IBM Security

# Wir bringen Stakeholder im gesamten Unternehmen bei der CIAM-Modernisierung zusammen.

IBM

Erste Schritte

# Einführung

Bei der Erstellung eines neuen Account, einem Kauf oder auch der Anmeldung für einen Newsletter verrtrauen Sie einer Organisation Ihre persönlichen Daten an. Nach diesem ersten Austausch möchten Sie wahrscheinlich nicht, dass Ihre Daten für andere Zwecke als die, denen Sie zugestimmt haben, verwendet werden, aber mit Ihrer Zustimmung würden Sie vielleicht personalisierte Angebote und Empfehlungen für die Zukunft begrüßen. Das Wichtigste ist, dass Sie dies selbst entscheiden und Ihre Meinung jederzeit ändern können. Wenn Sie bei Ihren Interaktionen irgendwelche Irritationen erleben, oder aus irgendeinem Grund das Vertrauen in die Organisation verlieren, dann brechen Sie den Kontakt zu ihr vermutlich ab und suchen eine andere. Das Identitäts- und Zugriffsmanagement für Verbraucher (CIAM) ermöglicht derartige bedarfsgerechte, personalisierte und vertrauenswürdigen Erfahrungen zwischen Verbrauchern und Anbietern, und da Sie selbst Konsument sind, können Sie sich in Ihre eigenen Verbraucher hineinversetzen, wenn Sie über Aktualisierungen der digitalen Strategien Ihres Unternehmens nachdenken, um wettbewerbsfähig zu bleiben.

Aber CIAM ist weit mehr als die Aktualisierung einer Website oder ein Marketingprojekt: es beeinflusst Funktionsbereiche in der gesamten Organisation, da Berührungspunkte zu den Konsumenten bewertet und modernisiert werden. Um sicherzustellen, dass das zeitlose Gleichgewicht zwischen Komfort und Sicherheit nicht kippt, müssen Organisationen sowohl geschäftliche als auch technische Interessenvertreter zusammenbringen, um CIAM als ergebnisorientierten Teil der digitalen Transformation zu begreifen, die Technologiekomponenten mit Workforce IAM teilen kann. Bei einem strategischen und zielgerichteten Einsatz, können Unternehmen ihr Engagement für die Verbraucher maximieren und gleichzeitig die Risiken für IT- und Sicherheitspersonal minimieren.

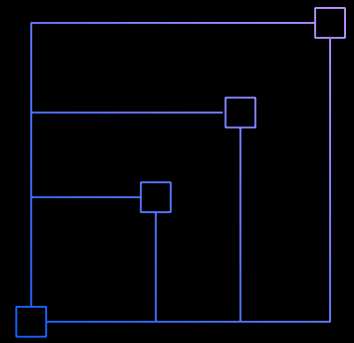
Ohne CIAM-Strategie riskieren Unternehmen einen Ertragsverlust aufgrund von Kundenabwanderung; die Markentreue bleibt instabil, wenn Alternativen direkt vor der Nase liegen. Ähnlich verhält es sich im öffentlichen Sektor: Behörden, die in erster Linie an bestehenden Infrastrukturen und Prozessen festhalten, könnten das Vertrauen ihrer Bürger verlieren und es versäumen, einen hohen Grad an Akzeptanz für öffentliche Dienstleistungen zu erreichen. Trotz ihrer unterschiedlichen Aufgaben sind sich der private und der öffentliche Sektor darin einig, dass sie den Verbrauchern ein reibungsloses und dennoch sicheres digitales Erlebnis bieten und einen datenschutzgerechten Informationsaustausch ermöglichen müssen. Viele Organisationen haben darauf geachtet, genau das zu tun, wodurch CIAM zum größten Segment des gesamten IAM-Markts wurde, für das ein Wachstum von 15,1 %[1] jährlich bis 2025 prognostiziert wurde. Für diejenigen, die mit ihrer digitalen Modernisierung noch nicht begonnen haben, besteht einer der ersten und wichtigsten Schritte in der Herstellung einer Leadership-Ausrichtung über mehrere Funktionsrollen hinweg, sodass alle von dem Projekt profitieren.

# Chief Marketing Officer (CMO)

## CIAM-Ziel: Erfassung, Vertiefung und Wachstum der Benutzer durch personalisierte Erfahrungen, die unter Berücksichtigung des Datenschutzes erfolgen und benutzergesteuert sind.

