

Präsentiert von:

okta

Customer Identity

für
dummies[®]
A Wiley Brand



Warum ein
starkes Customer Identity
Management den
Unterschied macht

Wie ein modernes Customer
Identity Management Ihr
Unternehmen voranbringt

Best Practices für Ihre
Customer Identity

Okta Sonderausgabe

Lawrence C. Miller
Jeremie Certes

Über Okta

Okta ist das weltweit führende Identity-Unternehmen. Wir helfen Menschen dabei, jede Technologie sicher zu nutzen – überall, mit jedem Device und jeder App. Unsere Workforce und Customer Identity Clouds ermöglichen sichere und flexible Zugriffe – mit starker Authentisierung und umfassender Automatisierung. So prägen wir die Art und Weise, wie Menschen sich in der digitalen Welt bewegen, und stellen starke Identitäten in den Mittelpunkt der Security und des Wachstums von Unternehmen.



Customer Identity

Okta Sonderausgabe

**von Lawrence C. Miller
und Jeremie Certes**

**für
dummies[®]**
A Wiley Brand

Customer Identity für Dummies®, Okta Sonderausgabe

Herausgegeben von
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2024 John Wiley & Sons, Inc., Hoboken, New Jersey

Kein Teil dieser Publikation darf ohne vorherige schriftliche Genehmigung des Verlags in irgendeiner Form oder mit irgendwelchen Mitteln – elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen, Scannen oder auf andere Weise – vervielfältigt, in einem Abfragesystem gespeichert oder übertragen werden, es sei denn, dies ist gemäß den Abschnitten 107 oder 108 des United States Copyright Act von 1976 zulässig. Anfragen an den Herausgeber zur Genehmigung einer Wiederverwendung richten Sie bitte an das Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, Fax (201) 748-6008, oder online unter <http://www.wiley.com/go/permissions>.

Warenzeichen: Wiley, For Dummies, das Dummies Man Logo, The Dummies Way, Dummies.com, Making Everything Easier und die zugehörige Aufmachung sind Marken oder eingetragene Marken von John Wiley & Sons, Inc. und/oder seinen Tochtergesellschaften in den Vereinigten Staaten und anderen Ländern und dürfen nicht ohne schriftliche Genehmigung verwendet werden. Alle anderen Marken sind Eigentum der jeweiligen Inhaber. John Wiley & Sons, Inc., steht in keiner Verbindung zu einem der in diesem Buch erwähnten Produkte oder Anbieter.

HAFTUNGSBESCHRÄNKUNG/GARANTIEAUSSCHLUSS: DER VERLAG UND DER AUTOR HABEN SICH BEI DER ERSTELLUNG DIESES BUCHES NACH BESTEM WISSEN UND GEWISSEN BEMÜHT, GEBEN JEDOCH KEINE ZUSICHERUNGEN ODER GARANTIE IN BEZUG AUF DIE RICHTIGKEIT ODER VOLLSTÄNDIGKEIT DES INHALTS DIESES BUCHES UND LEHNEN INSBESONDERE JEGLICHE STILLSCHWEIGENDE GARANTIE DER MARKTGÄNGIGKEIT ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK AB. KEINE GARANTIE KANN DURCH HANDELSVERTRETER, SCHRIFTLICHES VERKAUFSMATERIAL ODER AUF DIESES WERK BEZOGENE WERBEAUSSAGEN ERWEITERT WERDEN. DIE TATSACHE, DASS IN DIESEM WERK EIN UNTERNEHMEN, EINE WEBSITE ODER EIN PRODUKT ALS ZITAT UND/ODER POTENZIELLE QUELLE FÜR WEITERE INFORMATIONEN ANGEFÜHRT WIRD, HEISST NICHT, DASS DIE HERAUSGEBER ODER AUTOREN DIE INFORMATIONEN ODER SERVICES DES UNTERNEHMENS, DER WEBSITE ODER DES PRODUKTS ODER IHRE EMPFEHLUNGEN GUTHEISSEN. ES WIRD UNTER DER VORAUSSETZUNG VERKAUFT, DASS DER HERAUSGEBER KEINE PROFESSIONELLEN DIENSTLEISTUNGEN ERBRINGT. DIE HIERIN ENTHALTENEN RATSCHLÄGE UND STRATEGIEN SIND MÖGLICHERWEISE NICHT FÜR IHRE SITUATION GEEIGNET. WENN ERFORDERLICH, SOLLTEN SIE DIE DIENSTE EINES FACHMANNS IN ANSPRUCH NEHMEN DARÜBER HINAUS SOLLTEN SICH LESER IM KLAREN SEIN, DASS SICH DIE IN DIESEM WERK AUFGEFÜHRTEN WEBSITES, ZWISCHEN DEM ZEITPUNKT, AN DEM ES VERRASST WURDE, UND DEM ZEITPUNKT, AN DEM ES GELESEN WURDE, VERÄNDERT HABEN ODER NICHT MEHR EXISTIEREN KÖNNEN. WEDER DER HERAUSGEBER NOCH DER AUTOR HAFTEN FÜR GEWINNAUSFÄLLE ODER ANDERE KOMMERZIELLE SCHÄDEN, EINSCHLIESSLICH ABER NICHT BESCHRÄNKT AUF SPEZIELLE, ZUFÄLLIGE FOLGE- ODER ANDERE SCHÄDEN.

Für allgemeine Informationen über unsere anderen Produkte und Dienstleistungen oder darüber, wie Sie ein maßgeschneidertes *FÜR DUMMIES* Buch für Ihr Unternehmen oder Ihre Organisation erstellen können, wenden Sie sich bitte an unser Business Development Department in den Vereinigten Staaten unter 877-409-4177, schreiben Sie an info@dummies.biz oder besuchen Sie www.wiley.com/go/custompub. Für Informationen zur Lizenzierung der Marke *FÜR DUMMIES* für Ihre Produkte oder Dienstleistungen wenden Sie sich bitte an BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-22819-5 (pbk); ISBN 978-1-394-22820-1 (ebk)

Danksagung des Herausgebers

Zu den Personen, die bei der Veröffentlichung des Buches mitgewirkt haben, gehören:

Project Editor: Rachael Chilvers

Acquisitions Editor: Traci Martin

Editorial Manager: Rev Mengle

Business Development

Representative: Molly Daughy

Production Editor:

Saikarthick Kumarasamy

Einführung

Sicherlich haben Sie Customer Identity schon einmal im privaten Umfeld als Kunde eines anderen Unternehmens genutzt – ob Sie sich dessen bewusst waren oder nicht. Vielleicht haben Sie sich auch auf einer Website eingeloggt, um Konzerttickets zu kaufen. Oder Sie haben sich mit Ihrem Social Media Account bei einem neuen Online-Shop angemeldet. Möglicherweise haben Sie Ihr Smartphone für das Online-Banking genutzt und für den Login einen einmaligen Passcode per SMS erhalten. Dies sind nur einige alltägliche Beispiele, wie Kunden Customer Identity in Verbindung mit Ihren Lieblings-Apps, -Websites und -Portalen bereits heute nutzen.

In diesem Buch erfahren Sie, wie ein modernes Customer Identity Management Ihrem Unternehmen dabei hilft, Ihren Nutzern eine sichere und nahtlose Customer Experience zu bieten.

Über dieses Buch

Customer Identity für Dummies, Okta Sonderausgabe, umfasst acht Kapitel zu folgenden Themen:

- » Was ist Customer Identity? (Kapitel 1)
- » Warum Customer Identity wichtiger denn je ist (Kapitel 2)
- » Warum Sie nicht versuchen sollten, Ihre Customer Identity selbst zu entwickeln (Kapitel 3)
- » Worauf es bei einer modernen Customer-Identity-Lösung ankommt und wie sie Ihrem Unternehmen helfen kann (Kapitel 4)
- » Wie Sie die richtige Lösung für ein modernes Customer Identity Management für Ihr Unternehmen finden (Kapitel 5)
- » Wie Sie von einer Customer-Identity-Lösung, die auf die Anforderungen Ihres Unternehmens zugeschnitten ist, profitieren (Kapitel 6)
- » Die Zukunft von Customer Identity (Kapitel 7)

- » Zehn wichtige Punkte, die Sie bei einer Customer-Identity-Lösung beachten sollten, damit Ihr Unternehmen Erfolg hat (Kapitel 8)

Jedes Kapitel ist so geschrieben, dass es für sich alleinsteht. Wenn Sie also ein Thema sehen, das Ihr Interesse weckt, können Sie gerne zu diesem Kapitel springen. Sie können das Buch in der Reihenfolge lesen, die Ihnen gefällt (obwohl wir nicht empfehlen, es auf dem Kopf oder rückwärtszulesen).

Naive Annahmen

Über die Sinnhaftigkeit von Annahmen lässt sich streiten – nichtsdestotrotz gehen wir von ein paar Dingen aus!

Hauptsächlich gehen wir davon aus, dass Sie für die Entwicklung, Skalierung, Modernisierung, Integration, Architektur und/oder die Sicherung einer Kunden-/Partneranwendung, einer Website oder eines Portals verantwortlich zeichnen. Vielleicht sind Sie ein Anwendungsentwickler oder -architekt, ein Product Manager, ein Engineering Manager, ein Digital Manager, ein Chief Technology Officer (CTO), ein Chief Information Officer (CIO), ein Chief Product Officer (CPO), ein Chief Information Security Officer (CISO), ein Chief Marketing Officer (CMO) oder jemand, der sich auf Kundenidentitäten spezialisiert oder damit vertraut ist.

In diesem Buch verwendete Icons

In diesem Buch werden gelegentlich spezielle Symbole verwendet, um auf wichtige Informationen hinzuweisen. Hier sehen Sie, was Sie erwartet:



REMEMBER

Dieses Symbol weist auf wichtige Informationen, die Sie in ihrem nichtflüchtigen Speicher, sprich im Hinterkopf behalten sollten.



TECHNICAL
STUFF

Wenn Sie das vierte Level von NERD-vana erreichen wollen, dann spitzen Sie die Ohren. Dieses Symbol erklärt den Fachjargon hinter dem Fachjargon.



TIP

Tipps werden geschätzt, aber nie erwartet – und wir hoffen, dass es mit diesen nützlichen Nuggets genauso ist.



WARNING

Diese Icons weisen Sie auf die Dinge hin, vor denen Sie Ihre Mutter immer gewarnt hat (naja, wahrscheinlich nicht), aber sie geben auch praktische Ratschläge.

Über das Buch hinaus

In diesem kurzen Buch können wir nur so und so viel behandeln. Wenn Sie mehr erfahren möchten, besuchen Sie <https://okta.com/customer-identity/>.

IN DIESEM KAPITEL:

- » Definition von Customer Identity and Access Management
- » Verstehen, wie sehr sich ein schlechtes CIAM auf die Customer Experience auswirkt
- » Verbesserung der Customer Identity User Experience in mobile Apps, Websites und Portalen
- » Verstehen der wichtigsten Customer-Identity-Funktionen

Kapitel 1

Was ist Customer Identity?

Benutzernamen und Passwörter gehören heute zu unserem Alltag. Verbraucher verwalten mehrere Konten für Online-Shops, Bankkonten und Mobilgeräte-Apps. Das ist Customer Identity and Access Management (CIAM), und sicherlich kennen Sie einige der Unterschiede zwischen einem guten und einem schlechten Customer Identity Management aus vielen eigenen digitalen Erfahrungen. Ihre mobile Banking App gibt ihnen beispielsweise ein starkes Gefühl von Sicherheit und Benutzerfreundlichkeit, wenn Sie sie einfach mit einem Fingerabdruck authentifiziert. Andererseits haben Sie bestimmt schon mehr als einmal einen Online-Warenkorb beim Händler zurückgelassen, wenn dieser eine langwierige Registrierung verlangt. Die Registrierung kann mehr Zeit in Anspruch nehmen als die Suche nach den eigentlichen Produkten!

In diesem Kapitel befassen wir uns mit den Grundlagen von Customer Identity, einschließlich der Fragen, was Customer

Identity ist, wie sich ein schlechtes Customer Identity Management negativ auf das Kundenvertrauen auswirkt, warum Sie ein modernes Customer Identity Management für Ihre Kunden und Anwendungen benötigen und welche Schlüsselfunktionen jede Customer-Identity-Lösung haben muss.

Was ist Customer Identity?

Auch wenn Sie mit Customer Identities vielleicht nicht vertraut sind, sind sie Teil Ihres alltäglichen Lebens, wann immer Sie auf eine App auf Ihrem Smartphone zugreifen, sich bei einem neuen Online-Service oder Ihrer Lieblings-Website anmelden. Ein Customer Identity Management bietet eine digitale Identitäts-Ebene, die in Ihre Kunden-Apps, Websites und Portale eingebettet werden kann. Es hilft Ihnen, festzustellen, wer Ihre Kunden sind und worauf sie Zugriff haben, wenn sie mit ihren favorisierten Endgeräten von überall auf der Welt auf Ihre Services, einschließlich Ihrer Apps, Portale und Websites zugreifen. Customer Identity umfasst nicht nur die Sign-in/Login-Experience, sondern auch den Registrierungs- und Sign-up-Prozess entlang der gesamten Customer Journey.

Eine schlechte Customer-Identity-Experience treibt Ihre Kunden womöglich zu einem Wettbewerber, der eine reibungslosere und intuitivere Customer-Experience (CX) bietet. Was genau also macht ein schlechtes Customer Identity Management aus?

