okta

Transformieren der Kundenerfahrung mit einer modernen Kundenidentitäts- und Zugriffsmanagement-Lösung (CIAM)

Okta Deutschland
Oskar-von-Miller-Ring 20
80333 München

info_germany@okta.com
+49 (89) 26203329

“Die wachsende Auswahl an Kanälen, Geräten, Plattformen und Kontaktpunkten erhöht den Bedarf an CIAM.”

Die Sicherheitslandschaft verändert sich

Jedes Unternehmen wird heute im Zuge der digitalen Transformation seiner Kundenerfahrungen zu einem Technologieunternehmen. Angesichts der explosionsartigen Zunahme von Geräten, der sich rasch entwickelnden Kundenanforderungen und der höheren Erwartungen der Kunden an Sicherheit und Datenschutz müssen Unternehmen, die erfolgreich sein wollen, Wege finden, um sicherzustellen, dass ihre Kunden jederzeit und von jedem Gerät aus sicher mit ihren Anwendungen oder Diensten arbeiten können.

Hier kommt das Kundenidentitäts- und Zugriffsmanagement (CIAM) ins Spiel. CIAM ermöglicht es, moderne, reibungslose Kundenerfahrungen aufzubauen, schnell auf den Markt zu bringen und gleichzeitig den Bedarf an zukunftssicherer Identität, Sicherheit und Skalierbarkeit zu gewährleisten. CIAM ist eine grundlegende Technologie, die den immer komplexeren Kundenanforderungen gerecht wird und Unternehmen in die Lage versetzt, sichere, nahtlose digitale Erfahrungen zu liefern.

Die wachsende Auswahl an Kanälen, Geräten, Plattformen und Kontaktpunkten erhöht den Bedarf an CIAM. CIAM bietet jedoch mehr als nur die Möglichkeit für die richtigen Personen, zur richtigen Zeit auf die richtigen Ressourcen zuzugreifen.

Traditionell ist CIAM für Anwendungsfälle im Kundenkontakt (B2C) vorgesehen. Der Kunde eines Unternehmens kann aber auch ein Unternehmen sein (B2B). Da die Kunden von den Unternehmen, mit denen sie Geschäfte machen, mehr erwarten, können die Anforderungen mehrere Zielgruppen und Anwendungsfälle umfassen. Unternehmen, die mobile Anwendungen für ihre Kunden entwickeln, müssen möglicherweise Bestandsdaten anzeigen, die traditionell aus einem ERP-System stammen, das mit einer IAM-Lösung für die Mitarbeiter verbunden ist. Oder die Mitarbeiter müssen bei der Fehlerbehebung von Kundenproblemen auf die Erfahrungen der Kunden zugreifen. Dies sind nur einige wenige Beispiele, wobei zwischen den Anwendungen und Nutzertypen weitere vielfältige Integrationen stattfinden.

Folglich werden herstellerbasierte CIAM-Lösungen immer mehr zu einem Muss für Unternehmen. Mehr als 69 % der Befragten einer Gartner IAM-Umfrage verwenden verschiedene IAM-Technologien für B2C-Beziehungen oder planen deren Einsatz bis Ende 2018.* Gartner empfiehlt Unternehmen, „ihr CIAM-System als strategische Plattform zu konzipieren und zu verwalten.“*

Wichtige Trends im Design von CIAM-Lösungen

Wenn Unternehmen eine CIAM-Lösung in Betracht ziehen und ihr Design ausarbeiten, sollten sie Änderungen im Bereich der Kundenidentität berücksichtigen. Hier zeigen wir vier Haupttrends, um Unternehmen bei der Entwicklung einer CIAM-Lösung zu unterstützen, die ihren aktuellen und zukünftigen Anforderungen gerecht wird:

