okta

Dekodierung von Customer IAM (CIAM) im Vergleich zu IAM (Identity Access Management)

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

info_germany@okta.com
+49 (89) 26203329

Dekodierung von Customer IAM (CIAM) im Vergleich zu IAM

Beim Identity and Access Management (IAM) gehen die Meinungen selten auseinander. Allerdings wird derzeit darüber debattiert, wie wir als Branche über kundenorientierte Anwendungsfälle für IAM sprechen. Von vielen wird dies als Customer IAM oder Consumer IAM bezeichnet, beide abgekürzt als CIAM.

CIAM hat einige besondere Anforderungen. Aber das bedeutet nicht, dass Sie ein Produkt verwenden müssen, das sich nur auf CIAM konzentriert. Okta verfolgt den Ansatz, einen vielseitigen IAM-Cloud-Service mit einer leistungsfähigen Basisplattform und einem Funktionsumfang anzubieten, der CIAM-Anwendungsfälle mit abdeckt. Wir halten das für die langfristig bessere Lösung.

Zunächst einmal: Was ist IAM oder CIAM?

Eine kleiner Schnellkurs, falls Sie mit IAM-Software nicht vertraut sind: Das IT-Marktforschungs- und Beratungsunternehmen Gartner definiert IAM als die Instanz, die „den richtigen Personen zur richtigen Zeit und aus den richtigen Gründen den Zugriff auf die richtigen Ressourcen ermöglicht.“ Diese Definition ist sehr breit gefasst und deckt fast alles im Bereich Computer und IT ab.

Für die meisten Anwendungen sieht dies wie eine Datenbanktabelle aus, die Profile und Passwörter speichert. Es kann auch einige Berechtigungsdaten enthalten. Für komplexere Anwendungen oder groß angelegte Implementierungen kann gebündelte IAM-Software.

verwendet werden, die Sicherheit bietet und über vorgefertigte Frameworks verfügt, um wesentlich komplexere Berechtigungen zu verwalten, möglicherweise über viele Anwendungen hinweg.

Im Allgemeinen kann die IAM-Software viele Anwendungsfälle abdecken: wenn die Benutzer Mitarbeiter sind und die Berechtigung auf einer Rolle im Unternehmen basiert oder wenn die Benutzer Kunden sind und die Berechtigung auf einer Mitgliedschaft basiert. Letzteres führt uns in die Welt des Customer IAM, kurz CIAM.

Welche Parallelen bestehen zwischen CIAM und IAM?

Kurz gesagt, die Antwort ist Sicherheit, Skalierbarkeit und Hochverfügbarkeit.

Richtig ist, dass nicht alle IAM-Lösungen die Anforderungen der kundenseitigen Anwendungsfälle (sprich: B2C) erfüllen können. Aber die wichtigsten funktionalen Bausteine und Protokolle des IAM in Bereichen wie Authentifizierung, Autorisierung, Verzeichnisdienste und Lifecycle-Management sind gleich. Ein Anbieter, der eine Reihe von Kernfunktionen der IAM-Plattform – wie OpenID Connect und OAuth-Support – für Mitarbeiter, Auftragnehmer, Partner, Kunden und Verbraucher nutzt, kann viel mehr Einfluss gewinnen als ein Anbieter, der proprietäre Technologien entwickelt, um nur einen Anwendungsfall zu bedienen. Letztendlich führt diese Hebelwirkung zu mehr Innovation und langfristigem Markterfolg – und einem langfristigen Partner für Ihre App-Entwicklungsprojekte. Sie sollten auf einem Fundament aufbauen, das auf lange Sicht Bestand haben wird.

IAM-Systeme sind der Schlüssel, daher ist unabhängig vom Anwendungsfall die Sicherheit eines IAM-Produkts von größter Bedeutung. Die gleichen Sicherheitskontrollen rund um einen Authentifizierungs- oder Föderationsdienst gelten unabhängig davon, ob es sich bei dem Anwendungsfall um in Office 365 föderierte

Mitarbeiter, um in einem Support-Portal föderierte Kunden oder um zwischen mehreren Hotel-Websites eines großen Gastgewerbeunternehmens föderierte Gäste (beispielsweise MGM Resorts International) handelt. Kompromittierte Mitarbeiterkonten führen zu Hacking von internen Systemen und kompromittierte Verbraucherkonten laufen in der Regel auf eine Meldepflicht und ein PR-Desaster hinaus, auch wenn Sie kein Börsenunternehmen sind.

