Der Business Case als zentrales Element einer IAM-Investition

In diesem Whitepaper erläutern wir erste Argumente für ein unternehmensweites Projekt zur Modernisierung Ihres Identity and Access Management (IAM). Diese bilden eine hervorragende Grundlage, um die Vorteile eines fortschrittlichen IAM-Programms umfassend darzulegen.

IAM ist heutzutage das zentrale Element in der Verwaltung von Unternehmensnetzwerken – und gleichzeitig auch einer der größten Risikofaktoren. Durch die zunehmende Digitalisierung und Einbindung verschiedenster Steakholdergruppen, vom Mitarbeiter über den Zulieferer bis zum Endkunden, hat sich die Anzahl der Identitäten vervielfacht. Durch moderne IAM-Ansätze besteht enormes Potenzial, um unterschiedlichste Arten von Ressourcen einzusparen und Sicherheitslücken vorzubeugen.

Im Folgenden legen wir dar, warum ein Business Case eines der vier wichtigsten Elemente eines IAM-Programms ist.

Inhaltsverzeichnis

1. Einleitung

Dieses Dokument gibt Ihnen einen umfassenden Leitfaden an die Hand, um einen Business Case bzw. ein Geschäftsszenario für Identity und Access Management aus der betriebswirtschaftlichen und der Risiko-Perspektive zu entwickeln.

Im ersten Teil dieser Ausarbeitung betrachten wir, welche Phasen für den Aufbau eines IAM-Geschäftsszenarios notwendig sind. Darunter fallen die Entwicklung einer Vision, die Zielsetzung und typische Geschäfts- und Risikotreiber. Der zweite Teil beschreibt Risiko- und Geschäftskennzahlen, die für die wirtschaftliche und fachliche Beurteilung eines IAM-Investments herangezogen werden.

Abbildung 1:
Problem/Lösungsmatrix von ähnlichen Logistik Unternehmen aus der IAM-Perspektive

1. Herausforderungen

- Keine zentrale Sicht auf eine Identität hinsichtlich Berechtigungen
- Unterschiedliche Lebenszyklus-prozesse für interne und externe Identitäten
- Viele verschiedene 3rd Party Identitäten
- Hoher Grad an selbstentwickelten Apps
- Keine zentrale Authentifizierung und Berechtigungsvergabe
- Steigende Komplexität der Infrastruktur und Zugriffspunkte

2. Umfang der Themenbereiche

- Automatisierung Mitarbeiter-Lebenszyklus Prozess
- Zugriff nach dem Least Privilege Prinzip
- Anbindung von Hunderten an Apps und Systemen
- Revisionssicheres Reporting / vollständige Nachvollziehbarkeit, wer, warum, welche Rechte hat
- Governance- und Risikokontroll-funktionen zur Compliance-Erfüllung

3. Potentielle Lösungen

- Fachliche Konzeption und technische Realisierung der Identity Management Prozesse in Abstimmung mit Service-Verantwortlichen, CISO, HR- und IT- Fachabteilungen in verschiedenen Ländern
- Implementierung Genehmigungs-workflows
- Implementierung der Audit- und Reporting-Anforderungen
- Beratung von Kunden der Plattform und technische Anbindung von Zielsystemen

4. Vorteile

- Rückverfolgbarkeit, Aufzeichnung und Beschleunigung von Eintritten, Wechsel und Austritten von Mitarbeiter
- Governance-Funktionen zur Risikominimierung
- Automatisierte Anbindung von Zielsystemen
- Schnelle Replikation von Genehmigungsprozessen
- SaaS: Kosten für Betrieb, Wartung, Sicherheit, Upgrades entfallen

2. Die Entwicklung eines Business Case für eine IAM-Investition

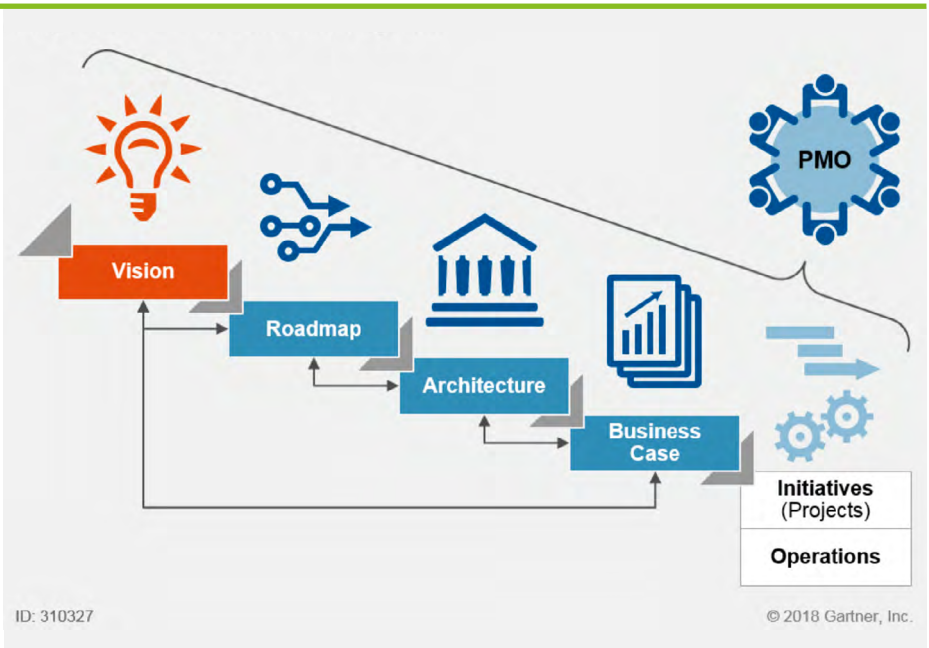
Sicherheits- und Risikomanagementverantwortliche haben oft Schwierigkeiten, angemessene Mittel für Investitionen in IAM-Funktionen zu erhalten. IT-Führungskräfte müssen einen überzeugenden Business Case vorlegen, der die Ausrichtung des Programms an den Geschäftsanforderungen nachweist und Messgrößen zur Erfolgsdefinition liefert.

