Praxis-Guide 2023:

11 Hebel, die IT bei der Benutzerverwaltung zu entlasten

Automatisiert. Regelbasiert. Compliant.

Herzlich willkommen!

Schön, dass Sie unseren Guide heruntergeladen haben.

Dieser wurde für Sie erstellt, damit Sie ab sofort einen treuen Begleiter bei der Planung und Konzeption Ihres Identity Management-Projekts an Ihrer Seite haben.

Nehmen Sie die folgenden Punkte immer zur Hand, wenn sie relevant für Sie sind.

Die IT spürbar entlasten, Datensicherheit erhöhen und IT-Audits einfacher bestehen?

Mit einem Identity and Access Management-System, sorgen Sie dafür, dass nur autorisierte Mitarbeiter **automatisiert und regelbasiert** einen **sicheren und angemessenen Zugang** zu Systemen und Daten haben.

Wenn Sie die **11 Hebel** in diesem Guide beachten, **entlasten** Sie Ihre IT-Abteilung, **schützen** sensible Daten und **optimieren** gleichzeitig Ihre IT- und Geschäftsprozesse.

Zudem können Sie eventuelle **IT-Audits einfacher bestehen**.

Ich wünsche Ihnen viel Freude und Erfolg beim Anwenden!

Ihr Jan-Pieter

Jan-Pieter Giele

Geschäftsführer

Seit der Gründung 1999 hilft Tools4ever Unternehmen bei der Vereinfachung der Benutzerkontenverwaltung. Über 1.500 Kunden in verschiedenen Bereichen weltweit setzen die IAM Lösungen erfolgreich ein.

Die Basis: Goodbye aufwendige, manuelle Datenverwaltung!

1

Das Personalsystem als Datenquelle

Das User Lifecycle Management startet und endet in der Personalabteilung! Eine **enge Zusammenarbeit zwischen HR und IT** ist unerlässlich für eine effiziente Benutzerverwaltung und IT-Sicherheit.

Verwenden Sie für Ihr automatisiertes User Lifecycle Management das **Personalsystem als Datenquelle**. Dies entlastet sowohl die IT, als auch die Personalabteilung und verbessert den Schutz Ihrer sensiblen Daten.

2

Benutzerverwaltung automatisieren

Verwenden Sie die Daten aus dem Personalsystem für **automatisierte Onboarding-, Change- und Offboarding-Prozesse** in Ihrem Netzwerk.

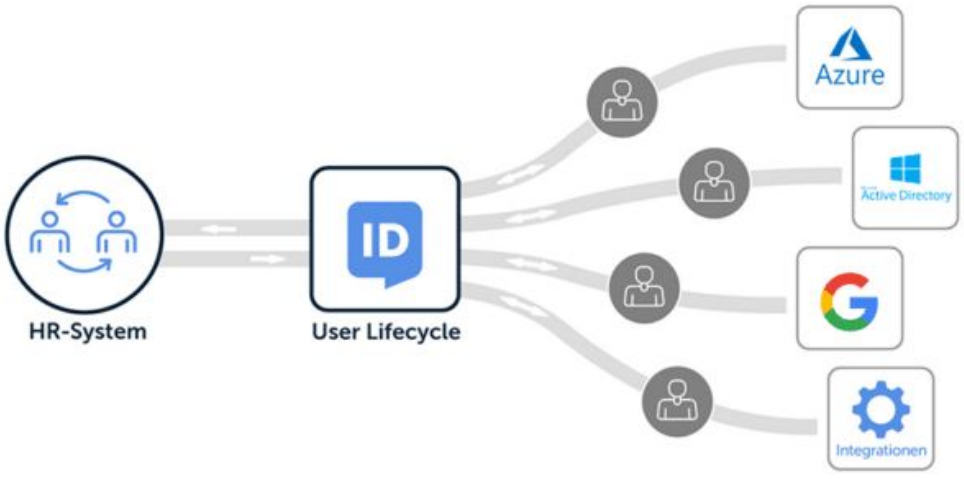
Vergessen Sie dabei, auch wegen der besonderen Anforderungen, Ihre **Cloud Systeme** nicht.

3

Regelbasierte Berechtigungsvergabe

Implementieren Sie ein **regelbasiertes Berechtigungsmodell**. Somit garantieren Sie eine **strukturierte und einheitliche Berechtigungsvergabe** über alle Systeme hinweg.

Beachten Sie hierfür die folgenden Hebel für **Datenschutz, Datensicherheit und Compliance** (nächste Seite).



Basis Plus: Datenschutz, Datensicherheit, Compliance

4

RBAC – Rollenbasierte Berechtigungsvergabe

RBAC (Role Based Access Control) ist ein Modell für die Zugriffskontrolle, bei dem Benutzer basierend auf ihren organisatorischen Rollen und Verantwortlichkeiten **Zugriff auf bestimmte Daten und Anwendungen** erhalten.

