okta

# Entwickeln oder kaufen?

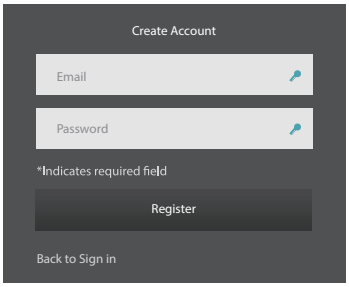
Wichtige Überlegungen sowie die Vorteile einer vorgefertigten Identitätslösung

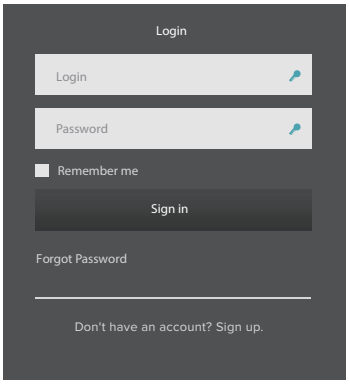
**Okta Deutschland**
Oskar-von-Miller-Ring 20
80333 München

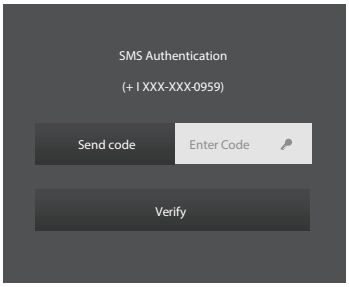
**info_germany@okta.com**
**+44 800 368 8930**

Jedes Team, das eine neue Web- oder Mobilanwendung erstellt, steht vor der Wahl, die gesamte Anwendung intern zu erstellen oder ausgewählte Out-of-the-box-Dienste zu nutzen, um die Arbeit zu vereinfachen und zu beschleunigen. Viele der heute erfolgreichen Teams entschieden sich für Letzteres und setzen auf Dienste wie Stripe und Braintree zur Auslagerung von Zahlungen und Twilio zur Auslagerung von Kommunikation. Ein weiterer solcher Service ist eine externe CIAM-Lösung (Customer Identity and Access Management). Eine digitale Identitätsschicht aus APIs, SDKs und sofort einsatzbereiten, anpassbaren Komponenten kann dazu beitragen, dass die Markteinführung beschleunigt und die Entwicklungskosten gesenkt werden und sich die internen Entwickler auf die Kernfunktionen der Anwendung konzentrieren können.

Kundenseitige Anwendungen – ob für Endanwender oder Geschäftskunden – erfordern grundlegende Funktionen für Authentifizierung, Autorisierung und Benutzerverwaltung. Die Anwendungen müssen gängige Arbeitsabläufe unterstützen, z. B. die Erstellung von Konten, Benutzeranmeldung, Passwortzurücksetzung, Kontowiederherstellung und Registrierung mit Multi-Faktor-Authentifizierung (MFA). Darüber hinaus müssen die Anwendungen je nach Benutzer unterschiedliche Zugriffsebenen ermöglichen.




Leitende Architekten und Ingenieure sind sich oft nicht sicher, ob eine umfassende Identitäts- und Zugriffsmanagement-Lösung (IAM) eines externen Anbieters für ihr Projekt geeignet ist. In diesem Whitepaper werden die wichtigsten Überlegungen für die Entscheidung zwischen einer Eigenentwicklung und einem Kauf sowie die Vorteile einer vorgefertigten Lösung erörtert.

