Holger Reibold

Identity & Access Management ohne Enterprise-Budget

Praxisstrategien für KMU, Startups und mittelständige IT

BRAIN-MEDIA.DE

Holger Reibold

Identity & Access Management ohne Enterprise-Budget

Praxisstrategien für KMU, Startups und mittelständische IT

BRAIN-MEDIA.DE

ISBN: 978-3-95444-335-2

Cover: Freepik

Brain-Media.de

Dr. Holger Reibold – Hubert-Müller-Str. 52c – 66113 Saarbrücken

info@brain-media.de – www.brain-media.de

Inhaltsverzeichnis

Vorwort

Identit ten sind die neuen Firewalls. Wer den Zugang kontrolliert, sch tzt das Unternehmen – auch ohne Millionenbudget.

Digitale Identitäten sind heute der zentrale Zugangspunkt zu nahezu allen Unternehmensressourcen. Anwendungen, Daten, Cloud-Dienste, administrative Systeme und sogar physische Infrastruktur werden über Benutzerkonten gesteuert. Wer eine Identität kontrolliert, kontrolliert in vielen Fällen auch den Zugriff auf geschäftskritische Systeme. Genau deshalb haben sich Identitäten in den letzten Jahren zu einem der wichtigsten Angriffspunkte für Cyberkriminelle entwickelt.

Trotz dieser Entwicklung wird Identity & Access Management (IAM) in vielen Organisationen noch immer als ein komplexes Enterprise-Thema betrachtet. Häufig herrscht die Vorstellung, dass ein funktionierendes IAM nur mit umfangreichen Plattformen, spezialisierten Tools und großen Budgets möglich ist. Für viele kleine und mittlere Unternehmen führt diese Annahme dazu, dass Identity & Access Management entweder gar nicht umgesetzt oder nur fragmentarisch betrieben wird.

Die Realität sieht jedoch anders aus. Die meisten erfolgreichen Angriffe nutzen keine hochkomplexen technischen Schwachstellen aus. Stattdessen basieren sie auf grundlegenden Problemen im Umgang mit digitalen Identitäten: unkontrollierte Benutzerkonten, dauerhaft privilegierte Administratorrechte, fehlendes Offboarding oder unzureichend abgesicherte Zugänge zu Cloud-Diensten. Diese Schwachstellen entstehen selten aus mangelnder Technologie, sondern meist aus fehlenden Prozessen, unklaren Verantwortlichkeiten oder historisch gewachsenen IT-Strukturen.

Ein Blick auf reale Sicherheitsvorfälle zeigt immer wieder ein ähnliches Muster. In vielen Fällen hätten einfache Maßnahmen einen Angriff zumindest deutlich erschweren können: aktivierte Multi-Factor Authentication, sauber verwaltete Administratorrechte, klare Prozesse für das Anlegen und Entfernen von Benutzerkonten oder transparente Zugriffsprotokolle. Genau diese grundlegenden Maßnahmen bilden den Kern eines funktionierenden Identity & Access Managements.

Parallel dazu steigen die Anforderungen an Unternehmen kontinuierlich. Kunden erwarten einen verantwortungsvollen Umgang mit Daten, regulatorische Vorgaben werden strenger, und auch Cyberversicherungen prüfen zunehmend genauer, welche Sicherheitsmaßnahmen tatsächlich umgesetzt wurden. In vielen Schadensfällen zeigt sich, dass fehlende oder unzureichende Kontrollen rund um digitale Identitäten ein zentraler Faktor sind – und Versicherung die Leistungen verweigern.

Dieses Buch richtet sich daher bewusst an Organisationen, die keine großen Security-Abteilungen oder umfangreichen Budgets zur Verfügung haben. Es richtet sich an IT-Leiter im Mittelstand, Administratoren in wachsenden Unternehmen, Security-Verantwortliche in kleinen Organisationen sowie Managed Service Provider, die Sicherheitsstrukturen für ihre Kunden aufbauen müssen.