Sicherheits- und Risikomanagementverantwortliche sollten:

- nachweisen, dass der Umfang, die Ziele und die Prioritäten des IAM-Programms einen funktionierenden Konsens zwischen den Beteiligten widerspiegeln, indem sie diese in die Entwicklung und Genehmigung der Programmvision einbeziehen.
- alle Ziele des IAM-Programms an den geschäftlichen Faktoren ausrichten und sie in einer für das Unternehmen verständlichen Sprache formulieren, indem Akronyme und technische Begriffe entfernt und durch allgemein verständliche Terminologie ersetzt werden.
- klar formulierte Risikokennzahlen definieren, die sich an den KPIs/KRIs orientieren, um die Notwendigkeit von Änderungen zu begründen und die Bedingungen festzulegen, unter denen der Erfolg anhand dieser Kennzahlen gemessen wird.
- die Risiken der Programmdurchführung kommunizieren und ihr Engagement für das Risikomanagement auf der Grundlage der Planung von Programminitiativen zeigen.

Der Business Case ist neben der Vision, Roadmap und der Architektur eines der vier wichtigsten Elemente eines IAM-Programms. Sein Zweck ist es, die Finanzierung der IAM-Strategie des Unternehmens zu begründen, die sowohl Ressourcen für spezifische Projekte als auch Personal für den laufenden Betrieb erfordert. Diese Finanzierung bildet die Grundlage für ein erfolgreiches IAM-Programm. Abbildung 2 zeigt die verschiedenen Phasen für den Aufbau eines IAM-Programms.

Abbildung 2:
Komponenten eines IAM-Programms laut Gartner, 2018



Source: Gartner (May 2018)

Leider sind viele IAM-Verantwortliche nicht sehr erfolgreich bei der Entwicklung von Business Cases, die es ihnen ermöglichen würden, die für Investitionen benötigten Mittel zu sichern. Diese Bemühungen scheitern meist, weil es den Teams nicht gelingt, überzeugend darzulegen, inwiefern das IAM-Programm für das Unternehmen relevant ist.

Ohne eine angemessene Finanzierung während des gesamten Programms – nicht nur im ersten Jahr, sondern auch in den Folgejahren – ist es für ein IAM-Programm nahezu unmöglich, Fortschritte bei der Erfüllung der Bedürfnisse der Stakeholder zu erzielen.

Wie können IAM-Führungskräfte einen überzeugenden Business Case entwickeln, der die Wahrscheinlichkeit einer angemessenen Finanzierung des IAM-Programms durch die Organisation erhöht?

Abbildung 3 zeigt vier Regeln, die IAM-Führungskräfte befolgen sollten, um einen überzeugenden IAM Business Cases zu entwickeln.

Abbildung 3:
Vier wichtige Regeln für die Entwicklung eines IAM-Programms laut Gartner, 2018

Source: Gartner (February 2018)

In Bezug auf diese Regeln werden wir auf zwei Punkte näher eingehen, die einen ersten Blick auf IAM schärfen sollen und aufzeigen, warum es gerade jetzt notwendig ist, sich mit dem Thema IAM näher zu befassen:

1. Vision, Ziele und Geschäftstreiber
2. Definition von Erfolgskennzahlen

Die anderen beiden Regeln „Konsens" und „Risiken eines IAM-Programms" bzw. die IAM-Aspekte „Roadmap" und „Architektur" lassen wir an dieser Stelle raus, da es den Rahmen des Whitepapers sprengen würde.

3. Vision und Ziele

Um die notwendige Finanzierung und Unterstützung für das IAM-Programm zu erhalten, muss die IAM-Vision die Erwartungen der Beteiligten widerspiegeln. Die für IAM zuständigen Sicherheits- und Risikomanagementverantwortlichen müssen eine gemeinsame organisatorische Vision entwickeln, die den Umfang, die Ziele und die Prioritäten des IAM-Programms festlegen, um genügend politisches Kapital aufzubauen, damit notwendige Prozessänderungen beeinflusst werden können.

Beispiel einer IAM-Vision für ein Logistikunternehmen:
Implementierung einer modernen, skalierbaren Lösung für das Identitäts- und Zugriffsmanagement, um digitale Identitäten der Mitarbeiter, Partner und Maschinen abzusichern und ihre Zusammenarbeit zu fördern. Durch die neue IAM-Lösung werden Anforderungen der Regulatorik erfüllt und Sicherheitsrisiken besser kontrolliert. Dies geschieht unter anderem durch sichere Authentifizierungsmöglichkeiten, einem optimierten Identity Lifecycle, der Berechtigungsvergabe nach Least Privilege und regelmäßige Rezertifizierungen.

Klar definierte Ziele und Dienstleistungen sowie ein eng gesteckter Rahmen zu deren Planung und Überwachung sind Erfolgsfaktoren eines jeden IAM-Projektes. Dies wiederum erfordert eine enge Zusammenarbeit zwischen erfahrenen Mitarbeitern, sowohl beim Anwender als auch dem implementierenden IAM-Hersteller. Es ist daher sicherzustellen, dass alle Daten und Ziele miteinander vereinbart und von jedem am Projekt Beteiligten verstanden werden, bevor die Einführung beginnt. Jede spätere Anpassung verlängert das Projekt unnötig, sowohl zeitlich als auch hinsichtlich des Budgets.

Beispiel einer IAM-Zielformulierung:
Die Ziele des Identitäts- und Zugriffsmanagements bestehen darin, Vertrauen, Integrität und Verfügbarkeit von Systemen und Daten zu gewährleisten. Das Identitäts- und Zugriffsmanagement soll es ermöglichen, Benutzer zu identifizieren, zu authentifizieren und für den Zugriff auf wichtige Ressourcen nach dem Least-Privilege-Prinzip zu autorisieren. Weitere Ziele sind Erfüllung von Compliance-Vorgaben, Risikoreduzierung von Datendiebstahl, operative Effizienz des Lebenszyklus und Kostenreduzierung von Personal und IT-Ausgaben.

4. Geschäfts- und Risikotreiber

Identitätsmanagement ist geschäftskritisch geworden und die Herausforderungen eines sicheren Zugangs sind heute komplizierter als je zuvor. Sie reichen von einem immensen Anstieg der genutzten Anwendungen (On Premise und in der Cloud), dem Trend zum Hyper-Outsourcing und nicht-linearen Karrierewegen über agile Transformationen, die zu funktionsübergreifenden Arbeitsplätzen führen, bis zur raschen Verlagerung zu einer virtuellen Belegschaft. Infolgedessen führten viele Unternehmen IAM-Systeme ein, um komplexe IT-Infrastrukturen mit Dutzenden oder sogar Hunderten von Systemen und Anwendungen sowie Tausenden von Konten und Zugriffsrechten unter Kontrolle zu bringen.