## Die Herausforderungen des Identitäts- und Zugriffsmanagements

Das Identitäts- und Zugriffsmanagement für kundenseitige Anwendungen umfasst Funktionen wie Authentifizierung, Autorisierung und Benutzerverwaltung. Die Authentifizierung ermöglicht Benutzern den Zugriff auf ein System über ein Passwort, einen Token oder einen API-Schlüssel, externe Verzeichnissen wie Active Directory oder LDAP, Unternehmens-IPD oder über ein Social-Media-Konto. Über die Autorisierung wird festgelegt, auf welche Ressourcen sie zugreifen können. Die Benutzerverwaltung umfasst die Speicherung und Sicherheit der personenbezogenen Daten der Benutzer, die Verwaltung des Lebenszyklus des Benutzers von der Registrierung bis zur Löschung sowie fortgeschrittenere Funktionen wie Single Sign-On und die Bereitstellung für nachgelagerte Anwendungen. Die Endbenutzer nehmen einen Großteil dieser Kernfunktionen als selbstverständlich hin, aber die Umsetzung des Projektplans bringt eine Vielzahl von Herausforderungen mit sich.

### Komplexität

Mit unternehmenseigenen Entwicklungsressourcen lassen sich zwar grundlegende Identitätsfunktionen wie Kontoerstellung, Anmeldung und Passwortzurücksetzung bewältigen, doch die Kunden verlangen heute zunehmend mehr Funktionen und mehr Sicherheit, was den Umfang von Projekten oft vergrößert. Die Entwicklung erweiterter Funktionen wie Single Sign-On-Unterstützung, Partitionierung von Kundendaten, Token-Authentifizierung, Multi-Faktor-Authentifizierung, Anmeldung über Social-Media-Konten und LDAP/Active Directory-Integration erfordert einen erheblich größeren Aufwand. Wenn sich die Entwicklungsteams in Unternehmen nicht regelmäßig miteinander abstimmen, stellen sie bei der Entwicklung neuer Anwendungen häufig fest, dass sie das Rad gerade neu erfunden haben. Die einzelnen Teams unterschätzen häufig den Aufwand für den Aufbau eines vollständigen, zukunftssicheren Identitätsdienstes, wodurch Deadlines verpasst werden. Zudem entwickeln sich die Anforderungen an das Identitätsmanagement ständig weiter. SAML und WS-Fed wurden durch modernere Standards wie OpenID Connect und OAuth 2.0 ersetzt, da in diesen Standards angreifbare Elemente gefunden wurden. Darüber hinaus wurden Unternehmensanforderungen wie die Entziehung des Zugriffs auf APIs durch den Entzug von Token anfangs möglicherweise nicht in den Standards berücksichtigt.

Typische Anforderungen in Bezug auf das Identitäts- und Zugriffsmanagement

| Komponente | Beschreibung |
|---|---|
| Terminierung von SSL-Verbindungen | Erstellung und Pflege sicherer Verbindungen mit jedem Client über HTTPS. Verwaltung von Webzertifikaten für Domänen. Einrichtung starker SSL/TLS-Konfigurationen. Laufende Aktualisierung der Kryptographiefunktionen. |
| Einrichtung, Wartung und Sperrung des Betriebssystems | Anpassung von Betriebssystem und Serversoftware zur Beseitigung von Sicherheitslücken. |
| Speicherung und Sicherheit von Passwörtern | Hashing von Passwörtern mit modernsten Algorithmen und kontinuierliche Wartung, wenn sich die Methoden weiterentwickeln. |
| Berichterstattung | Dashboard mit Metriken, um den allgemeinen Zustand von Benutzern und Anwendungen zu sehen. Einfacher Zugriff auf Benutzerberichte für Compliance-Zwecke. |
| Bereitstellen eines Token-Dienstes | Skalierbarer Dienst zum Tracking aller Benutzersitzungen, inklusive kontinuierlicher Datenbankwartung und Patching. |
| Bereitstellen eines Verzeichnisses mit erweiterbaren Profilen/Benutzern/Gruppen/Clients | Skalierbares Benutzer-Repository, das ein flexibles Benutzerprofil und flexible Benutzergruppen bietet. Umfasst Verzeichnis-App-Server, Datenbank, App-Datenbank und Verschlüsselung. |
| Benutzeroberfläche für Administratoren | Benutzeroberfläche für Administratoren zur Verwaltung von Benutzern, Anwendungen und APIs mit individuellen Administratorrollen. |
| Benutzeroberfläche für Kundendaten | Benutzeroberfläche für Kundendienst oder Helpdesk zur Verwaltung von Kundenprofilinformationen mit individuellen Administratorrollen. |
| Registrierung, Anmeldung, Kontowiederherstellung, MFA-Bildschirme | Erstellung von Benutzeroberflächen und Arbeitsabläufen, Hosting von Anmelde- und Registrierungsseiten. |

