IAM: Digitale Identitäten als Sicherheitsfaktor

Unsere Berufswelt hat sich in den letzten Jahren grundlegend verändert. Hybride IT-Infrastrukturen, Cloud Computing, neue Arbeits- und Zugriffsmöglichkeiten über mobile Endgeräte, Remote Work oder Homeoffice und die internationale Verflechtung vieler Unternehmen stellen immer höhere Anforderungen an die Cybersecurity. Während sich pandemiebedingt seit 2020 die Arbeitsplätze von Millionen Angestellten notgedrungen an den heimischen Schreibtisch verlagerten, nahm die Kriminalität im Netz kontinuierlich zu und hat nach Angaben des Bitkom e. V. im Rekordjahr 2021 bundesweit einen Gesamtschaden von 223 Mrd. EUR verursacht. Zunehmend erweisen sich dabei die digitalen Identitäten als Sicherheitsrisiko.

Damit tatsächlich nur autorisierte User einen sicheren Zugriff auf die von ihnen benötigten Ressourcen haben, nimmt das Identity and Access Management (IAM) eine Schlüsselrolle ein. Mit ihrer Innovationsstärke und langjährigen Branchenexpertise gehört die OEDIV SecuSys GmbH als Teil der Oetker-Gruppe zu den marktführenden Dienstleistern auf diesem Gebiet – zunehmend auch im immer wichtiger werdenden KRITIS-Umfeld.

Die Referenzen des Rostocker IAM-Anbieters sprechen dabei für sich und umfassen große Namen wie unter anderem die Flughafen München GmbH, die Stadtwerke Velbert GmbH, die Ehrmann GmbH, die BayWa IT GmbH, die TOYOTA Deutschland GmbH, das Goethe-Institut, den Caritasverband der Erzdiözese München und Freising e.V., die umlaut SE, die BNP Paribas Real Estate Deutschland oder die renommierte Hauck Aufhäuser Lampe Privatbank AG.

Warum aber kommt der sicheren Verwaltung von Identitäten eine so große Bedeutung zu? Dr. Anke Schäfer (AS) sprach dazu mit Patrick Piotrowski (PP), Sales Manager der OEDIV SecuSys GmbH.

AS: Seit Jahren warnen IT-Sicherheitsexperten davor, dass es nicht mehr darum ginge, „ob“ eine Cyberattacke stattfinde, sondern „wann“ dies geschehe. Dennoch trifft ein solcher Angriff viele Unternehmen erstaunlich unvorbereitet. Interessant ist dabei, dass immer häufiger von den eigenen Mitarbeiter/-innen das größte Sicherheitsrisiko ausgeht. Knapp ein Viertel der Datenschutzverletzungen wird inzwischen durch sogenannte interne Akteure verursacht – oft nicht einmal in böser Absicht. Wie kann ein leistungsstarkes IAM-System dabei unterstützen, Hackern möglichst keine leicht zugänglichen Einfallstore zu bieten?

PP: Neben Phishing-Betrug, der laut Symantec 70 % aller gezielten IT-Sicherheitsattacken ausmacht, beobachten wir immer wieder, dass verwaiste Accounts wie ein weit offenstehendes Fenster Cyberkriminellen eine willkommene Angriffsfläche bieten. Unternehmensführung und Angestellte sind sich oft nicht darüber im Klaren, welches Sicherheitsrisiko von fragmentierten oder ungenutzten digitalen Identitäten ausgeht. Die Einführung eines leistungsstarken IAM-Systems sensibilisiert nicht nur für diese immanenten Cyberbedrohungen, sondern bildet auch die Basis für ein rechtskonformes User Lifecycle Management. Im Mittelpunkt steht dabei die Frage: Wer darf was, wann und wo? Jede Person im Unternehmen oder auch jeder eng eingebundene externe Dienstleister hat dabei – je nach Position und Aufgabe – genau die für ihn angemessenen Berechtigungen. Hier sprechen wir von Least Privilege.

Unsere Produktsuite SecuIAM deckt die Gesamtheit aller Joiner-Mover-Leaver-Rejoiner-Prozesse ab – von der Vergabe der initialen Birthright-Zugriffsrechte beim Einstieg in das Unternehmen über die adäquate Abbildung der einzelnen beruflichen Stationen und persönlichen Meilensteine (z. B. Beförderung, Abteilungswechsel, Elternzeit) bis hin zur vollumfänglichen Entziehung aller Berechtigungen der jeweiligen IAM-Entität beim endgültigen Ausscheiden aus der Firma. So schützen wir sensible Daten vor unautorisierten Zugriffen und vereinfachen die Administration der konkreten Befugnisse über den gesamten User Lifecycle hinweg – vom Onboarding neuer Kolleg/-innen bis zum Offboarding bestehenden Personals.

Ein flexibel skalierbares Identity & Access Management, welches vor allem auf die Anforderung von Identity Governance and Administration (IGA) spezialisiert ist, wie wir es bieten, ermöglicht die passgenaue, effiziente und bereichsübergreifende Verwaltung von Benutzeridentitäten und -zugriffen und macht es Hackern schwer, diese in sich greifenden Kontrollmechanismen zu durchbrechen.

AS: Welche Leistungsbereiche werden hierbei abgedeckt?