Gutes und schlechtes Customer Identity Management im Vergleich

Entscheidend für die Customer Experience, die Sie Ihren Kunden bieten, ist die Fähigkeit, deren Zugriff und Daten zu sichern. Ein sicherer Zugriff ist jedoch wertlos, wenn die CX so schwierig und frustrierend ist, dass Ihre Kunden beschließen, dass es sich schlichtweg nicht lohnt, sich mit dieser Hürde auseinanderzusetzen. Bestimmt haben Sie selbst schon einmal schlechte Erfahrungen mit Customer Identity gemacht, sei es bei privaten oder geschäftlichen Transaktionen. Ein paar typische Pain Points im Zusammenhang mit Customer Identity sind:

- » einen Account und ein Passwort erstellen zu müssen, nur um eine Webseite zu besuchen
- » verschiedene Accounts und Passwörter für verschiedene Apps, Websites und Portale desselben Unternehmens erstellen zu müssen
- » sich mit unterschiedlichen Accounts und Passwörtern anmelden zu müssen, um auf unterschiedliche Services desselben Unternehmens zugreifen zu können
- » ihre Lebensgeschichte (so scheint es häufig) in einem langwierigen Registrierungsprozess offenlegen zu müssen, nur um Ihren Account erstellen zu können
- » durch unterschiedliche Login Experiences und Funktionalitäten auf verschiedenen Endgeräten navigieren zu müssen
- » den Customer Service anrufen zu müssen, um ein vergessenes oder falsches Passwort zurückzusetzen
- » bei jedem Login zusätzlich zu Ihrem Passwort einen SMS-Passcode eingeben zu müssen – auch wenn Sie sich immer vom selben Ort und Endgerät aus anmelden

Im Vergleich dazu könnte ein gutes Customer Identity Management Folgendes bieten:

- » eine einfache Registrierung und Account-Erstellung, die nur ein Minimum an Informationen erfordern
- » Gesichtserkennung auf Ihrem Smart-Gerät („Mama, schau mal, ohne Passwort!“)
- » Verifizierung per SMS oder E-Mail bei sensiblen Finanztransaktionen, damit Sie sich sicherer fühlen
- » Zugriff auf alle Services eines Unternehmens über ein und denselben Account

Ein schlechtes Customer Identity Management führt zu unnötigen Reibungsverlusten während der gesamten Customer Journey, etwa durch langwierige und aufdringliche Registrierungsprozesse und manuelle Passwort-Resets, die eine Interaktion mit dem Call Center erfordern. Es zwingt Ihre Entwickler dazu, maßgeschneiderte Integrationen und Connections für neue Apps zu entwickeln, was Ihre Time-to-Market verlängert. Ein schlechtes Customer Identity Management nötigt Kunden dazu, separate Accounts

für verschiedene Apps, Websites und Portale innerhalb des Digital Estate eines Unternehmens anzulegen – was wiederum Administratoren dazu zwingt, diese Accounts in separaten Directories zu managen. Zudem bietet ein schlechtes Customer Identity Management nicht die Zuverlässigkeit und Skalierbarkeit, die agile Unternehmen in der digitalen Wirtschaft benötigen.



Lassen Sie nicht zu, dass Ihre Customer Identity Touch Points zu Pain Points für Ihre Kunden werden. Machen Sie Customer Identity zum Ausgangspunkt einer hochwertigen CX, die sich durch die gesamte Customer Journey zieht.

Kunden, Geschäftsmodelle und Anwendungstypen

Sie benötigen eine moderne Customer-Identity-Lösung, um eine nahtlose Omnichannel-CX für alle Ihre Produkte und Services zu gewährleisten, 24/7/365, wo auch immer Ihre Kunden mit Ihnen interagieren. Customer Identity ist für viele Apps, Websites und Portale der erste Schritt auf der Customer Journey und damit entscheidend für die Customer Service Experience als Ganzes.

Ihr Unternehmen verkauft entweder direkt an einzelne Verbraucher, an andere Unternehmen oder an beide. Eine Customer-Identity-Lösung muss diese verschiedenen Arten von Kunden und eine Vielzahl von Geschäftsmodellen unterstützen, darunter Business-to-Consumer (B2C), Business-to-Business (B2B) und Business-to-Business-to-Consumer (B2B2C).

Einige Ihrer Kunden haben möglicherweise auch einen bevorzugten Kanal, über den sie mit Ihrem Unternehmen Geschäfte machen möchten. So nutzen Privatkunden vielleicht am liebsten Ihre Mobile-App, während Geschäftspartner es vorziehen, von ihrem Arbeitsplatz aus mit Ihrem Unternehmen in Kontakt zu treten. Customer Identity muss Ihre verschiedenen Kundentypen und deren bevorzugte Kanäle und Endgeräte unterstützen.

Um B2B- und B2B2C-Geschäftsmodelle zu unterstützen, müssen Sie außerdem eine sichere Anbindung und Integration der Apps und Portale Ihrer Partner gewährleisten. Möglicherweise müssen Sie Identities für Ihre Partner auch mit Hilfe von Enterprise Directory Services wie Active Directory und Lightweight Directory Access Protocol (LDAP) zusammenführen.

Letztendlich sollten Ihre Kunden über alle Ihre Mobile-Apps, Websites und Portale auf Ihre Services zugreifen können. Die Customer-Experience muss über alle Anwendungstypen hinweg einheitlich sein und die gleichen Funktionalitäten bereitstellen.

Schlüsselfunktionen

Die drei Hauptfunktionen einer effektiven Customer-Identity-Lösung sind Authentifizierung, Autorisierung und User Management. In puncto Customer Identity sind Ihre User Ihre Kunden und Partner.

Eine korrekte *Authentisierung* stellt sicher, dass die Personen, die sich bei ihren Accounts anmelden, auch die sind, für die sie sich ausgeben. So wird verhindert, dass böswillige Akteure auf sensible Benutzerdaten (z. B. Zahlungsdaten, Adressen und Sozialversicherungsnummern) zugreifen oder betrügerische Transaktionen durchführen (z. B. Geld von einem Bankkonto überweisen).

Eine wirksame *Autorisierung* hilft Unternehmen zu bestätigen, dass ein User die richtige Zugriffsstufe für eine Anwendung und/oder Ressourcen hat.

Ein übersichtliches *User-Management* ermöglicht es Administratoren, Zugriffsberechtigungen der Benutzer zu aktualisieren und Security Policies zu implementieren, um eine nahtlose und sichere Experience zu ermöglichen und das Vertrauen jedes einzelnen Kunden zu stärken.

- » Eine erstklassige Customer Experience bieten
- » Vertrauen als Grundstein von Kundenbeziehungen
- » Digitale Transformation ermöglichen und ordern

Kapitel 2

Warum Customer Identity wichtig ist (jetzt mehr denn je)

Kunden erwarten und verlangen heute eine moderne, nahtlose, personalisierte Customer Experience (CX) an jedem Touch Point Unternehmen, die keine solche Experience bieten können, werden weder in der Lage sein, neue Kunden zu gewinnen, noch bestehende Kunden zu binden.

Vertrauen ist außerdem nicht verhandelbar. Unternehmen, denen es nicht gelingt, die Sicherheit und den Schutz der persönlichen Daten ihrer Kunden zu gewährleisten, werden Kunden verlieren – auch solche, die zwar nicht direkt von einem Datenleck betroffen sind, aber aufgrund dessen das Vertrauen in das Unternehmen verloren haben.

Schließlich ist die digitale Transformation nicht länger nur ein „Kann“ – sie ist zum „Muss“ geworden. Jedes Unternehmen, unabhängig von der Branche, muss zum Technologieunternehmen werden, um in der modernen digitalen Wirtschaft zu überleben und Erfolg zu haben.

Dieses Kapitel zeigt, wie Customer Experience, Sicherheit und Datenschutz sowie die digitale Transformation eine moderne Customer-Identity-Lösung in Ihrem Unternehmen nicht nur sinnvoll, sondern unerlässlich machen – jetzt mehr denn je.

Die Nachfrage nach moderner Customer Experience befriedigen

Die moderne CX ist hochwertig, personalisiert und deckt alle Kommunikationskanäle ab. Sie bietet Ihren Kunden einen reibungslosen 24/7/365-Zugriff auf Produkte, Services, Informationen und andere Ressourcen auf ihrem bevorzugten Endgerät – egal ob es sich um ein Smart Device, einen Computer, ein Tablet oder ein Smartphone handelt.

Vor nicht allzu langer Zeit kauften die Menschen fast ausschließlich im Ladengeschäft ein und sahen sich Filme im Kino oder im Fernsehen an einem bestimmten Tag und zu einer bestimmten Uhrzeit an. Als die Menschen begannen, von ihren heimischen Computern aus mit Unternehmen zu interagieren, wurde es immer wichtiger, eine benutzerfreundliche Website zu bieten. Heute nutzen die Menschen ihre Smartphones, um Lebensmittel zu bestellen, die an ihre Haustür geliefert werden, während sie bei der Arbeit sind, und sie können ihre Lieblingssendungen jederzeit, überall und auf jedem Endgerät ansehen. Unternehmen wie Amazon und Netflix setzen den Standard für eine nahtlose Customer Experience über alle Kanäle hinweg, und Verbraucher erwarten dasselbe von jedem Unternehmen, mit dem sie Geschäfte machen – auch von Ihrem. Daher ist es für Unternehmen heute wichtiger denn je, ihren Kunden solche modernen Access Experiences zu bieten.



WARNING

PwC (The Future of Customer Experience Report, 2018) zufolge, kehren 32 Prozent der Kunden ihrer Lieblingsmarke bereits nach der ersten schlechten Erfahrung den Rücken, während 59 Prozent sich nach zwei schlechten Erfahrungen abwenden. Wie können Sie also davon ausgehen, dass Ihre Kunden eine langsame, umständliche und zeitintensive Login Experience tolerieren werden?

Unternehmen brauchen eine moderne Customer-Identity-Lösung, die ihnen hilft, eine erstklassige Customer Experience zu bieten:

- » **Durchgängige Online-Experiences über alle Endgeräte**
hinweg Kunden haben keine Lust, sich für verschiedene Services desselben Unternehmens mehrfach zu registrieren oder einzuloggen. Stattdessen wünschen sie sich eine konsistente und reibungslose Erfahrung, unabhängig davon, ob sie Ihre Website auf ihrem Computer oder ihrem mobilen Endgerät besuchen oder die verschiedenen Mobile-Apps in Ihrem Digital Estate nutzen. Dazu gehört ein nahtloser, sicherer und Brand-spezifischer Login auf jedem Endgerät, überall auf der Welt, 24/7/365.
- » **Personalisierte Customer Journeys:** Das Erfassen unmittelbarer, verbindlicher Präferenzinformationen – einschließlich des Consents – über alle Kanäle hinweg hilft Ihnen, eine 360-Grad-Sicht auf Ihre Kunden aufzubauen. Sie können dann Customer Identities und Profile an einem Ort konsolidieren und die Customer Journey auf der Grundlage individueller Präferenzen anpassen. Je mehr die Kunden das Gefühl haben, dass Sie sie verstehen, desto wahrscheinlicher ist es, dass sie mit Ihnen Geschäfte machen und ihre positiven Erfahrungen mit anderen teilen.
- » **Neue und modern Experiences:** Die Technologie entwickelt sich in rasantem Tempo weiter und prägt die Erwartungen und Trends der Kunden. Vor zehn Jahren nutzten Smartphone-Besitzer ihr Gerät zum Telefonieren und Checken von persönlichen E-Mails. Heute können Ihre Kunden ein Produkt über die auf ihrem Smartphone installierte App Ihres Unternehmens bestellen, während sie mit dem Bus oder Zug zur Arbeit fahren – und sie erwarten, dass es über Nacht geliefert wird. Eine moderne Customer-Identity-Lösung kann Ihnen dabei helfen, Ihren Kunden mit Innovationen wie passwortloser Authentisierung (z. B. Gesichts- und Fingerabdruckererkennung) eine nahtlose Erfahrung über verschiedene Endgeräte hinweg zu bieten.



Sowohl Workforce-Identity- als auch Customer-Identity-Lösungen sind wichtige Technologien im Tech-Stack eines Unternehmens. Ihre Mitarbeiter werden Ihr Unternehmen wahrscheinlich nicht wegen einer schlechten Login Experience verlassen. Ihre Kunden hingegen werden, ohne lange nachzudenken, zu Ihren Wettbewerbern wechseln, wenn Sie es nicht schaffen, über alle Kommunikationskanäle hinweg eine erstklassige End-to-End CX inklusive nahtloser, personalisierter Login Experience zu bieten.

Kundenvertrauen aufbauen

Das Vertrauen der Kunden aufzubauen und zu bewahren ist für den Erfolg eines jeden Unternehmens entscheidend, aber die persönlichen Daten und Kontoinformationen, die den Unternehmen anvertraut werden, sind ständig bedroht. Viel zu oft werden sie kompromittiert. Der Schutz von Kundenkonten und -informationen ist daher das A und O. Wenn Ihre Kunden Ihnen nicht vertrauen, werden sie schnell zu den Kunden ihrer Wettbewerber.



WARNING

Wenn Kunden schlechte Erfahrungen mit Ihrem Unternehmen gemacht oder das Vertrauen in Ihr Unternehmen verloren haben, behalten sie das nicht für sich. Dafür können Sie sich bei den sozialen Medien bedanken!

Moderne Cyber-Threats und Cyber-Angriffe sind raffinierter, zerstörerischer, häufiger und weiter verbreitet als je zuvor. Die Corona-Pandemie hat daran nichts geändert: Im ersten Halbjahr 2020 wurden fast 16 Milliarden Datensätze kompromittiert – ein Anstieg von 273 Prozent im Vergleich zum ersten Halbjahr 2019, so Security Boulevard (<https://securityboulevard.com>).

Dass ein Datenleck für Verbraucher finanziellen und persönlichen Schaden bedeutet, ist unstrittig. Es kann Jahre dauern, bis sich eine Person von einem Finanz- und/oder Identitätsdiebstahl erholt – und viele erholen sich womöglich nie.

Für Unternehmen kann der finanzielle Schaden leicht Dutzende oder Hunderte Millionen Dollar betragen. Im Jahr 2018 meldete Marriott International, dass Angreifer Daten von mehr als 380 Millionen Gästen gestohlen hatten. Der Breach kostete Marriott allein im ersten Quartal nach Bekanntwerden des Verstoßes mehr als 44 Millionen US-Dollar, und das Unternehmen wurde inzwischen vom britischen Information Commissioner's Office (ICO) zu einer Geldstrafe von 25 Millionen US-Dollar verurteilt. Doch die Kosten durch die Schädigung des Markenrufs und den Verlust des Kundenvertrauens sind unermesslich. Vom Vertrauensverlust ihrer Kunden als Folge kompromittierter persönlicher Daten und Accounts erholen sich viele Unternehmen nie.