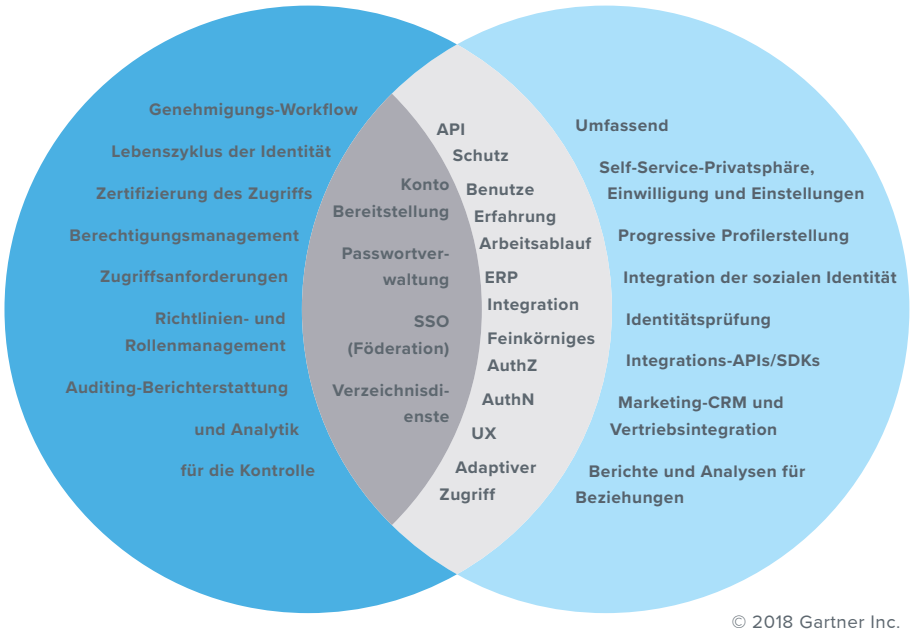
CIAM- und IAM-Funktionen überschneiden sich zunehmend

Eine CIAM-Lösung mag traditionell auf Verbraucher ausgerichtet sein, aber die zunehmende Komplexität der Kundenerfahrung, die zusätzlichen Zielgruppen, die berücksichtigt werden müssen, und die Überschneidung der Anwendungsfälle erfordern traditionellere IAM-Funktionen. Traditionelle IAM-Lösungen haben eine lange Geschichte in Bezug auf feinkörnige Zugriffskontrollen und Sicherheitserwägungen, die zunehmend erforderlich sind, um CIAM-Anwendungsfälle zu erfüllen. Wie in der folgenden Abbildung gezeigt wird, nimmt die Anzahl der IAM-Funktionen, die sowohl für den Einsatz von IAM für Verbraucher als auch für die Bereitstellung von Personal genutzt werden müssen, weiter zu.

Die traditionellen Überlappungsbereiche (dunkelgrau dargestellt und als Teil der Ende 2016 durchgeführten Forschung veröffentlicht) umfassen nur eine Handvoll Kernfunktionen wie Passwortverwaltung und Single Sign-On (SSO). Aber die funktionale Überschneidung zwischen IAM und CIAM nimmt mit der Hinzufügung neuer Funktionen (hellgrau dargestellt und nur 1,5 Jahre später hinzugefügt) rasch zu.

Eine Funktionsüberschneidung ist der API-Schutz, bei dem es darum geht, APIs vor böswilligen Angriffen und Bedrohungen zu schützen, z. B. APIs zur Unterstützung mobiler Anwendungen. Ein weiteres Überschneidungsmerkmal ist der adaptive Zugriff. Dieser ermöglicht eine kontextbezogene Zugriffsverwaltung durch intelligente Zugriffs- und Authentifizierungsrichtlinien, die auf dem Anmeldekontext basieren, einschließlich Gerät, Standort und Netzwerk. Der adaptive Zugriff

CIAM und IAM Funktionsüberlappung nimmt zu



Workforce IAM

Consumer IAM

Gartner, Abbildung 3, **CIAM und die Überlappung der Workforce-IAM-Features nehmen zu**, Gartner, Top 5 Trends in CIAM Solution Design, 5. März 2018

