Identity Manager von One Identity (OI)

Optimierte Verwaltung von Berechtigungen und Prozessen

Der One Identity Manager ermöglicht die zentrale Administration von Identitäten inklusive deren Berechtigungen und fördert die Automatisierung der hiermit im Zusammenhang stehenden Prozesse. Auf diese Weise unterstützt er Unternehmen dabei, die zunehmend komplexer werdenden Sicherheitsvorgaben und IT-Governance-Anforderungen zu erfüllen sowie das Zugriffsmanagement konsequent an den Geschäftsanforderungen auszurichten.

Zugriffsmanagement für Unternehmen ist anspruchsvoller denn je

Das Zugriffs- und Berechtigungsmanagement in Unternehmen ist ein erheblicher Zeit- und Kostenfaktor, da die Implementierung einer Identitäts- und Zugriffsverwaltung sowie deren Wartung meist mit viel Aufwand verbunden ist. Hinzu kommt, dass angesichts der fortschreitenden technischen Entwicklung immer mehr unterschiedliche Betriebssysteme und Applikationen Einzug in die Unternehmen halten. Zudem wächst die Zahl der mobil arbeitenden Mitarbeiter mit den entsprechenden Endgeräten stetig. Mehr denn je sind Nutzer also darauf angewiesen, zielgerichtet wie auch remote auf ihre notwendigen Daten und Applikationen zugreifen zu können. Und zwar stets vor dem Hintergrund von geltenden Sicherheitsbestimmungen und Gesetzesvorgaben. Mittels einzelner „Insellösungen“ und manuellen Prozessen lässt sich dem auf Seiten der IT-Abteilung jedoch kaum noch Herr werden.

Automatisierte Bereitstellung von Benutzeridentitäten und Berechtigungen

Der Identity Manager von One Identity hilft, die Komplexität der Zugriffsverwaltung mittels zentraler Administration und Automatisierung von Prozessen zu reduzieren, indem er alle sicherheitsrelevanten Richtlinien und Prozesse an einer Stelle bündelt. Mithilfe der Dashboard-Funktion können z. B. On-Demand- oder Routinebestätigungen geplant und der Status von Gruppen- oder Verteilerlisten in einer klar verständlichen Übersicht angezeigt werden. Die zentrale Administration und die Automatisierung der Prozesse führt zu einer spürbaren Entlastung der IT-Abteilung. Der Identity Manager schafft so die nötigen Voraussetzungen dafür, zukünftig die Geschäftsanforderungen als maßgebliches Kriterium zu etablieren. Dies bedeutet auch, dass die Mitarbeiter der einzelnen Geschäftsbereiche stärker in die Verantwortung genommen werden.

Self-Service-Zugangsportal und Passwort Manager

Das Self-Service-Zugangsportal ist ein besonderes Feature des Identity Managers, denn niemand weiß besser, wann er Zugriff auf welche Anwendungen benötigt, als die Mitarbeiter selbst. Hier können User basierend auf vordefinierten Genehmigungsprozessen und Workflows via „Online-Warenkorb“ z. B.

Zugriffsrechte und Berechtigungen, aber auch die Aufnahme in Gruppen- und Verteilerlisten anfordern. Außerdem kann der Funktionsumfang des Identity Managers mithilfe zahlreicher ergänzender Module noch erweitert werden. Der Password Manager erlaubt Mitarbeitern z. B., die Kennwörter ihrer Benutzerkonten eigenständig zurückzusetzen, nachdem die unternehmensspezifischen Kennwortrichtlinien für die verschiedenen Benutzerrollen zentral definiert und hinterlegt wurden. Hierdurch werden Prozesse nachhaltig verschlankt und personelle Ressourcen eingespart, denn der Umweg über die IT-Abteilung entfällt.

Produktmerkmale & Features

- Modular aufgebaute und skalierbare IAM-Lösung
- SAP-zertifiziert
- Vorhandene SAP-Anwendungen können problemlos integriert und erweitert werden
- Cloudbasierter Add-on-Service für hybride und SaaS-Anwendungen
- Dashboard zur Planung von On-Demand- und Routinebestätigungen
- Self-Service-Zugangsportal für Mitarbeiter
- Zahlreiche Erweiterung erhältlich (Password Manager, Starling Connect, Active Roles, Multi-Faktor-Authentifizierung etc.)

Ihr Nutzen auf einen Blick

- Administration des Zugriffs auf lokale, Cloud- und Hybridressourcen
- Risikoreduzierung dadurch, dass Benutzer nur Zugriff auf Anwendungen haben, die sie auch benötigen
- Einhaltung von Audit- und Compliance-Vorgaben mithilfe von hinterlegten Richtlinien zur (Re-)Zertifizierung
- Verlagerung von Zugriffsentscheidungen in die richtigen Hände (Geschäftsebene)
- Entlastung der IT-Abteilung durch Self-Service-Zugangsportal
- Hohe Systemkompatibilität, die den Aufbau auf vorhandenen Infrastrukturen mit entsprechender Erweiterung unterstützt

„In vielen Unternehmen bindet das Zugriffsmanagement für eine heutzutage meist recht heterogene und hybride Systemlandschaft zu viele personelle Ressourcen. Vor allem in der IT-Abteilung. Durch die Bündelung der Administration an zentraler Stelle und die Automatisierung von Prozessen hilft der Identity Manager dabei, die Komplexität des Zugriffsmanagements deutlich zu reduzieren. Er trägt maßgeblich dazu bei, dass Unternehmen regelkonform die tatsächlich notwendige Zugriffsebene für Mitarbeiter bereitstellen. Und zwar über den gesamten Identity-Lifecycle hinweg und unabhängig davon, ob der Nutzer gerade neu eintritt, intern wechselt oder austritt. “

Gerald Appel (Team Lead One Identity)