jede intern kontrollierte IT-Ressource von Hand. 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. Eine 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, welches Attribut aus den Personaldaten welche Berechtigungen im Zielsystem gewährt?

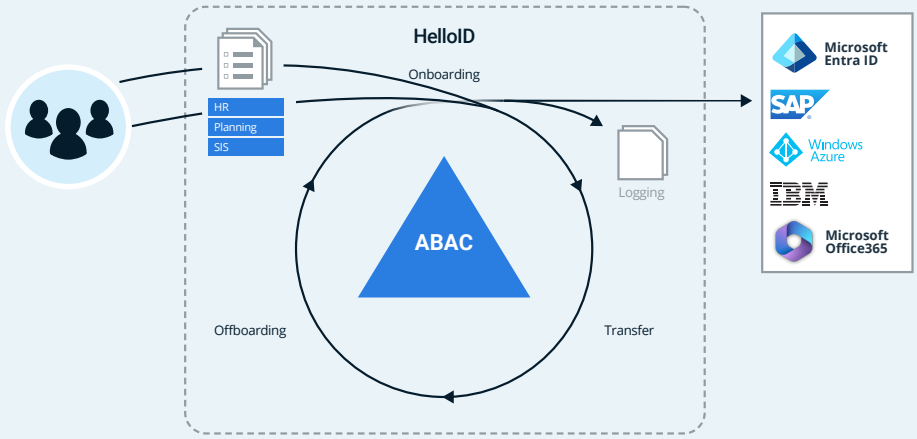
4. Einmal konfiguriert, überwacht die Provisioning-Lösung das Quellsystem und modifiziert automatisch alle Zielsystemkonten entsprechend.

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 unternehmensspezifischen 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: **Mühelose Benutzerverwaltung, mehr Kontrolle und verbesserte Datensicherheit.**

Ein perfekter erster Arbeitstag – So wird Onboarding zum Erfolg!

Euphorie, Vorfreude und etwas Nervosität: Der erste Tag im neuen Unternehmen ist immer aufregend. Die Kollegen begrüßen, den Schreibtisch einrichten und dann das erste mal den neuen Rechner hochfahren, einloggen und... alles läuft!

Der erste Eindruck zählt!

Gerade zu Beginn eines neuen Arbeitsverhältnisses möchten Mitarbeiter mit viel Elan die neuen Herausforderungen angehen.

Umso frustrierender ist es, wenn der Motivation bereits am ersten Arbeitstag ein Dämpfer verpasst wird. Anstatt sich an die Arbeit zu machen, heißt es allzu oft auf IT-Ressourcen warten, mit dem Laufzettel durch das Unternehmen eilen oder sich die notwendigen Arbeitsmittel selbst besorgen.

Unternehmen stehen heute im Wettbewerb um die besten Fachkräfte und geben dabei für das sogenannte Employer Branding viel Geld aus: Sie tunen ihre Anzeigen, geben sich modern auf Karrieremessen, ja sie frischen sogar ihre Arbeitsweisen auf mit Gleitzeit, flexibleren Urlaubszeiten und mit unzähligen Work-Life-Balance-Angeboten. Doch den ersten Arbeitstag haben viele nicht im Blick. Das mit großer Mühe aufgebaute Bild wird gleich zerstört – der neue Mitarbeiter ist frustriert.

Unternehmen verpassen oft beim sogenannten Onboarding neuer Mitarbeiter die Chance, sich positiv hervorzutun und den ersten Arbeitstag zum perfekten Erlebnis zu machen. Der Arbeitsplatz sollte zum Start richtig eingerichtet sein. Dafür sind ein Schreibtisch und der passende Stuhl ebenso wichtig wie die persönlichen Zugänge zu den Systemen. Und idealerweise läuft die Vergabe von Benutzerrechten automatisiert ab.

Häufig ziehen sich die mangelhaften Abläufe des Onboardings über die gesamte Dauer der Anstellung des Mitarbeiters durch bis zum Offboarding: Nach ein paar Jahren im Unternehmen wissen die Verantwortlichen meist nicht mehr, welche Schlüssel die Mitarbeiter ausgehändigt bekommen haben. Ebenso unklar ist, welche Zugriffsrechte ein Mitarbeiter hat, wenn identitätsbezogene Arbeiten schrittweise, undokumentiert und manuell ablaufen. So fällt es entsprechend schwer, den Mitarbeiter sofort nach Verlassen von allen Systemen und Berechtigungen abzukoppeln – vor Ort (On Prem) und in der Cloud.