Quelle: Gartner (März 2018

kann das Authentifizierungsrisiko ohne größere Reibungsverluste für alle Benutzer eines Unternehmens – Verbraucher, Mitarbeiter, Partner und andere Benutzer – reduzieren. Die feinkörnige Autorisierung, die traditionell mit Mitarbeitern und Geschäftspartnern, die auf sensible Daten zugreifen, verbunden ist, gilt jetzt auch für Kunden, die Zugriff auf genau die richtige Informationsebene erhalten.

Dem Bericht zufolge nehmen die Überschneidungen zwischen CIAM- und anderen IAM-Implementierungen weiter zu. Implementierungen, die mehrere Benutzerumgebungen bedienen, werden immer üblicher – zum Beispiel B2C und B2B oder IoT und B2C auf derselben CIAM-Plattform.* Wichtige IAM-Anforderungen für Mitarbeiter wie der Lebenszyklus der Identität werden zunehmend für CIAM-Anwendungsfälle zur Bekämpfung böswilliger Angreifer benötigt. Auditing, Berichterstattung und Analysen zur Kontrolle sind ebenfalls wichtig, um CIAM-Implementierungen eng an die Sicherheits- und DevOps-Prozesse eines Unternehmens zu binden. Darüber hinaus werden die üblichen CIAM-Anforderungen rund um die Integration von SDKs/APIs und Self-Service nun auch in IAM-Lösungen für die moderne Anwendungsentwicklung genutzt, ebenso wie für Mitarbeiter, die mit Erwartungen der Verbraucher konfrontiert waren. Diese einheitliche Implementierung kann betriebliche Effizienz bieten und sollte sich auch an die sich ständig ändernden Bedürfnisse der Unternehmen und ihrer Nutzer anpassen.

Reibungslose, konsistente Omni-Channel-Erlebnisse durch Single Sign-On

Kunden sind auf eine große Anzahl von Geräten angewiesen – und diese Zahl steigt weiter. Auch die Kundennachfrage nach biometrischen Daten als zweitem Faktor der Authentifizierung oder sogar nach einem passwortlosen Zugriff nimmt zu.

Aus diesem Grund sollten sich Unternehmen auf Möglichkeiten zur Reduzierung von Reibungsverlusten konzentrieren, da unnötige Reibung zu Kundenabwanderung führt. Die Verwaltung von Kundenidentitäten kann eine bedeutende Herausforderung sein, nicht nur, weil Unternehmen alle diese Kanäle unterstützen müssen.

Sie müssen auch sicherstellen, dass die Benutzererfahrung für jeden einzelnen optimiert wird, während sie dennoch für alle konsistent ist.

Um dies zu erreichen, empfiehlt Gartner die Bereitstellung„einer einheitlichen Anmeldung (SSO) über alle digitalen Eigenschaften hinweg, wenn das Unternehmen dies nicht bereits getan hat.“ Die Aktivierung eines einzigen Logins, der für den Zugriff auf alle verbraucherorientierten Systeme der Organisation verwendet werden kann, reduziert die Reibung für den Verbraucher und bietet eine einzige Quelle für maßgebliche Informationen aus erster Hand.*

Verbesserte Entwicklerunterstützung

In einer Welt, in der jedes Unternehmen ein Technologieunternehmen ist, müssen CIAM-Systeme eine Plattform für kontinuierliche Veränderungen bieten, und die CIAM-Systeme entwickeln sich zu flexibleren Entwicklerplattformen. Entwickler spielen eine Schlüsselrolle beim Aufbau von anspruchsvollen Kundenerfahrungen. Sie benötigen eine agile CIAM-Lösung, die eine schnellere Markteinführung ermöglicht, um die sich schnell ändernden Kundenbedürfnisse zu erfüllen. Darüber hinaus sollte eine CIAM-Lösung Entwickler bei der Bereitstellung einer Identitätsschicht für sichere Kundenerfahrungen unterstützen. Auf diese Weise muss das Rad nicht neu erfunden werden, wenn es um Authentifizierung, Autorisierung und Benutzerverwaltung geht, sondern man kann sich stattdessen auf die Merkmale der Anwendungen konzentriert werden, die sie von ihren Mitbewerbern unterscheiden.