PP: Das reicht von der Verwaltung der Identitäten und Zugriffe über die prozessuale Steuerung und automatisierte Provisionierung von Benutzerkonten und die Abbildung verbindlicher Workflows, Benutzerrollen und zusätzlicher Freigaben bis hin zur rechtskonformen Erfüllung gesetzlicher Reporting- und Compliance-Vorgaben. Letzteres spielt z. B. eine Rolle beim Prinzip der Funktionstrennung (segregation of duties / SOD), mit der toxische Rollen- und Berechtigungskombinationen vermieden werden sollen – etwa bei der strikten Trennung der Kreditoren- und Debitorenbuchhaltung oder der Entflechtung von Netz und Vertrieb im KRITIS-Segment.

AS: Welche konkreten Vorteile hat eine zentrale Benutzerverwaltung?

PP: Compliance, Cybersicherheit und Automatisierung – das sind die drei großen Motoren, die uns bei der ständigen Weiterentwicklung unseres IAM-Systems antreiben. Dabei sind die konkreten Vorteile so vielschichtig, wie es unterschiedliche Zielgruppen gibt.

Dank maßgeschneiderter, automatisierter Self Services – etwa zur Änderung oder Löschung spezifischer Benutzerrechte – profitieren die Nutzenden von einer besseren User Experience und einer messbaren Zeitersparnis gegenüber dem alten Ticketsystem. Sie müssen nicht mehr auf die Unterstützung der Administration warten, die wiederum ihrerseits spürbar entlastet wird und sich auf ihre Kernaufgaben und die fachliche Weiterentwicklung des Systems konzentrieren kann. Auch für leitende Angestellte, die Geschäftsführung und Vorstände verringert sich der administrative Aufwand: Eine einmal beantragte und automatisch zugewiesene Rolle bedeutet Arbeitsfähigkeit von Tag 1 an. Zugleich können bei rechtlichen Unklarheiten, Nachfragen durch Wirtschaftsprüfende oder im Rahmen der Prokura-Haftung mit einem einzigen Knopfdruck die entsprechenden Compliance-Nachweise erbracht werden. Das schafft Rechtssicherheit, Transparenz und Prozesseffizienz. Und auch die Vorteile für die Kund/-innen, Stakeholder und Externe liegen auf der Hand: niedrigere Gesamtkosten, ein geringeres Geschäftsrisiko und ein schneller ROI durch die Erschließung wertvoller Vereinfachungspotentiale.

AS: Was raten Sie Entscheider/-innen, die die Einführung eines IAM-Systems in Erwägung ziehen?

PP: Am Anfang sollte immer eine sorgfältige Anforderungs- und Reifegradanalyse stehen. Dabei sollten sich Entscheider/-innen eines Aspektes besonders bewusst sein: Während man ein ERP-System z. B. als das prozessuale Herzstück einer IT-Infrastruktur definieren könnte, steht die zentrale Benutzerverwaltung im technisch-organisatorischen Mittelpunkt. Die Einführung eines IAM-Systems hat immer auch direkte Auswirkungen auf das Zusammenspiel mit anderen Unternehmensbereichen, wie es sich z. B. im Directory widerspiegelt. Es ist also von zentraler Bedeutung, dass alle Angestellten sowie alle anderen Stakeholder frühzeitig eingebunden und ehrlich und auf Augenhöhe für die Vorteile eines zukunftsstarken IAM begeistert werden. Für einen nachhaltigen Erfolg ist genau diese gelebte Identity Awareness mindestens genauso wichtig wie eine sauber strukturierte, professionelle Projektplanung.

Hier finden sich auch weitere spannende Synergien zu anderen integrativen IAM-Ansätzen wie der Microsoft-Azure-Identitäts- und Zugriffsverwaltung (Identity and Access Management / Privileged Access Management). Ausgehend von ihren konkreten Anforderungen, unterstützen wir unsere Kund/-innen auf der gesamten Bandbreite – von der ersten Beratung, Standortbestimmung und Evaluierung geeigneter Förderprogramme über die Umsetzung des Einführungsprojektes bis hin zu eventuellen Anpassungen und Erweiterungen im laufenden Softwarebetrieb. Ob als On-Premise-Lösung oder aus der Cloud: Die Software für die Nutzer- und Berechtigungsverwaltung ist weitestgehend frei konfigurierbar und kann flexibel an aktuellen und zukünftigen Anforderungen ausgerichtet werden.

AS: Kommen wir zu einem abschließenden Ausblick: Wie sieht das IAM-System der Zukunft aus?

PP: Ein effektives IAM-System umfasst schon heute nicht mehr nur Personen, sondern auch Geräte, Anwendungen, Dienste oder Microservices. Gerade vor dem Hintergrund der zunehmenden smarten Vernetzung im Internet der Dinge gewinnen diese sogenannten Machine Identities an Bedeutung und stellen neue Anforderungen an ein intelligentes, zukunftsstarkes Identity and Access Management – nicht zuletzt auch unter IT-Sicherheitsaspekten. Unsere Muttergesellschaft OEDIV Oetker Daten- und Informationsverarbeitung KG kann bei Themen rund um Microsoft Azure eine große Expertise aufweisen.

Neben neuen, innovativen RPA-Methoden (Robotic Process Automation) und dem Einsatz Blockchain-gestützter Verifizierungen wird zukünftig selbstverständlich auch die Zahl KI-gestützter Analysen und Role-Mining-Prozesse steigen. Dank unserer agilen Softwareentwicklungsstrukturen sind wir schnell, flexibel und innovativ genug, um unser IAM-System kontinuierlich auf eine neue Qualitätsebene zu heben.

AS: Vielen Dank für das Gespräch!

Patrick Piotrowski
Sales Manager
OEDIV SecuSys GmbH

Dr. Anke Schäfer
Dr. Schäfer PR- und Strategieberatung

Das Interview führte Dr. Anke Schäfer, Dr. Schäfer PR- und Strategieberatung.