Identity und Access Management im Mittelstand: Notwendigkeit und Herausforderung

C-IAM GMBH
IDENTITY & ACCESS MANAGEMENT AS A SERVICE

Cybersecurity und Datensicherheit sind nicht erst seit der Einführung der Datenschutzgrundverordnung (DSGVO) in aller Munde und das vollkommen zu Recht. Durch die zunehmende Digitalisierung von Daten und Prozessen ist die Menge an schützenswerten persönlichen und geschäftlichen Daten größer denn je – und Bedrohungen von außen werden oft viel intensiver wahrgenommen als Risiken, die innerhalb von Unternehmen bestehen. Doch deren Schadenspotenzial, ob mutwillig oder schlicht fahrlässig, ist mindestens ebenso hoch.

Das hausgemachte Problem stellt sich dabei wie folgt dar: Oftmals ist in Unternehmen nicht nachvollziehbar, wer zu welchen Ressourcen Zugriff hat, welche Systeme überhaupt unternehmensweit existieren und ob die aktuellen Zugänge und Rechte der einzelnen Personen tatsächlich notwendig sind.

Wird für jedes Unternehmen zum Thema: Compliance

Abhilfe schaffen Identity- und Access-Management-Systeme (IAM). Sie ermöglichen eine zentrale Verwaltung der Rollen und Accounts der Mitarbeiter, Partner oder Kunden und der damit verbundenen Rechte, die sie benötigen um auf notwendige Daten, Dokumente und Accounts zuzugreifen. Mit diesen Funktionalitäten lösen sie die manuelle und oftmals sehr fragmentierte Benutzeradministration ab. IAM-Lösungen können den gesamten Lifecycle (On-Boarding, Wechsel, Off-Boarding) eines Nutzers, eine Audit-sichere Dokumentation der vergebenen Rechte und der damit verbundenen Vergabeprozesse sicherstellen, sowie Unternehmensprozesse abbilden, die durch eingebaute Sicherheitsprinzipien (4-Eyes Principle, Principle of Least Privilege, etc.) die Unternehmens-Compliance fördern.

Zudem fordert die DSGVO explizit eine Minimierung von Zugriffsrechten und verlangt von Unternehmen den Nachweis ihrer Compliance. Hier trägt die Einführung eines IAMs ebenfalls erheblich zur Konformität eines Unternehmens bei. Daher ist es nicht überraschend, dass das Interesse an IAM-Lösungen stark gestiegen ist.

IAM-Systeme – finanzierbar nur im Enterprise-Umfeld?

Identity- und Access-Management-Systeme sind nicht neu und Lösungen vieler verschiedener Anbieter sind dabei seit Jahren im Enterprise-Umfeld im Einsatz, beispielsweise bei Banken oder Versicherungen, die strengen Regularien unterliegen und verpflichtet sind, entsprechende Systeme zu nutzen – ungeachtet der Hindernisse, Kosten oder negativen Seiten einer Lösung. Kleinen und mittelständischen Unternehmen (KMU) dagegen blieb aus verschiedenen Gründen der Einsatz solcher Enterprise-Lösungen verwehrt.

Das Haupthindernis lag bislang darin, dass Enterprise-Lösungen sehr komplex sind, sowohl in ihrer programmatischen und oftmals monolithischen Struktur als auch in ihrer Bedienung. Die Einführung einer Lösung, aber auch der fortlaufende Betrieb sowie die notwendigen Anpassungen erfordern leistungsstarke Hardware und ein Expertenwissen, das

entweder im Haus aufgebaut werden muss oder von extern dazugekauft wird. Aufgrund der Marktlage ist dies in der Regel nicht einfach zu bewerkstelligen und mit intensiven Kosten verbunden. So kann das notwendige Budget allein für eine initiale Einführung und die damit verbundenen Anpassungen leicht auf einen kleinen bis mittleren Millionenbetrag anwachsen.

Diese Zeit- und Kostenintensität, die für Konzerne sicherlich darstellbar ist, stellt für viele mittelständische Unternehmen ein KO-Kriterium dar. Wenn die Höhe der Investition und die folgende Rentabilität natürlicherweise primäre Entscheidungskriterien sind, so liegt dieser Umstand im Mittelstand wie ein Bleifuß auf der Effizienzbremse.