Es lohnt sich also, die On- und Offboarding-Prozesse im eigenen Unternehmen einmal genau unter die Lupe zu nehmen: In vielen Fällen hilft ein professionelles Identity- und Accessmanagement, um eventuelle Datenschutzlücken zu schließen, Sicherheitsrisiken zu minimieren und gleichzeitig den ersten beziehungsweise letzten Eindruck vom Unternehmen zu verbessern

Fünf Gründe für ein automatisiertes Offboarding

Nicht nur der erste Eindruck zählt. Der letzte Eindruck kann ebenso weitreichende Konsequenzen haben: das Offboarding. Verzögerungen beim Offboarding entstehen typischerweise durch einen Mangel an Kommunikation. Oft ist im Unternehmen die Personalabteilung für das organisatorische Offboarding verantwortlich. Die IT-Abteilung kümmert sich um Deaktivierung von Konten und Entzug der Berechtigungen. Darüber hinaus sind Manager involviert, um Probleme im Tagesgeschäft zu vermeiden. Die Trennung dieser Prozesse führt dazu, dass man sich auf rechtzeitige E-Mails oder Spreadsheets verlässt, um ein vollständiges Offboarding sicherzustellen. Solche manuellen Benachrichtigungen werden jedoch oft vergessen, übersehen, gehen im täglichen Durcheinander verloren oder werden unvollständig verarbeitet. Mit automatisierten Provisioning-Prozessen können Verzögerungen beim Offboarding praktisch eliminiert werden. Finden Sie hier 5 Gründe, den Offboarding-Prozess für eine sofortige und gründliche Ausführung zu automatisieren.

1

Böswillige oder verärgerte Ex-Mitarbeiter

Wenn ein Mitarbeiter gekündigt wird oder die Kündigung eingereicht hat, ist es möglich, dass er dem Unternehmen in irgendeiner Weise schaden will. Ohne den sofortigen, vollständigen Entzug des Zugriffs auf Netzwerk- und Cloud-Ressourcen kann ein scheidender Mitarbeiter umso mehr Schaden anrichten: Geistiges Eigentum, Sales Leads, Informationen zu laufenden Projekten, sensible personenbezogene Daten über Mitarbeiter oder Kunden könnten unbemerkt entwendet werden. Die Handlungen eines einzigen böswilligen Ex-Mitarbeiters können zu einem schweren Reputationsschaden oder zum Verlust von Aufträgen an Konkurrenten führen. Darüber hinaus ist der unautorisierte Zugriff ein Verstoß gegen
gesetzliche Vorschriften, der massive finanzielle Strafen nach sich ziehen kann.

2

Überblick über Accounts und Berechtigungen im Netzwerk

Wenn Konten und Berechtigungen nicht widerrufen werden, entstehen verwaiste Konten, die nicht mehr mit einem aktiven Benutzer verbunden sind. Ihr Netzwerk wird unübersichtlich und es entstehen unnötige Kosten für Speicherplatz. Selbst wenn Sie Konten und Zugriffe überwachen oder Berichte erstellen können, liefern die verwaisten Konten falsche Daten und verschleiern, wie Ihr Netzwerk strukturiert ist.

3

Unnötige und teure Lizenzkosten verbrennen Ihr Budget

IT-Ressourcen sind nicht billig. Accounts bei CRM-Systemen, Adobe und anderen Anwendungen summieren sich und beeinflussen die laufenden Kosten und das Ergebnis Ihres Unternehmens erheblich. Insbesondere Cloud-Ressourcen erfordern Abonnements von Drittanbietern, wo ungekündigte Lizenzen praktisch verwaiste Konten sind, die sogar noch Geld kosten.

Besonders für mittlere und große Organisationen summieren sich die Lizenzkosten schnell. Wenn Sie keine Kontrolle über Ihre aktiven, aber ungenutzten Lizenzen haben, wirft Ihr Unternehmen Geld aus dem Fenster. Sofortiges automatisiertes Offboarding führt zu signifikanten Einsparungen, die es Ihnen ermöglichen, dieses Geld auf die hohe Kante zu legen oder dem nächsten Mitarbeiter im Unternehmen eine Lizenz zu stellen.