Bestimmte Geschäfts- und Risikotreiber sind häufig die Ursache, warum ein IAM-System aufgebaut wird. Sie nehmen eine strategische Bedeutung ein, um bei Entscheidern, die nicht aus dem Fachbereich kommen, aufzuzeigen, wie bestimmte Treiber das Risiko beeinflussen und welche Faktoren eine Wirkung auf Sicherheits-, Governance- und Berechtigungsprozesse haben.

Die folgenden Einflussfaktoren sind häufige Argumente, um die Anschaffung eines IAM Systems zu rechtfertigen:

- Verschiebung des Sicherheits-Perimeters: Die digitalen Identitäten stehen im Zentrum der Sicherheitsstrategie und nicht mehr die Netzwerksicherheit.
- Hybride Infrastrukturen: Daten wandern in die Cloud.
- Die Definition des Begriffs „unbefugter Zugriff" verlagert sich von den Systemen weg und konzentriert sich auf die Daten. Mit anderen Worten: Ein autorisierter Benutzer kann sich unbefugt Zugang verschaffen.
- Cyberattacken nehmen zu: Hacker suchen sich „verwaiste/schlafende" Berechtigungen von Identitäten und nutzen die Berechtigungen dieser, um in die Systeme einzudringen und Daten abzugreifen.
- 81 Prozent aller Datendiebstähle basieren auf schlecht geschützte oder zu weitreichende Berechtigungen[1].
- Wachsende Anforderungen von Industrie-Standards und Regulatorik in Bezug auf Datenschutz, Privatsphäre und Compliance.
- Keine zentrale Sicht auf die Berechtigungen von Identitäten. Ergebnis: Identitäten haben Berechtigungen ohne Least-Privilege-Prinzip.
- Die Verwaltung von Compliance-Anforderungen, wie z. B. „Least Privilege", wird mit zunehmender Größe schwieriger. Mitarbeiter, die aus der Ferne arbeiten, benötigen zeitnah Zugriff, aber die Verwaltung der Berechtigungen über mehrere Tools hinweg erhöht sowohl die Betriebskosten als auch das Compliance-Risiko.
- Die Anzahl der Zugangspunkte erhöht sich stetig, dadurch steigt die Komplexität der IT-Infrastruktur und das Risiko, die Einhaltung von Vorschriften zu verletzen.
- Berechtigungsvergabe und -entzug im Laufe eines Mitarbeiter- oder Partner-Lebenszyklus dauern in vielen Unternehmen immer noch Wochen oder Tage anstatt Stunden.
- Customer Experience Paradigma: Mitarbeiter und Dritt-Partner erwarten ein schnelles, sicheres, personalisiertes und einfaches Login- und Accesserlebnis.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes und Gestalter der sicheren Digitalisierung in Deutschland. Die BSI Richtlinie ORP.4.2 beschreibt Risikofaktoren und Gefahren, wenn ein IAM-System fehlt oder ungenügend ist (Im Appendix dieses Dokuments ist die ganze Richtlinie beigefügt).

1 Verizon, 2019 Data Breach Investigations Report https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein ORP.4 Identitäts- und Berechtigungsmanagement von besonderer Bedeutung[2]:

1. Fehlende oder unzureichende Prozesse beim Identitäts- und Berechtigungsmanagement
Sind Prozesse beim Identitäts- und Berechtigungsmanagement unzureichend definiert oder implementiert, ist nicht gewährleistet, dass Zugriffe auf das erforderliche Maß eingeschränkt sind und so gegen die Prinzipien „Need to know" bzw. „Least Privilege" verstoßen wird. Der Administrator erhält möglicherweise keine Informationen über personelle Veränderungen, so dass beispielsweise eine Benutzerkennung eines ausgeschiedenen Mitarbeiters nicht gelöscht wird. Er kann somit weiterhin auf schützenswerte Informationen zugreifen. Auch ist es möglich, dass Mitarbeiter, die in eine neue Abteilung versetzt wurden, ihre alten Berechtigungen behalten und dadurch mit der Zeit umfangreiche Gesamtberechtigungen ansammeln.

2. Fehlende zentrale Deaktivierungsmöglichkeit von Benutzerzugängen
In Institutionen haben Mitarbeiter oft Benutzerzugänge zu diversen IT-Systemen, wie Produktiv-, Test-, Qualitätssicherungs- oder Projekt-Systeme. Diese befinden sich meist in unterschiedlichen Verantwortungsbereichen und werden oft von unterschiedlichen Administratoren verwaltet. Das führt unter Umständen dazu, dass nicht auf allen IT-Systemen eine gleiche und eindeutige Benutzerkennung verwendet wird und es auch keine zentrale Übersicht über die Benutzerzugänge auf den einzelnen IT-Systemen gibt. In einem solchen Szenario ist es nicht möglich, bei einem Angriff oder einem Passwortdiebstahl in einem Arbeitsschritt alle Benutzerzugänge eines Mitarbeiters zu deaktivieren. Auch können in diesem Szenario bei dem Ausscheiden eines Mitarbeiters aus der Institution nicht in einem Arbeitsschritt alle Zugänge gesperrt werden.

3. Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten
Wenn die Vergabe von Zutritts-, Zugangs- und Zugriffsrechten schlecht geregelt ist, führt das schnell zu gravierenden Sicherheitslücken, z. B. durch Wildwuchs in der Rechtevergabe. Bei der Einführung von Identitätsmanagement-Systemen oder Revisionen stellt sich häufig heraus, dass verschiedene Personen in unterschiedlichsten Organisationseinheiten für die Vergabe von Berechtigungen zuständig sind. Dies führt unter Umständen dazu, dass Benutzer Berechtigungen auf Zuruf erhalten oder umgekehrt nur über unnötig komplizierte Wege an diese kommen. Dadurch können einerseits fehlende Berechtigungen die tägliche Arbeit behindern, andererseits können so Berechtigungen ohne Erfordernis vergeben werden und so ein Sicherheitsrisiko darstellen.

