

Identity- und Access-Management (IAM)

Mit einem leistungsstarken IAM Zugänge und Berechtigungen meistern

Mit zunehmender Digitalisierung steigt auch der Aufwand zur Verwaltung der Berechtigungen in den Unternehmen. Effiziente, automatisierte Lösungen werden in diesem Bereich immer wichtiger, denn ein Compliance-gesichertes Berechtigungsmanagement ist ohne ein zentrales System zur Verwaltung von Berechtigungen kaum möglich. Waldemar Reimche und Patrick Piotrowski stellen eine entsprechende Lösung vor.

Mit der stetig voranschreitenden Digitalisierung steigt nicht nur die Zahl der in den Unternehmen eingesetzten Softwareprodukte, sondern auch die der zu verwaltenden Berechtigungen. Vor allem Stadtwerke und Energieversorger stehen vor der Herausforderung, eine Vielzahl von Nutzern, Systemzugängen und individuellen Berechtigungen effizient zu verwalten – und das bei einer sinkenden Verfügbarkeit von Fachpersonal und knappen Budgets. Diese Aufgabe wird nicht nur durch gesetzliche Vorgaben bestimmt, sondern wirkt sich auch direkt auf die Kostenstrukturen und die betriebliche Effizienz aus.

Praxisbeispiel

Angenommen, ein typisches Stadtwerk beschäftigt rund 500 Mitarbeitende. Wenn jeder Mitarbeitende durchschnittlich 15 verschiedene Zugänge erhält, die wiederum mit durchschnittlich 27 Berechtigungen ausgestattet sind, ergeben sich:

- Zugänge:
 $500 \times 15 = 7\,500$
- Einzelberechtigungen:
 $7\,500 \text{ Zugänge} \times 27 \text{ Berechtigungen je Zugang} = 202\,500$

Zieht man in Betracht, dass diese umfangreichen Berechtigungen oft von wenigen Administratoren verwaltet werden müssen, die nebenbei noch für andere betriebliche Aufgaben zuständig sind, wird schnell klar, dass es nahezu unmöglich ist, diesen Verwaltungsaufwand mit der nötigen Aufmerksamkeit und Sorgfalt zu bewältigen. Außerdem gilt es zu bedenken, dass jederzeit sichergestellt und nachgewiesen werden muss, dass die vergebenen Zugriffe und die damit einhergehenden Berechtigungen in den IT-Systemen angemessen sind, um Minimalprinzipien zu entsprechen. Die enormen Zahlen machen deutlich, wie wichtig effiziente, automatisierte Lösungen in diesem Bereich sind,

da ein Compliance-gesichertes Berechtigungsmanagement ohne ein zentrales System zur Verwaltung von Berechtigungen kaum möglich ist (Bild 1).

Herausforderungen im Detail

Jeder einzelne Zugang und jede Berechtigung erfordert eine präzise Verwaltung. Von der erstmaligen Vergabe über die regelmäßige Überprüfung bis hin zur Anpassung an geänderte organisatorische Anforderungen müssen alle Schritte lückenlos dokumentiert und kontrolliert werden. Gerade in regulierten Bereichen, in denen strenge Sicherheitsstandards und Compliance-Richtlinien eingehalten werden müssen, kann ein einziger Fehler fatale Folgen haben. Falsch vergebene Berechtigungen erhöhen das Risiko unberechtigter Zugriffe und können potenziell kritische Sicherheitslücken öffnen, die nicht nur den operativen Betrieb, sondern auch das Vertrauen der Kunden gefährden.

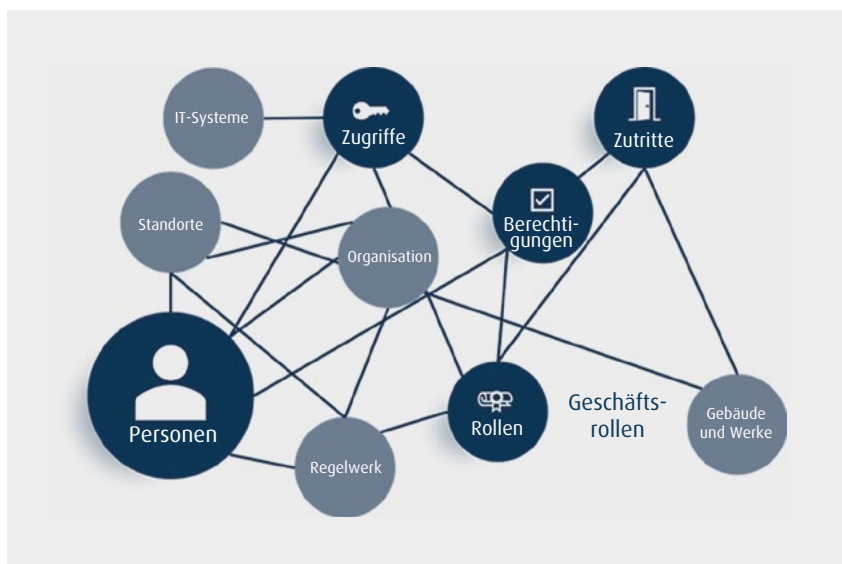


Bild 1. Effiziente Verwaltung von Zugängen und Berechtigungen

Die Verwaltung von Zugängen und Berechtigungen geht über die reine IT-Sicherheit hinaus und hat direkte wirtschaftliche Auswirkungen. Ein hoher manueller Aufwand bedeutet zusätzliche Personalkosten, die in Zeiten knapper Budgets kaum tragbar sind. Gleichzeitig führt eine unzureichende Kontrolle zu ineffizienten Arbeitsabläufen und möglichen Produktionsausfällen, die sich direkt auf den Gesamterfolg des Unternehmens auswirken. Durch gezielte Investitionen in automatisierte IAM-Lösungen können diese Risiken minimiert und die betriebliche Effizienz nachhaltig gesteigert werden.