4

Verwaiste Konten und Eindringlinge bleiben unbemerkt

Selbst wenn der ehemalige Mitarbeiter nicht für bösartige Aktivitäten verantwortlich ist, können seine Konten der Zugangspunkt für andere Eindringlinge sein. Ohne adäquaten Login-Schutz (Multi-Faktor-Authentifizierung oder sicheres Single Sign-On) sind insbesondere Cloud-Ressourcen extrem anfällig für Einbrüche. Wenn der Eindringling an die Anmeldedaten für z. B. Google Drive gelangt ist, braucht er nur die URL des Dienstes und dem Zugriff steht nichts im Wege.

Schlimmer noch: Weil die Wiederverwendung von Anmeldedaten für mehrere Konten weit verbreitet ist, erhält der Eindringling möglicherweise Zugriff auf weitere Ressourcen. Selbst wenn die ursprünglich gestohlenen Anmeldedaten zu persönlichen Konten des Ex-Mitarbeiters gehörten, könnten diese auch in der Organisation verwendet worden sein.

Um noch einmal auf verwaiste Konten zurückzukommen: Sie sind die perfekte Tarnung für Eindringlinge im Unternehmensnetzwerk. Wenn der Offboarding-Prozess nicht schnell oder gründlich genug ist, gibt es nichts, das das verwaiste Konto als fehl am Platz identifiziert. So hat ein Eindringling plötzlich (im Rahmen der dem Benutzer zugewiesenen Netzwerkberechtigungen) freie Hand.

5

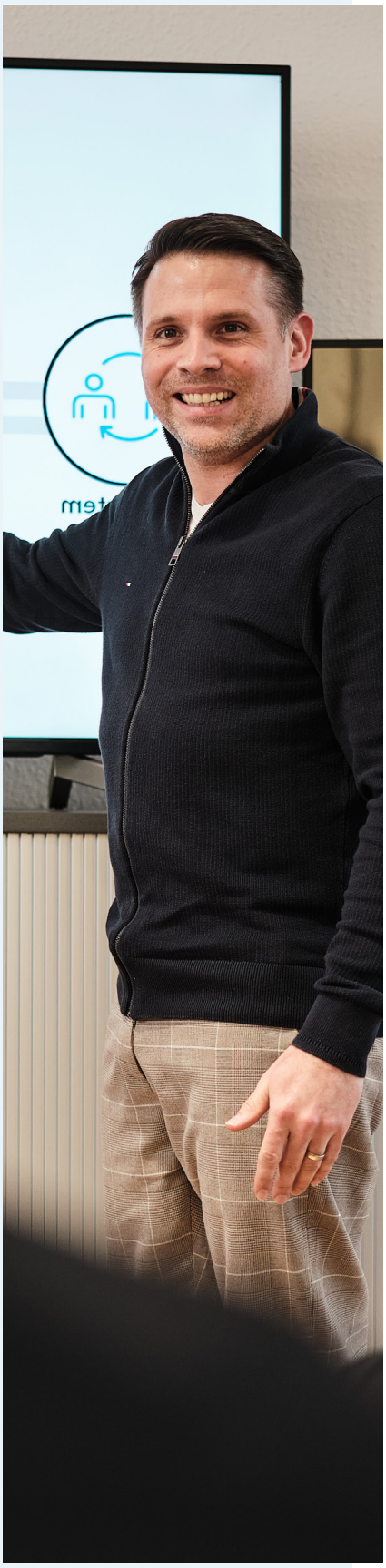
Arbeitsabläufe laufen ins Leere

Die Anpassung der Arbeitsabläufe nach dem Ausscheiden eines Mitarbeiters ist zwar weniger sicherheitskritisch, aber dennoch äußerst relevant für den Betrieb. Werden Manager und Teamleiter nicht rechtzeitig über das Ausscheiden eines Mitarbeiters informiert, können Sie die Arbeitsabläufe nicht so anpassen, dass Projekte und Tagesgeschäft so nahtlos wie möglich weiterlaufen.