Beim Thema Skalierbarkeit kommen wir in Bereiche, in denen spezialisierte CIAM-Anbieter gern auf die besonderen Anforderungen verweisen, was nicht falsch ist. Vergleicht man einen CIAM-Cloud-Service mit einem älteren lokalen IAM-Produkt, fällt auf: Der CIAM-Service muss in der Lage sein, einen einzelnen Kunden mit Abermillionen von Identitäten zu bewältigen. Viele ältere lokale und auch allgemeine IDaaS-Produkte (Identity-as-a-Service) wurden nicht für diese Größenordnung entwickelt. Eine IDaaS-Lösung jedoch, die alle Anwendungsfälle abdeckt und Tausende von Kunden mit Hunderten von Millionen an monatlichen Authentifizierungen verzeichnet, kann jedoch leicht skaliert werden, um einen neuen Kunden mit Millionen von Benutzern zu bedienen. Das Beharren auf der Besonderheit von CIAM überzeugt nicht, wenn Ihr Anbieter bereits einen Cloud-Service mit mehreren Mandanten in sehr großem Umfang betreibt.

Schließlich ist eine hohe Verfügbarkeit für alle Anwendungsfälle von entscheidender Bedeutung. Wenn Ihr IAM nicht funktioniert, können Sie keine Geschäfte machen. Verluste in der Produktivität der Mitarbeiter ist enorm, aber noch schlimmer: Ihre nicht verfügbare E-Commerce-Site bedeutet verlorene Umsätze. Auch hier bietet ein moderner Cloud-Service mit extremer Redundanz die für alle Anwendungsfälle erforderliche Hochverfügbarkeit.

Worin besteht dann der Unterschied zwischen CIAM und IAM?

Interne IAM-Systeme für Mitarbeiter werden typischerweise für den Zugriff auf interne Dienste verwendet und können ein Benutzerportal beinhalten. CIAM-Dienste werden in der Regel von Website-Benutzern oder App-Benutzern mit Mobilgeräten genutzt. Sie erwarten, dass sie sich auf einer Website anmelden können, ohne Umwege über das IAM-Anbieterportal eines Drittanbieters. Dazu müssen CIAM-Produkte grundsätzlich entwicklerfreundlich und einfach zu bedienen sein. Wenn der CIAM-Anbieter es einem Entwickler nicht leicht macht, Benutzerkonten für seine Anwendungen zu registrieren, anzumelden und zu verwalten, braucht der Entwickler einen neuen Anbieter. Der IAM-Dienst muss über ein REST-API verfügen, das flexibel genug ist, um auf die gesamte Funktionalität zugreifen zu können, und er muss moderne Entwicklerwerkzeuge bereitstellen, darunter SDKs für mehrere Programmiersprachen und einbettbare Widgets.

CIAM erfordert je nach Anwendungsfall mehr Flexibilität bei der Authentifizierung, von der B2B-Kundenföderation über die soziale Authentifizierung und die native Authentifizierung bis hin zur Authentifizierung ohne Passwort. Ein moderner IAM-Cloud-Service, der immer auf dem neuesten Stand der Authentifizierungstechnologie und -protokolle ist, ist hier klar im Vorteil, weil er über die volle Bandbreite an Optionen verfügt. Bei der Authentifizierung über sozialen Medien im Verbraucherbereich ist die Verknüpfung eines SM-Profils mit dem Kernprofil eines Benutzers wichtig. Meistens werden die Entwickler das Verhalten dieser sozialen Daten anpassen wollen, und das IAM-System muss flexibel genug sein, um verschiedene Vorgänge rund um das Benutzerprofil programmgesteuert durchzuführen.

Das Autorisierungsmodell für CIAM kann einfacher ausfallen als bei IT-Anwendungsfällen, denn Kundenrollen sind oft begrenzter als das breite Spektrum an internen Rollen in großen Unternehmen. In diesem Bereich kann ein IAM-System, das über eine ausreichend robuste Autorisierungsfähigkeit verfügt, um Unternehmensszenarien zu bewältigen, durchaus CIAM-Anforderungen abdecken, sofern sich Aspekte wie Gruppenmitgliedschaften und Benutzerattribute programmatisch steuern lassen.