Unternehmen benötigen eine moderne Customer-Identity-Lösung, die dabei hilft, Kundenvertrauen aufzubauen und zu erhalten, um:

- » **Kundenaccounts zu sichern:** Cyber-Angriffe werden immer raffinierter und zerstörerischer. Passwörter reichen nicht aus, um die Accounts Ihrer Kunden zu schützen – und mit Passwörtern hat sowieso niemand gerne zu tun. Sichern Sie den Customer Identity Life Cycle für alle Ihre Apps, indem Sie die Kunden bei der Registrierung, Authentifizierung und während der In-App-Aktivität mit Innovationen wie Multi-Faktor-Authentifizierung (MFA) und passwortloser Authentifizierung schützen.
- » **Datenschutz und Einwilligung zu managen:** Kunden verlangen Sicherheit und Datenschutz für ihre persönlichen Daten. Das Grundrecht auf Datenschutz ist inzwischen in vielen neuen Gesetzen verankert, unter anderem in der Datenschutz-Grundverordnung (DSGVO) und dem California Consumer Privacy Act (CCPA). Ihre CIAM-Lösung muss eine nahtlose und intuitive CX ermöglichen, die Ihre Kunden in die Lage versetzt, selbst zu bestimmen, welche persönlichen Daten sie Ihrem Unternehmen zur Nutzung, Weitergabe und Speicherung überlassen wollen. Wenn Ihre Identity-Plattform die neuesten Vorgaben nicht unterstützen kann, bringen Sie Ihr Unternehmen in rechtliche Schwierigkeiten.
- » **Gesetzliche Vorgaben erfüllen:** DSGVO und CCPA sind nur zwei Beispiele für Dutzende von strengen Sicherheits- und Datenschutzvorschriften, die in den letzten Jahren von Regierungen in aller Welt erlassen wurden. Dieser Trend wird sich in absehbarer Zukunft unweigerlich verschärfen. So war der CCPA beispielsweise noch nicht einmal ein ganzes Jahr in Kraft, bevor im November 2020 der California Privacy Rights Act (CPRA) verabschiedet wurde. Unternehmen, die die geltenden Vorschriften nicht einhalten, riskieren finanzielle Verluste aufgrund von nicht bestandenen Audits und/oder sind gezwungen, ihren Betrieb einzustellen.

Beschleunigung der digitalen Transformation

Heutzutage muss jedes Unternehmen zum Technologieunternehmen werden, um zu überleben und Erfolg zu haben. Jede Branche ist von der digitalen Transformation betroffen, und dieser Trend nimmt immer mehr Fahrt auf. So sind zum Beispiel Videotheken (und teilweise sogar Kinos) mit dem Aufkommen von Streaming-Diensten verschwunden, und Taxi-Unternehmen haben Mühe, sich gegen Ridesharing-Dienste zu behaupten. Viele Unternehmen sehen sich jedoch mit erheblichen technischen Altlasten konfrontiert, wenn sie versuchen, von schwerfälligen Legacy-Systemen wegzukommen. Die digitale Transformation zwingt Unternehmen, ihre technische Infrastruktur zu modernisieren, und kann den Einstieg in die API Economy (Application Programming Interface) ermöglichen.



Technische Altlasten sind die impliziten Kosten für Nacharbeiten, die entstehen, weil man sich zu einem früheren Zeitpunkt für eine einfachere Lösung entschieden hat, anstatt die richtige zu implementieren.

Unternehmen benötigen eine moderne Customer-Identity-Lösung, die die digitale Transformation vorantreibt und beschleunigt, auch mit Blick auf:

- » **den Wechsel in die Cloud:** Für die meisten Unternehmen ist die Cloud ein integraler Bestandteil ihrer Strategien zur digitalen Transformation. Veraltete Infrastrukturen schränken die Flexibilität eines Unternehmens ein und behindern seine Fähigkeit, eine zeitgemäße Customer Experience zu bieten. Es kann jedoch viele Jahre dauern, bis ein Unternehmen in die Cloud wechselt. Eine durchgängige Identitäts-Ebene für moderne Web- und Mobile-Apps sowie für Legacy-On-Premises-Apps vereinfacht das Management der hybriden Cloud-Umgebungen, die Public-Cloud-, Private-Cloud- und On-Premises-Ressourcen umfassen. Zu den Vorteilen der Cloud gehören:
 - *Verbesserung der Anwendungsentwicklung und -bereitstellung bei gleichzeitiger Kostensenkung:* Unternehmen können Cloud-Services und -Ressourcen



schnell bereitstellen und nach Bedarf skalieren. So lassen sich ältere Identity-Infrastrukturen außer Betrieb nehmen und hohe Wartungskosten vermeiden.

- *Nutzung von Microservices-Architekturen und APIs*
Heutzutage erstellen Softwareentwickler Anwendungen, die Microservices und APIs nutzen. Eine solche Architektur erfordert einen ganzheitlichen und zentralisierten Identity-Ansatz, um einen sicheren Zugriff für Ihre Kunden und Partner zu gewährleisten. Mit einer modernen Customer-Identity-Lösung aus der Cloud können Ihre Entwickler Authentifizierungs-, Autorisierungs- und User-Management-Funktionen nahtlos in die von ihnen entwickelten Anwendungen einbetten, sodass sie sich auf Ihr Kerngeschäft konzentrieren können.

Microservices sind kleine, containerisierte *Services*, die unabhängig voneinander eingesetzt werden können und lose gekoppelt sind, um die einzelnen Komponenten einer Anwendung bereitzustellen. Eine API (*Application Programming Interface*) ermöglicht es verschiedenen Anwendungen, über eine Softwareverbindung miteinander zu kommunizieren.

- » **Einstieg in die API-Ökonomie:** APIs sind nicht mehr nur eine Entwicklungstechnik, sondern haben sich zu einem eigenen, dynamischen Geschäftsmodell entwickelt, da ein Unternehmen durch die Monetarisierung des Zugriffs auf seine proprietären APIs neue Einnahmequellen erschließen kann. Einige gängige Beispiele sind das Überlagern einer Karte in einer Ridesharing-App oder der Secure Checkout über einen Social Media Account in einer Food-Delivery-App. Eine moderne Customer-Identity-Lösung kann den Zugriff auf APIs kontrollieren und sichern, sodass Unternehmen ihr API-getriebenes Geschäft ausbauen und skalieren können.

- » Aufbau einer hochwertigen und sicheren Customer Experience
- » Konzentration Ihrer begrenzten Entwickler-Ressourcen auf Ihr Kerngeschäft
- » Sicherstellung der Zuverlässigkeit bei der Skalierung, Integration mit Ihrem Tech-Stack und Verkürzung der Time-to-Market
- » Betrachtung der Gesamtkosten einer Build-versus-Buy-Entscheidung

Kapitel 3

Der Aufbau einer starken Customer Identity

Kapitel 2 zeigt, warum eine moderne Customer-Identity-Lösung für Ihr Unternehmen von entscheidender Bedeutung ist: um eine erstklassige Customer Experience (CX) zu schaffen, das Vertrauen der Kunden sicherzustellen und die digitale Transformation zu beschleunigen. An dieser Stelle denkt sich der Heimwerker in Ihnen vielleicht: „Das bekomme ich auch selbst hin.“ Aber glauben Sie uns: Freunde lassen Freunde nicht ihre eigene Customer-Identity-Lösung entwickeln. In diesem Kapitel erklären wir, warum.

Ein heikler Balanceakt: Customer Experience versus Security und Compliance

Bei der Entwicklung einer Customer-Identity-Lösung müssen Sie zwei wichtige Anforderungen sorgfältig abwägen, die sich manchmal diametral gegenüberstehen: eine erstklassige Customer Experience zu bieten und gleichzeitig Security und Compliance zu gewährleisten.

Denken Sie darüber nach, was für Sie eine erstklassige Customer Experience ausmacht – schließlich sind Sie in vielen Ihrer täglichen persönlichen Interaktionen selbst der Kunde. Was macht Sie zu einem zufriedenen Online-Kunden? Vielleicht gehört Folgendes zu Ihrer Idealvorstellung von Customer Experience:

- » **Ein reibungsloser Registrierungsprozess:** Der Onboarding-Prozess sollte einfach und schnell sein, wenn Sie zum ersten Mal eine Website besuchen oder eine App nutzen. Zum Beispiel könnten Sie bei Ihrem ersten Besuch und bei späteren Besuchen gebeten werden, ein paar relevante Informationen anzugeben, anstatt Ihre Lebensgeschichte in dem Moment zu erzählen, in dem Sie durch die virtuelle Tür eintreten. Das bezeichnet man als *Progressive Profiling*.
- » **Ein intuitiver und nahtloser Login-Prozess:** Der Login-Prozess sollte verschiedene Authentifizierungsmethoden zur Wahl stellen, die auf Ihre individuellen Präferenzen zugeschnitten sind. Menschen haben im Allgemeinen nicht gerne mit Passwörtern zu tun, daher sind alle Methoden ideal, bei denen sie kein weiteres Passwort erstellen und sich daran erinnern müssen, z. B. die Verwendung eines bestehenden Social Media Accounts oder die Gesichtserkennung auf einem Smartphone.
- » **Durchgängiger Single Sign-On für multiple Apps desselben Unternehmens:** Ein Kundenportal sollte alle Ihre Apps nahtlos in eine Single-Login-Experience integrieren.
- » **Eine unverwechselbare Customer Experience:** Sie sollten in der Lage sein, die Marken, die Sie kennen und denen Sie vertrauen, sofort zu erkennen, selbst bei verschiedenen Apps oder Services desselben Unternehmens (z. B. Amazon

Prime Video und Whole Foods – auf beide wird über dieselbe Amazon Website zugegriffen).

- » **Omnichannel in jeder Sprache:** Eine einheitliche Login Experience von jedem Endgerät aus, zu jeder Zeit, überall auf der Welt – in Ihrer bevorzugten Sprache.
- » **Personalisierte Empfehlungen:** Sie sollten relevante Empfehlungen für Produkte und Services erhalten, die auf Ihren Profilingen und Ihrer Kaufhistorie basieren.

Der erste Schritt zu einer hochwertigen Customer Experience in Ihrer eigenen Customer-Identity-Lösung beginnt bei der Definition der Anforderungen Ihrer Kunden – und davon gibt es einige. Um ein altes Sprichwort umzukehren: Des einen Schatz ist des anderen Müll. Was einige Ihrer Kunden begeistert, das stößt andere vor den Kopf.

AUCH B2B BRAUCHT CUSTOMER IDENTITY

Obwohl sich dieses Kapitel vor allem um die Customer Experiences im Business-to-Consumer-Bereich (B2C) dreht, müssen auch Business-to-Business-Anwendungen (B2B) eine nahtlose und intuitive Customer Experience bieten. In vielen B2B-Partnerschaften ist ein Unternehmen der Lieferant und das andere der Kunde. Daher sind viele Anforderungen an Customer Identity für B2B dieselben wie für B2C. Sie können jedoch einige zusätzliche B2B-Anforderungen hinzufügen, z. B. die Möglichkeit, sich mit Ihren Corporate Credentials bei einer Partner-Website oder -App anzumelden, anstatt einen weiteren Account erstellen zu müssen.

Security- und Compliance-Anforderungen unter einen Hut zu bringen und gleichzeitig eine reibungslose Customer Service Experience zu bieten, das ist eine Herausforderung für sich selbst.

Falls Sie ernsthaft über ein eigenes Customer Identity Management nachdenken, sollten Sie sich der folgenden Risiken bewusst sein:

- » **Sie müssen es erst aufbauen — und das ist leichter gesagt als getan.** Sie müssen die Security-Methoden entwickeln, die Ihre Kunden wollen und brauchen. Zu diesen Methoden gehören die Multi-Faktor-Authentifizierung (MFA), die adaptive MFA (AMFA), bei der zusätzliche Faktoren auf Basis einer Risikobewertung abgefragt werden, die passwortlose Authentifizierung, Einmal-Passwörter und andere.
- » **Cyber-Kriminellen einen Schritt voraus zu sein, ist ein ständiger Kampf.** Selbst engagierte Security-Teams tun sich oft schwer, im Wettlauf um den Schutz vor neuen Schwachstellen und Exploits mitzuhalten. Raffinierte Cyber-Threats und -Angriffe machen sich immer häufiger kompromittierte Account-Zugangsdaten zunutze. Und die Hacker werden kommen. Lassen Sie nicht zu, dass Ihre selbstentwickelte Customer-Identity-Lösung die User als das sprichwörtlich „schwächste Glied“ in der Security-Kette Ihres Unternehmens verdrängt.
- » **Die Anforderungen Ihrer Kunden werden sich ständig ändern.** Heute wollen sie keine Passwörter. Morgen werden sie vielleicht beschließen, dass Passwörter, die per Textnachricht an ihr Smartphone geschickt werden, zu viel Aufwand sind. Es ist schwer, mit den sich ändernden Vorstellungen Ihrer Kunden Schritt zu halten. Wenn Customer Identity nicht zu Ihrem Kerngeschäft gehört, ist es nur ein weiteres Thema, das Sie ständig anpassen müssen, um Ihre Kunden zufrieden zu stellen.
- » **Die Compliance-Landschaft entwickelt sich extrem dynamisch.** Oder genauer: Sie verändert sich ständig und wird immer komplexer. Sicherheits- und Datenschutzvorschriften wie der U.S. Health Insurance Portability and Accountability Act (HIPAA), die Datenschutz-Grundverordnung (DSGVO) und der California Consumer Privacy Act (CCPA) sind nur einige der verwirrenden und oft widersprüchlichen Anforderungen, die ständig neu erlassen, aktualisiert, ersetzt und überarbeitet werden. Eine nicht konforme DIY-Lösung für Customer Identity könnte zu hohen Geldstrafen und anderen Sanktionen für Ihr Unternehmen führen.