Die E-Mails und Anrufe für den fehlenden Mitarbeiter laufen ins Leere, Interessenten werden vergessen, Supportanfragen ignoriert, Aufträge pausiert. Für einen kontinuierlich optimalen Betrieb ist es entscheidend, dass die gesamte Kommunikation und die Arbeitsabläufe des Unternehmens auf Nachfolger oder Kollegen umgelenkt werden. Wenn es beim Offboarding zu Verzögerungen kommt, fallen notwendige Anpassungen durch die Maschen und führen zu Ineffizienzen, unzufriedenen Kunden, verpassten Chancen und negativen Ergebnissen.

Automatisiertes Offboarding für Effizienz & Sicherheit

Die sofortige Ausführung aller User-Lifecycle-Prozesse ist im heutigen modernen Geschäftsklima immer wichtiger geworden. Langsame, manuelle Reaktionen und übersehene Konten und Zugriffe sind ein Wettbewerbsnachteil. Mit automatisierten Offboarding-Prozessen via User Provisioning eliminiert Ihr Unternehmen diese Risiken praktisch. Sie brauchen nicht einmal mehr eine Offboarding-Checkliste.



Darüber hinaus gewinnen viele Ihrer Mitarbeiter, insbesondere die IT-Abteilung, erhebliche Bandbreite zurück. Strategische Projekte müssen nicht mehr fallen gelassen werden, um sich um unmittelbare Offboarding-Anforderungen zu kümmern. Wenn eine automatisierte Identity- und Access-Management-Lösung mit Ihrem HR-System verbunden ist, kann das Offboarding effektiv mit der Bearbeitung des scheidenden Mitarbeiters durch HR beginnen und enden.

Eine Änderung des Beschäftigungsstatus eines Users im HR-System zeigt dem individuell konfigurierten Identity-Management-Tool, dass Konten und Berechtigungen sofort widerrufen werden müssen. Die IT-Abteilung und die zuständigen Manager erhalten weiterhin Benachrichtigungen, aber das automatisierte Offboarding ermöglicht es, alle notwendigen Änderungen ohne manuellen Aufwand direkt im Netzwerk zu verarbeiten.

Im Interesse von Datensicherheit und Effizienz trägt ein automatisiertes Offboarding dazu bei, dass Ihr Unternehmen ernsthafte Sicherheitsrisiken vermeidet, unnötige Kosten eindämmt und einen reibungslosen Betrieb aufrechterhält.

Intelligentes Role Mining: Ein Booster für die rollenbasierte Zugriffskontrolle

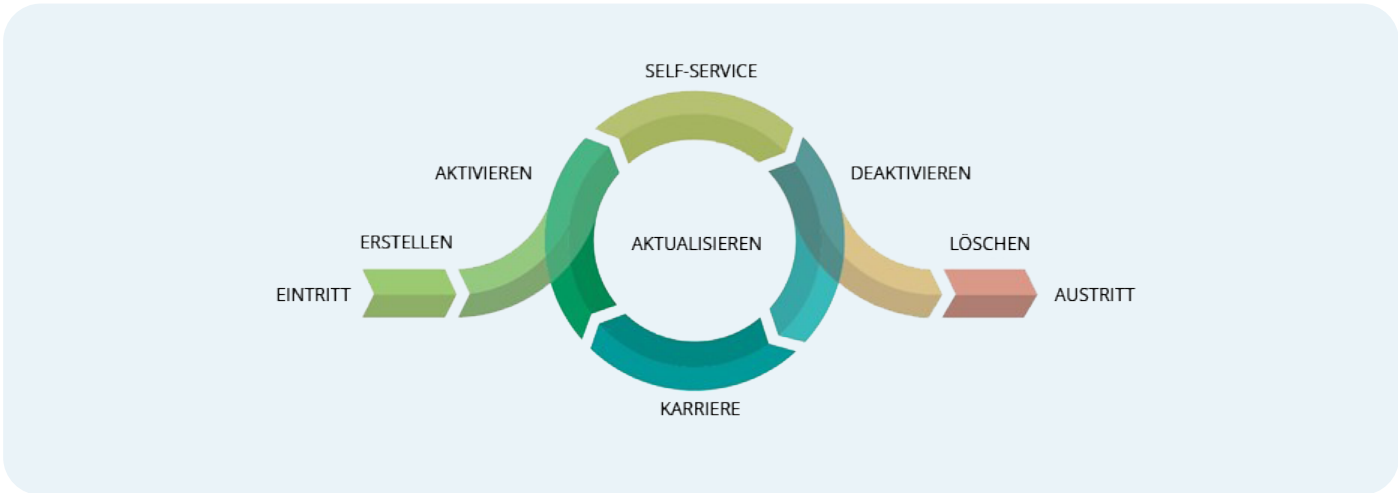
Über die Role Based Access Control (RBAC, rollenbasierte Zugriffskontrolle) managen Organisationen heute ihre Benutzerkonten und Zugriffsrechte auf transparente und sichere Weise. Dank klar definierten Rollen und Berechtigungen ist sichergestellt, dass alle Mitarbeiter zu jedem Zeitpunkt die passenden Rechte haben.