Der Ansatz dieses Buches ist bewusst pragmatisch. Statt theoretischer Frameworks oder komplexer Enterprise-Architekturen steht die Frage im Mittelpunkt: Welche Maßnahmen bringen mit begrenzten Ressourcen den größten Sicherheitsgewinn? Viele Organisationen verfügen bereits über leistungsfähige Werkzeuge – etwa Active Directory, Microsoft Entra, Google Workspace oder verschiedene Cloud-Dienste. Entscheidend ist nicht in erster Linie die Technologie, sondern wie diese Systeme strukturiert eingesetzt werden.

Das Buch beschreibt deshalb ein pragmatisches Minimal-IAM-Modell. Dieses Modell konzentriert sich auf wenige zentrale Prinzipien: klare Identitätsverwaltung, kontrollierte Berechtigungen, sichere Administratorzugänge, nachvollziehbare Zugriffsprozesse und einen sauberen Benutzer-Lifecycle vom Eintritt bis zum Austritt eines Mitarbeiters.

Das Ziel ist nicht, eine perfekte oder vollständig standardisierte IAM-Architektur aufzubauen. Vielmehr geht es darum, eine solide Grundlage zu schaffen, auf der Organisationen ihre Identitäten kontrollieren und Zugriffe nachvollziehen können. Genau diese Grundlagen

entscheiden oft darüber, ob ein Sicherheitsvorfall begrenzt bleibt oder zu einem größeren Schaden eskaliert.

Identity & Access Management ist daher keine Frage von Enterprise-Budgets oder komplexen Plattformen. Es ist in erster Linie eine Frage von Struktur, Priorisierung und Verantwortlichkeit.

Dieses Buch soll Ihnen dabei helfen, genau diese Struktur aufzubauen.

Herzlichst

Holger Reibold

1 Warum IAM geschäftskritisch ist

Passw rter sind das Prim rziel. In einer Welt ohne Netzwerkgrenzen ist die digitale Identit t die letzte Verteidigungslinie.

Digitale Identitäten sind heute der zentrale Zugangspunkt zu nahezu allen IT-Systemen eines Unternehmens. Mitarbeiter melden sich mit Benutzerkonten an Anwendungen, Cloud-Dienste und interne Plattformen an, Administratoren steuern Systeme über privilegierte Accounts und externe Partner erhalten Zugriff auf gemeinsame Ressourcen. Wer eine Identität kontrolliert, kontrolliert häufig auch den Zugriff auf geschäftskritische Daten und Systeme.

Gleichzeitig hat sich die IT-Landschaft vieler Unternehmen in den letzten Jahren stark verändert. Cloud-Dienste, mobile Arbeitsplätze und SaaS-Anwendungen haben klassische Netzwerkgrenzen weitgehend aufgelöst. Während früher vor allem das Unternehmensnetzwerk geschützt werden musste, steht heute zunehmend die Kontrolle von Identitäten und Zugriffsrechten im Mittelpunkt der Sicherheitsarchitektur.

Trotz dieser Entwicklung wird Identity & Access Management in vielen Organisationen noch immer unterschätzt oder als komplexes Enterprise-Thema betrachtet. Dieses Kapitel zeigt, warum IAM heute geschäftskritisch ist, welche typischen Fehlannahmen existieren und

wie ein pragmatischer Ansatz auch mit begrenzten Ressourcen umgesetzt werden kann.

1.1 Der Mythos Security = Enterprise-Budget

In vielen Organisationen existiert eine weit verbreitete Annahme: Effektive IT-Sicherheit ist nur mit großen Budgets und komplexen Enterprise-Lösungen möglich. Besonders im Bereich Identity & Access Management wird häufig davon ausgegangen, dass erst umfangreiche Plattformen, spezialisierte Security-Tools und große Teams eine angemessene Kontrolle über Identitäten und Zugriffsrechte ermöglichen.

Diese Wahrnehmung hat historische Gründe. In den frühen Jahren moderner IAM-Systeme waren entsprechende Lösungen tatsächlich stark auf große Unternehmen ausgerichtet. Komplexe Identity-Plattformen, umfangreiche Rollenmodelle und hochgradig automatisierte Governance-Prozesse wurden vor allem für internationale Konzerne entwickelt. Die Implementierung solcher Systeme war teuer, zeitaufwendig und organisatorisch anspruchsvoll. Für viele kleine und mittlere Unternehmen erschien IAM daher als ein Thema, das außerhalb ihrer Möglichkeiten liegt.