Wenn Sie sich für die Aufbau einer eigenen Customer-Identity-Lösung entscheiden, müssen Sie zusätzliche Kompromisse in Betracht ziehen:

- » **Security-Innovationen stehen nicht still, und auch Sie werden nicht mehr zur Ruhe kommen.** Alle innovativen Funktionen, die Sie entwickeln wollen – wie adaptive Multifaktor-Authentifizierung (AMFA), passwortlose Authentifizierung, biometrische Identifizierung und Einmal-Passwörter – müssen zukunftssicher und auf dem neuesten Stand sein. Allerdings müssen diese Funktionen für Ihre Kunden auch reibungslos funktionieren. Dies ist der erste Kompromiss, denn jeder zusätzliche Authentifizierungsfaktor bedeutet auch Mehraufwand.
- » **Die internen Mitarbeiter eines Unternehmens werden unterschiedliche Meinungen und Prioritäten vertreten.** Das Marketing will eine nahtlose und erstklassige User Experience. Der Vertrieb will es „gestern“. Die Security will vor allem einen extrem sicheren Zugriff. Product and Engineering möchte sich auf das Kernprodukt konzentrieren und nicht auf die Entwicklung der Authentifizierung. Finance möchte die Option, die den größten Return on Investment (ROI) bietet – und das bei minimaler Investition. Und Ihr CEO wird alles haben wollen!



REMEMBER

Auf der einen Seite müssen Unternehmen eine erstklassige Customer Service Experience bieten, die einen reibungslosen und intuitiven Registrierungs- und Login-Prozess für einen schnellen und einfachen Zugriff auf Ihre Anwendungen umfasst. Andererseits verlangen die Kunden, dass Unternehmen ihre persönlichen Daten sicher und privat halten. Wenn Ihre Kunden Ihrem Unternehmen nicht vertrauen, werden sie zu Ihren Wettbewerbern wechseln. Bevor Sie sich dazu entschließen, ein Customer Identity Management selbst zu entwickeln, sollten Sie alle Herausforderungen bedenken, die sich ergeben, wenn Sie das richtige Gleichgewicht zwischen einer nahtlosen CX auf der einen Seite und robuster Security und Compliance auf der anderen Seite finden wollen. Sprechen Sie dann mit Ihren Entwicklern (siehe nächster Abschnitt).

Qualifizierte Entwickler gewinnen und binden

Okay, Sie haben fähige Entwickler. Wahrscheinlich würden Sie sogar sagen, Sie haben einige der besten Entwickler der Welt. Deshalb bezahlen Sie ihnen auch so viel, oder? Aber haben Sie auch genügend qualifizierte Entwickler? Angesichts des weltweiten Mangels an qualifizierten Entwicklern haben die meisten Unternehmen Schwierigkeiten, Spitzenkräfte anzuwerben und zu halten.

Welche anderen IT-Fachkräfte sind weltweit Mangelware? Richtig, Security Engineers. Wenn Sie einen Entwickler haben, der in der Lage ist, sichere Customer-Identity-Funktionen zu entwickeln, die eine erstklassige CX, robuste Security und Datenschutz sowie lückenlose Compliance mit gesetzlichen Vorschriften bieten, dann handelt es sich in der Tat um ein seltenes Einhorn. Wenn Identity and Access Management (IAM) aber nicht Ihr Kerngeschäft ist, warum lassen Sie dann nicht Prinzessin Twilight Sparkle, Rainbow Dash und Spike (für die Uneingeweihten: das sind My Little Pony Einhörner) eine Customer-Identity-Lösung entwickeln? Sollten sich Ihre Entwickler nicht zu 100 Prozent auf Ihr Kerngeschäft und die Apps und Websites konzentrieren, die Ihren Umsatz generieren?



CIAM selbst zu entwickeln, erfordert eine Menge eigenentwickelten Code. Laut den *Top Ten des Open Web Application Security Project (OWASP)* (<https://owasp.org>), werden 93 Prozent aller Anwendungsschwachstellen in eigenentwickeltem Code entdeckt. Diese Schwachstellen setzen Ihr Unternehmen und Ihre Kunden erheblichen Gefahren aus und verursachen signifikante technische Altlasten und Opportunitätskosten. Darüber hinaus verbringen Entwickler laut Stripe.com (<https://stripe.com/files/reports/the-developer-coefficient.pdf>) 42 Prozent ihrer Zeit mit dem Debuggen und der Maintenance von fehlerhaftem Legacy-Code, anstatt neue Apps zu entwickeln. Es ist viel schwieriger, Spitzenkräfte zu gewinnen und zu halten, wenn Ihre Entwickler ständig mit „Bug Duty“ beschäftigt sind.

Zusätzliche Überlegungen

Abgesehen davon, dass Sie eine nahtlose Customer Experience mit zuverlässiger Security und Compliance in Einklang bringen und teure Entwickler-Ressourcen von der Konzentration auf Ihr Kerngeschäft abziehen müssen, sollten Sie einige weitere Herausforderungen bedenken, bevor Sie sich für die Entwicklung einer eigenen Customer-Identity-Lösung entscheiden:

- » **Zuverlässigkeit im großen Maßstab:** Kunden erwarten einen nahtlosen und sicheren Zugriff auf Ihre Mobile-Apps, Kunden-Websites und Partnerportale mit ihren bevorzugten Endgeräten von überall aus, 24/7/365 – egal, ob am Black Friday, nach der Lohnsteuerrückzahlung, beim Kartenvorverkauf für ein angesagtes Konzert, ein großes Sportereignis oder einen Blockbuster oder während anderer Lastspitzen. Ausfallzeiten führen zu Umsatzeinbußen und schaden Ihrer Marke. Die Entwicklung, der Aufbau und die Wartung der erforderlichen Infrastruktur für einen zuverlässigen und skalierbaren Service sind komplex und teuer. Wollen Sie wirklich Ihre eigene Infrastruktur managen und sich mit Systemausfällen, Maintenance Downtime und Upgrades herumschlagen?
- » **Integration in den bestehenden Tech-Stack:** Ihre Customer-Identity-Lösung muss sicher mit den anderen Tools und Anwendungen in Ihrem Tech-Stack verbunden werden – wie z. B. Security-, Datenschutz-, Marketing- und Service-Management-Software – um dessen Effizienz zu steigern und Ihren ROI zu maximieren.
- » **Verkürzung der Time-to-Market:** Unternehmen müssen neue, nahtlose und sichere CX schnell auf den Markt bringen, um die immer anspruchsvolleren Kundenerwartungen zu erfüllen und die immer komplexeren Security- und Compliance-Risiken zu bewältigen. Wie Sie inzwischen festgestellt haben, ist der Aufbau von maßgeschneiderten Customer-Identity-Funktionen zur Erfüllung solcher Anforderungen zu jedem Zeitpunkt schwierig und kostspielig. Was aber, wenn Ihre Kunden keine Textnachrichten mehr für MFA verwenden möchten oder Sie die gesetzlichen Anforderungen in einem neuen Land erfüllen müssen, in das Ihr Unternehmen

expandiert? Der Aufbau einer Customer-Identity-Lösung ist keine einmalige Angelegenheit. Es handelt sich um einen ständigen Zyklus, der kontinuierliche Innovation und Produktentwicklung erfordert, um mit den sich schnell verändernden Kundenanforderungen und Security Threats Schritt zu halten.

Eine klassische Build-versus-Buy-Entscheidung

Es ist äußerst schwierig, eine Customer-Identity-Lösung zu entwickeln, die auf die spezifischen Bedürfnisse Ihrer Kunden zugeschnitten ist, und es ist auch sehr kostspielig, sie in Zukunft zu pflegen. Es erfordert ein klares Verständnis der Anforderungen Ihrer Kunden für eine nahtlose und dennoch sichere Customer Experience; ein Team von schwer zu findenden, gut ausgebildeten und hoch bezahlten Entwicklern, um sicheren Code zu entwickeln und zu pflegen; eine sehr komplexe, teure Infrastruktur, um einen skalierbaren 24/7/365-Zugriff zu gewährleisten und um Integrationen mit Ihrem gesamten Tech-Stack zu erstellen und gleichzeitig die Time-to-Market für neue Funktionen in Apps Ihres Kerngeschäfts zu verkürzen.

Bevor Sie sich für den Aufbau einer Customer-Identity-Lösung entscheiden, sollten Sie die Gesamtkosten einschließlich der technischen Altlasten, des Risikos von Security Breaches und der Opportunitätskosten bedenken.



Der Aufbau einer eigenen Customer-Identity-Lösung ist schwierig – und unnötig. Gehen Sie keine Kompromisse ein! In Kapitel 4 erfahren Sie, wie eine moderne Customer-Identity-Lösung Ihr Unternehmen unterstützen kann, und in Kapitel 5 verraten wir Ihnen, worauf Sie bei der Auswahl einer modernen Customer-Identity-Lösung achten sollten.

- » Definition einer modernen Customer-Identity-Lösung
- » Erweiterung der Customer-Identity-Funktionen durch einen Plattformansatz
- » Bereitstellung von sicheren, zuverlässigen und skalierbaren Services mit modernem Customer Identity Management
- » Exemplarische Betrachtung von Use Cases und Customer Success Stories

Kapitel 4

Wie ein modernes Customer Identity Management Ihr Unternehmen voranbringt

Wie in Kapitel 3 dargelegt, ist es äußerst schwierig und kostspielig, selbst eine Customer-Identity-Lösung zu entwickeln. Es macht für Unternehmen einfach keinen Sinn, knappe Ressourcen für die App-Entwicklung von ihrem Kerngeschäft abzuziehen, um Customer Identity im Alleingang zu entwickeln. In diesem Kapitel erläutern wir, warum Sie sich für

eine Partnerschaft mit einem Experten entscheiden sollten, der eine moderne Customer-Identity-Lösung anbietet, mit der Sie Ihre Probleme angehen und eine nahtlose und sichere Customer Experience (CX) bieten können.

Was versteht man unter einer modernen Customer-Identity-Lösung?

Eine moderne Customer-Identity-Lösung bietet eine digitale Identitätsebene, die schnell und nahtlos in Ihre Kunden-Apps, -Websites und -Portale integriert werden kann. Diese hilft Unternehmen, die Anforderungen ihrer Kunden zu erfüllen und bietet eine reibungslose User Experience, schnelle Time-to-Market, zentralisiertes Management aller Identities und Access Policies sowie robuste Security.

Hochwertige User-Experiences

Um eine reibungslose User Experience bieten zu können, müssen Sie Ihre Kunden kennen und verstehen. Mit einer modernen Customer-Identity-Lösung erhalten Sie eine 360-Grad-Sicht auf Ihre Kunden über alle Ihre Apps und Produkte hinweg, unabhängig davon, welches Endgerät sie verwenden – wann und wo auch immer sie mit Ihrer Marke interagieren. Anschließend können Sie diese Informationen nutzen, um eine maßgeschneiderte User Experience anzubieten und gleichzeitig Zugriffsprobleme zu verringern, indem Sie:

- » Einheitlichkeit und Konsistenz über alle Ihre verschiedenen Apps und Websites hinweg bieten, anstatt Ihre User aufzufordern, sich bei jeder einzelnen davon anzumelden
- » weniger (oder gar keine) Passwörter über alle Ihre Kanäle und User-Endgeräte hinweg abfragen
- » die Menge an Informationen, die Sie von Ihren potenziellen Kunden während des Registrierungsprozesses verlangen, minimieren
- » es Ihren Geschäftspartnern ermöglichen, sich mit ihren Corporate Credentials anzumelden, anstatt sie zu bitten, einen weiteren Benutzernamen und ein weiteres Passwort zu erstellen

- » personalisierte und Brand-spezifische Anpassungen verwenden, um das Vertrauen Ihrer Kunden zu stärken



Progressive Profiling ermöglicht es Ihnen, während der gesamten Customer Journey schrittweise Benutzerinformationen zu sammeln, anstatt von Ihren Kunden zu verlangen, einen langwierigen Registrierungsprozess zu durchlaufen, bevor sie auf Ihre Anwendung zugreifen können. Beim Social Login können Ihre User zustimmen, einige grundlegende Informationen aus ihren Social Media Accounts zu teilen, anstatt sie manuell einzugeben, um schneller auf Ihre Services zugreifen zu können.

Schnelle Markteinführung

Eine moderne Customer-Identity-Lösung hilft Ihnen, Ihre Time-to-Market mit einer breiten Palette von Tools zu verkürzen, um Identity and Access Management schnell und effektiv in Ihre Kunden-Apps, -Websites und -Portale einzubetten. Diese Tools reichen von Out-of-the-Box-Lösungen, die einfach zu konfigurieren und schnell bereitzustellen sind (für Unternehmen mit einfachen Identity-Anforderungen, die Low-Code Deployments bevorzugen) bis hin zu einem umfangreichen Angebot an Application Programming Interfaces (APIs) und Software Development Kits (SDKs) für Unternehmen mit komplexeren Anforderungen und einem hohen Individualisierungsgrad. Dank dieser Tools können Ihre Development-Teams Customer Identity schnell in Ihre Customer Experience einbetten, anstatt es von Grund auf neu zu entwickeln, und so Ihre Time-to-Market verkürzen.

Zentralisiertes Management

Mit der zunehmenden Anzahl Ihrer Customer Experiences über alle Ihre Kanäle hinweg, wird die Zentralisierung des Identity and Access Management immer wichtiger. Eine Single Source of Truth über alle Identities hinweg für alle User, Gruppen und Endgeräte kann mit Ihrem Unternehmen wachsen und den Verwaltungsaufwand mit einem Single-Pane-of-Glass Interface reduzieren, das es Ihnen ermöglicht, all die verschiedenen Access Policies, Group Memberships und Security Policies zu managen. So lassen sich Konsistenz und Compliance gewährleisten, Konfigurationsfehler reduzieren und Sicherheitslücken verhindern.