Für viele Unternehmen scheint es jedoch mühselig und zeitaufwendig, eine Autorisationsmatrix mit entsprechenden Geschäftsregeln, Rollen und Berechtigungen auszuarbeiten. Dabei würde sich der Aufwand lohnen, denn nur so lässt sich ein zukunftssicheres, wirksames Identity Management einrichten. Darüber hinaus ist die Implementierung einer RBAC nicht so kompliziert, wenn man richtig vorgeht. Ein zentraler Punkt ist dabei das Role Mining, das wir im Folgenden erläutern werden.

So funktioniert die rollenbasierte Zugriffskontrolle

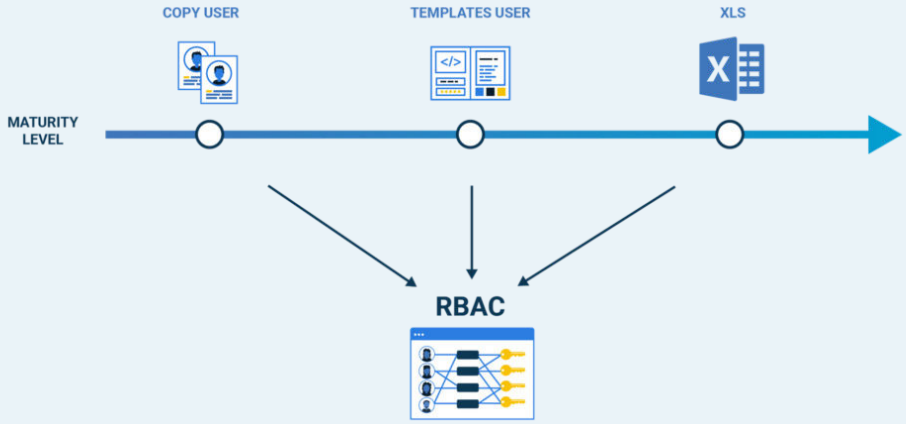
Bei der RBAC (Role Based Access Control) wird jedem Anwender innerhalb einer Organisation eine eindeutige„Rolle“ zugewiesen, die häufig an dessen Aufgaben, Abteilung und/oder seinen Standort gebundenist. Für jede Rolle werden anschließend Zugriffsrechte auf bestimmte Anwendungen und Daten festgelegt.Bei der RBAC bilden Geschäftsregeln die Grundlage für die rollenspezifischen Berechtigungen,sodass Personen mit derselben Rolle automatisch dieselben Berechtigungen haben. Wenn sich eine Rolle ändert, werden die Rechte automatisch entsprechend angepasst.

Wer beispielsweise in der Finanzabteilung arbeitet, benötigt neben Outlook und Office auch Zugriff auf die Finanzverwaltungssoftware und -daten. Wechselt die Mitarbeiterin in den Vertrieb? Dann wird diese Änderung im Personalsystem registriert und automatisch vom Identity-Management-System erkannt. Auf Grundlage des bestehenden RBAC-Modells werden dieser Anwenderin die „Finanzberechtigungen“ entzogen, und sie erhält stattdessen Zugang zum CRM-System. Das geschieht komplett automatisch, d. h. die IT-Abteilung hat nur minimalen Aufwand mit der Benutzer- und Berechtigungsverwaltung. Und noch wichtiger ist die vollständige Kontrolle: Niemand hat zu viele, aber auch nicht zu wenige Berechtigungen. RBAC bildet so die Basis für Sicherheit und Compliance im Unternehmen.