Diese Perspektive führt jedoch zu einem grundlegenden Missverständnis. Sicherheit entsteht nicht primär durch die Anzahl eingesetzter Tools oder durch hohe Investitionen in Technologie. Entscheidend sind vielmehr klare Strukturen, definierte Prozesse und eine

konsequente Kontrolle über digitale Identitäten. Viele Sicherheitsprobleme entstehen gerade dort, wo diese Grundlagen fehlen.

Typische Beispiele finden sich in nahezu jeder Organisation: Benutzerkonten ehemaliger Mitarbeiter bleiben aktiv, Administratorrechte werden dauerhaft vergeben, mehrere Personen teilen sich ein gemeinsames Konto oder Zugriffsrechte wachsen über Jahre unkontrolliert an. Solche Situationen entstehen selten aus bewusster Nachlässigkeit. Häufig sind sie das Ergebnis von Zeitdruck, organisatorischen Veränderungen oder historisch gewachsenen IT-Strukturen.

Gerade kleine und mittlere Unternehmen sind davon besonders betroffen. IT-Abteilungen bestehen oft aus wenigen Mitarbeitern, die gleichzeitig Infrastruktur, Support, Projekte und Sicherheitsaufgaben betreuen. In solchen Umgebungen liegt der Fokus verständlicherweise auf der Stabilität der Systeme und dem täglichen Betrieb. Themen wie strukturiertes Identity Management werden daher häufig erst dann adressiert, wenn konkrete Probleme auftreten.

Dabei zeigt die Praxis, dass viele grundlegende IAM-Maßnahmen mit vergleichsweise geringem Aufwand umgesetzt werden können. Ein sauberer Benutzer-Lifecycle, klare Trennung von Administrator- und Standardkonten, konsequente Nutzung von Multi-Factor Authentication oder regelmäßige Überprüfung von Berechtigungen erfordern keine komplexen Enterprise-Plattformen. Oft reichen vorhandene Systeme wie Active Directory, Cloud-Identitätsdienste oder einfache organisatorische Prozesse aus.

Der entscheidende Unterschied liegt daher nicht im Budget, sondern im Ansatz. Organisationen, die Identity & Access Management als strukturelles Thema verstehen, können auch mit begrenzten Ressourcen eine solide Sicherheitsbasis schaffen. Statt auf umfassende Enterprise-Lösungen zu warten, geht es darum, schrittweise klare Regeln für Identitäten und Zugriffsrechte zu etablieren.

Der Mythos, dass Sicherheit ausschließlich eine Frage des Budgets ist, führt daher häufig zu einer gefährlichen Passivität. Unternehmen verschieben notwendige Maßnahmen, weil sie glauben, zunächst umfangreiche Investitionen tätigen zu müssen. In Wirklichkeit beginnt wirksames Identity & Access Management jedoch mit einfachen Prinzipien – und genau diese lassen sich auch ohne Enterprise-Budget umsetzen.

1.2 Der Cyber-Insurance-Weckruf

In den letzten Jahren hat sich ein weiterer Faktor zu einem wichtigen Treiber für IT-Sicherheit entwickelt: Cyberversicherungen. Immer mehr Unternehmen schließen entsprechende Policen ab, um sich gegen finanzielle Schäden durch Cyberangriffe, Datenverluste oder Betriebsunterbrechungen abzusichern. Gleichzeitig analysieren Versicherer sehr genau, unter welchen Umständen Sicherheitsvorfälle entstehen und welche Schutzmaßnahmen in betroffenen Organisationen vorhanden waren.

Dabei zeigt sich ein wiederkehrendes Muster. Viele Schadensfälle weisen ähnliche strukturelle Schwächen auf – insbesondere im Bereich der digitalen Identitäten. In zahlreichen Vorfällen konnten Angreifer Systeme nicht deshalb kompromittieren, weil hochkomplexe Sicherheitsmechanismen versagt haben, sondern weil grundlegende Kontrollen fehlten. Häufig geht es um einfache, aber kritische Maßnahmen wie aktivierte Multi-Factor Authentication, kontrollierte Administratorrechte oder ein strukturiertes Benutzer- und Berechtigungsmanagement.