WARNING

Identity and Access Management für einzelne Apps ist ineffizient und riskant. Es führt unweigerlich zu Doppelarbeiten und macht Sie anfällig für Sicherheitslücken, da Sie nicht sicher sein können, dass Access- und Security-Policies über Ihre gesamte IT-Landschaft hinweg einheitlich durchgesetzt werden.

Hochskalierbare Security

Eine moderne Customer-Identity-Lösung setzt auf einer sicheren Cloud-basierten Plattform auf, die vom Service Provider gemanagt wird. Sie müssen sich also nicht um die Absicherung und die Aktualisierung der zugrundeliegenden Plattform oder Infrastrukturkomponenten kümmern – dafür ist allein der Service Provider zuständig.

Eine moderne Customer-Identity-Lösung bietet leistungsstarke Security-Funktionen wie adaptive Multi-Faktor-Authentifizierung für eine Vielzahl von Faktoren, die auch aktuelle Threat Intelligence und Contextual-Response-Optionen berücksichtigen. Umfassende Analysetools und Dashboards bieten Echtzeiteinblicke in potenzielle Threats und Angriffe und ermöglichen es den Teams, Probleme schnell zu adressieren, zu untersuchen und zu beheben.



REMEMBER

Eine moderne Customer-Identity-Lösung ermöglicht es Ihnen, die neuesten Security-Innovationen wie risikobasierte Policies und passwortlose Authentifizierung zu nutzen, ohne sie selbst entwickeln zu müssen. Ihre Development-Teams können sich auf Ihr Kerngeschäft konzentrieren, anstatt sich mit den neuesten Security Threats zu beschäftigen.

Plattformansatz

Eine moderne Customer-Identity-Lösung verfolgt einen plattformbasierten Ansatz für das Identity and Access Management, um jeden Identity Use Case für jeden User und jede Technologie umfassend abdecken zu können.

Ein Plattformansatz ermöglicht es Ihrem Unternehmen, IAM-Synergien (Identity and Access Management) für all Ihre verschiedenen User zu finden, von den Mitarbeitern über die Partner bis hin zu den Kunden, unabhängig von deren Standorten, Apps oder Endgeräten. Beispielsweise benötigen ein B2B-Reseller-Partner und ein interner Sales-Mitarbeiter höchstwahrscheinlich Zugriff auf ähnliche Sales-Tools und -Apps, Produktkataloge und

so weiter. Wenn ein Unternehmen eine Customer-Identity-Lösung selbst entwickelt, kann es sein, dass diese von verschiedenen Produktteams entwickelt wird – ein Team konzentriert sich auf den internen Use Case, das andere auf den Partner-Use-Case. Jedes Team wird eine andere User Experience schaffen und unterschiedliche Security- und Access-Policies festlegen, wodurch wertvolle Zeit und andere Ressourcen verschwendet werden. Das Ergebnis ist eine inkonsistente User Experience, während gleichzeitig potenziell neue Sicherheitsrisiken entstehen. Eine moderne Customer-Identity-Lösung, die auf einer einheitlichen Plattform aufsetzt, bietet einen konsistenten IAM-Ansatz für jeden User und nutzt Synergien optimal aus.



TIP

Ein unabhängiger und neutraler Plattformansatz erweitert außerdem das Customer-Identity-Feature-Set, da er Ihre digitalen Assets mit jeder beliebigen Technologie integriert. Sie können Ihre On-Prem- und Cloud-Anwendungen nahtlos miteinander verbinden, um Ihren Kunden einen einheitlichen Zugriff auf Ihre Legacy- und Ihre aktuellen Produkte zu bieten, während Sie Data Points aus Ihren bevorzugten Tools mit Hilfe vorgefertigter Integrationen in Best-of-Breed-Technologie nutzen. So können Sie beispielsweise die während des Registrierungsprozesses gesammelten Kontaktdaten der User in ein Marketing-Tool einspeisen, das die Kundenansprache automatisiert.

Aufbau einer sicheren, zuverlässigen und skalierbaren Infrastruktur

Für Unternehmen, die versuchen, ihre eigene Customer-Identity-Lösung zu entwickeln, ist es eine ständige und teure Herausforderung, die Infrastruktur zu designen, zu entwickeln und zu warten, um das für ein erfolgreiches Unternehmen notwendige Maß an Sicherheit, Zuverlässigkeit und Skalierbarkeit zu erreichen.

Wenn sie nicht sicher ist, werden Sie Kunden verlieren, weil sie Ihrem Brand nicht vertrauen. Wenn sie nicht zuverlässig ist, können die User nicht einmal auf Ihre Services zugreifen, weil Ihre Website nicht verfügbar ist. Wenn die Lösung nicht skalierbar ist, werden viele Kunden es leid sein, während einer Lastspitze auf den Login zu warten, und sich stattdessen umorientieren.



Eine moderne Customer-Identity-Lösung setzt auf einer sicheren, zuverlässigen und skalierbaren nativen Cloud-Infrastruktur auf und wird als Service bereitgestellt.

Auf diese Weise müssen Sie sich nicht um die Einstellung und Bezahlung interner Infrastrukturrexperten, die Budgetierung Ihrer Cloud-Infrastrukturkosten oder die Skalierung Ihrer Infrastruktur zur Bewältigung von Lastspitzen kümmern. Sie müssen sich auch nicht mit System- oder Software-Patches und -Upgrades befassen, die Maintenance Downtime erfordern und den Service für Ihre Kunden unterbrechen.

Um die Zuverlässigkeit zu gewährleisten, muss eine moderne Customer-Identity-Lösung auf jeder Ebene des Infrastruktur-Stacks hochgradig redundant sein, für den Fall, dass beispielsweise ein Server oder ein Network Link ausfällt. Diese redundante Infrastruktur muss über automatisierte Workflows verfügen, die den Traffic bei Bedarf über mehrere Standorte hinweg umleiten können, um eine maximale Uptime zu gewährleisten, ohne dass menschliches Eingreifen erforderlich ist.

Um die Skalierbarkeit zu gewährleisten, benötigen Sie On-Demand-Kapazitäten, die je nach Bedarf automatisch hoch- oder heruntergefahren werden können, damit Sie kein Geld für ungenutzte Kapazitäten verschwenden oder aufgrund unzureichender Kapazitäten Geld (sprich Umsatz) verlieren.

Um die Sicherheit zu gewährleisten, müssen Sie über die neuesten Threats und Schwachstellen in Ihrer gesamten Infrastruktur auf dem Laufenden bleiben.



Ein dedizierter externer Customer-Identity-Partner kann all diese Anforderungen für Ihr Unternehmen abdecken, damit Sie sich auf Ihr Kerngeschäft konzentrieren können.

Neue Use Cases

Eine moderne Customer-Identity-Lösung hilft Unternehmen dabei, ein breites Spektrum an Use Cases abzudecken, um unterschiedlichen Anforderungen gerecht zu werden. In den folgenden Abschnitten werden wir einige der häufigsten Use Cases untersuchen und einige Success Stories von Okta-Kunden kennenlernen.

Schutz vor Kontoübernahmen

Die Übernahme von Konten ist eine immer häufiger vorkommende Methode von identitätsbasierten Angriffen, bei der sich ein böswilliger Akteur unbefugten Zugriff auf den Account eines Users verschafft, um sich zu bereichern oder Daten zu stehlen. Diese Angriffe können entweder von Angreifern lanciert oder mit Hilfe von Bots automatisiert werden. Um die Übernahme von Konten zu verhindern, benötigen Sie eine Identity-Plattform, die Security mit einer nahtlosen User Experience kombiniert.

Entwicklung hoch skalierbarer Anwendungen

Unternehmen entwickeln Apps und Websites, um möglichst viele Kunden zu gewinnen. Das bedeutet, dass Ihre Customer-Identity-Lösung zuverlässig und skalierbar sein muss, insbesondere dann, wenn der Customer Traffic oder die Nachfrage stark ansteigt – sei es bei Tickets für ein Konzert oder Sportereignis oder bei einem Flash Sale während der Feiertage.

Anwendungsübergreifende Vereinheitlichung von Customer Identities

Ihre Kunden haben nicht unbedingt Spaß daran, sich für neue Accounts zu registrieren und unterschiedliche Credentials für verschiedene Apps und Websites zu managen – vor allem, wenn sie zum selben Unternehmen oder Brand gehören. Die Vereinheitlichung von Customer Identities über alle Ihre digitalen Assets hinweg ist entscheidend für eine reibungslose Customer Experience.

ARDUINO

Arduino trägt zur Demokratisierung der IoT-Revolution (Internet of Things) bei und öffnet Lehrbeauftragten, Studenten und Bastlern aller Art den Zugang zu Open-Source Software und Hardware. Da Arduino seinen Sitz in Europa hat und so der DSGVO unterliegt, haben Datenschutz und Sicherheit höchsten Stellenwert.

Auth0s Plattform unterstützte Arduino bei der schnellen Integration einer Zwei-Faktor-Authentifikation – und stellte so die Weichen für eine zuverlässige Einhaltung gesetzlicher Auflagen und der Umsetzung hoher Sicherheitsstandards. Sie beschleunigte zudem die Skalierung im Back-End und ermöglichte Arduinos Entwicklerteams so, schneller neue Produkte bereitzustellen.

Für die App Arduino IoT Cloud, bei der Entwickler sowohl IoT- als auch Android-Logins benötigten, konnte das Unternehmen beide Logins in zweieinhalb Tagen implementieren – und verkürzte die Zeit bis zum Release so um mehrere Wochen.

SIEMENS

Siemens verfügt über zahlreiche verschiedene Prozesse über eine Vielzahl von Abteilungen hinweg und suchte deshalb dringend einen Ansatz zur Standardisierung und Sicherung der Login-Prozesse. Vor zwei Jahren zog das Unternehmen Auth0 hinzu, um eine einheitliche Login Experience für seine Kunden und Partner zu schaffen.

Gemeinsam entwickelten sie Siemens ID: ein Single Login Service, der sich schnell in den Anwendungs-Stack eines jeden operativen Betriebs integrieren lässt. Alle Kunden und Partner haben mit Siemens ID Zugriff auf Hunderte von Siemens Apps und Services weltweit. Über Siemens ID lassen sich nicht nur die Nutzerdaten und die Login-Seite zentral speichern – die Lösung erlaubt einzelnen Abteilungen, die Anwendung ihren individuellen Anforderungen entsprechend zu integrieren.

Integration von Enterprise Identities

Mit einer modernen Customer-Identity-Lösung müssen B2B-Kunden keine separaten Identities und Credentials mehr erstellen, um sich mit Partneranwendungen, Websites und Portalen zu verbinden. Stattdessen integriert modernes Customer Identity Management sämtliche Enterprise Identities, damit B2B-Kunden ihre bestehenden Corporate Identities und Credentials über alle digitalen Assets ihrer Partner hinweg verwenden können.

Sicherer Zugriff auf APIs

Für Unternehmen, die in die API Economy einsteigen (siehe Kapitel 2), ist der Schutz der API-Zugriffe von entscheidender Bedeutung, um sicherzustellen, dass böswillige Akteure keine Schwachstellen ausnutzen oder unbefugten Zugriff auf verbundene Anwendungen erhalten können.

BAZAARVOICE

Nach mehreren Jahren raschen Wachstums stand Bazaarvoice über eine Vielzahl voneinander isolierter Produkte mit den Kunden in Kontakt. Die IT-Abteilung sah sich nun vor der Herausforderung, sämtliche Benutzeridentitäten über die Produktpalette hinweg zu konsolidieren.

Während Bazaarvoice die Nutzer der Kunden in die neuverknüpften Apps integrierte, prüfte das IT-Team Oktas Föderationsfunktionen für eingehende Verbindungen, um den Kunden den Login über ihren eigenen Identity Provider zu ermöglichen. Die Föderation vereinfachte das User Management für die Kunden und erlaubte Bazaarvoice, die Verantwortung für die User-Authentifizierung und Datenspeicherung der über 590 Millionen Verbraucher, die jeden Monat mit den Anwendungen des Unternehmens interagieren abzugeben.

XERO

Als Xero sich in der Frühphase der Entwicklung auf einen starken Wachstumsschub vorbereite, suchte die IT-Abteilung nach einem Partner für das Identity Management, um die Anwendungsinfrastruktur zu schützen und eine Automatisierung zu ermöglichen. Okta Workflows war dafür die perfekte Lösung.

Das Scripting eines automatisierten Prozesses erfordert oft die Integration eines Keys, Tokens oder Passworts zum Abruf einer Drittanbieter-API. Dieses Token wird jedoch oftmals in einer Datei auf dem Unternehmensserver gespeichert – ohne eine ausreichende Security sicherzustellen. Workflows wird über die Okta Plattform und nicht On-Premises über einen Computer oder Server ausgeführt und schützt und aktualisiert so automatisiert die API-Token.

- » Die wichtigsten Funktionalitäten einer Customer-Identity-Lösung
- » Unterstützung aller Identity Use Cases durch eine unabhängige und neutral Plattform
- » Sicherstellung eines zuverlässigen, sicheren und skalierbaren Services
- » Partnerschaft mit einem Branchenführer

Kapitel 5

Worauf es bei einer modernen Customer-Identity-Lösung ankommt

Wenn Sie wissen, wie eine moderne Customer-Identity-Lösung Ihrem Unternehmen hilft, eine sichere und reibungslose Customer Experience (CX) zu bieten (siehe Kapitel 4), können Sie beginnen, Ihre Optionen abzuwägen. In diesem Kapitel erfahren Sie, auf welche Eigenschaften und Funktionen Sie bei einer modernen Customer-Identity-Lösung achten sollten.

Auf der Suche nach dem besten Produkt

Eine moderne Customer-Identity-Lösung sollte Out-of-the-Box-Funktionen bieten, die einfach zu konfigurieren und schnell zu implementieren sind, und entwicklerfreundliche Tools wie Application Programming Interfaces (APIs), Software Development Kits (SDKs) und Hooks unterstützen, um die Customer-Identity-Lösung weiter anzupassen und auszubauen.