Der Sprung ins kalte Wasser

Ein einfaches, ideales Modell, und doch schrecken viele Organisationen vor der Umsetzung zurück. Immer noch werden Benutzerkonten händisch gepflegt, und auch der Ansatz „vorhandenen Benutzer kopieren“ kommt noch regelmäßig vor. Der Übergang von einer solchen manuellen Vorgehensweise zu einem strukturierten, rollenbasierten Ansatz mit abgestuften Rollen und Geschäftsregeln kann herausfordernd wirken. Wie entwerfe ich ein komplexes Schema mit Dutzenden von Rollen und Berechtigungen? Wie integriere ich Abteilungsleiterinnen und andere Schlüsselpersonen in den Prozess? Wie lange wird es dauern, bis ein tragfähiger Kompromiss erreicht ist? Und ist das Modell nicht schon veraltet, bevor wir fertig sind? Das sind verständliche Sorgen, die der folgende Ansatz aber vielleicht entkräften kann.



RBAC Schritt für Schritt dank Role Mining

Die meisten Informationen, die für eine Autorisationsmatrix benötigt werden, sind meist schon vorhanden,denn auch bei einer manuellen Berechtigungsverwaltung wurde selbstverständlich bereits über diebenötigten Benutzerkonten und Zugriffsrechte nachgedacht. So haben Finanzmitarbeiter mit Sicherheitbereits Zugriff auf die Finanzsysteme und Verkäufer auf das CRM- und das ERP-System. Möglicherweise sind die Berechtigungen dabei nicht konsistent vergeben und es gibt den einen oder anderen Fehler sowie unnötige Berechtigungen, aber die Grundlage sollte vorhanden sein. Aber wie entschlüsseln und analysieren wir diese Informationen, um daraus eine erste Rollenmatrix zu entwickeln? Genau dazu dient Role Mining, ein mächtiges Werkzeug, das einen Top-Down- und einen Bottom-Up-Ansatz vereint.

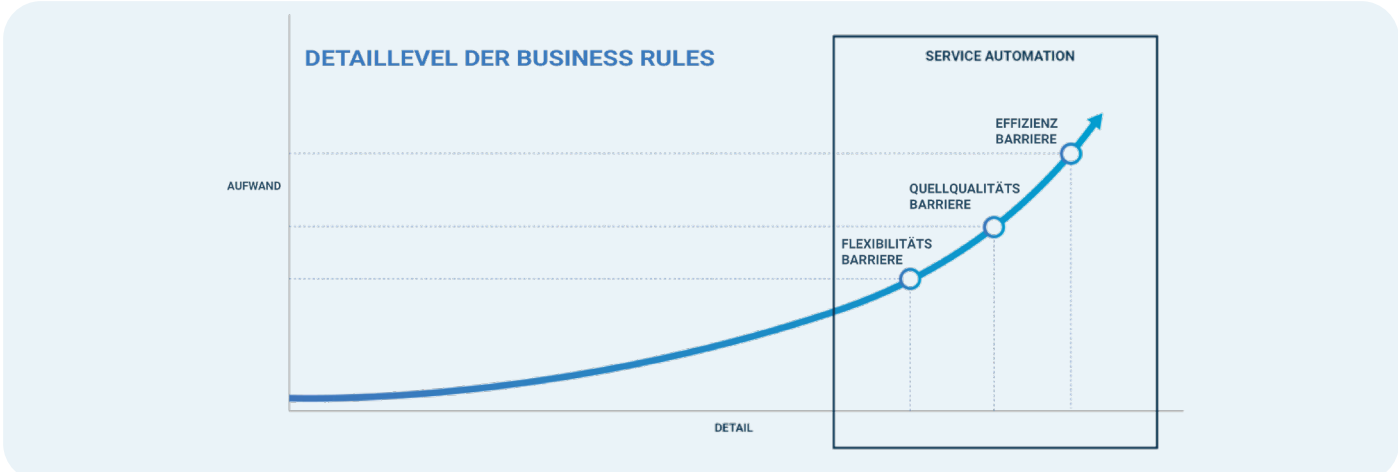
Role Mining besteht aus mehreren zentralen Schritten