| | |
|---|---|
| Implementierung von Protokollen | Vertraut machen mit und Umsetzen der Spezifikationen für SAML, OIDC, OAuth 2.0. |
| Aufbau des Autorisierungsservers | Aufbau einer Autorisierungs-Engine für die Geschäftslogik, einschließlich anpassbarer Bereiche und Ansprüche. |
| Autorisierung über Social-Media-Konten und Profilsynchronisierung | Unterstützung der Authentifizierung über beliebige Identitätsanbieter in sozialen Medien und Synchronisierung von Profilattributen. |
| SSO-Konnektoren | Erstellung, Wartung und Tests kundenspezifischer SSO-Konnektoren für Anwendungen von Drittanbietern. |
| MFA | Hohe Verfügbarkeit, redundante MFA mit Unterstützung mehrerer Faktoren (SMS, Sprache, E-Mail, Google Authenticator, Biometrie, Push). |
| Authentifizierungsrichtlinien | Konfigurierbare Richtlinien und Richtlinien-Framework zur Steuerung der kontextbasierten Anmeldung anhand von Benutzer, Anwendung, Gruppe, Standort, IP-Bereich, Verhalten, Gerät usw. |
| Provisionierungs-Engine | Engine zur Verwaltung von Benutzerobjekten in nachgelagerten Diensten. |
| Provisionierungs-Konnektoren | Erstellung, Pflege und Tests kundenspezifischer, API-basierter Konnektoren für CRUD-Funktionen. |
| Verzeichnis/IDP-Integration | Erstellung von Integrationen mit externen Verzeichnissen wie AD/LDAP und Unterstützung eingehender Föderation über SAML, OIDC und WS-Fed für bestehende IDPs. |
| Gateway-Integration | Integration mit API-Gateways wie Apigee und Mulesoft. |

### Erforderliche Ressourcen

Häufig fehlen Unternehmen die hochspezialisierten Ressourcen, die für den Aufbau sicherer und skalierbarer Identitätsfunktionen für ihre Anwendungen benötigt werden. Dazu sind Teammitglieder mit unterschiedlichen technischen Kenntnissen erforderlich, darunter Kryptografie, Datenbanksicherheit, Performance Engineering, Systementwicklung und Sicherheitsaudits sowie eine fortschrittliche Datenarchitektur zur Verwaltung von Berechtigungen. Deshalb sind in großen Unternehmen wie LinkedIn und Salesforce Identitätsteams mit 25 oder mehr Mitarbeitern allein für die Gewährleistung der Benutzerverwaltung verantwortlich. Da Entwicklungsexperten rar gesät sind, haben viele Unternehmen Schwierigkeiten, die benötigten Ressourcen zu finden, um die Arbeit intern zu erledigen.

### Verfügbarkeit

Kundenseitige Anwendungen erfordern eine extrem hohe Verfügbarkeit, damit sich die Endbenutzer unabhängig von der Belastung der Anwendung anmelden können. Wenn bei einem Problem mit dem Backend für die Benutzerverwaltung die Anwendung abstürzt, wird die Kundenerfahrung nachhaltig beeinträchtigt. Dadurch kann die Anwendung die ihr zugewiesenen Aufgaben nicht mehr erfüllen: die Verbesserung der Kundenerfahrungen und die Steigerung des Umsatzes. Eine negative Online-Erfahrung kann das Vertrauen der Kunden schädigen und dafür sorgen, dass sie sich der Konkurrenz zuwenden.