Einige wichtige Out-of-the-Box-Features, auf die Sie achten sollten:

» Authentifizierung, Autorisierung und User Management

— die Grundpfeiler einer jeden Customer-Identity-Lösung (siehe Kapitel 1). Über die Grundfunktionen hinaus sollten Sie ein Auge auf die folgenden erweiterten Funktionen haben:

- *Authentifizierung:* Unterstützung von Social Login und OpenID Connect (OIDC), Single Sign-On für Anwendungen von Drittanbietern, passwortlose Authentifizierung, risikobasierte Authentifizierung, ein vorgefertigtes Sign-in Widget und individuelles Branding auf Anwendungsebene.
- *Autorisierung:* API Access Management auf der Grundlage von OAuth 2.0, Integration mit API Gateways und Role Based Access Control für Anwendungen.
- *User Management:* Ein hoch skalierbarer, Cloud-basierter Benutzerspeicher, um alle User, Gruppen und Endgeräte zu managen; Mapping von Benutzerprofilen; und Unterstützung für den von Ihnen bevorzugten Ansatz zur User-Migration (Bulk Import, Just-in-Time, bestehendes Directory).

» **Vordefinierte und anpassbare User Flows**, um schneller hochwertige User- und Customer-Support-Funktionen wie Self-Service-Registrierung, Passwortrücksetzung und Wiederherstellung von Account/Benutzername bereitstellen zu können.

» **Ein intuitives, zentralisiertes Admin-Interface** und anpassbare Management Dashboards, die Security- und Admin-Teams die Möglichkeit bieten, Security Policies zentral und konsistent zu verwalten.

- » **Multi-Faktor-Authentifizierung (MFA) und adaptive MFA** mit Unterstützung für verschiedene Faktoren und Methoden, von einfachen E-Mails und Textnachrichten bis hin zu fortschrittlicheren Methoden wie Biometrie (z. B. TouchID und FaceID). Adaptive MFA erweitert die risikobasierte Authentifizierung um eine intelligente Komponente, die Kontextinformationen wie Standort und Endgerät nutzt und MFA nur dann verlangt, wenn es notwendig ist.
- » **Automatisiertes Provisioning mit Lifecycle Management** einschließlich automatisierter Workflows, die sich daran orientieren, wo sich Ihre Kunden in ihrem Lifecycle befinden, sodass Sie User für nachgelagerte Apps und Systeme innerhalb Ihres Tech-Stack provisionieren und entprovisionieren können (z. B. automatischer CRM-Zugriff für B2B-Vertriebspartner, sobald die Partnerschaft beginnt).
- » **B2B-Integration** zur Anbindung von Partneranwendungen und -portalen und zur Zusammenführung von Identities über Enterprise Directories wie Active Directory und Lightweight Directory Access Protocol (LDAP) hinweg, um den Login für Corporate User zu vereinfachen (ohne neue Credentials erstellen zu müssen) und damit Unternehmen, die CIAM verwenden, stets über ihre Corporate User auf dem Laufenden sind.
- » **Integration mit bestehenden On-Premises-Apps**, um Ihren Kunden einen einheitlichen Zugriff auf all Ihre Produkte zu bieten und Ihre digitale Transformation zu beschleunigen.

Unternehmen, die über diese Out-of-the-Box-Funktionen hinausgehen möchten oder müssen, sollten sich nach einer Lösung umsehen, die ein umfangreiches Set an APIs, SDKs und Hooks für die von Ihren Development-Teams verwendeten Sprachen bietet. Diese entwicklerfreundlichen Tools werden Ihnen dabei helfen:

- » **Customer Identity schnell und effizient in Ihre Apps einzubinden**, ohne alles von Grund auf neu entwickeln zu müssen.
- » **Customer Identity genau an Ihre Bedürfnisse anzupassen**, sodass Sie eine maßgeschneiderte CX bieten und sich einen Wettbewerbsvorteil verschaffen können.

» **Best-of-Breed-Lösungen aus Ihrem Tech-Stack zu nutzen**, um Ihr Customer-Identity-Portfolio zu erweitern und Ihre Kunden noch mehr zu begeistern (Details dazu finden Sie im nächsten Abschnitt).

Die Wahl der richtigen Plattform

Halten Sie Ausschau nach einer Customer-Identity-Lösung, die auf einer offenen, unabhängigen und neutralen Plattform basiert. Darauf können Sie sicher aufbauen, jeden Identity Use Case für jeden User, der mit Ihrem Unternehmen interagiert, lösen und jede von Ihnen gewünschte Technologie nutzen.

Sie sollten sich für eine Customer-Identity-Lösung entscheiden, die ein breites Spektrum von Usern abdeckt, darunter Verbraucher, Partner und sogar Ihre Mitarbeiter. Ein Plattformansatz liefert dafür ein zukunftssicheres Fundament, da sich Ihre Anforderungen im Laufe der Zeit wahrscheinlich weiterentwickeln werden. Zum Beispiel könnte Ihr Unternehmen derzeit nach einer Customer-Identity-Lösung suchen, die eine sofort einsatzbereite B2B-Integration für ein Partnerportal bietet. In einem Jahr expandiert Ihr Unternehmen vielleicht in den Consumer-Bereich und benötigt eine adaptive, passwortlose Authentifizierung für eine neue B2C-Mobile-App. Das bedeutet jedoch nicht, dass Sie zwei verschiedene Customer-Identity-Lösungen benötigen. Beide Use Cases können von ein und derselben plattformbasierten Customer-Identity-Lösung abgedeckt werden, was Kosteneinsparungen und betriebliche Effizienz durch einfacheres Management und einfachere Workflows ermöglicht. Darüber hinaus möchte Ihr Unternehmen vielleicht auch die IAM-Funktionen für seine Mitarbeiter optimieren. All diese Benutzertypen können nahtlos über dieselbe Customer-Identity-Plattform gemanagt werden.

Ein Plattformansatz ermöglicht es Ihnen außerdem, Best-of-Breed-Lösungen für Ihre verschiedenen Use Cases und Tech-Stack-Anforderungen zu nutzen, On-Premises oder in der Cloud, sodass Sie das beste Tool auf dem Markt verwenden können, anstatt sich mit einem Bundle aus mittelmäßigen Lösungen zufriedener zu geben. Daher sollten Sie nach einer Customer-Identity-Lösung suchen, die eine breite Palette an vorgefertigten Integrationen mit den wichtigsten Anwendungen und Services in Ihrem Tech-Stack bietet, wie z. B.:

- » API Gateways
- » Bot Detection
- » Customer Data Integrators
- » Identity Proofing
- » Infrastructure as a Service
- » Privileged Access Management
- » Security Analytics

Sie sollten auch nach einer Lösung suchen, die No-Code-Konnektoren bietet, damit Ihre Teams automatisierte Workflows für Ihre Schlüsseltechnologien erstellen können, ohne eigenen Code schreiben zu müssen.

Schließlich muss Ihre Customer-Identity-Lösung auch eine einfache Integration über APIs, SDKs und Hooks bieten. Inline-Hooks ermöglichen es Entwicklern, laufende Okta-Prozesse mit benutzerdefinierter Logik und Daten aus Nicht-Okta-Quellen zu modifizieren. Inline-Hooks ermöglichen es Entwicklern, laufende Customer-Identity-Prozesse mit benutzerdefinierter Logik und Daten aus einer externen Quelle zu modifizieren. Abbildung 5-1 zeigt ein Beispiel für einen Inline Hook und einen Event Hook.

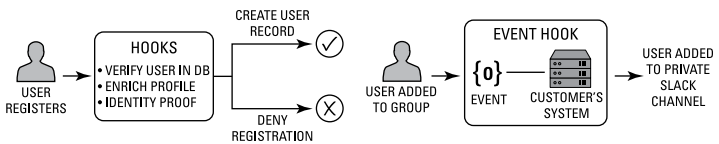


ABBILDUNG 5- 1: Ein Beispiel für einen Inline Hook (links) und einen Event Hook (rechts).

Sichere und vertrauenswürdige Infrastrukturen

Ein entscheidender Vorteil einer modernen Customer-Identity-Lösung besteht darin, dass sie als Service bereitgestellt wird. Sie müssen die Infrastruktur, die Ihnen die Skalierbarkeit, Zuverlässigkeit und Sicherheit bietet, die Ihr Unternehmen in der heutigen schnelllebigen und sich rasch verändernden digitalen

Wirtschaft benötigt, nicht mehr selbst betreiben und warten. Halten Sie nach einer modernen Customer-Identity-Lösung Ausschau, die Folgendes leistet:

- » **Skalierbarkeit:** Ihre Lösung muss den Anforderungen Ihres Unternehmens jetzt und in Zukunft gerecht werden. Schließlich wollen Sie nicht, dass das System in die Knie geht oder zum Flaschenhals für Traffic wird, wenn Ihre Apps viral gehen und die Kundennachfrage in die Höhe schießt. Und Sie wollen Ihren Customer-Identity-Anbieter nicht wechseln müssen, weil er mit dem Wachstum Ihres Unternehmens nicht Schritt halten kann. Suchen Sie deshalb nach einer Customer-Identity-Lösung, die Hunderttausende von Authentifizierungen pro Minute abbilden kann, und nach einem Anbieter, der nachweislich kontinuierlich in seine Lösung investiert und sie innovativ weiterentwickelt.
- » **Zuverlässigkeit:** Suchen Sie nach einem Customer-Identity-Partner, der lückenlose Verfügbarkeit garantiert – und liefert. Ausfallzeiten bedeuten Umsatzeinbußen, Markenschäden und den potenziellen Verlust von Kunden an Wettbewerber aufgrund schlechter Customer Experiences und Bewertungen. Was nützt es, die besten Produkte zu haben, wenn Ihre Kunden nicht darauf zugreifen können?
- » **Security:** Suchen Sie nach einem Customer-Identity-Partner, der Sie vor Credential-Stuffing-Attacks schützt, bei denen User gestohlene oder geleakte Daten nutzen. Auf Anmeldedaten-basierte Angriffe nutzen schwache, verbreitete oder gestohlene Identity-Informationen und imitieren so einen legitimen User oder übernehmen die Kontrolle über einen legitimen Account. Credential-Stuffing-Attacks verwenden beispielsweise Usernamen und Passwörter, die bei einem Data Breach gestohlen, über eine Phishing-Kampagne erbeutet oder in einem Online-Forum verkauft wurden. Mithilfe automatisierter Tools testen Angreifer diese dann in anderen Online-Services. Brute-Force- und Password-Spray-Attacks setzen auf das systematische oder automatisierte Testen schwacher und gängiger Passwörter – oftmals in Verbindung mit einer Reihe bekannter Usernamen.



Ihre Customer-Identity-Lösung wirkt sich unmittelbar auf Ihre CX und Ihr Business aus. Ihre Kunden werden für Skalierbarkeits-, Zuverlässigkeits- und Sicherheitsprobleme nicht Ihren Customer-Identity-Anbieter, sondern Sie verantwortlich machen – und zu Ihren Wettbewerbern abwandern, wenn Sie ihren Anforderungen nicht gerecht werden. Sie müssen mit einem vertrauenswürdigen Partner zusammenarbeiten, der nachweislich eine moderne Customer-Identity-Lösung bereitstellt, die hoch skalierbar, zuverlässig und sicher ist.

Branchenführerschaft

Zu guter Letzt sollten Sie bei der Abwägung Ihrer Optionen für eine moderne Customer-Identity-Lösung Ihre Due Diligence erfüllen. Customer Identity Management ist ein kontinuierlicher Prozess, und Sie brauchen einen Partner, der sich langfristig für Ihren Erfolg einsetzt – keinen „One-and-Done“-Anbieter, der Ihnen sein Produkt verkauft und dann weiterzieht. Die Kundenerwartungen werden sich ständig weiterentwickeln, ebenso wie Security Threats, gesetzliche Vorschriften und technologische Innovationen. Entscheiden Sie sich für einen Partner, der seine Branchenführerschaft beispielsweise durch Folgendes unter Beweis stellt:

- » **Unabhängige Validierung durch Dritte** einschließlich Analystenberichte und Zertifizierungen wie:
 - Service Organization Control (SOC) 2 Typ I und Typ II
 - Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR) Level 2 Attestation
 - International Organization for Standardization (ISO) 27001:2013 and ISO 27018:2014
- » **Einhaltung gesetzlicher Vorschriften** wie der Datenschutz-Grundverordnung (DSGVO) und des Health Insurance Portability and Accountability Acts
- » **Nachgewiesene Kompetenz durch Kundenreferenzen und Success Stories**, die für Ihre Branche, Unternehmensgröße und Region relevant sind und die Sie direkt kontaktieren können, um Referenzen zu erhalten

» **Eine zukunftssichere Lösung mit einem** erwiesenen Track Record im Hinblick auf Innovation, Product Roadmaps, Thought Leadership und das Mitwirken an Developer Communities und Standardisierungsgremien

IN DIESEM KAPITEL

- » Der Weg zur Customer-Identity-Reife
- » Die Grundlagen
- » Automatisieren für Wachstum und Skalierung
- » Optimierung Ihrer Customer Experiences ohne Abstriche bei der Security
- » Als Branchenführer neue Maßstäbe setzen

Kapitel 6

Wie Ihr Customer Identity Management sein Potenzial entfaltet und Ihren Business-Anforderungen gerecht wird

Kapitel 5 erläutert, worauf Sie bei einer modernen Customer-Identity-Lösung achten sollten. Aber wo sollten Sie anfangen? Ihr Unternehmen ist einzigartig, und Sie möchten sicherstellen, dass Sie die Lösung wählen, die Ihren spezifischen Anforderungen entspricht. Dieses Kapitel zeigt Ihnen, wo und wie Sie Ihren Weg zur Customer-Identity-Reife beginnen können.

Der Weg zur Customer-Identity-Reife

Unabhängig davon, an welchem Punkt sich Ihr Unternehmen auf seiner Identity Journey befindet, gibt es eine Reihe von Herausforderungen, denen Sie sich bei jedem Schritt stellen müssen. Daher lässt sich der Weg zur Customer-Identity-Reife in vier Hauptstufen unterteilen: Grundstufe, Automatisiert, Intelligent und Durchgängig (siehe Abbildung 6-1).