Für Versicherungen hat dies direkte wirtschaftliche Konsequenzen. Wenn sich herausstellt, dass grundlegende Sicherheitsmaßnahmen nicht umgesetzt wurden, kann dies dazu führen, dass Versicherungsleistungen eingeschränkt oder sogar vollständig abgelehnt werden. In vielen Fällen argumentieren Versicherer, dass elementare Schutzmaßnahmen Teil der organisatorischen Sorgfaltspflicht sind und daher erwartet werden können.

Diese Entwicklung verändert die Rolle von IT-Sicherheit erheblich. Während Sicherheitsmaßnahmen früher häufig als rein technische Entscheidung betrachtet wurden, haben sie heute auch eine direkte wirtschaftliche und rechtliche Dimension. Unternehmen müssen zunehmend nachweisen können, dass sie angemessene Kontrollen zum Schutz ihrer Systeme implementiert haben. Identity & Access Management spielt dabei eine zentrale Rolle, weil nahezu jeder Angriff früher oder später mit der Kompromittierung einer digitalen Identität verbunden ist.

Cyberversicherungen reagieren auf diese Entwicklung mit immer detaillierteren Risikofragen. In Antragsformularen finden sich heute häufig konkrete Fragen zu Identitätskontrollen: Wird Multi-Factor Authentication für Administratoren eingesetzt? Existieren getrennte Konten für administrative Tätigkeiten? Werden Benutzerkonten beim Austritt von Mitarbeitern automatisch deaktiviert? Werden privilegierte Zugriffe protokolliert?

Diese Fragen zeigen deutlich, welche Maßnahmen als grundlegende Sicherheitsanforderungen betrachtet werden. Es geht dabei nicht um hochkomplexe Sicherheitsarchitekturen, sondern um zentrale Prinzipien eines funktionierenden Identity & Access Managements.

Für viele Organisationen wirkt diese Entwicklung wie ein Weckruf. Während Sicherheitsmaßnahmen früher oft erst nach einem Vorfall umgesetzt wurden, entsteht heute zusätzlicher Druck durch externe Anforderungen. Unternehmen müssen ihre Identitäts- und Zugriffsstrukturen nicht nur aus technischer Sicht verbessern, sondern auch, um Versicherbarkeit und Compliance sicherzustellen.

Der Blick der Cyberversicherer verdeutlicht damit eine zentrale Erkenntnis: Sicherheit beginnt nicht mit hochentwickelten Abwehrmechanismen, sondern mit der Kontrolle über digitale Identitäten. Genau hier setzt ein pragmatisches Identity & Access Management an – und genau hier können Organisationen mit vergleichsweise einfachen Maßnahmen einen erheblichen Sicherheitsgewinn erzielen.

1.3 Warum Identitäten das neue Angriffsziel sind

In der klassischen IT-Sicherheitsarchitektur lag der Schwerpunkt lange Zeit auf dem Schutz des Unternehmensnetzwerks. Firewalls, Netzwerksegmentierung und Intrusion-Detection-Systeme sollten verhindern, dass Angreifer von außen in interne Systeme eindringen konnten. Dieses Modell basierte auf einer klaren Annahme: Innerhalb des Netzwerks befanden sich vertrauenswürdige Systeme und Benutzer, während Bedrohungen primär von außen kamen.

Diese Annahme hat sich in der modernen IT-Landschaft grundlegend verändert. Cloud-Dienste, mobile Arbeitsplätze, SaaS-Anwendungen und externe Partnerzugänge haben die traditionellen Netzwerkgrenzen weitgehend aufgelöst. Mitarbeiter greifen von verschiedenen Standorten und Geräten auf Unternehmenssysteme zu, Anwendungen laufen nicht mehr ausschließlich im eigenen Rechenzentrum, und Daten werden über zahlreiche Plattformen hinweg verarbeitet.

