

IAM – Identity & Access Management

EINFACHE UND SICHERE ZUGRIFFSSTEUERUNG DURCH ZENTRALE NUTZER- UND BERECHTIGUNGSVERWALTUNG

Mit unserer Softwarelösung im Bereich „Identity & Access Management“ steuern Sie zentral, wer auf welche Daten, Anwendungen und Geräte Zugriff hat. SecuIAM legt sich über Ihre Systeme, die Berechtigungen erfordern. Von dieser zentralen Stelle aus werden alle Mitarbeitenden sowie deren Berechtigungen und Ressourcen administriert. Dies kann innerhalb einer statischen Aufbauorganisation erfolgen, aber auch in dynamischen Strukturen wie Teams und Projekten.

Die Komplexität der IT-Landschaften in Bezug auf Systeme, Accounts und Passwörter steigt stetig an. Das verschlingt Ressourcen und birgt Risiken!

Berechtigungen werden in Rollen zusammengefasst, wodurch die Zugriffssteuerung transparent und erheblich vereinfacht wird. Diese Berechtigungen und Rollen können über ein Self-Service-Portal durch Mitarbeitende oder deren Vorgesetzte beantragt und nach einer etwaigen Genehmigung automatisiert vergeben werden. Mithilfe generischer Standardprozesse erzielen Sie in vielfacher Hinsicht schnelle Erfolge in der Automatisierung sowie in den Joiner-, Mover- und Leaver-Prozessen.

Eine zentrale Stelle zur Verwaltung sämtlicher Berechtigungen – kein Mehraufwand durch Insellösungen!

Sie können jederzeit nachvollziehen, wer, was wann und wo darf sowie wer die Genehmigung dazu erteilt hat. Diese Daten werden historisch gespeichert, wodurch sich das Haftungsrisiko von Vorständen und Geschäftsführungen verringert. Auffällige Vorgänge können somit aufgedeckt und Risiken bereits im Vorfeld vermieden werden. Gegenüber Wirtschaftsprüfungen und der internen Revision ist das Management mit unserer IAM-Lösung SecuIAM ad hoc auskunftsfähig. Somit sind Sie auf der sicheren Seite!

Anforderungen an Compliance werden erfüllt!

IHRE VORTEILE

- Zentrale Zugriffssteuerung
- Einfache Berechtigungsverwaltung über Rollen
- Kostenersparnis durch geringen Administrationsaufwand
- Hohe Effizienz durch Prozessautomatisierung
- Erhöhung des Security-Levels
- Schneller und sicherer Nutzerzugriff auf Systeme und Ressourcen
- Einhaltung der Nachweispflichten im Sinne der Wirtschaftsprüfung und Revision – schnell und stichtagsgenau