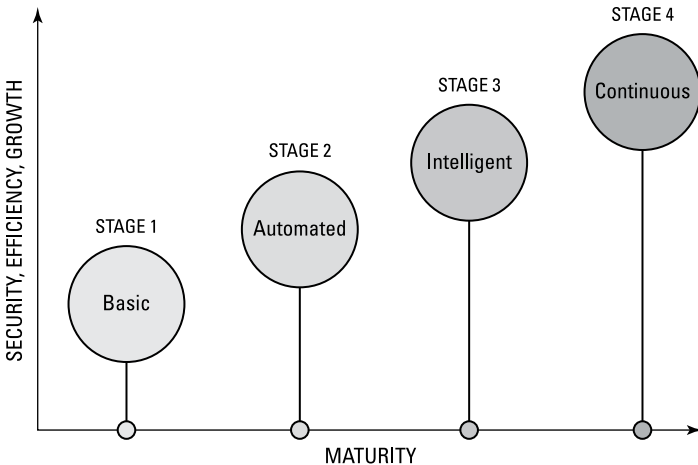


ABBILDUNG 6- 1: Wo steht Ihr Unternehmen auf der Customer-Identity-Reifekurve?

Wo auch immer Sie sich auf Ihrer Reise befinden: Die weiteren Schritte auf dem Weg zu einem durchgängigen Customer Identity and Access Management sind klar vorgezeichnet. In den folgenden Abschnitten werden die einzelnen Stufen und ihre Bedeutung für Ihr Unternehmen näher beleuchtet.

Grundstufe: Build versus Buy

Die erste Stufe ist die Grundstufe. Ihr Business steht noch ganz am Anfang und Sie versuchen gerade, die Eignung Ihres Produkts für den Markt zu dokumentieren. Ihr Unternehmen hat vielleicht eine großartige Idee für eine neue Kunden-App und möchte diese so

schnell wie möglich auf den Markt bringen. Ihre App befindet sich noch in einem frühen Stadium der Produktentwicklung und Sie müssen ihre Markttauglichkeit nachweisen. Das Hauptaugenmerk Ihres Teams liegt auf dem Design, der Entwicklung und der Validierung der App als Business Case, aber es ist ein kleines Team. Sie kommen also nicht um Kompromisse herum.

Einerseits müssen Sie:

- » schnell ein frühes marktfähiges Produkt vorlegen, für das grundlegende Identity Voraussetzung ist
- » ihr Produkt potenziellen Kunden präsentieren
- » beweisen, dass Sie relevante Probleme Ihrer Kunden lösen

Andererseits stehen Sie vor mehreren Herausforderungen:

- » Sie müssen Ihr Produkt ausliefern und es nach und nach verbessern, während Sie dazulernen
- » Fundamentale Sicherheitsprobleme könnten das gesamte Projekt zum Scheitern bringen
- » Sie haben nur begrenzte Entwicklerkapazitäten und wissen nicht, wie Identity in Ihr Design passt

Dies ist die erste Stufe auf dem Weg zur Customer-Identity-Reife: die Grundstufe, auf der Sie entscheiden müssen, ob Sie Ihre begrenzte Zeit und Ihre wertvollen Ressourcen für die Entwicklung Ihrer eigenen Customer-Identity-Lösung verwenden oder eine Partnerschaft mit einem Third-Party-Provider eingehen.

Wie in Kapitel 3 gezeigt, zieht die interne Entwicklung und das Management von Tools wertvolle Entwicklungszeit ab, die Ihr Team sonst für die Produkte Ihres Kerngeschäfts verwenden würde. Daher sollten Sie die Vorteile einer externen Lösung nutzen, um die benötigten Customer-Identity-Kernfunktionen (Authentifizierung, Autorisierung und User Management) schnell bereitzustellen. Damit schaffen Sie die richtige Grundlage, um Ihren Kunden eine sichere Access Experience zu bieten und gleichzeitig die Effizienz der Entwickler zu maximieren.



Laut einer von Stripe.com durchgeführten Umfrage verbringen Entwickler durchschnittlich 17,3 Stunden pro Woche mit dem Debuggen und Warten von Legacy- und fehlerhaftem Code. Eine moderne Customer-Identity-Lösung kann die Entwicklung

beschleunigen und den Aufwand für die spätere Wartung verringern, damit Sie sich auf Ihr Kerngeschäft konzentrieren können.

Der Meilenstein der grundlegenden Customer-Identity-Reife belegt, dass Sie wichtige Identity-Security-Funktionen in Ihre App integriert haben – und dass Sie sie erfolgreich auf den Markt gebracht haben. Nun ist es an der Zeit, über die Erweiterung Ihres Produktportfolios nachzudenken, um einen wachsenden Kundenstamm zu bedienen.

Automatisiert: Zentralisieren und Skalieren

Gratulation! Ihre Anwendung war ein Erfolg und Sie möchten nun weitere Produkte für Ihre Kunden entwickeln. Sie stellen Mitarbeiter ein, und Sie haben sogar einen CTO oder einen VP of Product oder Engineering, der Ihr Projekt leitet. Diese neue Wachstumsphase bringt jedoch eine Reihe neuer Herausforderungen mit sich. Ihr wachsender zahlender Kundenstamm verlangt zum Beispiel nach leistungsfähigeren oder Enterprise-Grade-Funktionen, für deren Entwicklung Sie möglicherweise nicht die Zeit oder die Erfahrung haben. Sie müssen Ihre eigenen Vorhaben also priorisieren, um effektiv zu skalieren und weiter zu wachsen.

Mit Blick auf Customer Identity aus könnten Sie die Inhouse-Entwicklung von Identity-Funktionen in Betracht ziehen, weil es für Ihre Kunden so wichtig ist, aber Sie sollten sich wirklich auf andere wichtige Ziele konzentrieren – wie die Entwicklung und erfolgreiche Einführung neuer Produkte, um Ihren Kundenstamm weiter auszubauen.

Sie befinden sich jetzt auf der Stufe „Automatisiert“, auf der Ihnen die richtige externe Customer-Identity-Lösung dabei helfen wird,

- » das Risiko und Management externer Customer Identities aus der Hand zu geben. Ihre User sollten sich bei bestehenden Identity-Providern anmelden können, und Sie sollten in der Lage sein, die Authentifizierung an bestehende Active Directories oder LDAP-Directories zu delegieren. So kann Ihr Unternehmen das User Management zentralisieren und mühelos skalieren.

- » moderne Authentifizierungsstandards wie OpenID Connect, OAuth und Security Assertion Markup Language (SAML) zu nutzen, um automatisch die neuesten Security und Identity Practices zu übernehmen, ohne ständig hinterherzulaufen.
- » verschiedene Compliance-Anforderungen wie die Datenschutz-Grundverordnung (DSGVO) und den California Consumer Privacy Act (CCPA) zu erfüllen.
- » Prozesse wie Provisionierung und Entprovisionierung mit Hilfe von Customer Lifecycle Management zu automatisieren.
- » die Sicherheit zu erhöhen, wenn Sie skalieren und zu einem größeren Ziel werden, indem unsichere oder kompromittierte Passwörter automatisch geflaggt werden.
- » Ihren Kunden moderne Möglichkeiten zu bieten, ihre Passwörter zurückzusetzen oder sich zu authentifizieren (Textnachrichten, Voice, E-Mail oder Einmalpasswörter) und diese Security Policies in einer zentralisierten Admin-Konsole zu managen.

Haben Sie die Stufe „Automatisiert“ in Ihrer Customer-Identity-Reife hinter sich gelassen, bedeutet das, dass Sie Ihre Produktreichweite erweitert und Ihre User-Management-, Compliance- und Security-Funktionen ausgebaut haben. Wenn Sie weiter skalieren, müssen Sie in robustere Security und neue Customer-Experience-Funktionen investieren.

Intelligent: Optimieren ohne Kompromisse

In diesem Stadium sind Unternehmen gut positioniert, um ihren Markt anzuführen. Um weiter zu wachsen, müssen sie ihr Produktportfolio optimieren, dürfen aber keine Kompromisse bei den Identity-Anforderungen einer komplexen Gruppe interner Stakeholder (z. B. Product, Engineering und Marketing) eingehen, die alle versuchen, eine nahtlose und sichere User Experience in großem Umfang zu bieten.

Eine moderne Customer-Identity-Lösung wird Ihnen diese Kompromisse ersparen und dabei helfen, Ihre Infrastruktur für die Nutzung von Application Programming Interfaces (APIs) und

Microservices zu optimieren, indem sie:

- » eine erstklassige Onboarding Experience mit einem höheren Maß an Sicherheit durch Identity-Proofing- und Account-Verification-Funktionen bietet
- » eine reibungslose User Experience ohne Kompromisse bei der Sicherheit gewährleistet, durch Lösungen wie adaptive Multi-Faktor-Authentifizierung (eine adaptive Intelligence-Ebene, die kontextbezogene Informationen und verhaltensbasierten Input nutzt, um das Risiko zu kalkulieren und bei Bedarf zusätzliche Authentifizierungsstufen zu implementieren), passwortlose Authentifizierung (z. B. E-Mail-Magic-Links und WebAuthn) und Progressive Profiling, das Benutzerprofilattribute im Laufe der Zeit erfasst
- » die neuesten Datenschutz- sowie Security- und Compliance-Anforderungen durch Konsolidierung des User-Lifecycle- und Data-Management in einem zentralen, konnektiven System erfüllt
- » das Ganze durch Erweiterung der Customer-Identity-Funktionen auf Ihren gesamten Tech-Stack optimiert – mit Hilfe von vorgefertigten Integrationen oder benutzerdefinierten Workflows und Nutzung von Best-of-Breed-Technologie (z. B. Bot Mitigation, Customer Relationship Management und Marketing-Analyse-Tools)

An diesem Punkt bietet Ihre Anwendung den Kunden einen starken, vielleicht sogar passwortlosen Schutz. Ihre Nutzung und Speicherung von Kundendaten ermöglicht personalisierte Verbesserungen und ist vollständig konform mit den Datenschutzbestimmungen. Dank branchenführender Integrationen ist Ihre Identity Security stringent und Sie können Risiken proaktiv erkennen und minimieren. Ihre Kunden nutzen Ihre Services mit Vertrauen und Leichtigkeit, und Sie sind gut positioniert, um erweiterte Funktionalitäten in Betracht zu ziehen.

Durchgängig: Vorangehen und neue Maßstäbe setzen

Das ist die letzte Stufe auf der Customer-Identity-Reifekurve, die von Branchenführern erreicht wird, die die Digitale Transformation abgeschlossen haben. Sie verfügen über ein engagiertes internes Customer-Identity-Team, das eine Omnichannel-Strategie fährt, die sowohl Sicherheit als auch User Experience optimiert. Was diese Marktführer von ihren Wettbewerbern unterscheidet, ist, dass sie Identity als eine kontinuierliche Reise verstehen und betrachten, die eine langfristige Strategie erfordert.

Um an der Spitze zu bleiben, müssen Sie kontinuierlich neue Maßstäbe setzen. In diesem Stadium bedeutet Customer Identity mehr als nur sicherzustellen, dass sich Kunden nahtlos und sicher einloggen können. Es sollte Ihnen helfen:

- » Ihre Kunden über alle Kanäle hinweg zu tracken (Web und Mobile sowie Ladengeschäft), um einen 360-Grad-Blick auf Ihre Kunden zu erhalten und sie mit personalisierten Erfahrungen über alle Kanäle hinweg begeistern zu können.
- » eine feingranulare und risikobasierte Autorisierung für ein Höchstmaß an Access Control über alle Daten zu implementieren, strenge Industriestandards wie Financial-Grade API (FAPI) zu erfüllen und Reibungsverluste für Kunden zu minimieren. Risiko-Alerts lassen sich für Kategorien wie Netzwerk, Standort, Endgerät und Transaktionstyp festlegen. Ein Risk Score kann dynamisch berechnet oder anhand bestimmter Bedingungen (wie Timing und User Events) ermittelt werden.
- » die Security-Orchestrierung und -Response mit Hilfe von flexiblen Workflows zu automatisieren und den Zeit- und Arbeitsaufwand für das Management von Identity und Security Policies mit Hilfe von künstlicher Intelligenz (KI) und Machine-Learning-Funktionen (ML) zu reduzieren.



Unabhängig davon, ob Sie zum ersten Mal ein Produkt entwickeln oder ein etablierter Marktführer sind, ist die Einbindung von Customer Identity in Ihre Product Roadmap entscheidend. Wenn Sie wissen, auf welcher Stufe der Customer-Identity-Reifekurve Sie sich befinden, kann Ihr Unternehmen Erfolge tracken und Schwerpunktbereiche identifizieren, die Ihnen einen Wettbewerbsvorteil verschaffen.

- » **Attraktivere Customer Experiences bieten, um Ihre Kunden zu begeistern**
- » **Bessere Security Outcomes für mehr Vertrauen in Ihren Brand**
- » **Einhaltung von Compliance-Vorgaben und Datenschutz**
- » **Unterstützung zunehmender komplexer Architekturen und Use Cases**

Kapitel 7

Die Zukunft von Customer Identity

In diesem Kapitel werfen wir einen Blick in die Zukunft, beleuchten vier wichtige Trends, die die Zukunft von Customer Identity prägen werden, und erläutern, wie diese Ihrem Unternehmen zum Erfolg verhelfen.

Kundenbindung erhöhen

Unternehmen mit Kundenkontakt müssen die Art und Weise, wie User mit ihrem Brand interagieren, ständig weiterentwickeln und verbessern, um die Kundenbindung zu erhöhen und den Customer Lifetime Value zu maximieren. Es ist daher nur logisch, dass einer der größten Trends, der die Zukunft von Customer Identity prägt, die Erhöhung der Kundenbindung und die Verkürzung der Wertschöpfungszeit ist. Wenn Sie ein neues Produkt entwickeln, möchten Sie, dass sich die User mit dem Produkt auseinandersetzen – und um diese Beziehungen zu fördern, ist es wichtig, eine

hervorragende Customer Experience (CX) zu bieten.