In dieser Umgebung verliert das klassische Sicherheitsmodell des geschützten Netzwerks zunehmend an Bedeutung. Stattdessen rückt eine andere Frage in den Mittelpunkt: Wer greift auf Systeme zu und mit welchen Rechten? Genau hier kommen digitale Identitäten ins Spiel.

Für Angreifer sind Benutzerkonten heute eines der attraktivsten Ziele. Wenn es gelingt, eine gültige Identität zu kompromittieren, können Sicherheitsmechanismen häufig umgangen werden, ohne dass sofort Alarm ausgelöst wird. Der Zugriff erfolgt dann scheinbar legitim

– mit echten Benutzerkonten, gültigen Anmeldedaten und korrekten Zugriffsrechten.

Entwicklung moderner Cyberangriffe. Während früher Netzwerke oder Software-Schwachstellen im Fokus standen, konzentrieren sich Angreifer heute zunehmend auf Benutzerkonten und digitale Identitäten. 80 Prozent aller Datenpannen involvieren gestohlene oder kompromittierte Zugangsdaten.

Viele moderne Angriffe folgen genau diesem Muster. Anstatt technische Schwachstellen auszunutzen, versuchen Angreifer zunächst Zugangsdaten zu erlangen. Dies kann über Phishing, gestohlene Passwörter, Credential-Stuffing-Angriffe oder kompromittierte Endgeräte erfolgen. Sobald eine Identität kontrolliert wird, bewegen sich Angreifer oft schrittweise durch die Infrastruktur, erweitern ihre Berechtigungen und suchen nach weiteren Zugriffsmöglichkeiten.

Besonders kritisch sind dabei privilegierte Konten. Administrator-Accounts verfügen häufig über weitreichende Rechte innerhalb von Systemen und Netzwerken. Wenn ein Angreifer Zugriff auf ein solches Konto erhält, kann dies weitreichende Konsequenzen haben –

vom Zugriff auf sensible Daten bis hin zur vollständigen Kontrolle über zentrale IT-Systeme.

Ein weiterer Faktor verstärkt diese Entwicklung zusätzlich: In vielen Organisationen existiert eine große Anzahl digitaler Identitäten. Neben Mitarbeiterkonten gehören dazu Service-Accounts, API-Zugänge, Cloud-Identitäten, Partnerzugriffe und temporäre Benutzerkonten. Ohne klare Struktur und Kontrolle kann schnell die Übersicht verloren gehen, welche Identitäten existieren und welche Rechte sie besitzen.

Angreifer profitieren genau von dieser Komplexität. Jede nicht verwaltete oder vergessene Identität stellt ein potenzielles Einfallstor dar. Ein ehemaliger Mitarbeiter mit aktivem Konto, ein Service-Account mit dauerhaftem Administratorzugriff oder ein schwach abgesicherter Cloud-Zugang können ausreichen, um in eine Infrastruktur einzudringen.

Die zunehmende Bedeutung digitaler Identitäten hat daher zu einem grundlegenden Wandel in der Sicherheitsstrategie geführt. Moderne Sicherheitsmodelle – etwa Zero-Trust-Architekturen – basieren auf der Annahme, dass kein Zugriff automatisch vertrauenswürdig ist. Stattdessen wird jeder Zugriff auf Basis der Identität, der Authentifizierung und der vergebenen Berechtigungen bewertet.

Identity & Access Management bildet damit eine zentrale Grundlage moderner IT-Sicherheit. Wer Identitäten kontrolliert, kontrolliert den Zugang zu Systemen, Anwendungen und Daten. Genau deshalb

stehen digitale Identitäten heute im Mittelpunkt vieler Angriffe – und genau deshalb ist ein strukturiertes IAM für Unternehmen jeder Größe unverzichtbar.

1.4 Typische IAM-Probleme im Mittelstand

Während große Unternehmen häufig über spezialisierte Security-Teams und etablierte Governance-Strukturen verfügen, sieht die Realität im Mittelstand oft anders aus. IT-Abteilungen bestehen hier häufig aus wenigen Mitarbeitern, die gleichzeitig für Infrastruktur, Support, Projekte und Sicherheitsaufgaben verantwortlich sind. In diesem Umfeld entsteht Identity & Access Management selten als bewusst geplante Architektur, sondern wächst über Jahre hinweg organisch.