Unbedingt implementieren: RBAC ist eine wichtige **Basis für Ihren Datenschutz, die Datensicherheit und Compliance**!

5

Principle of Least Privilege

Die DSGVO erfordert das **Prinzip des geringsten Privilegs**, d.h. Benutzer sollen nur auf die für ihre Arbeit **unbedingt erforderlichen Daten und Anwendungen** zugreifen können.

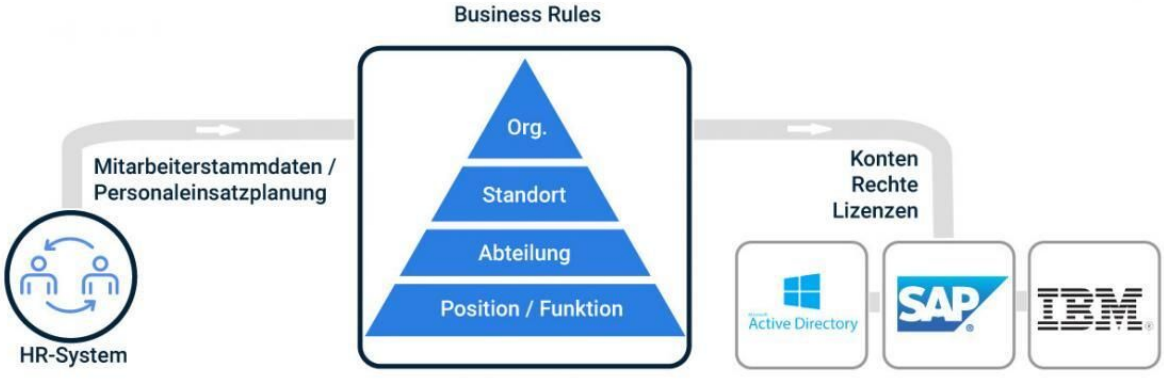
IAM und RBAC unterstützen Organisationen bei der Umsetzung dieser Anforderung.

6

Zeitnahes Onboarding, Change und Offboarding

Am ersten Arbeitstag keinen Zugang zu Systemen und Daten zu haben, ist ärgerlich. Aber noch schlimmer wäre es, wenn Ex-Mitarbeiter immer noch Zugang zu sensiblen Daten hätten.

Mithilfe von IAM können **Zugriffsrechte schnell und effizient eingerichtet** oder wieder entzogen werden. So reduziert sich das **Risiko von Sicherheitsverletzungen** und **Compliance-Anforderungen** werden eingehalten.



Es geht weiter: Aufgaben delegieren

7

Delegieren an den Service Desk

Nicht alle Verwaltungsaufgaben können automatisiert werden, dafür werden aber manuelle Prozesse durch **Standardisierung** vereinfacht:

Delegieren Sie mithilfe von einem **IAM-System** solche Aufgaben an den **First-Line-Support**, um Administratoren zu entlasten.

8

Delegieren an Key-User oder Ressource Owner

Eine große Entlastung für die IT und relativ einfach und schnell umsetzbar:

Manager oder Ressource Owner können die Berechtigungen zu ihren **IT-Ressourcen selber pflegen**, ohne dass die IT eingreifen muss.

9

User Self Service und Workflows

Optimieren Sie Ihr Service Level und entlasten Sie Ihre IT-Abteilung mit einem **Self Service Portal für die End-User**.

Klarer Überblick mit Reporting

10

Wer hat welche Berechtigungen und warum?

Mit einem **Audit-Reporting** schaffen Sie eine transparente Benutzer- und Berechtigungsverwaltung, wodurch Sie IT-Audits einfacher bestehen.

11

Berechtigungs-Reporting & Anomalien

- Wer hat Zugang zu meinen Daten?
- Für welche User ist das Attribut “XYZ” nicht gepflegt?
- Gibt es Gruppen ohne Mitglieder?

Implementieren Sie ein **Reporting**. Das verschafft Ihnen Überblick und Vertrauen.

+

Bonus Tipp!

Nach 20 Jahren Berufserfahrung ist unser **Bonustipp** für Sie:

Machen Sie es **nicht zu kompliziert**. Theorie und Praxis liegen oft etwas auseinander und Komplexität lässt sich nicht skalieren. 😉

Fragen oder Feedback?

Vereinbaren Sie gerne einen Termin zum persönlichen Gespräch.

Ihr Jan-Pieter

Vereinbaren Sie Ihren Termin zum Gespräch über diesen Link:

👉 **Zur Terminbuchung [Link]**

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION