Aufgedeckt: Identity

Innovationskraft stärken, persönliche Daten schützen und Kunden zufriedenstellen – kein Problem!

okta

Ein Blick auf die Voraussetzungen für hervorragende Sicherheit und Compliance – ohne die Innovationskraft oder die Customer Experiences zu beeinträchtigen.

Die Absicherung von Kundendaten und Verwaltung der wachsenden Kundenbasis, die auf Ihr Unternehmen zugreift, fordert alle Ihre Ressourcen. Gleichzeitig müssen Sie ansprechende Customer Experiences gewährleisten und Innovationen im gesamten Unternehmen vorantreiben. Dies ist unverzichtbar, wenn Sie gegenüber Mitbewerbern nicht ins Hintertreffen geraten wollen.

Doch während Sie mit einer CIAM-Lösung für Kundenidentitäts-Management perfekte und gleichzeitig sichere Customer Experiences gestalten, laufen Sie Gefahr, genau die Schwachstellen zu schaffen, die Sicherheitsverletzungen und Datendiebstahl ermöglichen – was Sie doch eigentlich verhindern wollten. Der Aufbau einer CIAM-Umgebung könnte sich sogar als derart zeitaufwändig erweisen, dass Ihre IT-Ressourcen aufgrund von Schwierigkeiten bei Aufbau und Pflege der Lösung keine Zeit für Innovationen mehr haben.

Ihre aktuelle Situation könnte wie folgt aussehen:

1

Sie verfügen bereits über eine Identitätslösung

2

Sie planen die Entwicklung Ihrer eigenen Lösung oder sind gerade dabei

3

Sie sind auf der Suche nach möglichen Partnern

Ganz gleich, wie weit Sie bei der Customer Identity-Implementierung sind: Erfüllt Ihre Lösung Ihren Zweck?

Das sind die Voraussetzungen für Kontrolle und Innovationen:

Anforderungen auf Sicherheitsebene:

Bedrohungsakteure müssen draußen bleiben

Adaptive Sicherheitsmaßnahmen müssen mithilfe von Ansätzen wie Multi-Faktor-Authentifizierung (MFA) und passwortloser Authentifizierung verhindern, dass Betrüger sich als legitime Benutzer ausgeben oder Identitätsdiebstahl begehen können.

Einhaltung von Compliance-Vorschriften

Mit effizienter Verwaltung von Kundendatensätzen und Datenaustausch zwischen unterschiedlichen Systemen.

Anforderungen von Entwicklern und Technikern:

Integration mit vorhandenen Systemen

Reibungslose Integration mit robusten SDKs, APIs und Widgets, um Funktionen zusammenzuführen und Workflows sowie die User Journey benutzerfreundlich zu gestalten.

Schnelle Skalierbarkeit

Bewältigen Sie eine große Anzahl von Benutzern – mit der Möglichkeit, flexibel verschiedene Authentifizierungsprotokolle zu unterstützen.

Für den CTO sind folgende Faktoren wichtig:

Kanalübergreifende Konsistenz

Für einheitliche User Experiences unabhängig davon, wo und wie Kunden auf Ihr Unternehmen zugreifen – ein zentrales Login, verschiedene Apps.

Höchst innovativ

Dank modernster Funktionen halten Sie mit der dynamischen Landschaft Schritt, um die immer anspruchsvolleren Kunden zu binden.

Customer Experiences

In jeder Phase reibungslos und ansprechend, bietet neue Sicherheitsprotokolle ebenso wie Plattform-Updates und ermöglicht die Einbindung neuer Kanäle.

Keynote:
Sie benötigen eine Lösung, die die Anforderungen des Unternehmens, der Entwickler oder des CTO erfüllt.

Eine Plattform, die jederzeit anpassbar ist:

Sicherheitsmaßnahmen entwickeln sich weiter

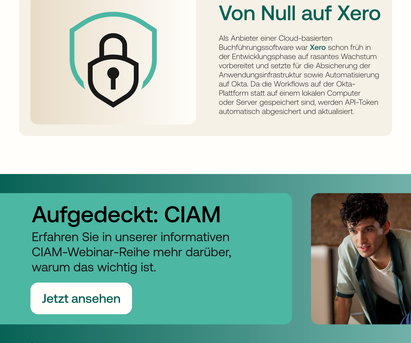
Von MFA über passwortlose Authentifizierung und Einmal-Passwörter. Ganz gleich, was als nächstes gefordert wird, Ihre Plattform muss dafür bereit sein.