Typische Anforderungen in Bezug auf Hochverfügbarkeit

| Komponente | Beschreibung |
|---|---|
| DDOS-Schutz | Automatisierte Bandbreitenbegrenzung für alle Endgeräte, um DDOS-Angriffe abzuwehren. Erfordert häufig ergänzende IaaS-Funktionen. |
| DevOps | Systeme und Bereitschaftsdienstteam zur Bereitstellung und Verwaltung des Dienstes in Echtzeit. Automatisierte Konfiguration der Maschinen, Datenbank-Backups (mit Tests der Aktualität und Zuverlässigkeit der Backups) und Verwaltung privilegierter Zugriffsrechte. |
| Verfügbarkeit der Infrastruktur | Implementierung automatisierter Funktionen zur Überwachung und Verwaltung der Maschinenressourcen (Entfernung ausgefallener Nodes, Bereitstellung von Ersatzteilen). |

**Skalierbarkeit**

Unternehmen fällt es schwer, das Benutzeraufkommen für ihre Anwendungen vorherzusagen, und können daher Opfer ihres eigenen Erfolgs werden. Wenn bei einem größeren Nachrichtenereignis oder nach der Veröffentlichung eines Features zu viele Benutzer versuchen, sich gleichzeitig anzumelden, muss Ihr Identitätsdienst diese Belastung bewältigen können. Ressourcenintensive Aktionen wie Authentifizierung, Passwortverschlüsselung und Suche müssen während dieser Spitzenzeiten mit der Benutzernachfrage skaliert werden. Unternehmen müssen die Auslastung ihrer verschiedenen Produktions-, Qualitätssicherungs-, Entwicklungs-, Integrations- und Disaster-Recovery-Umgebungen sowie Puffer für Überprovisionierung berücksichtigen. Anwendungen mit hohem Aufkommen können Dutzende von Servern für die Benutzerverwaltung erfordern. Die Skalierbarkeit ist ein kritischer Faktor, da Online-Kunden einfach die Website verlassen, wenn sie sich nicht anmelden können.

**Sicherheit**

Verstöße gegen den Benutzerdatenschutz machen schnell Schlagzeilen und sind sehr teuer. Anwendungen sind eine Goldgrube für personenbezogene Daten und enthalten zudem oft auch sensible Daten wie Sozialversicherungsnummern, Kreditkartennummern usw. Die Sicherheitsumgebung ändert sich ständig und die Datenhack-Techniken haben dank der Möglichkeiten von Cloud Computing ein neues Niveau erreicht. Jüngste Untersuchungen haben gezeigt, dass Anwendung im Durchschnitt erstaunliche 26,7 schwerwiegende Schwachstellen aufweisen, von denen der Großteil auf benutzerdefinierten Code zurückzuführen ist. Registrierungs-, Anmelde- und Wiederherstellungs-Workflows werden am häufigsten als Angriffsvektor ausgenutzt und führen zu Sicherheitsrisiken wie fehlerhafter Authentifizierung oder Zugriffskontrolle, Gefährdung sensibler Daten sowie zu unzureichender Protokollierung und Überwachung. Diese Risiken werden jedes Jahr unter den OWASP Top 10 gelistet.

Unternehmen müssen ihren Code und ihre Bibliotheken kontinuierlich überwachen, pflegen und patchen, um die Sicherheit der Benutzerdaten zu gewährleisten. Häufig aktualisieren die Entwicklungsteams die Sicherheits-algorithmen nicht zeitnah. Netzwerk- und Anwendungssicherheit werden in der Regel in verschiedenen Unternehmensbereichen betrieben. In Anwendungen entstehen technische Schwachstellen, wenn Entwickler unter Termindruck arbeiten. All dies kann zu potenziellen Sicherheitslücken in Anwendungen führen.