Die Verwaltung der Kundenidentitäten erfordert besondere Sorgfalt bei der Einhaltung von Vorschriften wie z. B. der Datenschutz-Grundverordnung der EU (DSGVO), die die Privatsphäre der Benutzer schützt und ihre Einwilligung zur Datenverarbeitung voraussetzt. Für verbraucherseitige Anwendungen bedeutet dies: Sie müssen Kontrollkästchen und Schaltflächen anbieten können, mit der Benutzer der Verarbeitung ihrer Daten zustimmen. Die wesentliche IAM-Anforderung besteht jedoch weiterhin in der sicheren Pflege der Benutzerdaten. Diese grundlegende Sicherheitsanforderung ist für alle IAM-Anwendungsfälle von größter Bedeutung. Entscheidend ist daher die Wahl einer Plattform, die höchste grundlegende Sicherheit bietet. Das Einfügen von Kontrollkästchen und Schaltflächen bei der Implementierung ist vergleichsweise einfach, zumal diese Anpassung ohnehin erforderlich sein wird.

Und was ist mit Marketinganalysen?

Einige CIAM-Anbieter begannen mit der Entwicklung ihrer Dienste, als der digitale Wandel noch am Anfang stand. Sie mögen Visionäre gewesen sein, aber ihr ursprünglicher Schwerpunkt lag auf der Verfolgung des Nutzerverhaltens und dessen Auswertung für Marketinganalysen. Das sind wichtige Anforderungen, doch der Markt für diese Produkte ist gereift. Mittlerweile haben Entscheider im Marketing unzählige Lösungen für Marketinganalysen zur Auswahl.

Gleichzeitig steht die IAM-Technologie nicht still. Neue Protokolle wie OpenID Connect und OAuth ermöglichen eine moderne App-Architektur (mobile oder einseitige App, die Backend-REST-APIs nutzt) und Microservices (Server-Server-Kommunikation über APIs). Entwickler, die diese modernen Anwendungen konzipieren, benötigen eine IAM-Plattform, die ihre Anwendungen mit diesen modernen Protokollen absichern kann. Ein moderner IAM-Service kann diese Szenarien besser abdecken als spezialisierte CIAM-Produkte, die einseitiger auf Marketing ausgerichtet sind marketingorientierten Fokus haben.

Das Gesamtbild der Unternehmens-IT

Wie sich gezeigt hat, spricht in der Welt der B2C-Anwendungsfälle für IAM viel dafür, dass eine marktführende IDaaS-Lösung wie Okta die beste Wahl ist. Okta bietet moderne IAM-Funktionen und ist von Grund auf für Sicherheit, Skalierbarkeit und Hochverfügbarkeit von Kundenanwendungen konzipiert.

All das beschränkt sich nicht auf B2C, es gibt bei Anwendungsfällen und Anforderungen viele Grautöne. Okta sieht seine Kunden in einem weiten Feld von Anwendungsfällen: B2C-Verbraucher-Apps, B2B-Kunden-Apps, B2B-Partner-Collaboration, Supply-Chain-Integration, Support-Portale, interne Apps für Remote-Mitarbeiter, nahtlose Integration über kundenseitige E-Commerce-Websites, Anbindung von Mitarbeitern an SaaS-Apps, Bereitstellung eines lebenslangen Zugriffs für Universitätsabsolventen, schnelle Aktivierung von sicherem E-Commerce und schließlich Unterstützung von Unternehmen bei der Monetarisierung ihrer Daten und dem Aufbau eines Geschäftsmodells auf der API Economy.

Wir sehen CIOs, CDOs, CTOs und CMOs, die alle Arten von Unternehmen in diesem weiten Feld von Anwendungsfällen leiten. Und die beste Unterstützung in diesem facettenreichen Umfeld ist ein IAM-Partner, der diese enorme Bandbreite abdeckt. Jede andere Wahl schränkt Ihre zukünftige Innovationsfähigkeit dramatisch ein.

Mehr zum Thema Consumer Identity Management für CMOs, CISOs, CIOs und andere Entscheidungsträger erfahren Sie hier:
https://www.okta.com/resources/whitepaper-consumer-identity-management-for-the-cmo-ciso-and-cio/