Identity & Access Management (IAM)

Nutzer, Rollen und Zugriffsberechtigungen professionell managen

Professionelles Identity & Access Management gehört in Zeiten des digitalen Wandels zu den kritischen Erfolgsfaktoren eines Unternehmens und ist essentieller Bestandteil einer professionellen IT-Sicherheitsstrategie.

IAM – Für Unternehmen unverzichtbar!

Primäre Aufgabe von IAM ist es, Nutzern eindeutige digitale Identitäten zuzuweisen, die es erlauben, Rollen, Gruppen und Zugriffsberechtigungen von Anwendern zu verwalten, zu aktualisieren, systematisch zu managen und die einzelnen Aktivitäten über den gesamten Access Lifecycle zu überwachen. Professionelle IAM-Systeme stellen die für diesen Zweck notwendigen Tools und Technologien bereit und helfen, Sicherheitsvorgaben und in- und externe Compliance Anforderungen unternehmensübergreifend um- und durchzusetzen. Denn es gibt zahlreiche gesetzliche Anforderungen und länderspezifische Vorschriften, die es zwingend erforderlich machen, dass sich Unternehmen mit dem Thema Identity & Access Management auseinandersetzen. Für in Europa ansässige Unternehmen gelten spätestens seit dem 25. Mai 2018 die strengen Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO/GDPR). Wird gegen diese verstoßen, drohen empfindliche und möglicherweise sogar geschäftsbedrohende Strafen. In den USA hingegen bilden der Sarbanes-Oxley-Act, der Gramm-Leach-Bliley-Act und HIPAA-Act die rechtliche Grundlage.

Die Kernfunktionen: Authentifizierung und Autorisierung

Im Zusammenhang mit Zugriffsrechten muss ein System einen Benutzer erst authentifizieren, um ihn anschließend entsprechend seiner Aufgaben und Tätigkeiten autorisieren zu können. Die eindeutige Authentifizierung eines Users kann mittels biometrischen Merkmalen sowie Username- und Passwortabfragen sichergestellt werden. Privilegierte Benutzer wie System- und Datenbankadministratoren authentifizieren sich mittels Multifaktor-Authentifizierungen (z. B. auch mithilfe von Hardware- oder Software-Token).

Im Rahmen der Autorisierung wird festgelegt, auf welche Systeme oder Ressourcen der jeweilige Benutzer Zugriff erhält. In welchem Umfang genau er diesen erhält, hängt dabei von den unternehmensspezifischen Regeln und Rollendefinitionen ab.

Übergeordnetes Ziel des Prinzips von Authentifizierung und Autorisierung ist stets, das gesamte Unternehmensnetzwerk – und hiermit untrennbar verbunden – die Assets und Produktivität der Organisation gegen Angriffe zu schützen, seien sie von außen oder innen. Ein leider nach wie vor zu weit verbreitetes Szenario ist, dass Nutzer eher mehr Berechtigungen im System haben, als sie de facto benötigen. Professionelles IAM kann an dieser Stelle als zusätzliches Sicherheitsnetz verstanden werden, welches das Risiko unberechtigter Zugriffe durch klar definierte Zugriffsberechtigungen, -regeln und -prüfungen minimiert. Und zwar sowohl für hybride Cloud- und IT-Landschaften im Kontext von Software-as-a-Service-Modellen (SaaS) als auch für On-Premise-Lösungen, die der Kunde vor Ort unterhält. Aber professionelles IAM bietet noch mehr.

Die Vorteile von IAM auf einen Blick

Automatisierung der Prozesse

Bei der Einführung eines IAM werden zunächst alle IT-Geschäftsprozesse unter Anleitung eines Beraters oder Systemarchitekten in Workshops mit den jeweils für den Geschäftsprozess zuständigen Prozessverantwortlichen detailliert definiert und beschrieben. Alle für einen automatisierten Ablauf definiert Prozesse können nach einem festgelegten Zeitplan oder mittels eingerichtetem Trigger sowie auch manuell angestoßen werden. Der im Vorfeld für einen Prozess definierte Workflow läuft dann automatisiert im Hintergrund ab.

Vereinfachte Administration und hohe Datenkonsistenz

Die Mitarbeiterdaten müssen nur einmal – beispielsweise in der Personalverwaltung - zentral erfasst werden. Angeschlossene Systeme können dann auf diese zugreifen (Metadirectory). Mittels Self-Service-Schnittstellen für die Benutzer und automatischer Prozesse reduziert sich der Administrationsaufwand erheblich. Bei Änderungen der relevanten Daten z. B. im Rahmen eines Abteilungswechsels erfolgt die Anpassung von Berechtigungen automatisiert nach den im System hinterlegten Regeln. Entsprechend werden beim Ausscheiden eines Mitarbeiters auch automatisch Benutzerkonten gesperrt, Berechtigungen gelöscht, Laptop und Handy eingezogen etc.