Diese Entwicklung führt dazu, dass sich in vielen Organisationen ähnliche strukturelle Probleme rund um Identitäten und Zugriffsrechte bilden. Sie entstehen nicht aus mangelnder Professionalität, sondern aus pragmatischen Entscheidungen im laufenden Betrieb. Dennoch können genau diese Strukturen langfristig erhebliche Sicherheitsrisiken darstellen.

Ein häufiges Problem ist die unklare Übersicht über vorhandene Benutzerkonten. In vielen IT-Umgebungen existieren mehrere Verzeichnisse oder Identitätsquellen gleichzeitig – beispielsweise Active Directory, Cloud-Verzeichnisse, SaaS-Plattformen oder lokale Anwendungen. Ohne zentrale Verwaltung kann schnell der Überblick

verloren gehen, welche Identitäten tatsächlich existieren und welche Zugriffsrechte sie besitzen.

Eng damit verbunden ist das Thema Berechtigungswachstum. Mitarbeiter wechseln im Laufe der Zeit häufig ihre Aufgabenbereiche oder übernehmen zusätzliche Verantwortlichkeiten. In vielen Organisationen werden neue Zugriffsrechte hinzugefügt, ohne alte Berechtigungen konsequent zu entfernen. Auf diese Weise entstehen sogenannte „Privilege Accumulation"-Effekte: Benutzer besitzen im Laufe der Zeit immer mehr Rechte, als sie für ihre aktuelle Tätigkeit tatsächlich benötigen.

Ein weiteres typisches Problem betrifft privilegierte Konten. Administratorrechte werden in vielen Umgebungen dauerhaft vergeben, weil sie im täglichen Betrieb benötigt werden. Häufig verwenden Administratoren sogar ihre regulären Benutzerkonten für administrative Tätigkeiten. Diese Praxis erhöht jedoch das Risiko erheblich, da ein kompromittiertes Benutzerkonto unmittelbar weitreichende Systemzugriffe ermöglichen kann.

Auch das Offboarding von Mitarbeitern stellt in vielen Organisationen eine Herausforderung dar. Wenn Mitarbeiter das Unternehmen verlassen, müssen ihre Konten in allen relevanten Systemen deaktiviert oder gelöscht werden. Ohne klare Prozesse kann es jedoch passieren, dass einzelne Accounts aktiv bleiben – insbesondere in Cloud-Diensten oder spezialisierten Anwendungen. Solche vergessenen Konten können über lange Zeit unbemerkt bestehen bleiben.

Zusätzlich wächst in vielen Unternehmen die Zahl externer Zugänge. Dienstleister, Partner oder temporäre Projektmitarbeiter benötigen Zugriff auf bestimmte Systeme oder Plattformen. Ohne strukturierte Verwaltung entstehen dabei häufig temporäre Accounts, deren Berechtigungen nicht regelmäßig überprüft werden.

Schließlich fehlt in vielen Organisationen eine klare Dokumentation von Zugriffsrechten und Verantwortlichkeiten. Wer darf welche Systeme administrieren? Welche Rollen existieren im Unternehmen? Welche Rechte sind für bestimmte Aufgaben erforderlich? Ohne definierte Rollenmodelle werden Berechtigungen häufig individuell vergeben, was langfristig zu komplexen und schwer nachvollziehbaren Strukturen führt.

Diese Herausforderungen sind im Mittelstand besonders verbreitet, weil IAM selten als eigenständiges Architekturthema betrachtet wird. Stattdessen entstehen Identitätsstrukturen oft als Nebenprodukt des IT-Betriebs.