Typische Anforderungen in Bezug auf die Gewährleistung der Sicherheit

| Komponente | Beschreibung |
|---|---|
| Sicherheitsüberwachung der technischen Prozesse | Automatisierte Protokollierung und Überwachung aller Aktivitäten innerhalb des Dienstes, einschließlich Administrationsaktionen, Anwendungsverhalten, Dateiintegrität, Änderungskontrolle, Erkennung von Eindringungsversuchen. Kontrolle von Datenübertragungsversuchen. Bei verdächtigem Verhalten Warnungen an DevOps- und Sicherheitsteams im Bereitschaftsdienst. |
| Tools zur Sicherheitsüberwachung | SIEM für die Sicherheitsüberwachung (z. B. Splunk, AppD, New Relic, Zabbix, Wavefront). |
| Sichere Entwicklungsverfahren | Organisatorische Kontrollen und Prüfung der Software-Entwicklung durch Dritte.<br>• Überprüfungen des Sicherheitscodes<br>• Schwachstellenscans auf Codebasis<br>• Sicherheits- und Autorisierungskontrollen auf Endgeräteebene<br>• Penetrationstests durch Dritte<br>• Bug-Bounty-Programm |
| Einhaltung von Vorschriften | Prozesse zur Erlangung und Aufrechterhaltung von Zertifizierungen, Akkreditierungen und Compliance für SOC 2 Typ 2-Zertifizierung, ISO 27001, CSA Star, TrustE, FedRAMP, DSGVO, Open Banking, PSD2, SMART auf FHIR. |
| Benutzeroberfläche für Berichte | Benutzeroberfläche für Sicherheit und Compliance zur Verwaltung von Ereignisinformationen mit individuellen Administratorrollen. |

## Vorteile einer modernen CIAM-Lösung

Das Bewusstsein führender Entwickler für die Schwierigkeiten bei der Entwicklung, Absicherung und Wartung der Benutzerinfrastruktur ist gestiegen, sodass sie proaktiv nach Lösungen suchen. Anstatt aufgrund der zunehmenden Komplexität auf Funktionen zu verzichten, verlagern sie die Identitätsschicht ihrer Anwendungen zunehmend auf Drittanbieter von CIAM-Lösungen (Customer Identity and Access Management). Dieser Ansatz hat eine Reihe von Vorteilen gegenüber der Entwicklung im eigenen Haus.

### Schnellere Markteinführung

Entwicklungsteams stehen unter großem Druck, Web- und mobile Anwendungen pünktlich zu liefern. Da der Wettbewerbsdruck zunimmt, werden die Zeitvorgaben immer ehrgeiziger. Jede Verzögerung der Markteinführung bedroht den Umsatz und birgt das Risiko, einen potenziellen Kunden zu verlieren. Die Auslagerung des Identitätsmanagements an einen vertrauenswürdigen Dritten hilft Ihrem Team, pünktlich zu liefern.

Beispiel für die Kosten einer verzögerten Markteinführung (pro Projekt oder Initiative):

$$\frac{50.000\ \$}{\text{Monat}}\ (\text{erwarteter Umsatz}) \times 6\ (\text{Monate Verzögerung}) = 300.000\ \$\ (\text{potenzieller Umsatzverlust})$$

* Wenn die Zahl der Projekte und Initiativen zunimmt und diese jeweils eigene, maßgeschneiderte Authentifizierungsprozesse nutzen, kann der Aufwand erheblich zunehmen.

„Wenn [Okta] zu meinem Toolkit gehört, weiß ich, dass wir schneller vorankommen, weil wir die Identitätskomponente abhaken können."

– Scott Howitt, CISO, MGM Resorts International

MGM RESORTS INTERNATIONAL

**Reduzierung der TCO für die Anwendungsentwicklung**

Beim Identitätsmanagement ist das Risiko für Kostenüberschreitungen besonders hoch, weil die Komplexität der Funktionen und Systeme so oft unterschätzt wird und permanent Weiterentwicklungen berücksichtigt werden müssen. Ein selbstentwickelter Ansatz führt zu größerer Unsicherheit. Zudem steigen die Kosten erheblich, wenn interne Teams durch zusätzliche Benutzerfunktionen abgelenkt werden oder feststellen, dass sie ihre Anforderungen an Veränderungen anpassen müssen. Die Teams liefern zwar immer noch pünktlich – jedoch nur mit der Unterstützung teurer externer Ressourcen. Wenn Sie die Identität an einen vertrauenswürdigen Anbieter auslagern, tragen Sie dazu bei, dass das Entwicklungsteam den vollen Projektumfang im Rahmen des Budgets liefert.