Kurze Reaktionszeiten im Ernstfall

Sollte es notwendig sein, dann kann ein Benutzer in einer Notsituation blitzschnell und ohne großen Aufwand auf sämtlichen Systemen (Mail, Fileserver, Intranet, PC usw.) gesperrt werden.

Höhere Produktivität durch Provisioning

Durch eine zentrale Verwaltung und Provisionierung mittels IAM, können alle Berechtigungen und Rollen eines Benutzers für alle angeschlossenen Systeme systemübergreifen zentral gesteuert werden. Die aufwendige Pflege von Daten für einzelne Applikationen entfällt. Jeder Mitarbeiter kann also in kürzester Zeit und völlig automatisiert von einer Instanz aus für alle angeschlossenen Systeme zugelassen werden und somit sofort produktiv arbeiten. Die IT-Abteilung wird hierdurch spürbar entlastet und Wartezeiten entfallen.

Vereinfachtes Anmeldeverfahren dank Single Sign-On (SSO)

Setzt ein Unternehmen ergänzend SSO ein, müssen sich die Benutzer nur noch einmal am System anmelden, alle weiteren Logins erfolgen automatisch im Hintergrund. Dies geht einher mit einer erhöhten Benutzerzufriedenheit, einer Entlastung des Helpdesks sowie reduzierten Aufwänden und Kosten.

Entlastung des Helpdesks

Durch die gebündelte und systematische Administration bezogen auf Accounts und Berechtigungen werden deutlich weniger Anfragen an das Helpdesk gestellt.

Sicherer Zugang auch für Kunden und Partnerunternehmen

Auch Kunden und Geschäftspartner benötigen ggf. Zugang zu den Systemen. Ein IAM gewährleistet zuverlässige Verwaltung von Benutzerkonten, Zugriffsrechten, Daten und Ressourcen, selbst über die Unternehmensgrenzen hinaus.

Erfüllung von Compliance-Anforderungen

Alle Vorgänge innerhalb des IAM können mit Hilfe von Audit- und Reporting-Tools historisch dokumentiert und gespeichert werden. Hierdurch lassen sich rechtliche oder gesetzliche Anforderungen hinsichtlich Transparenz bei den Zugriffsrechten erfüllen.

Geringerer Rezertifizierungsaufwand im Kontext mit IT-Governance

Die im Kontext mit IT-Governance regelmäßig durchzuführenden Rezertifizierungen können auf Basis eines professionellen und IT-gestützten Identity & Access Managements mit deutlich geringerem Aufwand realisiert werden.

Einsparung von Kosten

Der Arbeitsaufwand für die Verwaltung von Benutzern und deren Berechtigungen wird durch Einführung eines professionellen IAM um ein Vielfaches reduziert. Auch Lizenzkosten werden eingespart, denn jeder User erhält nur Zugriff auf diejenigen Applikationen, die er auch wirklich benötigt.

ASCONSIT: Professionelles IAM basiert auf durchdachtem Prozessdesign!

Will ein Unternehmen erfolgreich ein professionelles Identity & Access Management einführen, dann sollte zunächst in einer abteilungsübergreifenden Zusammenarbeit eine gut durchdachte Strategie erarbeitet werden. Wichtig und essentiell ist es im ersten Schritt, ein Gesamtbild der Geschäftsprozesse und der vorliegenden Systemlandschaft zu erstellen. Dies hilft bei der Analyse und dem Verstehen vorherrschender Prozesse, um im nächsten Schritt – falls notwendig - bestehende Workflows anpassen oder komplett neue Abläufe sinnvoll erstellen zu können. Zudem gilt es angesichts verschiedener Datenquellen, die Nutzeridentitäten nachhaltig und über alle Systeme hinweg zu synchronisieren. Dies erfordert eine sorgfältige Planung und ein durchdachtes Prozessdesign. Schließlich soll ein IAM das Unternehmen in die Lage versetzen, eine große Anzahl von Benutzern inklusive der dazugehörigen Devices in verschiedenen Softwareumgebungen effizient und automatisiert zu verwalten, während gleichzeitig höchste Sicherheitsstandards zu erfüllen sind.

Wir von ASCONSIT unterstützen Sie beim Prozessdesign mit unserer mehr als 15-jährigen Expertise!