Unter den vielen Komponenten einer CIAM-Lösung sollten Unternehmen nach entwicklerfreundlicheren Funktionen suchen, wie z. B.:

- **Gut dokumentierte APIs mit Beispielcode**
- **Sprach- und Framework-Unterstützung (SDKs)**
- **Umfassende Dokumentation**
- **Anpassbare UI und Workflows**

- **Fähigkeit zur Integration mit API-Gateways**
- **Unterstützung für ereignisgesteuerte Verarbeitung**

Gartner schlägt vor, CIAM-Angebote mit Funktionen anzubieten, die Entwickler in die Lage versetzen, sich kontinuierlich an neue Kunden- und Geschäftsanforderungen anzupassen.* Eine CIAM-Lösung muss entwicklergetrieben und agil genug sein, um neue Architekturen, Protokolle, Dienste und andere Fortschritte berücksichtigen.

Mehr Fokus auf Sicherheit und Compliance

Sicherheit ist das A und O – ein Versuch des Missbrauchs von Kundendaten ist jederzeit möglich. Und wenn dies geschieht, kann es enorme Auswirkungen auf die Lebensfähigkeit eines Unternehmens und die Sicht der Kunden auf dieses Unternehmen haben.

Dies unterstreicht die Notwendigkeit von Sicherheitsfunktionen und -lösungen der nächsten Generation.

Laut Gartner „muss die Sicherheitsarchitektur alle CIAM-Initiativen unterstützen.“* Der Zugriff von Kunden sollte durch adaptive Authentifizierungsmethoden geschützt werden, die einen kontextabhängigen Ansatz zur Überprüfung der Identität eines Kunden implementieren. Die Unternehmen müssen sich überlegen, wie sie die Kundeninteraktionen sichern und gleichzeitig die Benutzerfreundlichkeit und eine reibungslose Authentifizierungserfahrung gewährleisten. Der adaptive Zugriff würde dynamische Identifikatoren wie den Standort eines Kunden, das Gerät, die IP-Adresse und andere vom Anbieter gesammelte Daten berücksichtigen. So werden Kunden, die sich mit einem neuen Gerät bei einer sensiblen Anwendung anmelden, zur MFA aufgefordert. Auf der anderen Seite können Kunden, die sich mit einem zuvor registrierten mobilen Gerät anmelden, eine passwortlose Authentifizierung verwenden, womit höhere Sicherheit und bessere Benutzerfreundlichkeit vereint sind.

In dem Bericht heißt es: „Viele der ausgeklügelten verbraucherorientierten Initiativen, wie z. B. die Entwicklung einer mobilen Kundenanwendung oder einer neuen browserbasierten Anwendung, beinhalten die Entwicklung neuer APIs, auf die die Verbraucher über das Internet zugreifen können. Diese externen APIs müssen durch eine Kombination von Sicherheits- und IAM-Maßnahmen geschützt werden. Für jede extern angesprochene API (und viele interne), muss ein API-Gateway, das oft Teil einer umfassenderen API-Lebenszyklusmanagement-Lösung ist, in die API-Schutzinfrastruktur aufgenommen werden.