Im privaten Sektor kämpfen Marketingexperten um die Aufmerksamkeit potentieller Kunden, und das Letzte, was sie wollen, ist eine komplizierte Anmeldeerfahrung, durch die Kunden im letzten Moment abgeschreckt werden. Ein Kundenabbruch kann sich direkt auf den Umsatz auswirken. Daher zielen CIAM-Programme darauf ab, die Registrierung und das Onboarding zu optimieren, um dieses Problem zu vermeiden und unbekannte Kontakte in Geschäftsmöglichkeiten zu verwandeln. Ideale Onboarding-Formulare fragen so wenig Kundeninformationen wie möglich ab, wobei die Berührungspunkte sinnvoll eingerichtet werden, um mit der Zeit und zunehmender Beziehung mehr über einen Kunden zu erfahren.

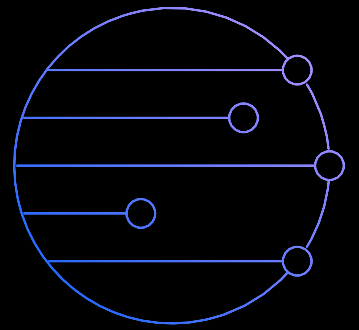
Große Organisationen mit mehreren Marken sollten ihre Datenbestände so anlegen, dass eine einzelne Identität für jeden Konsumenten erhalten wird, die sich dabei in das Customer-Relationship-Management (CRM) und andere Tools und Systemen von weiteren Anbietern einfügt. Mithilfe von zentralisierten Konsumentenidentitäten kann die strategische Implementierung der CIAM Best Practices Marketingexperten in die Lage versetzen, das Verhalten der Konsumenten besser zu verstehen und zielgerichtetere, personalisierte Marketingkampagnen durchzuführen. CIAM spielt eine zentrale Rolle in der digitalen Erfahrung für Interessenten und Kunden, daher ist es für Marketingführungskräfte selbstverständlich, beim Planungsprozess für die Modernisierung eine Schlüsselrolle einzunehmen.



# Manager von Geschäfts-bereichen

## CIAM-Ziel: Erreichen einer rationalisierten, reibungslosen Erfahrung mit modernen Schnittstellen und Engagement, um einen Beitrag zur Erreichung der Ziele der Organisation zu leisten.

Führungskräfte in Unternehmen oder Behördenleiter sind gleichermaßen daran interessiert, Konsumenten an Bord zu holen und reibungslose Interkationen zu ermöglichen, wenn auch nicht notwendigerweise aus Ertragsinteressen. Beispielsweise müssen Behörden den Bürgern öffentliche Dienstleistungen effizient anbieten und das Engagement über eine große Bandbreite von Benutzervorgaben und Kanäle modernisieren, üblicherweise ohne über eine echte Marketingfunktion in der Organisation zu verfügen. Behördenleiter suchen nach einer ähnlichen Umgestaltung des Nutzererlebnisses, um die Registrierung zu vereinfachen und die Zahl der Abbrüche zu verringern, um eine erfolgreiche Bereitstellung von Diensten zu gewährleisten. Während sie wahrscheinlich keine Marketingkampagnen durchführen, sind diese Führungskräfte dennoch daran interessiert, eine einzelne Identität für jeden Konsumenten zu schaffen, um die Interaktionen der Konsumenten über die Abteilungen hinweg zu rationalisieren, Redundanzen abzubauen und das Verhalten besser zu verstehen.

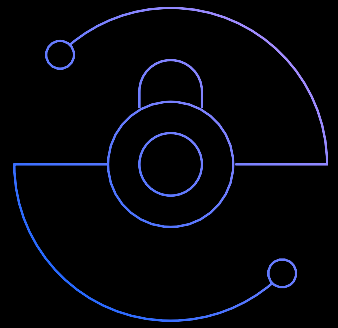


# Sicherheits- und Datenschutzbe-auftragte

## CIAM-Ziel: Sichere Kundeninteraktionen zur Verhinderung von Betrug und Kontokompromittierung, Bereitstellung transparenter und benutzergesteuerter Erlebnisse und Einhaltung von Vorschriften und Compliance-Anforderungen