Cloud-Lösungen – attraktiv für den Mittelstand

Mittlerweile gibt es Alternativen zu den herkömmlichen Enterprise-Lösungen. Angeboten werden sie von einigen IAM-Herstellern und der ausschlaggebende Punkt dabei ist: Software-as-a-Service (SaaS) oder Identity-as-a-Service (IdaaS). Cloud-IAM Lösungen können, im Rahmen ganzheitlicher Sicherheitskonzepte, schnell eingeführt und kosteneffizient betrieben werden. Darüber hinaus ermöglichen Standardisierung in den Prozessen und in den Prozessformaten den Unternehmen, die Entwicklungszeit zu ihrer Anpassung deutlich zu verkürzen und sie zudem unabhängig zu machen von Spezialisten. Gleichzeitig bleibt die Option erhalten, die Lösungen individuell an die Unternehmensanforderungen anzupassen.

Ein Identity- und Access-Management System ist dabei weit davon entfernt, für ein durchschnittliches Unternehmen off-the-shelf nutzbar zu sein, da sich Unternehmen zu sehr in ihren Anforderungen unterscheiden. Was es jedoch leisten kann ist, oft genutzte Lösungen bereitzustellen und die Anpassung und Neuentwicklung möglichst kundenfreundlich zu gestalten.

Masterplan für Workflows und Vergabeprozesse

Natürlich bedeutet die konkrete Umsetzung eines IAM-Projektes eine intensive Vorbereitung – auch um die auftretenden Schwierigkeiten und Hürden zu meistern. Verdeutlichen lässt sich dies an einem Fallbeispiel.

Die Ausgangslage: Ein Unternehmen hat 500 Identitäten, die verwaltet werden sollen. Im vorliegenden Fall sind dies die Mitarbeiter des Unternehmens, könnten aber auch zum Beispiel Partner oder Kunden sein. Der Zugang all dieser Identitäten zu den Zielsystemen soll mithilfe des IAM-Systems geregelt werden. In diesem Zusammenhang sind Zielsysteme all diejenigen Systeme, die an das IAM angeschlossen sind und die von diesem provisioniert werden, aber auch z.B. ein HR-System, welches lediglich lesend angeschlossen wird. Das betrachtete Unternehmen hat zehn solcher Systeme, darunter Standardsysteme wie Active Directory, LDAP, Relationale Datenbanken oder auch proprietäre Systeme, deren Anbindung eine neu zu entwickelnde Schnittstelle benötigt. Aktuell werden die Rechte über Gruppen in AD vergeben, sie sollen zukünftig durch ein Rollenkonzept ersetzt werden. Zudem sollen die Unternehmensprozesse im IAM abgebildet werden. Diese reichen von einfachen Prozessen, beispielsweise ein Urlaubsantrag oder das Zurücksetzen eines Passworts, bis hin zu mehrstufigen Vergabeprozessen für die Beantragung und Bewilligung von Rollen.

Jeder der genannten Schritte beinhaltet eine gewisse Komplexität und inhärentes Konfliktpotenzial innerhalb der Firma. Allein die Definition der Workflows kann ohne klare

Zuständigkeiten und ein gemeinsames Ziel der Stakeholder endlos in die Länge gezogen werden und damit die Kosten in die Höhe treiben.

Definition von Prozessen und Rechten ist eine Chance

Die Einführung eines IAM benötigt eine gründliche Vorbereitung und intensive Planung, bietet andererseits aber auch die Möglichkeit die Prozess- und Rechtelandschaft des Unternehmens von Grund auf zu bereinigen. Unternehmen ohne ein IAM-System benötigen viele manuelle Schritte und Abstimmungen zwischen HR, Administratoren, Mitarbeitern aller weiteren Abteilungen und Vorgesetzen *(Abb. 1).*

Benötigte Berechtigungen werden zunächst definiert, Rechte händisch erteilt und Passwörter für jede Anwendung vergeben.

Mit Einsatz eines IAM-Systems sind diese manuellen Schritte deutlich reduziert. Der Mitarbeiter bekommt eine Rolle zugeteilt, mit der er bereits die benötigte Liste an Rechten erhält. Weitere Berechtigungen werden zentral über das IAM-Dashboard beantragt. Durch digitalisierte und automatisierte Prozesse und Genehmigungen werden die Compliance-Regeln eingehalten und Mitarbeiter arbeiten ab dem ersten Tag mit den notwendigen Berechtigungen *(Abb. 2).*

Schlüssige Konzepte für angemessene Sicherheit

Ein IAM-System bietet bei korrekter und vollständiger Umsetzung einen Rahmen, innerhalb dessen die Konformität der Prozesse sichergestellt ist. Was dennoch bleibt, ist der Risikofaktor Mensch. Eine zwingende Genehmigung zur Voraussetzung der Vergabe von Rechten oder eine Rezertifizierung von bestehenden Berechtigungen verfehlen ihren Zweck, wenn sie, wie die meisten AGBs, einfach abgenickt und weggeklickt werden. Die zentral gesteuerte Provisionierung macht auch keinen Sinn, wenn die Vergabeprozesse umgangen werden könnten. Wenn der Kollege beim Zusammentreffen an der Kaffeemaschine nach einem Zugang auf eine Maschine fragen und diesen erhalten kann, wird die vermeintliche Sicherheit untergraben.