Cyberkriminelle sind hartnäckig

Sie finden ständig neue raffinierte Methoden und nutzen für ihre Angriffe sogar KI. Bei all dem selbst geschriebenen Code, der für Customer Identity erforderlich, ist es wichtig, dass Sie damit keine Schwachstellen schaffen.

Kleine Abkürzungen, große Geldstrafen

Ob DSGVO (Datenschutz-Grundverordnung) oder NIS 2 (Network and Information Security Directive): Die Compliance-Vielfalt wächst und wird immer komplexer. Gleichzeitig gibt es keine Fehlertoleranz und die Einhaltung der Vorschriften ist Pflicht.



Ein kritischer Blick auf Ihre eigene Umgebung

Können Sie Zuverlässigkeit im großen Maßstab gewährleisten? Auf jedem Gerät rund um die Uhr?

Auch wenn nicht gerade Black Friday, das nächste Großevent oder die Abgabe der Steuererklärungen ansteht – es gibt keine gute Zeit für Ausfälle.

Ist Customer Identity auf sichere Weise in Ihren Technologie-Stack integriert?

CIAM muss sich in Ihre Software-Umgebung für Sicherheit, Datenschutz, Marketing und Service-Management einfügen, damit Sie den ROI und das Geschäftspotenzial maximieren können.

Nutzen Sie Ihre erfahrenen Entwickler und Sicherheits-experten optimal?

Möchten Sie deren Arbeitszeit für die Verwaltung von Customer Identity nutzen – oder sollten sie sich besser auf Ihr Kerngeschäft konzentrieren?

In der Praxis: Customer Identity, wie sie sein sollte:

2,5 Tage

So lange dauerte es bei **Arduino**, dem Open-Source-Anbieter einer elektronischen Prototyping-Plattform, die IoT- und Android-Anmeldung für seine App (Arduino IoT Cloud) zu implementieren. Dank der erfolgreichen Partnerschaft mit Auth0 wurde die Produktbereitstellung um mehrere Wochen beschleunigt. Gleichzeitig ist die Einhaltung der DSGVO-Vorschriften gewährleistet.

Hunderte Apps und Services. Eine Anmeldung.

Gemeinsam mit Auth0 konnte **Siemens** eine einheitliche Anmeldung für Kunden und Partner bei allen Prozessen und Abteilungen implementieren. Siemens ID ist ein zentraler Login-Dienst, der sich schnell mit dem gesamten Tech-Stack jedes Unternehmens integrieren lässt. Er zentralisiert die Benutzerdatenbank sowie die Anmeldeseite, bietet jedoch gleichzeitig allen Abteilungen die Möglichkeit, die Anwendung individuell zu integrieren.

590 Millionen

So viele Verbraucher nutzen die **Bazaarvoice**-Anwendungen jeden Monat. Durch die Zusammenarbeit mit Okta konnte der Plattformanbieter für benutzergenerierten Content seinen Kunden die Möglichkeit geben, sich mit ihrem eigenen Identitätsanbieter anzumelden. Das vereinfacht die Benutzer-verwaltung und erlaubt es Bazaarvoice, die Benutzerauthentifizierung und Daten-speicherung in vertrauenswürdige Hände zu geben.

Von Null auf Xero

Als Anbieter einer Cloud-basierten Buchführungssoftware war **Xero** schon früh in der Entwicklungsphase auf rasantes Wachstum vorbereitet und setzte für die Absicherung der Anwendungsinfrastruktur sowie Automatisierung auf Okta. Da die Workflows auf der Okta-Plattform statt auf einem lokalen Computer oder Server gespeichert sind, werden API-Token automatisch abgesichert und aktualisiert.

Aufgedeckt: CIAM

Erfahren Sie in unserer informativen CIAM-Webinar-Reihe mehr darüber, warum das wichtig ist.

Jetzt ansehen

okta

Über Okta

Okta ist das weltweit führende Identity-Unternehmen. Als ein Eckpfeiler unabhängiger Identity-Anbieter ermöglichen wir es unseren Partnern und Kunden, jede Technologie sicher zu nutzen – überall, mit jedem Gerät und jeder Anwendung. Die weltweit anerkannten Marken vertrauen dem Schutz von Zugriff, Authentifizierung und Automatisierung auf Okta. Im Mittelpunkt unserer Okta Workforce Identity Cloud sowie der Okta Customer Identity Cloud stehen Flexibilität und Neutralität. Mit unseren individualisierbaren Lösungen und unseren über 7.000 vorkonfigurierten Integrationen können sich Führungskräfte und Entwickler ganz auf neue Innovationen und eine rasche Digitalisierung konzentrieren. Wir entwickeln eine Welt, in denen Ihre Identity ganz Ihnen gehört. Mehr unter okta.com/de.