Als Richtlinie sollten Konsumenten wissen, wer ihre Daten verwaltet und wie diese verwendet werden, wobei die Gelegenheit zur Verwaltung der eigenen Daten und der Änderung der Genehmigungen zu jeder Zeit gegeben sein soll. Dieser Grund ist ausreichend, um Organisationen zu veranlassen, Datenschutz und die Verwaltung von Genehmigungen für ihre digitalen Erfahrungen zu priorisieren, dennoch verhelfen auch weltweite Bestimmungen dem Thema eine gewisse zwangsweise Dringlichkeit. Unternehmen müssen sich an die Vorschriften der jeweiligen Region halten, in der sie tätig sind, oder sie riskieren hohe Strafen und Bußgelder. Die Datenschutzgesetze gehen zwar detailliert darauf ein, was Organisationen zu tun haben, aber sie enthalten in der Regel keine spezifischen Anweisungen, wie sie das Ziel erreichen können. Eine ordnungsgemäße Implementierung von CIAM fungiert als einzige Quelle der Wahrheit für alle persönlichen Daten (PII). Datenschutzbeauftragte und Compliance-Experten können Regeln und Richtlinien für verschiedene Zwecke des Einwilligungsmanagements definieren, die von den technischen Mitarbeitern einfach auf die erforderlichen Anwendungen angewendet werden. Das ermöglicht es Datenschutz- und Compliancemitarbeitern, sich über die Tabellen hinaus zu bewegen, sich der dynamischen Realität der Datenschutzgesetzgebung zu stellen und diese zugänglicher zu machen.

Während CISOs sicherliich ebenfalls an Datenschutz und Einwilligungsmanagement interessiert sind wie Datenschutz- und Compliancebeauftragte, kann doch gelegentlich für CISOs die Versuchung entstehen, CIAM insgesamt als Marketingprojekt zu betrachten und angesichts anderer Prioritätsinitiativen das Interesse zu verlieren. Die Ergebnisse traditioneller Mitarbeiter-IAM und Konsumenten-IAM sind tatsächlich sehr unterschiedlich, allerdings werden beide von kommerziellen Lösungen profitieren, bei denen Daten sicher gespeichert werden und das Risiko einer Datenschutzverletzung gemildert wird - sowohl die Identität von Mitarbeitern wie die von Konsumenten haben das Recht auf Schutz. Wenn darüber hinaus CIAM-Initiativen ohne strategische Betrachtung des aktuellen Standes der IAM-Infrastruktur fortgesetzt werden, kann es sein, dass der CISO am Ende weitere fragmentierte Lösungen in der Umgebung seiner Organisation betreibt, die das Risiko durch zusätzliche Zugriffspunkte erhöhen. Es ist also mit Sicherheit im Interesse der CISOs, die Nutzungsfälle Mitarbeiter-IAM und Konsumenten-IAM wenn möglich unter einer gemeinsamen Lösung zusammenzuführen, um unnötigen Datensilos zu vermeiden.

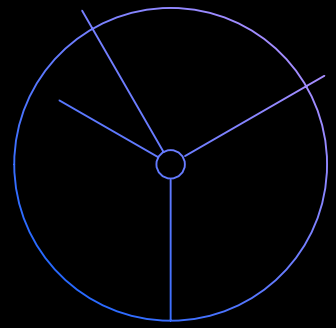


# Chief Information Officer (CIO)

## CIAM-Ziel: Verringerung der Komplexitäten bei der Aufnahme und dem Erhalt von IAM-Lösungen bei gleichzeitiger Einhaltung der neuesten Identitätsstandards zur Beibehaltung einer modernen Sicherheitsposition

Abgesehen von den Vorteilen des Konsumentenengagement durch CIAM müssen CIOs jede Entscheidung für neue Technologien auf Passform innerhalb der ganzheitlichen Infrastruktur der Organisation und des Betriebsplans prüfen. Einfachheit und Standardisierung sind ideal, also sollen IT-Führungskräfte an einem einzelnen Tool, das IAM- und CIAM-Funktionen vereint, ebenso viel Interesse haben wie die Sicherheitsteams. Mit diesem Ansatz wächst die Komplexität der gesamten IT-Umgebung nicht, und es werden auch keine neuen Fähigkeiten von den vorhandenen Mitarbeitern verlangt. Die Wiederverwendung derselben Lösung auch für externe Populationen wird wahrscheinlich einen Kostenvorteil bringen und die IT-Gesamtbetriebskosten reduzieren.