1. Ein Inventar der bestehenden Rollen aufstellen: Von oben nach unten (Top-Down) werden alle Rollen erfasst, die in der Personalverwaltung existieren.
2. Ein Inventar der bestehenden Berechtigungen (bzw. Berechtigungsgruppen) aufstellen: Aus den Anwendungen und IT-Systemen, wie z. B. (Azure) Active Directory, werden von unten nach oben (Bottom-Up) die aktuell tatsächlich zugewiesenen Berechtigungen und Gruppen ausgelesen.
3. Ein RBAC-Konzept entwerfen: Die Ergebnisse aus Schritt 1 und 2 werden zusammengeführt und analysiert, um Muster in den Berechtigungen zu ermitteln, die in ein erstes Konzept mit Rollen und zugehörigen Geschäftsregeln einfließen.
4. Das Konzept mit Stakeholdern wie z. B. Abteilungsleitern evaluieren: Nun werden Fehler und unerwünschte Effekte (zum Beispiel Anhäufungen von Berechtigungen) ausgewertet und beseitigt. Damit wird aus dem Konzept ein erstes verwendbares Modell.
5. Das Ergebnis ist eine Basisversion des Rollenmodells, das sich im Geschäftsbetrieb anwenden lässt.Von hier aus lässt sich das Modell erweitern, aktualisieren und an neue Erkenntnisse und Gegebenheiten anpassen.

Role Mining kombiniert demnach geeignete technische Werkzeuge (zur Gewinnung der Daten aus dem Directory und den Personalsystemen) mit der Analyse dieser Daten und einer zielgerichteten Beratung, um daraus ein erstes Rollenmodell für die Organisation zu entwickeln. Der große Vorteil ist dabei, dass Sie nicht von null an beginnen müssen, um ein RBAC-Modell zu erstellen. Die ermittelten Rollen und Geschäftsregeln stellen einen wertvollen Startpunkt dar, von dem aus mit allen Beteiligten weitergearbeitet werden kann. So erreichen Sie gemeinsam in kurzer Zeit Ihre erste RBAC-Implementierung.

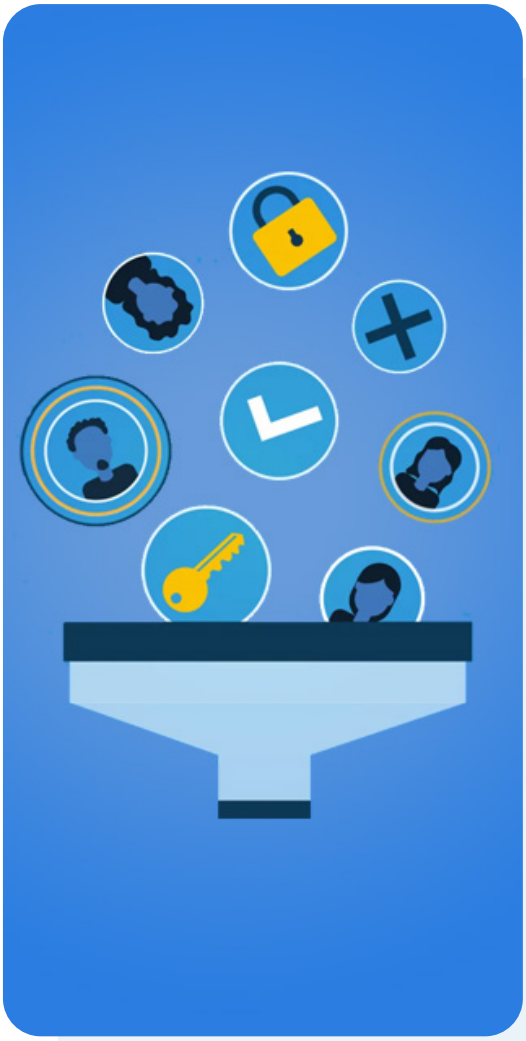
RBAC simpel halten und Ausnahmen automatisieren

Zwei genau identische Rollen, das kommt so gut wie nie vor. Auch wenn die primäre Aufgabe von zwei Mitarbeitern vielleicht dieselbe ist, gibt es doch zahlreiche Abweichungen und Ausnahmen. Beispielsweise kann jemand eine spezielle Aufgabe haben oder an einem bestimmten Projekt arbeiten. Oder ein Mitarbeiter wird Mitglied im Betriebsrat oder lässt sich zum Betriebssanitäter ausbilden – all das führt dazu, dass diese Person spezifische Rechte benötigt, was eine Autorisationsmatrix sehr schnell sehr komplex machen kann. Damit die rollenbasierte Zugriffskontrolle handhabbar bleibt, empfehlen wir, das System auf die sogenannten Erstrechte zu begrenzen, d. h. die Standardberechtigungen, die zur primären Rolle des Mitarbeiters gehören. Diese werden dann ergänzt durch optionale Berechtigungen, z. B. für teure Einzelanwendungen wie Photoshop oder für den Zugang zu freigegebenen Projektplänen. So verhindern Sie, dass Ihr RBAC-Modell komplett „zugenagelt“ wird.