Oftmals muss zwischen Sicherheit und Benutzerfreundlichkeit abgewogen werden, zum Beispiel bei einer 2-Faktor-Authentifizierung. Diese bedeutet zwar einen weiteren Zwischenschritt des Nutzers, ist aber in manchen Bereichen absolut notwendig. Daher gilt es das Sicherheitsbedürfnis von Fall zu Fall zu prüfen, um zu entscheiden, wo erhöhte Sicherheit notwendig ist und wo es Prozesse zulassen, die Benutzerfreundlichkeit zu erhalten.

Der Nichteinsatz eines IAM-Systems öffnet die Türen für Hacker – und diese Erfahrung machen immer mehr Unternehmen. Nach eigenen Angaben waren 75 Prozent der Betriebe in Deutschland im Jahr 2019 von Datendiebstahl, Industriespionage oder Sabotage betroffen.

Dies erklärt den Trend zu einem Einsatz von IAM-Systemen. Mittelständische Unternehmen müssen bei ihren Sicherheitskonzepten berücksichtigen, dass ein IAM-System hinsichtlich der aufgezeigten Risiken kein Allheilmittel ist, aber dennoch einen wichtigen Bestandteil ihres Werkzeugkastens darstellt.

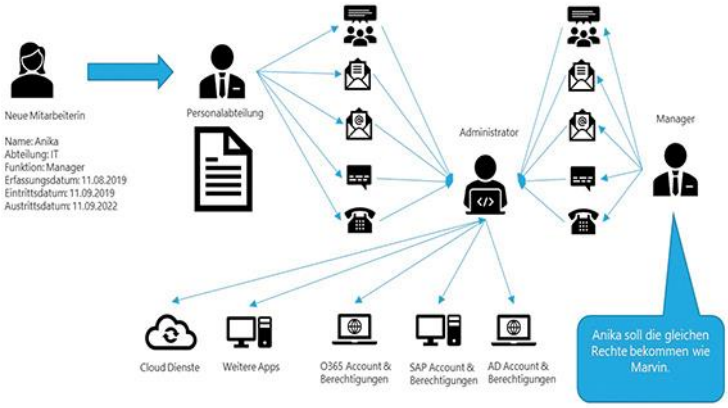

Abb. 1

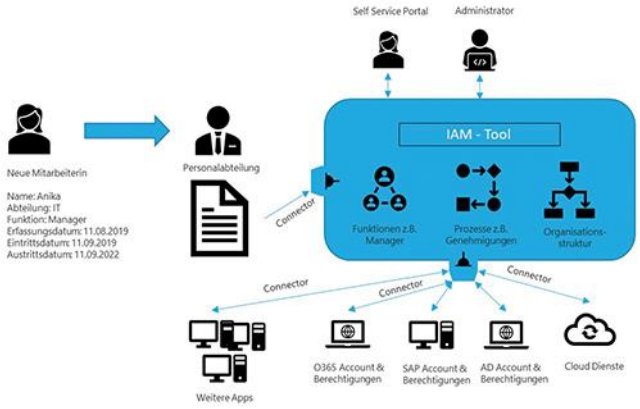

Abb. 2

“Die Einführung eines IAM benötigt eine gründliche Vorbereitung und intensive Planung – und bietet die Möglichkeit, die Prozess- und Rechtelandschaft des Unternehmens von Grund auf zu bereinigen.”
“Ein IAM-System bietet bei korrekter und vollständiger Umsetzung einen Rahmen, innerhalb dessen die Konformität der Prozesse sichergestellt ist. Was dennoch bleibt, ist der Risikofaktor Mensch.”
Dr. Babak Ahmadi, Geschäftsführer C-IAM GmbH

Die C-IAM GmbH schafft für Unternehmen ab 200 Mitarbeitern ideale Voraussetzungen, interne Compliance kostengünstig abzubilden und mehr Produktivität, Effizienz und Nachvollziehbarkeit in interne Prozesse zu bringen. DAS C-IAM System MY-CAMP Identity Suite (Made in Germany) schützt und vereinfacht Verfügbarkeit, Integrität und Vertraulichkeit.