Zusammenfassung, warum sich eine Investition in eine zentrale IAM-Lösung rechnet:

- IAM-Lösungen werden eingesetzt, um Zugriffsrisiken zu reduzieren, zu kontrollieren und Compliance für Auditoren bereitzustellen.
- IAM reduziert Sicherheitsrisiken, erfüllt Governance-Regeln und senkt Prozesskosten.
- Ein robustes IAM-Programm wird zum Eckpfeiler des Datenschutz- und Sicherheitsprogramms einer Organisation.
- Orchestrierung des richtlinienbasierten Benutzeridentitätsmanagements und der Zugriffskontrollen während des Zugriffsanforderungs- und Zertifizierungsprozesses, auch Provisioning genannt, zur Erfüllung gesetzlicher Anforderungen.
- Das BSI empfiehlt den Einsatz von zentralen IAM-Lösungen, besonders für global operierende Unternehmen.
- Datenmissbrauch, Lösegeldzahlungen und Strafzahlungen bei Compliance-Missachtung werden erheblich reduziert.

2 Bundesamt für Sicherheit in der Informationstechnik, ORP-Organisation und Personal, ORP-4: Identitäts- und Berechtigungsmanagement, Februar 2020

- Das Unternehmen ist in der Lage, alle Berechtigungen zentral zu verwalten und eine zentrale Sicht auf die Berechtigungen aller Mitarbeiter, Partner und Maschinen zu haben.

5. Kennzahlendefinition für einen IAM Business Case

Die Definition von Kennzahlen ist wesentlich für die Einführung und Kontrolle eines IAM-Systems. Hierbei ist zu unterscheiden zwischen KPIs und KRIs. Die monetäre Bewertung eines IAM-Programms mit wirtschaftlich-orientierten KPIs ist viel schwieriger als risikoorientierte Kennzahlen (KRIs) für den Business Case hinzuzuziehen. Entscheider schauen in erster Linie auf wirtschaftliche Kennzahlen, um Budget für ein IAM-Investment bereitzustellen. Bei IAM kommt eine solche Betrachtung zu kurz, da das Thema Sicherheit einen hohen Anteil einnimmt. Daher ist es zu empfehlen, risikoorientierte Kennzahlen im Business Case beizufügen. Die monetäre Bewertung solcher Kennzahlen können potenzielle Lösegeldzahlungen sein oder auch der Verlust von sensiblen Unternehmensdaten wie Innovationen und Blueprints, wenn privilegierte Mitarbeiter das Unternehmen verlassen und zur Konkurrenz wechseln. Außerdem gehören Strafzahlungen bei Nicht-Erfüllung von regulatorischen Vorgaben zur monetären Bewertung.

5.1. Betriebswirtschaftliche Kennzahlen (KPIs)

Wird eine ROI-Berechnung herangezogen, um ein IAM-Programm zu rechtfertigen, können Fallen lauern:

Falle Nummer 1: ROI innerhalb der IT
Versuchen Sie nicht, den ROI ausschließlich innerhalb der IT zu berechnen. Ein modernes IAM-Programm wirkt sich auf eine Vielzahl von Business Units aus. Wenn Sie lediglich die reduzierten Administrationskosten für die IT betrachten, rechnet sich die IAM-Investition kaum. Addieren Sie jedoch die Vorteile aller Geschäftsbereiche, steigert sich dementsprechend auch der ROI.

Falle Nummer 2: ROI über das Business
SSO und automatisierte Passwortrücksetzung erhöhen die Produktivität im Unternehmen. Außerdem bewirken Identity Lifecycle Management und Rollenmanagement, dass Identitäten schneller „arbeitsfähig" sind. Die Kosten müssen jedoch oft vom IT-Budget getragen werden, da im Unternehmen in der Regel keine abteilungsübergreifenden Budgets zur Verfügung stehen. Das operative Geschäft ist aufgrund des vermeintlich mangelnden Nutzens oft nicht bereit, zur Finanzierung etwas beizutragen.
Ausnahme: Customer Identity and Access Management (CIAM) kann einen quantifizierbaren wirtschaftlichen Nutzen haben.

Die Formulierung folgender Erfolgskennziffern hilft bei der Erfolgsdarstellung eines IAM Programms. Die Zahlen sind bei der Durchführung von verschiedenen IAM-Projekten in Unternehmen erhoben worden:

- Reduktion der jährlichen Betriebskosten im Bereich Desktop Service und Betrieb von Applikationen von 3,7 Mio. € auf 2,1 Mio. € (-44 Prozent)
- Halbierung der Mitarbeiteranzahl und der damit verbundenen Personalkosten im Bereich Benutzer-, Software- und Assetmanagement von 36 auf 18 FTEs durch starke Automatisierung der manuellen Prozesse
- Erzielung einer Payback Periode des Projektes von nur 1 Jahr bei Investitionen in Höhe von 1,7 Mio. €
- Transparenzerhöhung durch die Möglichkeit HW-/ SW-Kosten verursachergerecht (kostenstellengenau) zu verrechnen
- Änderung des Bestellverhaltens der Mitarbeiter durch Kostentransparenz: Reduktion der SW-Kosten je User um 50 Prozent und Reduktion des PC-Bestandes um mehr als 20 Prozent
- Steigerung der Nutzerzufriedenheit durch Self-Service-Anwendungen für Mitarbeiter und schnellere und fehlerfreie Administrations- und Bereitstellungsabläufe für Berechtigungen, Umzüge, SW-/HW-Pakete etc.
- Erzielung der Konformität mit Anforderungen des Betriebsverfassungsgesetztes (Einsicht in SW- und Zugriffs-Rechte je Mitarbeiter)

Häufig werden andere Nutzeneffekte für eine Erfolgsdarstellung hinzugezogen. Jedoch gibt es bei den folgenden Aspekten Schwierigkeiten, diese quantifizierbar zu machen:

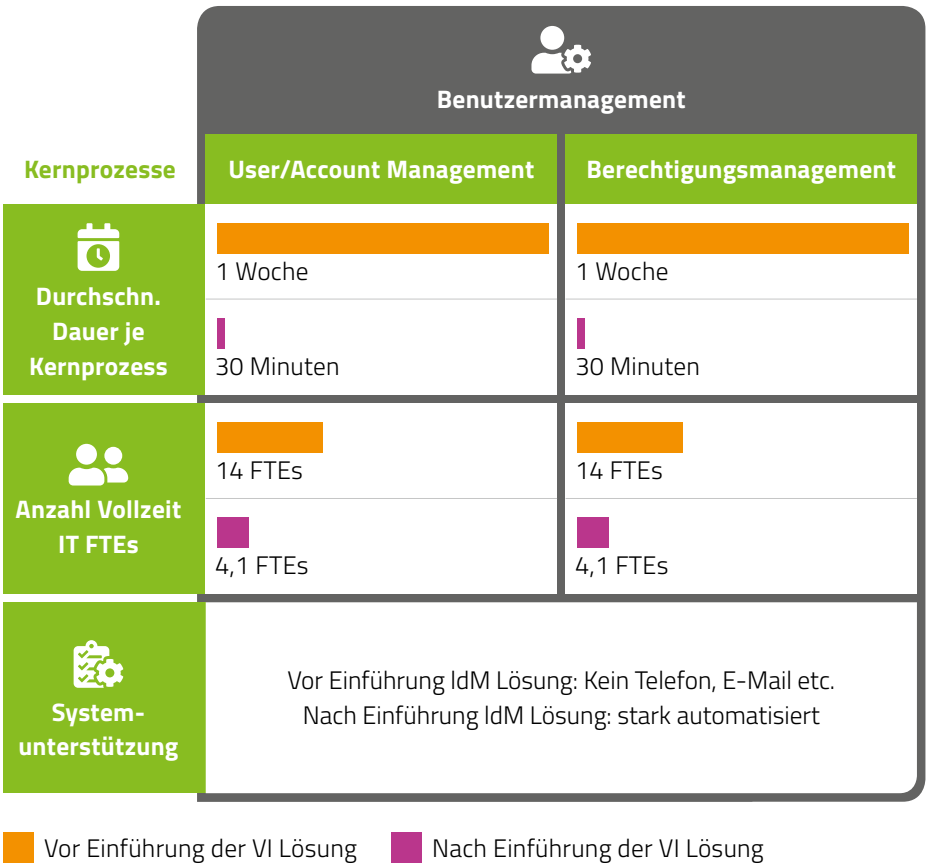
- Nutzerzufriedenheit: Wichtiges Argument und quantifizierbar, aber wie berechnet man den geschäftlichen „Wert"?
- Risiko-gesteuerte Investition: Oft schwer zu quantifizieren und schon gar nicht monetär bewertbar
- Compliance-getriebene Investition: Häufig wird in solchen Fällen nach organisatorischen „Lösungen" gesucht. Sie sind nur in regulierten Branchen quantifizierbar, dann aber häufig „binär"
- Business Enablement durch höhere Effizienz der Bereitstellung: Monetäre Berechnung ist komplex und Verrechenbarkeit praktisch nicht gegeben

Weitere Beispiele für KPIs mit den Dimensionen Effizienz, Effektivität und Enablement

Effizienz	Effektivität	Enablement
▪ Durchlaufzeiten von Bestellungen ▪ Anzahl von Helpdesk-Calls ▪ Quote von Direkt-zuweisungen versus regel- oder rollenbasierten Zuweisungen	▪ Überdeckungsrate gemanagter versus administrierter Applikationen bzw. Berechtigungen ▪ Reduktion des administrativen Aufwands durch Rollen ▪ Überwindung bzw. Vermeidung von Audit-Findings	▪ Einfacheres Onboarding von Geschäftspartnern ▪ Benutzerzufriedenheit ▪ Unterstützung neuer Geschäftsmodelle

Ein weiterer Ansatz ist der Fokus auf die **Verkürzung der Prozessdauer und massive Ressourceneinsparung durch Automatisierung**. Die folgende Grafik zeigt eine Beispielrechnung:

Abbildung 4: Betriebswirtschaftliche Betrachtung für die Einführung einer Identity Management Technologie mit dem Fokus Automatisierung des Mitarbeiter Lebenszyklus, eigene Darstellung aus einem Kundenprojekt, 2019



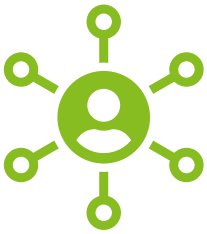
5.2. Risiko-orientierte Kennzahlen nach ISO 27001 (KRIs)

Basierend auf ISO 27001 – Industrienorm zur Informationssicherheit – werden 8 verschiedene Kennzahlen-Gruppen vorgegeben, die für die Darstellung eines Business Case herangezogen werden können. Die folgenden Faustregeln und Analyse-Metriken beruhen auf Erfahrungen, die bei der Durchführung verschiedener IAM-Kundenprojekte gesammelt wurden.

Die Risiken reichen von Datenverlust und Missbrauch vertraulicher Informationen bis hin zu Downtime und einem stillstehenden Geschäftsbetrieb.

WICHTIG: Sollte Ihr Team aufgrund einer ungenügenden Datenlage nicht dazu im Stande sein die meisten Kennzahlen zu quantifizieren, dann haben Sie einen Nachweis bzw. starke Argumente, warum die Anschaffung eines IAM-Systems sinnvoll ist.

Abbildung 5:
IAM-Risikokennzahlen basierend auf ISO 27001

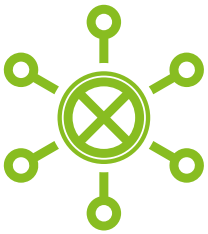


1. Identitäts- und Rollenspeicher
Selbst relativ einfache Metriken über die Größe des Identitäts- und Rollenspeichers ermöglichen bereits eine erste Bewertung der Qualität der IAM-Prozesse. Wenn die Anzahl der Benutzer im IAM-System die Anzahl der Mitarbeiter (oft in einem HR-System zu finden) bei weitem übersteigt, ist wahrscheinlich etwas nicht in Ordnung. Darüber hinaus kann die Beobachtung der Entwicklung dieser Kennzahlen im Laufe der Zeit interessante Trends aufzeigen (z. B. Wachstumsraten). Denken Sie beispielsweise an eine fast konstante Zunahme der Rollenanzahl. Außerdem sollte der Wert von Kennzahlen nicht unterschätzt werden, da diese einen guten Hinweis auf die Verwaltbarkeit des IAM-Systems geben.