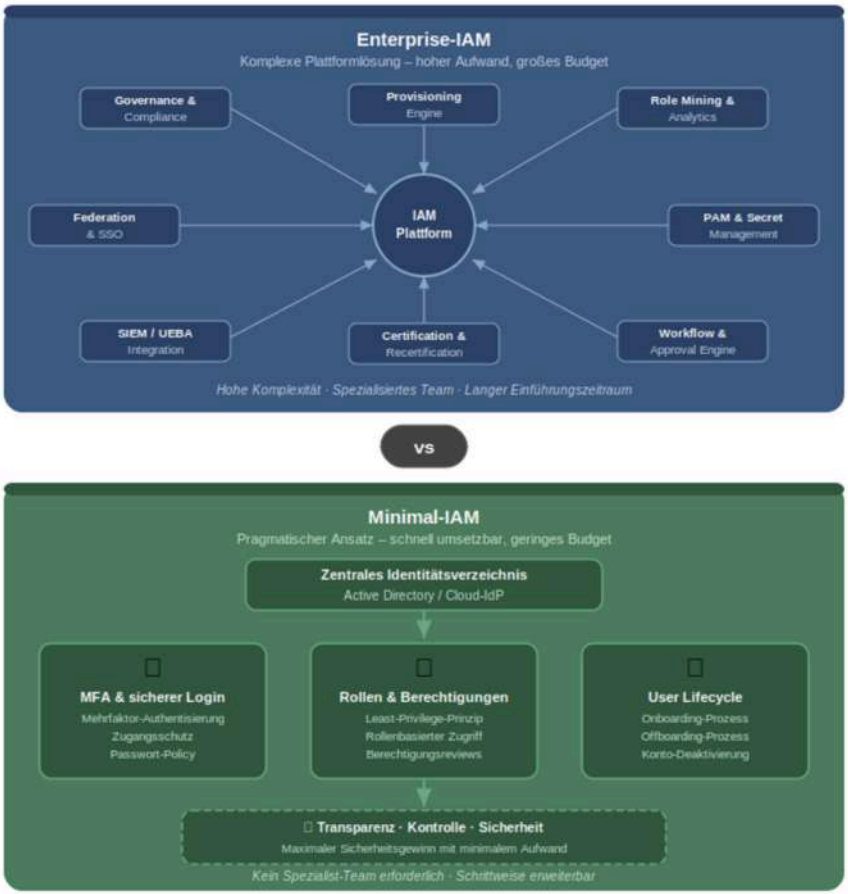
Genau hier setzt ein pragmatischer IAM-Ansatz an. Ziel ist nicht, sofort komplexe Enterprise-Strukturen aufzubauen, sondern zunächst Transparenz zu schaffen, grundlegende Prozesse zu definieren und privilegierte Zugriffe kontrolliert zu verwalten. Bereits diese Maßnahmen können einen erheblichen Beitrag zur Verbesserung der Sicherheitslage leisten.

1.5 Zielbild: Minimal-IAM statt Enterprise-IAM

Viele Organisationen verbinden Identity & Access Management automatisch mit komplexen Enterprise-Plattformen, umfangreichen Rollenmodellen und großen Transformationsprojekten. Tatsächlich wurden viele IAM-Lösungen ursprünglich für sehr große Unternehmen entwickelt, die tausende Benutzer, internationale Standorte und hochgradig regulierte Prozesse verwalten müssen. Die Einführung solcher Systeme ist häufig mit erheblichen Kosten, langen Projektlaufzeiten und umfangreichen organisatorischen Veränderungen verbunden.

Für kleine und mittlere Unternehmen ist ein solcher Ansatz jedoch selten realistisch. Die vorhandenen IT-Ressourcen sind begrenzt, Security-Teams bestehen oft aus wenigen Personen, und der operative IT-Betrieb hat verständlicherweise hohe Priorität. Wenn IAM ausschließlich als großes Enterprise-Projekt betrachtet wird, entsteht daher schnell eine Blockade: Die Umsetzung wird aufgeschoben, weil sie als zu komplex oder zu teuer erscheint.

Ein pragmatischer Ansatz besteht deshalb darin, Identity & Access Management zunächst auf ein Minimal-IAM-Modell zu reduzieren. Dieses Modell konzentriert sich auf wenige grundlegende Prinzipien, die den größten Sicherheitsgewinn liefern. Statt sofort vollständige Governance-Strukturen oder komplexe Rollenmodelle aufzubauen, geht es darum, zunächst Transparenz über vorhandene Identitäten zu schaffen und zentrale Zugriffsrisiken zu reduzieren.