Für CIAM-Anwendungsfälle ist das CIAM-System der Identitätsanbieter, der über OAuth und/oder OpenID Connect mit dem API-Gateway verbunden ist. Je nach dem spezifischen Anwendungsfall benötigen Sie möglicherweise auch eine oder mehrere der neueren Erweiterungen des OAuth-Stand-dards.“*

Neben Sicherheit müssen Unternehmen auch die Einhaltung von Vorschriften planen: Die Maßnahmen zum Schutz von Kundendaten werden immer strenger, wie die Datenschutz-Grundverordnung der Europäischen Union (DSGVO), das neue kalifornische Datenschutzgesetz und branchenspezifische Anforderungen wie MFA für Finanzanwendungen in New York zeigen. Eine CIAM-Lösung kann durch einen automatisierten Ansatz für gemeinsame Anforderungen eine reibungslose Kundenerfahrung in jeder Rechtsordnung ermöglichen.

“Sicherheit ist das A und O – ein Versuch des Missbrauchs von Kundendaten ist jederzeit möglich.”

Die Okta Identity Cloud: Eine moderne CIAM-Lösung

Eine moderne CIAM-Lösung sollte nicht nur den heutigen Sicherheits- und Konformitätsstandards entsprechen, sondern auch die Anforderungen erfüllen, reibungslose Kundenerfahrungen der nächsten Generation anzubieten. Die Okta Identity Cloud leistet genau das und bietet die sicherste und zuverlässige CIAM-Lösung, um Kundendaten sicher aufzubewahren. Gleichzeitig bietet sie eine Reihe hochinteressanter Entwicklertools für zukünftige Agilität.

Okta wurde in der und für die Cloud entwickelt. Oktas Identity Cloud-Lösung bietet einen einzelnen, kompletten, integrierten Service für jede Art von Benutzer. Mit Funktionen, die einander überschneidende IAM- und CIAM-Anwendungsfälle unterstützen, bietet die Okta Identity Cloud eine zentrale Zugriffskontrolle für alle Arten von Kundenerfahrungen. Sie ermöglicht eine höhere Effizienz für IT-Teams, die den Benutzerzugriff verwalten und für Entwickler, die Benutzererfahrungen aufbauen. Sie lässt sich skalieren, um die Anforderungen jeder Organisation effizient zu erfüllen.

Damit ermöglicht sie Millionen von Benutzern die sichere Verbindung zu den von ihnen benötigten Erfahrungen. Unternehmen können entweder Oktas vorgefertigte Funktionen verwenden oder Oktas APIs und Toolkits nutzen, um maßgeschneiderte Kundenerlebnisse zu ermöglichen.

Die Okta Identity Cloud bestimmt mit ihren Produkten und Funktionen alle wichtigen Trends im Design von CIAM-Lösungen:

Single Sign-On

Oktas Identity Cloud bietet Single-Sign-On-Fähigkeiten, die beliebige Portale und Anwendungen mit einem einzigen Satz von Berechtigungsnachweisen verbinden – oder im Falle von passwortlosen Anwendungen ganz ohne Berechtigungsnachweis: Die Benutzer müssen nur einmal klicken, um sich bei allem anzumelden.

Adaptive Multi-Faktor-Authentifizierung

Okta Adaptive MFA verbindet eine breite Palette von zweiten Faktoren und ein robustes Richtlinien-Framework, das Identitätsangriffe mit einer zusätzlichen Authentifizierungsebene verhindert. Diese Funktion ermöglicht es Unternehmen, Richtlinien für die Aufforderung zur MFA auf der Grundlage des Benutzerprofils, der Anwendung und des Authentifizierungskontexts festzulegen. Mit der Unterstützung einer Reihe von Verifizierungsfaktoren wie SMS, Okta Verify with Push und Biometrie ist Okta Adaptive MFA flexibel, um das richtige Maß an Sicherheit auf die unterschiedlichen Bedürfnisse der Benutzer anzuwenden.