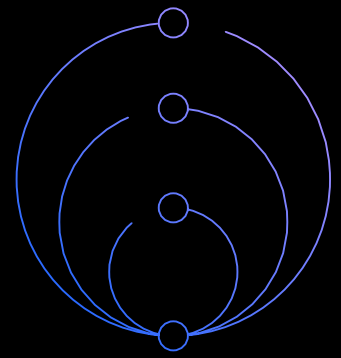
Sobald eine CIAM-Lösung in Betrieb ist, kann jede Minute Ausfallzeit für die Organisation, deren Kunden nicht auf ihre Konten zugreifen können, einen erheblichen Zeit- und Umsatzverlust bedeuten. Dies erklärt, warum viele IT-Verantwortliche Cloud-basierte Lösungen für CIAM-Anwendungsfälle aus Sicht einer ROI Betrachtung bevorzugen, da sie in der Regel eine viel höhere Verfügbarkeit und Skalierbarkeit bieten als lokale Alternativen. Cloud IAM bietet zusätzliche Anreize für IT-Abteilungen, wie z. B. eine geringere Wartung der Infrastruktur, automatische Software-Updates und eine schnellere Wertschöpfung.



# IAM-Administratoren und -Entwickler

## CIAM-Ziel: Vereinfachung der Entwicklungsarbeit sowie Schutz und Erhaltung der Anwendungsrichtlinien durch konfigurationsbasierte Low-Code-Arbeitsabläufe Arbeitsabläufe

Während sich die Führungskräfte an übergeordneten Geschäftszielen, Betriebskosten und Risikominderung orientieren, können IAM-Administratoren und -Entwickler die Entwicklung des CIAM-Programms beeinflussen, indem sie die technischen Fähigkeiten der Lösungen umfassend bewerten. Sie können die Logistik für die Migration oder die Zusammenführung von Datenquellen und Anwendungen sowie Schlüsselelemente wie unterstützte Authentifizierungsprotokolle, MFA-Verfahren und Bereitstellungskanäle betrachten. Zur Realisierung einer kürzeren Zeit bis zu Wertschöpfung kann dieses Team die API-Dokumentation der Lösungen, geführte Ressourcen und Low-Code-Erfahrungen auswerden und sicherstellen, dass ihr Team durch Lösungsimplementierung und Wartung hindurch gut unterstützt wird. Workflow-basierte Funktionen wie das Einwilligungsmanagement im CIAM-Tool können Entwicklern Probleme ersparen, indem sie beispielsweise Details aus den Datenschutzrichtlinien auf einfache API-Aufrufe abstrahieren, die sich automatisch an veränderte Anforderungen anpassen. Bevor ein weiteres Tool hinzugefügt wird, sollte das technische Personal die Kompatibilität und Integration mit den bestehenden IAM-Lösungen ganzheitlich bewerten, um langfristig eine optimale Anpassung zu gewährleisten.



# Der integrierte CIAM-Ansatz von IBM

**Modernisierung der digitalen Erfahrungen durch den integrierten CIAM-Ansatz von IBM**

Mit IBM Security kann Ihre Organisation Ihre Konsumenten erfassen und mit ihnen über bedarfsgerechte, personalisierte und sichere Ommichannel-Engagements mithilfe einer Mischung aus Identitätsstrategie, digitaler Designkompetenz und systemeigener Cloud-CIAM-Technologie Verbindung herstellen. Durch den Einsatz von IBM Security Verify in Verbindung mit IBM Security Services können Sie die organisatorische Abstimmung verbessern, Verbraucherinformationen respektvoll und genau verfolgen und Verbraucher mit einfachen, sicheren digitalen Erfahrungen mit Ihrer Marke überzeugen.

# Nächste Schritte

**Tiefer einsteigen mit CIAM**
Lesen Sie mehr über die CIAM Best Practices, Planungsüberlegungen und vermeidbare Fallstricke

Hier können Sie den Overview Guide herunterladen →

**IBM Security Verify erkunden**
Nutzen Sie IDaaS zur Modernisierung der Nutzererfahrungen durch Social-Login und adaptive Authentifizierung bei gleichzeitigem Erhalt des Datenschutzes dank Einwilligungsmanagement

Mehr über Verify →

**IBM Security Services**
Planen und gestalten Sie ein CIAM-Programm, um es dann bezüglich Unternehmenszielen mithilfe eines einzigartigen beratenden und kollaborativen Ansatzes bereitzustellen und auszuführen

Hilfe zu CIAM anfordern →

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
**ibm.com**/de

Produziert in den USA.
Februar 2021



[1] Markets and Markets, Globale Verbraucherprognose IAM Market bis 2025