OEDIV SecuSys GmbH erweitert Cybersecurity-Angebot um individuelle IAM-Assessments

Bestandsaufnahme und konkrete Handlungsempfehlungen

Sicherheit ist kein statischer Zustand, sondern ein kontinuierlicher Verbesserungs- und Selbstoptimierungsprozess. In den letzten Jahren hat sich dabei das Thema Identity & Access Management (IAM) – also eine zentrale Identitäts-, Rollen- und Zugriffsverwaltung über sämtliche Systeme und Anwendungen einer Organisation hinweg – zu einer der tragenden Säulen der Cybersicherheit entwickelt und ist heute aus keinem IT-Sicherheitskonzept mehr wegzudenken. Angesichts der weltweit stetig steigenden Bedrohungslage und immer strikter werdender regulatorischer Anforderungen – wie die des IT-Sicherheitsgesetzes 2.0 und der noch in nationales Recht umzusetzenden NIS2-Richtlinie der EU – entscheiden sich immer mehr Unternehmen für die Implementierung leistungsstarker IAM-Tools. Grundsätzlich wird dabei jede in die internen Strukturen eingebundene Person mit einer individuellen digitalen Identität verknüpft, die nachvollziehbar macht, wer (auch über unterschiedliche Accounts) wann auf welche Daten, Ordner und Systeme Zugriff hat.

Doch wie steht es um die eigene, idealerweise rollen- und regelbasierte Daten-Compliance? Im Rahmen eines IAM-Assessments erstellen die Branchenexperten der OEDIV SecuSys GmbH eine ehrliche sowie den Kundenbedürfnissen entsprechende Bestandsaufnahme, geben konkrete Handlungsempfehlungen und entwickeln im engen partnerschaftlichen Austausch mit ihren Kund/-innen ein ganzheitliches Zielbild für ein effektives, rechtskonformes und sicheres Benutzer- und Berechtigungsmanagement. Konzipiert wurde das Vorgehensmodell von Patrick Piotrowski (PP), der aus seiner mehrjährigen Praxis als Sales Manager der OEDIV SecuSys GmbH die damit verbundenen Herausforderungen wie kein anderer kennt. Dr. Anke Schäfer (AS) sprach mit ihm über Methodik und Mehrwerte.

AS: Auch wenn sie erst noch in Bundesrecht eingehen muss: Die Anfang des Jahres in Kraft getretene NIS2-Richtlinie der EU bedeutet für viele Unternehmen eine neuerliche Verschärfung der regulatorischen Anforderungen hin zu einer länder- und sektorenübergreifenden Sicherheitskultur. Die Implementierung einer IAM-Lösung könnte hier eine zukunftssichere Option sein. Welchen Weg sollten Entscheider/-innen dabei einschlagen? Welche Tools empfehlen Sie konkret?

PP: Zunächst sollte man sich bewusst sein, dass IAM kein Softwareprodukt, sondern eine Sicherheitsdisziplin ist. Leider gibt es nicht die eine, hocheffektive IAM-Software, die alle Sicherheitsrisiken auf ein Minimum reduziert, sämtliche Compliance-Anforderungen erfüllt, die Berechtigungsverwaltung weitgehend automatisiert und dazu noch die User Experience auf ein neues Level hebt. Glauben Sie keinem Anbieter, der das dennoch verspricht. Welches Tool oder auch welche unterschiedlichen Tools bestmöglich miteinander abgestimmt den ganz spezifischen Herausforderungen jeder einzelnen Organisation gerecht werden, lässt sich am besten im Rahmen eines umfassenden 360-Grad-IAM-Assessments herausfinden.

AS: Sie führen gemeinsam mit Ihren Kunden individuelle IAM-Assessments durch, um herauszufinden, welche Tools in Frage kommen. Welche IAM-Tools sind das in der Regel?

PP: Hauptsächlich sind dies Lösungen mit einer Spezialisierung auf Identity Governance & Administration (IGA), Privileged Access Management (PAM) oder das klassische Access Management. Im Cloud-Umfeld erfreuen sich zudem CASB-Tools, also Cloud Access Security Broker, immer größerer Beliebtheit.

AS: Das klingt erst einmal sehr kompliziert. Bevor es zu technisch wird: Erläutern Sie uns doch bitte kurz die jeweiligen Begriffe und Mehrwerte!

PP: Gern, ich versuche es auf den Punkt zu bringen.

Die Identity Governance & Administration (IGA) beschäftigt sich hauptsächlich mit der Verwaltung und Überwachung von Identitäten innerhalb einer Organisation. Es wird meist aus einem Personalverwaltungssystem mit Stammdaten gespeist und provisioniert gekoppelte Systeme. Unter dem Begriff Provisionierung versteht man übrigens das automatische Anlegen, Editieren und Deaktivieren bzw. Löschen von Benutzerkonten oder Ressourcen, wie Shared Mailboxes inkl. zugehöriger AD-Gruppen. Dank entsprechender Regelwerke können Nutzende über Self-Services die Rollen, Accounts, Berechtigungen oder Ressourcen ordern und nach erfolgter Freigabe wird die Provisionierung angestoßen. Das verringert die Bereitstellungszeiten und entlastet den Service Desk. Grundlage für die Automatisierung ist ein Business-Rollenmodell. Dazu kommen weitere Self-Services, unter anderem für Compliance-Praktiken wie den Kennwort-Reset, die Rezertifizierung von Rollen oder das Monitoring der Umsetzung der Segregation of Duties.