Universal Directory

Oktas Universal Directory bietet einen zentralen Ort für Unternehmen, um Benutzer, Anwendungen, Geräte und APIs zu verwalten. Universal Directory kann eine unbegrenzte Anzahl von Kundenattributen speichern, einschließlich Einwilligungs- und Datenschutzpräferenzen. Zusätzlich kann Universal Directory mit jeder Anwendung und jedem Verzeichnis synchronisiert werden, um eine 360-Grad-Sicht auf einen Kunden zu ermöglichen. Als Ergebnis können Organisationen ein Repository für Benutzeridentitätsinformationen aufbauen, aus dem eine konsistente, personalisierte Erfahrung über alle Anwendungen hinweg geschaffen werden kann.

API Access Management

Immer mehr kundenspezifische Anwendungen werden mit einem API-Backend entwickelt. Die API-Zugriffsverwaltungsfunktionen von Okta sind für moderne mobile und Webanwendungen mit standardkonformer Unterstützung für OAuth 2.0 konzipiert. Diese Tools sparen zwei Wochen Entwicklungszeit pro Jahr und schützen eine unbegrenzte Anzahl von API-Ressourcen hinter jedem API-Gateway.

APIs und Entwicklerwerkzeuge

Okta APIs und Entwickler-Tools bieten programmatischen Zugriff auf die Okta Identity Cloud und ermöglichen es Entwicklern, innerhalb von Minuten die Authentifizierung, Autorisierung und Benutzerverwaltung in ihre Anwendungen zu integrieren. Okta verfügt über Entwickler-Toolkits (SDKs) in jeder wichtigen Programmierumgebung, unterstützt durch eine Vielzahl von Dokumenten- und Schnellstart-Assistenten, um die Produktivität der Entwickler zu erhöhen. Registrieren Sie sich noch heute für ein kostenloses Okta-Entwicklerkonto, um mit der Einrichtung zu beginnen.

Sicherheitsanalysen und Compliance

Okta verfolgt mit seiner geprüften, sicheren Infrastruktur und seinen Prozessen einen umfassenden Sicherheitsansatz, der das Personal, den Entwicklungslebenszyklus sowie die Strategien und den Betrieb von Rechenzentren umfasst. Zusätzlich ermöglicht Okta eine ganzheitliche Transparenz und Reaktion durch Echtzeitberichte, die auch in eine Sicherheitsanalyselösung integriert werden können.

Okta Integration Network

Oktas umfangreiches Netzwerk von Integrationen ermöglicht es Entwicklern, neue Anwendungen schneller auf den Markt zu bringen, während gleichzeitig die Sicherheit der Kunden gewährleistet ist und ihnen durch Integrationen wie API-Gateways und ID-Proofing eine reibungslose Benutzererfahrung geboten wird.

Die Okta Identity Cloud bietet eine breite Palette an CIAM-Funktionen. Aus diesem Grund ist Okta die führende CIAM-Lösung, die entwickelt wurde, um Kundenkonten zu schützen, mehr Benutzer zu gewinnen und die Erträge von Unternehmen zu steigern.

USSTEN SIE SCHON?

Okta wurde in den letzten fünf Jahren im Magic Quadrant von Gartner für IdaaS und Access Management als führend eingestuft.**

BEREIT FÜR DEN START?
Kontakt aufnehmen

*Gartner, Top 5 Trends in CIAM Solution Design, 5 March 2018

**Gartner, Inc., Magic Quadrant for Access Management, Worldwide, Gregg Kreizman, 18 June 2018.

Gartner unterstützt keine Anbieter, Produkte oder Dienstleistungen, die in seinen Forschungspublikationen dargestellt werden, und rät Technologieanwendern nicht, nur die Anbieter mit den höchsten Bewertungen oder anderen Bezeichnungen auszuwählen. Die Forschungspublikationen von Gartner bestehen aus den Meinungen der Forschungsorganisation von Gartner und sollten nicht als Tatsachenaussage ausgelegt werden. Gartner lehnt jede ausdrückliche oder stillschweigende Gewährleistung in Bezug auf diese Forschung ab, einschließlich jeglicher Gewährleistung der Marktgängigkeit oder Eignung für einen bestimmten Zweck.