Moderne Ansätze im Identity- und Access-Management

Traditionelle IAM-Konzepte stoßen häufig an ihre Grenzen. Moderne, automatisierte Lösungen, die auf rollenbasierten Zugriffskontrollen aufsetzen, sind ein entscheidender Schritt, um den administrativen Aufwand zu reduzieren. Durch die Bündelung von Berechtigungen in Standardrollen und den Einsatz kontinuierlicher Überwachungssysteme wird das Risiko von Sicherheitsverletzungen deutlich minimiert. Gleichzeitig gewinnen innovative Technologien wie KI-Agenten zunehmend an Bedeutung und tragen dazu bei, Prozesse im IAM-Umfeld noch effizienter zu gestalten. Die Vorteile dieser Ansätze im Überblick:

Effizienzsteigerung: Die automatisierte Verwaltung von Zugängen und Berechtigungen reduziert den manuellen Aufwand erheblich. KI-Agenten analysieren kontinuierlich Nutzerdaten und Verhaltensmuster, erkennen Anomalien in Echtzeit und können so bei der dynamischen Anpassung von Berechtigungen unterstützen. Administratoren haben so die Möglichkeit, sich auf strategisch wichtigen Aufgaben zu konzentrieren.

Skalierbarkeit: Auch bei wachsender Mitarbeiterzahl und steigenden Zugriffszahlen können Änderungen schnell und zuverlässig umgesetzt werden. Moderne Systeme, die von KI-Agenten unterstützt werden, passen sich flexibel an sich verändernde Umgebungen an und ermöglichen eine reibungslose Skalierung, was vor allem in expandierenden Unternehmen von großem Vorteil ist.

Sicherheitsgewinn: Regelmäßige Audits und ein robustes Monitoring erhöhen kontinuierlich das Sicherheitsniveau. KI-Agenten leisten dabei einen

wichtigen Beitrag, potenzielle Sicherheitslücken frühzeitig zu erkennen, indem sie unregelmäßige Aktivitäten analysieren und in Echtzeit Gegenmaßnahmen einleiten. So wird das Risiko von Angriffen und Datenmissbrauch nachhaltig reduziert.

Neben der reinen Automatisierung steht auch die Benutzerfreundlichkeit im Fokus moderner IAM-Lösungen. Eine intuitive Oberfläche und klare Richtlinien erleichtern den Mitarbeitern den Umgang mit ihren Zugängen, während automatisierte Prozesse den administrativen Aufwand drastisch reduzieren. Durch den gezielten Einsatz von künstlicher Intelligenz und maschinellem Lernen in Form von KI-Agenten können Unregelmäßigkeiten schneller erkannt und potenzielle Sicherheitsvorfälle nahezu in Echtzeit adressiert werden. Dieser proaktive Ansatz ermöglicht ein Sicherheitsmanagement, das nicht nur reaktiv auf Vorfälle reagiert, sondern bereits im Vorfeld Risiken minimiert. Insgesamt tragen diese modernen Ansätze dazu bei, das Identitäts- und Zugriffsmanagement sowohl effizienter als auch sicherer zu gestalten.

Der konsequente Einsatz moderner und automatisierter IAM-Konzepte ermöglicht es, den gestiegenen Anforderungen gerecht zu werden. Nur durch den Einsatz innovativer Technologien und optimierter Prozesse können Effizienz und Sicherheit auch in regulierten Branchen langfristig gewährleistet werden. In einer zunehmend digitalisierten Welt gilt es, diese Entwicklungen kontinuierlich voranzutreiben, um den komplexen Herausforderungen der Zukunft erfolgreich begegnen zu können.



Waldemar Reimche,
Geschäftsführer,
OEDIV SecuSys GmbH, Rostock



Patrick Piotrowski,
Senior Business Consultant IAM
und Sales Representative,
OEDIV SecuSys GmbH, Rostock

>> info@secusys.de

>> www.secusys.de

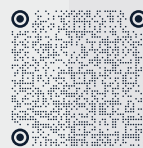
zenon.

Für eine sichere Zukunft

Softwareplattform für Cyber-Resilienz



- ▶ NIS2 und CRA Konformität
- ▶ Detektion von Spionage-Tools
- ▶ Echtzeit Anomalie-Erkennung im Netzwerk
- ▶ Überwachung Zugriff- und Rechteverwaltung
- ▶ Security Gateway



COPADATA.COM/DE/CYBERSECURITY



zenon
by COPA-DATA