Beispiele:
- Die Anzahl der in das aktuelle IAM-System integrierten Anwendungen
- Die Anzahl der Rollen im Verhältnis zur Anzahl der Abteilungen
- Die Anzahl der IT-Rollen im Verhältnis zur Anzahl der Geschäftsrollen
- Die Anzahl der Berechtigungen im Verhältnis zur Anzahl der Benutzer
- Die Anzahl der Berechtigungen im Verhältnis zur Anzahl der Rollen

Faustregel:
Wie ist das Verhältnis zwischen der Anzahl der Rollen und der Benutzer in Ihrer Organisation?

Die Faustregel für die Anzahl der Rollen in Ihrem IAM-System lautet: Die Gesamtzahl der Rollen sollte nicht mehr als 10 Prozent der Gesamtzahl der Benutzer betragen. In vielen Organisationen, die über kein angemessenes Rollenmanagement verfügen, wird dieser Prozentsatz weit überschritten. Dies bedeutet ein zu komplexes Rollenmodell, das schwer zu pflegen ist und zu Fehlern und betrieblicher Ineffizienz führen kann.



2. Verwaiste Konten

Ein Weg, um Zugang zu Unternehmensressourcen, Anwendungen oder Systemen zu erhalten, führt über Benutzer- und Dienstkonten, die nicht mehr aktiv genutzt werden. Dies gilt sowohl für Konten von scheidenden Mitarbeitern als auch von externen Auftragnehmern, die ein Projekt im Unternehmen abgeschlossen haben. Unternehmen, die nicht die notwendigen Schritte einleiten, um diese Zugangspunkte zu schließen, lassen Angreifern Tür und Tor offen.

Wenn ein Mitarbeiter das Unternehmen verlässt oder das Projekt eines Auftragnehmers beendet ist, müssen seine Benutzerkonten deaktiviert (d. h. abgeschaltet) werden. Dies sollte Teil des typischen Offboarding-Verfahrens (oft automatisiert durch das IAM-System) von Mitarbeitern und Auftragnehmern sein. In der Praxis kommt es jedoch vor, dass diese Konten falsch oder gar nicht deaktiviert werden. Durch das Erkennen und Bereinigen dieser Konten werden die Risiken erheblich reduziert. Indem man herausfindet, warum diese Konten nicht deaktiviert wurden, können IAM-Prozesse (Offboarding) verbessert werden.

Einige Metriken zu verwaisten Konten:

- Benutzer, die sich seit geraumer Zeit nicht mehr angemeldet haben, bzw. Konten, die über einen bestimmten Zeitraum nicht genutzt wurden, werden auch als ruhende Konten bezeichnet. Wie lange dieser Zeitraum genau sein sollte, kann von Unternehmen zu Unternehmen unterschiedlich sein. 90 Tage werden jedoch häufig als Grenzwert angesehen. Für bestimmte Konten, wie z. B. Administratorkonten, kann ein kürzerer Zeitraum im Vergleich zu anderen Konten sinnvoll sein. Daher kann dieser KPI in mehrere Unter-KPIs aufgeteilt werden.
- Benutzer, die sich nie angemeldet haben.
- Unkorrelierte Benutzerkonten, auch bekannt als Geisterkonten. Dies sind Konten, die nicht mit einem aktiven Benutzer oder überhaupt nicht mit einem Benutzer verknüpft sind.
- Benutzerkonten mit einem Status, der auf Inaktivität hinweist. Was genau dieser Status ist, hängt von dem IAM-System ab, das in der Organisation verwendet wird. Denken Sie zum Beispiel an einen Beschäftigungsstatus „im Ruhestand" oder einen Aktivitätsstatus „inaktiv". Der Anhaltspunkt ist, sich die Benutzereigenschaften im IAM-System anzusehen, die auf die Inaktivität eines Benutzers hinweisen könnten.

3. Privilegierte Konten

Privilegierte Konten, also solche, die deutlich mehr Zugriffsrechte haben als normale Konten, gibt es in vielen Formen und Ausprägungen. Wenn sie jedoch nicht ordnungsgemäß verwaltet und überwacht werden, stellen privilegierte Konten erhebliche Sicherheitsrisiken dar. Diese Risiken können von allen Seiten kommen: von böswilligen „Außenstehenden" (z. B. Hackern) oder von unvorsichtigen oder verärgerten „Insidern". Wer sich Zugang zu diesen privilegierten Konten verschafft, kann Unternehmensressourcen kontrollieren, auf sensible Daten zugreifen oder sogar (Sicherheits-)Systeme ändern oder deaktivieren.

Es ist wichtig zu wissen, wie viele und welche Art von privilegierten Konten in der Organisation existieren. Beachten Sie jedoch, dass sich einige der unten genannten Arten von privilegierten Konten überschneiden können:

- Administratorkonten, wie Local Admin und Domain Admin.
- Versteckte Konten. Diese verfügen über administrative Rechte auf einem oder mehreren Systemen, existieren aber oft unter dem Radar, da sie nicht als „Admin" gekennzeichnet sind.

- Privilegierte Dienstkonten wie z. B. Domänendienstkonten.
- Nicht-personenbezogene Konten (NPA). Diese Konten stehen nicht in direktem Zusammenhang mit einer eindeutig identifizierbaren Person/einem Mitarbeiter und sie sind auch nicht das Ergebnis der „Joiner-Mover-Leaver"-Personalprozesse in einer Organisation. Solche Konten sind oft recht leistungsfähig (z. B. Admin- oder Root-Konto), aber schwer zu erkennen. Hinzu kommt, dass die Anmeldung mit dem Konto keine Prüfspur hinterlässt, die zeigt, welche Person es tatsächlich benutzt hat. Mit anderen Worten, es gibt keine bestimmte Person, die zur Rechenschaft gezogen werden kann.
- Benutzerkonten für privilegierte Daten. Auch wenn es sich bei diesen Benutzern nicht um typische privilegierte Konten handelt, sollten sie aufgrund der sensiblen Daten, auf die sie zugreifen können, dennoch als privilegiert betrachtet werden. Denken Sie an den Buchhalter, der Zugang zu den Finanzdaten seiner Kunden hat, einen Mitarbeiter der Personalabteilung, der Zugang zu sensiblen Mitarbeiterdaten hat, oder einen Arzt, der Zugang zu Patientendaten hat.
- Privilegierte rollenbasierte Konten. Je nach Rollenmodell können bestimmte Rollen als privilegiert angesehen werden. Daher sollten wir Benutzer, denen eine oder mehrere dieser Rollen zugewiesen sind, als privilegierte Konten betrachten.

