TIMETOACT GROUP
SOFTWARE & CONSULTING

Identity & Access Governance / Management (IAG / IAM)

Your connected company

Wo liegt die Herausforderung?

Früher war die Verwaltung von IT-Identitäten geprägt von geschlossenen (Firmen-)Umgebungen und dediziert berechtigten Geräten zum Zugriff für wohldefinierte Nutzer. Heute werden vermehrt auch private und /oder mobile Geräte eingesetzt. Aufgaben und Verantwortlichkeiten ändern sich permanent, während gleichzeitig weitere Systeme hinzukommen, die zusätzlich in bestehende Prozesse integriert werden müssen. Wie aber stellen Sie sicher, dass jeder Nutzer genau die notwendigen Rechte für die jeweils für ihn relevanten Systeme hat? Und wie lassen sich diese über alle erlaubten Geräte hinweg gewährleisten?

We enable YOUR connected company

Sichere Rechtevergabe

Mit unseren Identity & Access Governance-Leistungen stellen Sie sicher, dass jeder Kollege, Kunde und Partner stets genau die Berechtigungen im IT-System erhält, die er auch tatsächlich benötigt. Dies gilt sowohl für die Laufbahn des Kollegen – mit der Aufnahme neuer Tätigkeiten über Versetzungen bis hin zum Ausscheiden – als auch für alle Faktoren einer Geschäftsbeziehung. Wir erarbeiten ein Rechtekonzept, das der digitalen Transformation dauerhaft Rechnung trägt und sicherstellt, dass jeder Zugriff von einem Account einer realen Person zugeordnet werden kann. Zugrunde liegt dabei immer eine zentrale, automatisierte und systematische Steuerung, so dass der gesamte Prozess über alle Personen, Zugänge und Rechte hinweg transparent nachvollzogen werden kann. Ändern sich die Aufgaben eines Nutzers, oder kommen neue hinzu, kann dieser damit auf Knopfdruck vom ersten Tag an produktiv arbeiten.

Die Business Unit Identity & Access Governance der TIMETOACT unterstützt die Prozesse der ISO 27.00x. Unser Betriebskonzept lehnt sich an das Access Management der ITIL V3-Service Operation Prozesse an.

Mit unseren Services im Identity & Access Governance können Sie sich sicher sein, alle Zugriffsberechtigungen über alle Systeme und alle Geräte hinweg jederzeit vollständig unter Kontrolle zu haben. Neben der maximalen Compliance setzen Sie dabei auf ein Höchstmaß an Sicherheit und schaffen ein effizienteres Arbeiten bei zugleich deutlich reduzierten Kosten.

Mit Erfahrung zum Ziel - Wie wir vorgehen

Identity & Access Governance / Management (IAG / IAM)

TIMETOACT bietet im IAG alle Services im Application-Lifecycle an: Von der Analyse und Evaluierung eines geeigneten Produktes über die fachliche und technische Konzeption der Lösung, die technologische Umsetzung innerhalb eines Projektes, bis hin zur Pflege, Weiterentwicklung und dem Betrieb der Lösung. Hierbei greifen wir auf unser langjährig gereiftes Vorgehensmodell zurück. Ein Reifegradmodell ermöglicht es, jederzeit den Status und den Erfolg zu messen und die nächsten Schritte bedarfsorientiert zu definieren. Ziel ist es, eine weitgehend automatisierte, revisionssichere Lösung mit Endnutzer-geeigneten Antragsverfahren verfügbar zu haben. Diese erfüllt alle Anforderungen an Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität und Nachvollziehbarkeit.

Auch nach Beendigung des Einführungsprojektes unterstützen wir unsere Kunden sowohl bei der Weiterentwicklung der Lösung, der Pflege der kunden-individuellen Umsetzung, als auch dem fachlichen und technischen Betrieb. Alle diese Leistungen können auch als Managed Service eingekauft werden.

Wir verfolgen stets die Philosophie, dass die Lösung auf den Bedarf des Kunden zugeschnitten werden muss und nicht der Kunde auf ein spezielles Produkt. Deshalb ist es unser erklärtes Ziel, unsere Kunden auf Wunsch im gesamten Prozess der IAG/IAM-Einführung zu unterstützen und zu beraten.

Priviledged Account Management

Privilegierte Accounts sind heutzutage in einer Vielzahl von Facetten in Unternehmen vorhanden:

- Shared Accounts zur Nutzung in Social Media,
- Administratorenkonten auf Appliances und in Applikationen oder in Security-Systemen,
- Administrationskonten für Provider,
- technische User-Accounts ...

Die geregelte Verwaltung dieser privilegierten Accounts wird zur Risikominimierung für Unternehmen zunehmend bedeutender. Zu diesem Zweck liefern wir mit unseren Technologiepartnern erstklassige Produkte und Lösungen. Die Einführung erfolgt hierbei in überschaubaren Projektschritten, welche weder die Organisation noch die Anwender überfordern.

Consumer IAM (CIAM)

Im Identity & Access Management (IAM) richtet sich der Fokus traditionell vor allem auf die Mitarbeiter, deren Benutzerkonten und Zugriffsberechtigungen zentral und automatisiert verwaltet werden sollen. Mit Voranschreiten der Digitalisierung rückt aber auch immer mehr der Endkunde ins Blickfeld: Das Management von Kundenidentitäten, die Unterstützung von Social Logins und die Zugriffssteuerung auf interne (Web-)Anwendungen und Cloud-Dienste werden immer wichtiger.

TIMETOACT verbindet Kunden mit einer eindeutigen digitalen Identität, damit zum Beispiel Banken ihre Kunden unabhängig von deren aktuellen Standort identifizieren können, ohne sie persönlich kennenlernen zu müssen. Das erlaubt es, neue digitale Services auf individuelle Kundenanforderungen anzupassen und geräteunabhängig zugänglich zu machen. Auf diese Weise werden Wettbewerbsvorteile geschaffen, z. B. für Services für:

- Kreditkarten
- das Privatkundengeschäft
- Anlagenmanagement
- Prämienprogramme

TIMETOACT sichert die digitalen Identitäten von Benutzern, Geräten, Services und vernetzten Dingen. Wir nutzen kontinuierliche, kontextbezogene Sicherheit, um ungewöhnliche Ereignisse jederzeit und überall erkennen zu können. Das bedeutet für Sie, dass Sie Ihren Kunden ein weitaus persönlicheres und sichereres Erlebnis als bisher bieten können. In unserer zunehmend wettbewerbsorientierten Landschaft ist dies etwas, worauf Sie bauen können.

Ihr Ansprechpartner:

Karl-Heinz Masser
Head of IAG Sales & Partner Management

+49 172 3093037
karl-heinz.masser@timetoact.de

Die drei größten IT-Sicherheitsrisiken für Organisationen

in den kommenden fünf Jahren

67 %
Datenmissbrauch / Datenintegrität

50 %
Cyber-Kriminalität (Betrug, Erpressung, Datendiebstahl)

41 %
Spionage/Spyware/ Ransomeware (Wirtschaftsspionage)

Quelle: Arbeitsmarktstudie von Robert Half Technology, Befragte: 200 CIOs und CTOs, Mehrfachnennungen möglich

TIMETOACT GROUP
SOFTWARE & CONSULTING