Um diese optionalen Rechte zu managen, bieten sich Self-Service-Anwendungen bzw. Service-Automation-Lösungen an. Auf diese Weise können Anwender – oder deren Vorgesetzte – selbstständig Zugang zu Anwendungen, Daten und Dateien beantragen. Unser HelloID-Modul Service Automation stellt dabei sicher, dass alle erforderlichen Freigabeschritte korrekt ablaufen und die Berechtigungen anschließend im IT-System aktiviert werden. So vermeiden Sie mögliche Fehler, die zu Risiken führen können.

Dank automatisierter Konfigurationsregeln bleibt der Katalog der Dienstleistungen immer aktuell. Neue Freigaben werden beispielsweise direkt im Katalog angezeigt. Diese Kombination aus einem Rollenmodell und einer effektiv eingerichteten Service Automation sorgt insgesamt für ein sicheres, effizientes und beherrschbares Management sämtlicher Benutzerrechte.



Mehr zum Role-Mining-Konzept von Tools4ever

Wenn eine Organisation noch kein Rollenmodell hat, führen wir zunächst ein Data Mining im Personalsystem und der Nutzerverwaltung durch, um aus diesen Daten ein erstes RBAC-Modell zu erstellen.

Diese Methode des Role Mining erfordert neben der technischen Datengewinnung auch Methoden zum Analysieren, Verifizieren und Auswerten, damit eine wertvolle Basis entstehen kann. Dabei geht es unter anderem darum, vorhandene Fehler oder unerwünschte Effekte, zum Beispiel Anhäufungen von Berechtigungen, zu bereinigen.

Unsere Beratungsexperten haben viel Erfahrung in diesem Bereich und würden sich freuen, Ihnen mittels eines klar definierten Role-Mining-Projekts zu helfen, in kurzer Zeit eine Autorisationsmatrix in Ihrer Organisation einzurichten.

Tools4ever bietet Unternehmen einzigartige und europäische Identity- & Access-Management-Lösungen mit einem effektiven, phasenbasierten Implementierungsansatz, der schnell zu Resultaten führt.

Unser Identity und Access Manager sorgt dafür, dass Organisationen auf strukturierte Weise die Kontrolle über die Verwaltung von Identitäten und Rechten erlangen.

Seit 20 Jahren verbindet Tools4ever Menschen mit ihren Daten und vereint Datensicherheit mit Flexibilität in einer vernetzten, digitalen Geschäftswelt.

Weltweit vertrauen über 5.200 große und mittelständische Unternehmen aus allen Branchen auf die innovativen Lösungen von Tools4ever – von angepassten IAM-Komplettsystemen über integrierbare Software-Module bis zu speziellen Komponenten wie dem Berechtigungsoder Passwortmanagement im Self-Service.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Über Tools4ever

In unserer heutigen digitalen Welt. mit immer mehr Systemen on-premise oder in der Cloud, entscheidet die richtige Verbindung zwischen Mitarbeiter und Daten über den Unternehmenserfolg: Die Mitarbeiter müssen zu jeder Zeit und von überall Zugang zu den Daten haben, die sie für ihre Arbeit benötigen – und zwar einfach, schnell und sicher.

Und genau das gewährleistet Identity und Access Management von Tools4ever.

„Unsere Mission ist es, Organisationen zu helfen, ihre IAM-Ziele schnell, sicher und effizient zu realisieren."

Jan-Pieter Giele, Managing Director
DACH, Nord- & Osteuropa

Vielen Dank!

Tools4ever Informatik GmbH
Hauptstraße 145-147
51465 Bergisch Gladbach
Deutschland
+49 2202 2859 0
www.tool4ever.de
info@tools4ever.de