Vergleich zwischen Enterprise-IAM und Minimal-IAM. Während große Plattformen zahlreiche Funktionen integrieren, konzentriert sich ein Minimal-IAM auf zentrale Sicherheitsmechanismen wie MFA, Rollenmodelle und Lifecycle-Prozesse.

Ein wesentliches Element eines Minimal-IAM ist die zentrale Verwaltung von Identitäten. Unternehmen sollten möglichst eine klare

Stichwortverzeichnis

H

I

J

K

L

M

N

O

P

Q

R

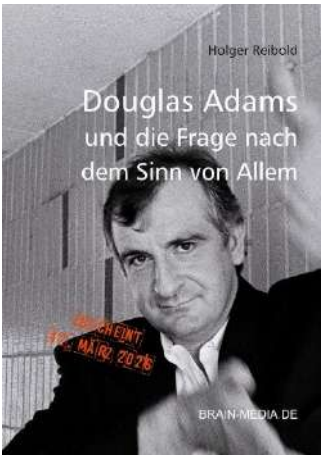
S

T

V

Z

Mehr von Brain-Media.de



42 – Douglas Adams und die Frage nach dem Sinn von Allem

Am 11. Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.

Umfang: 140 Seiten

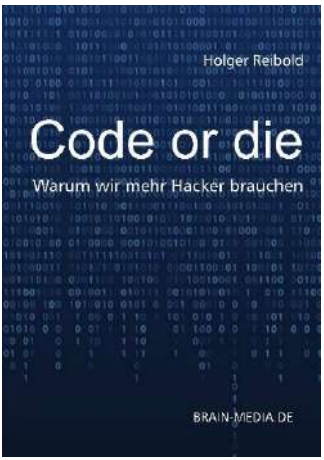
Preis: 14,99 EUR

Erscheint: 42. März 2026

Towelday, das ultimative Handtuch für alle Fans

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.

100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.



Code or die – Warum wir mehr Hacker brauchen

Ein Manifest für mehr digitale Selbstbestimmung, Neugierde und Eigenverantwortung. Medienkompetenzen alleine genügen nicht; die Gesellschaft von morgen braucht Digitalkompetenzen.

Umfang: 120 Seiten

Preis: 14,99 EUR

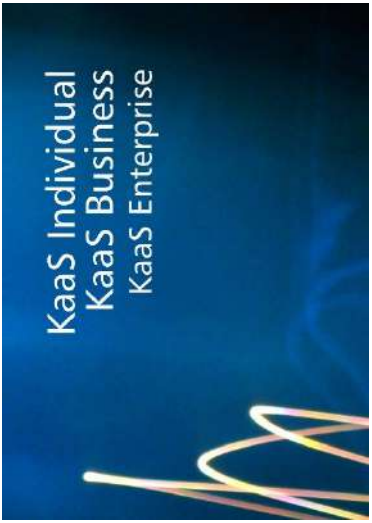
Erscheint Frühjahr 2026

Lokale KI – Sichere Architektur, Betrieb und Governance von GenAI- und RAG-Systemen

RAG- und LLM-Plattformen mit klarer Architektur, Guardrails, Monitoring und Governance kontrolliert und resilient betreiben.

Umfang: 270 Seiten

Preis: 24,99 EUR



Brain-Media KaaS

Individual

Business

Enterprise

– die E-Book-Flatrate –

Brain-Media.de ist ein **Pionier** in Sachen E-Book-Flatrates. Bereits 2014 wurden mit Plus+ E-Books als attraktives und preisgünstiges Abo angeboten. Im April 2026 erlebt Plus+ eine Renaissance.

Abonnementen erhalten **1 Jahr Zugriff auf alle E-Books**, die bereits erschienen sind, und auf alle Neuerscheinungen des Abozeitraums. Sie können über 30 verfügbare E-Books herunterladen – dazu editierbare Checklisten, Vorlagen, Beispiele etc. Sie können die E-Books ausdrucken und auf mehreren Lesegeräten verwenden. Die Inhalte werden kontinuierlich an die Dynamik der Entwicklung angepasst.

Und das alles zum **unschlagbaren Sonderpreis**!