TIP

Um die Kundenbindung zu erhöhen, wird es Ihnen eine moderne, mit Blick auf die Zukunft entwickelte Customer-Identity-Lösung ermöglichen:

- » **Den richtigen Input zur richtigen Zeit von der richtigen Person während der Customer Journey zu verlangen.**
Anstatt zu versuchen, im Zuge eines langwierigen Registrierungsprozesses möglichst umfangreiche Informationen über potenzielle Neukunden zu sammeln, sollten Sie Innovationen wie Progressive Profiling nutzen, um den Reibungsverlust zu minimieren und die Conversion Rate zu verbessern.
- » **Ihren Kunden die richtigen Inhalte zu bieten, in der Sprache und dem Format, das sie am besten anspricht.**
Schaffen Sie Vertrauen, indem Sie Ihre Kunden in deren Muttersprache ansprechen, und managen Sie Übersetzung und Personalisierung separat.
- » **Jeden Identity Touch Point Brand-spezifisch zu gestalten, um Vertrauen und Kundenbindung aufzubauen.** Binden Sie Ihre Brand Assets in jeden Schritt der Customer Identity Journey ein. Nutzen Sie ein Software Development Kit (SDK) oder Application Programming Interfaces (APIs), um Ihren Kunden beispielsweise Ihre eigene, Brand-spezifische App zur Multi-Faktor-Authentifizierung (MFA) zur Verfügung zu stellen.



REMEMBER

Eine hochwertige Customer Experience ist einer der schnellsten Wege, um die Kundenbindung zu erhöhen – und stark eingebundene Kunden kaufen mit größerer Wahrscheinlichkeit mehr Ihrer Produkte, und das häufiger.

Bessere Security Outcomes erzielen

Eine moderne Customer-Identity-Lösung muss das richtige Gleichgewicht zwischen Security und CX finden, um den Aufbau vertrauensvoller Beziehungen zwischen Ihren Kunden und Ihrem Brand zu unterstützen. Da Cybersecurity Threats immer raffinierter und gefährlicher werden, ist die Versuchung groß, dieses empfindliche Gleichgewicht zu Gunsten der Security und zu Lasten der Usability zu verschieben.

Unternehmen können aber bessere Security-Outcomes erzielen – sowohl für sich selbst als auch für ihre Kunden –, wenn sie User in die Lage versetzen, ihre Daten auf einem für sie angemessenen Niveau zu schützen, und indem sie Security-Lösungen implementieren, die keinen direkten Kunden-Input erfordern. Das Ziel sollte nicht nur mehr Security, sondern bessere Security sein.



TIP

Anstatt die strengsten und disruptivsten Security-Optionen zu implementieren, die eine moderne Customer-Identity-Lösung bietet, sollten sich Unternehmen darauf konzentrieren, das richtige Level an Security zur richtigen Zeit anzuwenden, flexible Policies bereitzustellen und die Dinge so einfach wie möglich zu halten.

Um in Zukunft bessere Security Outcomes zu erzielen und das Vertrauen in Ihren Brand zu stärken, sollten Sie die folgenden Tipps berücksichtigen:

» **Legen Sie das *richtige* Maß an Security zum richtigen Zeitpunkt in der Customer Journey an.**

Selbst Unternehmen mit Tausenden von Kunden-Apps können die Dinge einfach halten, indem sie nur das Minimum an Input an der richtigen Stelle in der Customer Journey (z. B. bei der Registrierung) verlangen und so Reibungsverluste vermeiden. Fordern Sie Ihre Kunden nur dann zur MFA auf, wenn es notwendig ist, z. B. wenn sie sich von einem verdächtigen Ort oder einem unbekanntem Endgerät aus anmelden.

» **Legen Sie für jede Anwendung *spezifische* Security Policies fest, um die optimale Balance zwischen reibungsloser User Experience und Sicherheitsrisiko zu finden.**

Beispielsweise sollten Anwendungen, die es Kunden ermöglichen, sich zu registrieren und einen Kauf zu tätigen, ein höheres Security-Level erfordern als Anwendungen, die es Kunden nur ermöglichen, den Status einer Bestellung zu überprüfen – selbst wenn es sich um denselben User und Brand handelt.

» **Ermöglichen Sie es Usern, sich aktiv für MFA zu entscheiden.** Anstatt Ihre Kunden zu verpflichten, sich für MFA zu registrieren, sollten Sie ihnen die Möglichkeit dazu

geben. Obwohl MFA zunehmend zur Selbstverständlichkeit wird, sind viele Menschen immer noch genervt davon. Stattdessen könnten Sie andere Risikofaktoren ohne deren Input tracken (z. B. Endgerät, Standort oder Netzwerk).

- » **Machen Sie es Ihren Kunden leicht, ihre Accounts auf jedem beliebigem Weg wiederherzustellen.** Bieten Sie Ihren Kunden flexible Self-Service-Optionen (z. B. E-Mail, Textnachricht, Einmalpasswort usw.), damit sie ihre Accounts wiederherstellen oder ihre Passwörter zurücksetzen können, ohne sich an ein Call Center wenden zu müssen – das ist immer ein Gewinn.
- » **Erweitern Sie Customer Identity auf alle Touch Points, um Third-Party-Services zu integrieren.** Nutzen Sie dedizierte Technologien, um Funktionalitäten hinzuzufügen und die CX an jedem Touch Point entlang der Customer Journey zu verbessern.

Datenschutz sicherstellen

Datenschutzbestimmungen wie die Datenschutz-Grundverordnung (DSGVO) und der California Consumer Privacy Act (CCPA) prägen schon heute die Art und Weise, wie Geschäfte abgewickelt werden, und weitere Bestimmungen sind weltweit auf dem Weg, da Kunden mehr Kontrolle über ihre persönlichen Daten verlangen. Um auch weiterhin Kundenvertrauen aufbauen zu können, müssen sich Unternehmen anpassen, aber Datenschutz ist komplex und geht über die einfache „Zustimmung“ hinaus. Vom Customer-Identity-Standpunkt aus betrachtet, müssen künftige Funktionen drei zentrale Use Cases abdecken:

- » **Preference-Management:** Verarbeitung und Speicherung von Kundendaten
- » **Datenschutz-Management:** Weitergabe von Kundeninformationen
- » **Compliance-Management:** Mapping und potenzielle Löschung von personenbezogenen Daten

Diese Funktionen können von einer Customer-Identity-Lösung out-of-the-box oder durch Integrationen mit Drittanbietern, die sich auf Privacy and Consent Management Use Cases spezialisiert

haben, bereitgestellt werden.

Wirksamer Datenschutz führt zu höherem Kundenvertrauen, durchgängiger Compliance und Unternehmenserfolg.



Nutzen Sie eine moderne Customer-Identity-Lösung, um das Preference-, Datenschutz- und Compliance-Management der persönlichen Daten Ihrer Kunden zu orchestrieren und heute sowie in Zukunft sicher durch die komplexe Gesetzeslandschaft zu navigieren.

Komplexität managen

Unternehmen müssen heute überall mit Komplexität umgehen: von der Entwicklung, dem Testen und der Einführung moderner nativer Cloud-Apps für anspruchsvolle Kunden bis hin zur Konsolidierung externer und fragmentierter Identity Stores über Partnerportale hinweg, während gleichzeitig Legacy-Produkte gepflegt werden, bis eine mehrjährige Digital-Transformation-Initiative abgeschlossen ist. Diese Komplexität bedeutet, dass Customer Identity nicht mehr nur eine einfache Lösung ist, die es Ihren Kunden ermöglicht, sich bei einer einzigen App oder Website einzuloggen.

Ihre Customer-Identity-Lösung muss trotz dieser Komplexität die Weichen für Flexibilität und Wachstum stellen. Ganz konkret muss sie Folgendes leisten:

- » eine skalierbare Multi-Org-Architektur mit zahlreichen Testing-, Staging- und Produktionsumgebungen unterstützen
- » einen Mix aus modernen Cloud-Apps und Legacy-On-Premises-Produkten koordinieren und dabei die Segregation des Traffics sicherstellen
- » erweiterte API-Abdeckung und intuitives, organisationsübergreifendes Management bieten
- » bei der Organisation fragmentierter Identity-Systeme unterstützen

- » Praxisorientierte Checkliste zur Implementierung von Customer Identity
- » Identifizierung Ihrer technischen und betrieblichen Anforderungen
- » Auswahl der richtigen Customer-Identity-Lösung für Ihr Unternehmen
- » Customer Identity auf die nächste Innovationsstufe bringen
- » Nahtlose User Experiences, die Wettbewerbsvorteile bringen

Kapitel 8

Zehn Überlegungen zu Customer Identity

Im Folgenden finden Sie zehn wichtige Überlegungen, die Sie bei der erfolgreichen Planung und Implementierung der richtigen Customer-Identity-Lösung für Ihr Unternehmen unterstützen:

- » **Verstehen Sie die Pain Points Ihrer Kunden und internen Teams.** Sind Ihre Kunden aufgrund eines langwierigen Registrierungsprozesses frustriert? Waren Sie Opfer eines Angriffs? Werden Ihre Digitalisierungsvorhaben ausgebremst?
- » **Definieren Sie Ihre Erwartungen an die Customer Experience.** Was möchten Sie Ihren Kunden bieten, wenn sie mit Ihrem Brand interagieren? Möchten Sie den Zugriff auf alle Ihre Apps mit einer einzigartigen und Brand-spezifischen Login Experience ermöglichen? Über welche Kanäle soll das geschehen?

- » Legen Sie Ihre Security-Spezifikationen fest. Wie können Sie jetzt einen sicheren Zugriff gewährleisten? Was wollen Sie in Zukunft anbieten? Gibt es Sicherheits- und Datenschutzvorschriften, die Sie einhalten müssen?
- » **Definieren Sie Ihre Geschäftsziele.** Was wollen Sie für Ihr Unternehmen erreichen? Vielleicht eine internationale Expansion oder die Einführung eines neuen Produkts? In welchem Zeitrahmen?
- » **Stellen Sie alle Ihre Customer-Identity-Anforderungen zusammen.** Differenzieren Sie Ihre Anforderungen an die User Experience, die Sicherheit und das Business nach „Must-haves“ und „Nice-to-haves“. Stimmen Sie sich intern ab und entscheiden Sie, wie Sie potenzielle Kompromisse finden wollen.
- » **Kalkulieren Sie die Opportunitätskosten für Build-versus-Buy.** Der Aufbau und die Wartung einer eigenen Customer-Identity-Lösung sind schwierig und kostspielig. Daher sollten Sie sich lieber auf Ihr Kerngeschäft konzentrieren. In Kapitel 3 erfahren Sie, mit welchen Kosten und Aufgaben der Aufbau einer eigenen Lösung einhergeht.
- » **Übertragen Sie das Management der Identitäten einem Customer-Identity-Experten (damit es richtig gemacht wird).** Finden Sie mithilfe dieses Guides den richtigen Customer-Identity-Experten für Ihr Unternehmen. Suchen Sie nach einem zuverlässigen Partner mit einem entsprechenden Track Record, der Ihre aktuellen und zukünftigen Anforderungen erfüllt.
- » **Stellen Sie die Weichen für hochwertige Customer Experiences.** Sobald Sie sich für eine moderne Customer-Identity-Lösung entschieden haben, können Sie damit beginnen, diese schnell und umfassend mit all Ihren Kunden-Apps, Websites und Portalen zu integrieren, um nahtlose und sichere Customer Experiences zu bieten.
- » **Nutzen Sie das Reifegradmodell, um weitere Innovationen zu erschließen.** Eine moderne Customer-Identity-Lösung öffnet die Tür zu einer Welt voller Möglichkeiten für Ihr Unternehmen. In Kapitel 6 erfahren Sie mehr über unser Customer-Identity-Reifegradmodell.

- » Konzentrieren Sie sich auf die Stärken Ihres Unternehmens. Eine moderne Customer-Identity-Lösung kann ein Wettbewerbsvorteil für Ihr Unternehmen sein und Ihnen dabei helfen, einen guten Ruf in puncto Vertrauenswürdigkeit, Innovativität und erstklassiger Customer Experiences aufzubauen.



okta

Kundenidentität: Wir haben
das Buch dazu geschrieben.



bit.ly/OktaCIAudiobook

Hier geht
es zum
Audiobook

Bieten Sie jederzeit eine sichere und hochwertige Customer Experience

Wenn Sie schon einmal ein Konzertticket über eine Website gekauft oder sich mit Ihrem Social Media Account bei einem neuen Online-Shop eingeloggt haben, dann haben Sie auch schon Erfahrung mit Customer Identity gemacht. Customer Identity bietet eine digitale Identitäts-Ebene, die sich in Kunden-Apps, Websites und Portale einbetten lässt. Erfahren Sie in unserem Guide, wie ein modernes Customer Identity Management Ihnen hilft, Ihren Kunden und Partnern eine sichere, reibungslose Experience bereitzustellen.

Inhalt:

- Was ist Customer Identity?
- Warum Customer Identity wichtiger denn je ist
- Warum Sie bei der Entwicklung Ihrer Customer Identity auf Experten setzen sollten
- Worauf es bei einer modernen Customer-Identity-Lösung ankommt
- Worauf Sie bei einer Customer-Identity-Lösung achten sollten
- Wie eine maßgeschneiderte Customer-Identity-Lösung die Weichen für Erfolg stellt
- Die Zukunft von Customer Identity



okta

Lawrence C. Miller arbeitet seit mehr als 25 Jahren in der IT-Branche und verfasste mehr als 200 Dummie-Guides.

Jeremie Certes ist Senior Product Marketing Manager bei Okta.

Auf Dummies.com™
finden Sie die neuesten Videos,
Step-by-Step-Infografiken
und Anleitungen – und
unseren Online-Shop!

ISBN: 978-1-394-22819-5
Nicht zum Verkauf

für
dummies®
A Wiley Brand



WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.