4. Benutzer mit übermäßigen Zugriffsrechten

Der Unterschied zwischen privilegierten Konten und Benutzern mit übermäßigen Zugriffsrechten besteht darin, dass sich erstere auf Benutzer konzentrieren, die per Definition (viele) sensible Zugriffsrechte haben sollten, während sich letztere auf Benutzer konzentrieren, die versehentlich (zu) viele Zugriffsrechte haben.

Einer der wichtigsten Grundsätze der Informationssicherheit ist das Prinzip der geringsten Privilegien (PoLP, Principle of Least Privilege). Dieser Grundsatz besagt, dass die Zugriffsrechte der Benutzer auf das absolute Minimum beschränkt werden, das sie für die Ausführung ihrer beabsichtigten Arbeit benötigen. Es ist ein weit verbreiteter Irrtum, bei der Anwendung des PoLP nur an böswillige Mitarbeiter zu denken. Vielmehr können Mitarbeiter auch versehentlich durch Phishing oder einen verlorenen Laptop Daten preisgeben. Aber unabhängig davon, ob absichtlich oder nicht – je weniger Daten Ihre Mitarbeiter verlieren können, desto besser.

Es ist eine Tatsache, dass die kumulierten Zugriffsrechte und Berechtigungen aller Benutzer zusammen die Größe der Angriffsfläche Ihres Unternehmens bestimmen, die natürlich so klein wie möglich gehalten werden sollte. Leider klafft oft eine Lücke zwischen gewährten und genutzten Zugriffsrechten. Dies deutet darauf hin, dass Benutzer zu viele Zugriffsrechte haben, was Ihre Angriffsfläche unnötig vergrößert.

- Ausreißer: Dies sind Benutzer, die mehr Zugriffsrechte haben (d. h. denen mehr Rollen zugewiesen wurden oder die über mehr Privilegien verfügen) als ihre Kollegen. Oft ist dies das Ergebnis eines Abteilungs- oder Funktionswechsels von Mitarbeitern, ohne dass die früheren - und nun unnötigen - Zugriffsrechte entzogen wurden. Eine andere Möglichkeit, Ausreißer zu finden, besteht darin, sie mit einem idealen Rollenprofil zu vergleichen. Je nach der Funktion, die ein bestimmter Mitarbeiter innehat, kann ein bestimmter Satz von Rollen angemessen sein. Dies gilt jedoch nur für Organisationen, die mit solchen Rollenprofilen arbeiten.
- Benutzer, denen eine große Anzahl von Rollen oder Berechtigungen zugewiesen wurde. Was als „hoch" angesehen wird, hängt vom Rollenmodell und dem organisatorischen Kontext ab.

Faustregel:
Eine Faustregel, wann ein Benutzer als Benutzer mit einer hohen Anzahl von Rollen oder Berechtigungen identifiziert werden kann, lautet: Die Gesamtzahl der Rollen oder Berechtigungen übersteigt das Doppelte des Durchschnitts.

5. Aufgabentrennung (SoD)
Die Aufgabentrennung oder Funktionstrennung, auch als Segregation of Duties bekannt, gilt als eine der schwierigsten und oft auch kostspieligsten Identitätskontrollen, die ordnungsgemäß umzusetzen sind. Das Ziel besteht darin, die Aufgaben und die damit verbundenen Berechtigungen auf mehrere Personen zu verteilen. Auf diese Weise ist es viel schwieriger, einen Betrug zu begehen, da dafür mindestens zwei Personen zusammenarbeiten müssen. Das Ziel ist jedoch nicht mehr auf die Betrugsbekämpfung beschränkt, sondern umfasst auch die Sicherheit und den Datenschutz. Wenn SoD richtig konzipiert und umgesetzt wird, stellt es sicher, dass die Mitarbeiter keine widersprüchlichen Verantwortlichkeiten oder Interessen haben. So sollte beispielsweise die Person, die eine Richtlinie festlegt, nicht die Möglichkeit haben, deren Ausführung zu genehmigen. Abgesehen von den SoD-Kontrollen selbst sind die Metriken wichtig, um zu sehen, wie Sie vorankommen:

- SoD-Verstöße. Neben der Gesamtzahl der SoD-Verstöße kann es auch interessant sein, die Anzahl spezifischer SoD-Verstöße zu betrachten. So sollen „toxische" Kombinationen identifiziert werden, die scheinbar am schwersten zu umgehen sind. Bei diesen Verstößen wird eine taktische Bereinigung wahrscheinlich nicht ausreichen. Eine strategische Umgestaltung könnte die Situation jedoch verbessern.
- Unklare Kombinationen von Zugriffsrechten. Dies sind Kombinationen von Rollen, Berechtigungen oder Anwendungen, bei denen nicht klar ist, ob sie als „toxisch" gelten oder nicht. Wenn eine solche Kombination in der Praxis auftritt, ist es wichtig zu wissen, ob sie erlaubt ist oder nicht, um (falls erforderlich) geeignete Maßnahmen zu ergreifen.

Wie wird die Implementierung eines SoD-Kontrollansatzes gestartet?
Die Implementierung eines angemessenen SoD-Kontrollsatzes beginnt mit der Definition „toxischer" Kombinationen von Zugriffsrechten (Rollen, Berechtigungen, Anwendungen, ...). Wenn Benutzer über solche Kombinationen von Zugriffsrechten verfügen, sollte dies abgeschwächt oder behoben werden. Die manuelle Kontrolle von SoD-Verletzungen ist jedoch sehr zeitaufwändig und fehleranfällig. Daher liegt der Schlüssel zur tatsächlichen Risikominderung in der Automatisierung, um SoD-Konflikte mit Hilfe eines agilen Ansatzes zu identifizieren.

6. Identitätshygiene
Es ist wichtig zu erkennen, dass die Identitätshygiene (d. h. die ordnungsgemäße Pflege des Repository) und die Informationssicherheit eng miteinander verbunden sind: Eine gut gepflegte IT-Umgebung ist besser gegen Informationssicherheitsrisiken geschützt. Die Anwendung bewährter Verfahren für Benutzer, Rollen und Berechtigungen trägt nicht nur zur Risikovermeidung bei, sondern ist auch viel einfacher und erfordert wesentlich weniger Aufwand als eine Situation, in der man regelmäßig aufräumen muss. Mit anderen Worten: Vorbeugen ist besser als heilen.