AS: Durch die organisatorische Funktionstrennung zwischen den einzelnen Organisationseinheiten oder Stellen im Geschäftsprozess werden ja auch mögliche Interessenkollisionen vermieden.

PP: Genau. So können die IT-Sicherheit und Compliance nachhaltig gestärkt werden.

Ein zweiter großer Bereich umfasst das Privileged Access Management (PAM). Es verwaltet privilegierte Zugänge, beispielsweise administrative Konten mit hohen Berechtigungen. Die Credentials – also die Berechtigungsnachweise – dieser Konten werden gehärtet, die Zugriffsrechte der administrativen Konten streng reguliert, die Sessions geloggt und Bedrohungsanalysen gefahren.

Kommen wir zum Schluss zum dritten übergreifenden Segment: den klassischen Access Management Systemen. Sie bestehen im Kern meist aus einem Identity Provider (IdP), der Identitäts- und Authentifizierungsinformationen an andere IdP oder Anwendungen weitergibt und damit unter anderem einen Single Sign-On (SSO) – also eine Einmalanmeldung – ermöglicht. Das bekannteste Beispiel sind die Verzeichnisdienste von Microsoft. Es ist gängige Praxis, verschiedene Anwendungen an das Azure Active Directory (Azure AD) zu koppeln, so dass die Benutzerverwaltung in und die Authentifizierung an diesen Systemen über das Azure AD erfolgt. Für die Benutzerin oder den Benutzer bedeutet das letztlich, dass sie oder er sich mit einem einzigen Zugang an verschiedensten Anwendungen anmelden kann. Den IT-Verantwortlichen wird die Verwaltung der Anwendungen durch diese Zentralisierung erleichtert.

AS: Ein gewaltiges Spektrum, bei dem es tatsächlich schwerfällt, den Überblick zu behalten. Wie können wir uns den Ablauf eines IAM-Assessments konkret vorstellen?

PP: Zunächst identifizieren wir die IAM-Anforderungen und IAM-Risiken der Organisation. Vor allem die Risiken sind vielen gar nicht bewusst. Sobald wir die Anforderungen und auch die Risiken kennen, bewerten wir diese und geben dann basierend auf unserem breiten Lösungsportfolio eine objektive Empfehlung zu passenden Tools. Im Vordergrund steht dabei die Frage, welche IAM-Praktiken die Organisation nach Best Practices implementieren sollte. Dabei geht unser Lösungsangebot dank der Partnerschaften mit verschiedenen Unternehmen, die auf Security spezialisiert sind, über unsere eigene IAM-Lösung hinaus. So können wir bedarfsorientierte Empfehlungen aussprechen, die den individuellen Kundenanforderungen gerecht werden.

AS: Sind Ihre Assessments auf die ganz spezifischen Anforderungen jedes einzelnen Unternehmens abgestimmt?

PP: Ja, das ist und war uns von Anfang an sehr wichtig. Es gibt immer eine Phase des Initial Consultings. Hier werden Anforderungen an die Compliance, die Komplexität der Organisation und weitere Faktoren grob abgesteckt, um unseren Kundenunternehmen eine individuelle Empfehlung zu Umfang und Themen des Assessments geben zu können. Bei einem mittelständischen Unternehmen aus dem produzierenden Gewerbe beispielsweise, das 300 Mitarbeitende beschäftigt und nur geringfügigen regulatorischen Anforderungen unterliegt, beschränken wir uns auf das Wesentliche. Weiterführende und komplexe Themen wie AI-gestützte Identity Intelligence könnten wiederum für vernetzt agierende, größere Unternehmen der Kritischen Infrastruktur interessant werden.

AS: Als Teil der Oetker-Gruppe und 100%ige Tochtergesellschaft der OEDIV Oetker Daten- und Informationsverarbeitung KG gehört die OEDIV SecuSys GmbH zu den marktführenden Dienstleistern im IAM-Segment. Werden Sie mit Ihrem IAM-Assessment nicht auch ein wenig zur Konkurrenz Ihrer Muttergesellschaft, die mit Ailaa – basierend auf einem unverbindlichen und kostenfreien Basis-Check – ein Angebot zur Cybersecurity-Absicherung macht? (https://www.ailaa.de/news/artikel/sicherheit-und-orientierung-fur-kmu, Website: https://www.ailaa.de/)

PP: Im Gegenteil. Im Interesse unserer Kundenunternehmen verstehen wir uns als Einheit. Wir schätzen und ergänzen uns. So sind zum Beispiel Teile des IAM-Assessments auch in Ailaa implementiert. Wenn man so will, kann man sagen, dass die Nutzenden mit Ailaa also bereits ein Assessment „light“ geboten bekommen. In unserem IAM-Assessment gehen wir neben den IT-Sicherheitsaspekten zusätzlich auf IAM-Spezifika ein und verstehen es daher ganz eindeutig als Ergänzung zu Ailaa. Es rundet unser gemeinsames Cybersecurity-Lösungsangebot ab, gibt eine wichtige Positionsbestimmung und Zielorientierung. Das schafft wertvolle Synergien, von denen unsere Kunden- und Partnerunternehmen gleichermaßen profitieren.

AS: Vielen Dank für das Gespräch!

www.secusys.de

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.