Einige Metriken, mit denen Sie messen können, wie gut Sie es mit der Benutzerhygiene halten:

- Benutzer, denen keine Rollen oder Berechtigungen zugewiesen sind.
- Benutzer, die keinen Zugriff auf irgendwelche Anwendungen haben.

- Benutzerkonten, die über einen bestimmten Zeitraum hinweg nicht geändert wurden. Wie lange dieser Zeitraum genau sein sollte, kann von Unternehmen zu Unternehmen unterschiedlich sein.
- Benutzerkonten mit direkten Berechtigungen, die nicht über Rollen zugewiesen werden.
- Benutzerkonten für Testzwecke (d. h. Testkonten).
- Benutzer (und insbesondere deren Zugriffsrechte), die innerhalb eines bestimmten Zeitraums nicht überprüft werden. Auch hier gilt, dass der genaue Zeitraum von Unternehmen zu Unternehmen unterschiedlich sein kann und oft von der Häufigkeit der Re-Zertifizierungskampagnen abhängt.
  Dieser KPI kann auch für bestimmte Arten von Konten eingerichtet werden, z. B. für Administratorkonten.
- Falls die Organisation eine Richtlinie zum Ablauf von Passwörtern durchsetzt: Benutzerkonten mit abgelaufenen Passwörtern.

7. Qualität der Daten

Um genaue Ergebnisse aus allen oben genannten Kontrollen zu erhalten, ist es entscheidend, dass alle relevanten Daten („Attributwerte") korrekt eingegeben werden. Die KPIs spiegeln nur dann den tatsächlichen Zustand wider, wenn die Daten im IAM-System korrekt, vollständig und aktuell sind. Viele der Prozesse wie Onboarding, Offboarding und ganz allgemein die Änderung von Daten werden mit Hilfe von IAM-Systemen automatisiert. Das Auffinden von Ungenauigkeiten oder leeren Feldern ist daher auch eine Gelegenheit, diese Prozesse zu verbessern. Spezifische Datenprobleme können nicht gelöst werden, ohne die eigentliche Ursache zu berücksichtigen.

Es gibt viele KPIs die dabei helfen, dies zu messen. Denken Sie an all die verschiedenen Datenattribute im IAM-System, die leer gelassen werden könnten. Es ist jedoch wichtig, sich auf die Attribute zu konzentrieren, die für andere KPIs entscheidend sind, oder Maßnahmen zur Verbesserung festgestellter Probleme zu ergreifen. Denken Sie daran, dass tiefer gehende Informationen und handlungsorientierte Erkenntnisse erforderlich sind, um erkannte Probleme tatsächlich zu verbessern. Ohne die richtigen Informationen ist es fast unmöglich zu entscheiden, ob ein bestimmtes Benutzerkonto oder eine bestimmte Rolle deaktiviert/aufgehoben werden kann oder nicht.

Einige Metriken, die für die meisten Unternehmen unerlässlich sind:

- Benutzer ohne Manager, Abteilung oder E-Mail.
- Rollen ohne (korrekte und klare) Beschreibung oder Besitzer.
- Berechtigungen ohne (korrekte und eindeutige) Beschreibung und Eigentümer.
- Anwendungen ohne (korrekte und eindeutige) Beschreibung und Eigentümer.

8. Unternehmensspezifische KPIs

Neben den allgemeineren KPIs, die in den vorherigen Abschnitten erwähnt wurden, ist es wichtig, diese KPI-Sätze mit geschäftsspezifischen Metriken zu ergänzen. In Finanzinstituten ist es beispielsweise häufig der Fall, dass ein Mitarbeiter für die Durchführung einer bestimmten Tätigkeit eine entsprechende Zertifizierung/Schulung benötigt. Ein solcher geschäftsspezifischer KPI könnte daher die Anzahl der Mitarbeiter sein, die zwar die Berechtigung haben, diese Aktion auszuführen, aber nicht über die entsprechende Zertifizierung verfügen. Eine andere häufig anzutreffende Situation ist die, dass Unternehmen sich auf die Schulung des Sicherheitsbewusstseins konzentrieren und messen wollen, für wen diese Schulung zu lange gedauert hat, insbesondere wenn diese Benutzer über viele Berechtigungen verfügen.

6. Zusammenfassung

Schlussfolgernd ist festzuhalten, dass die oben beschriebenen Geschäfts- und Risikotreiber bzw. die Ermittlung verschiedener Kennzahlen (KPIs+KRIs) erste Argumente liefern, um ein Veränderungsprojekt für Identitäts- und Berechtigungsmanagement bei Management und Operative anzustoßen.

Die Entwicklung eines IAM Business Case umfasst häufig die Einbeziehung verschiedener Stakeholder aus Infrastruktur, Service, Sicherheit und HR. Es ist ein mehrstufiger Prozess, der aus Vision, Roadmap, Architektur und Business Case besteht. Die Kommunikation eines IAM-Geschäftsszenarios vor Vorstand und anderen Entscheider sollte nicht nur betriebswirtschaftlich orientiert sein, sondern auch risikoorientierte Kennzahlen beinhalten. Der Aufbau eines erfolgreichen IAM-Programms beinhaltet den Konsens zwischen den Stakeholdern, die Definition von Geschäftstreibern, eine Risiko-Analyse und die Definition von Erfolgsmetriken.

Referenz: BSI ORP.4 – Identitäts- und Berechtigungsmanagement
https://bit.ly/3oOnDPc

Das sind wir

iC Consult ist der führende unabhängige Berater, Systemintegrator und Managed Services Anbieter für Identity & Access Management (IAM) mit mehr als 800 Mitarbeitenden weltweit.

Mit unserer Hingabe zu Exzellenz und Innovation und den besten Technologien im IAM-Umfeld bieten wir unseren Kunden erstklassige Cyber Security Lösungen. Unser Service-Portfolio umfasst Managed Services für IAM einschließlich Beratung, Architektur, Implementierung, Integration, Support und Betrieb.

iC Consult hat seinen Hauptsitz in München und Niederlassungen in Deutschland, der Schweiz, Österreich, Frankreich, Belgien, Spanien, Bulgarien, Großbritannien, den USA, Kanada, Indien und China. Die größten Marken der Welt vertrauen auf unsere Expertise, um ihre wertvollsten Güter zu schützen und zu verwalten: Ihre Identitäten.

Mehr Informationen unter www.ic-consult.com