Beispiel für die Reduzierung der TCO für die Anwendungsentwicklung:

3 Entwickler × 6 Monate Zeitrahmen × 200.000 $ Gehaltskosten × 90 % Verbesserung = 270.000 $ Reduzierung der TCO

„Beim Identitätsschutz ändern sich die Dinge fast stündlich. Wir brauchen daher einen Technologiepartner, der mit diesem schnellen Wandel jederzeit Schritt halten kann."

– Eash Sundaram, EVP Innovation,
Chief Digital & Technology Officer, JetBlue Airways

jetBlue

**Konzentration der Ressourcen auf Kernfunktionen**

Ihr Erfolg hängt davon ab, wie gut Sie die wichtigsten Produktfunktionen ausführen, die Ihre Anwendung für die Endbenutzer nützlich machen. Mit einer modernen Identitätsschicht kann Ihr Team sich weiterhin ganz auf Funktionen zu konzentrieren, die den Umsatz und die Kundenbindung fördern. Gleichzeitig können Ihre Entwickler schneller zu einer zweiten, dritten oder vierten Anwendung übergehen, die Ihre Kunden verlangen.

Beispiel für die Opportunitätskosten der zugewiesenen Ressourcen:

$$\frac{\underset{\text{EBITDA pro Jahr}}{10\text{ Mio. }\$}}{\underset{\text{Entwickler im Unternehmen}}{50}} \times \underset{\text{Entwickler am Projekt}}{3} \times \underset{\text{Monate Zeitrahmen}}{6} = \underset{\text{verlorene Gewinnmöglichkeit}}{300.000\ \$}$$

* Übliche, an Google angelehnte Berechnung des Wertes eines Entwicklers für Unternehmen, bei denen die Technologie der Hauptumsatzträger ist. Der durchschnittliche jährliche Umsatzbeitrag eines Entwicklers wird hier mit der Anzahl der Entwickler multipliziert, die aus dem Entwickler-Pool entfernt werden, um eine Identitätsschicht zu liefern.

„Ich möchte das Rad für unsere Identitätsumgebung nicht neu erfinden. Stattdessen möchte ich die branchenweit besten Lösungen nutzen und dann die Adobe-spezifischen Anforderungen auf diesen Stack anwenden, damit wir unseren Kunden wirklich schnell etwas bieten können. Durch die Verwendung von Okta für Adobe können wir uns auf die wichtigsten Unterscheidungsmerkmale unseres Produkts konzentrieren, Wert für unsere Kunden schaffen und unsere Zeit und Mühe in die Dinge investieren, die unsere Kunden erfolgreich machen."

– Scott Castle, Director Product Management, Digital Media, Adobe

Adobe™

**Verringerung des Risikos von Sicherheits- und Compliance-Verstößen**

Wann hat Ihr Team das letzte Mal den Passwort-Hashing-Algorithmus aktualisiert? Benutzerdaten und personenbezogene Informationen sind das häufigste Ziel von Angriffen. Die durchschnittliche Lebensdauer eines effektiven Verschlüsselungsalgorithmus beträgt 18 Monate. Der Schutz der Anwender bleibt jedoch oft zugunsten von Anforderungen, die das Wachstum oder den Umsatz fördern, auf der Strecke. Damit Ihr Identitätsdienst sicher ist, muss Ihr Team über das Wissen und die Zeit verfügen, um Schwachstellen auf jeder Ebene der Infrastruktur beheben zu können – von der Betriebssystem-, Datenbank- und Transportschicht bis hin zum Anwendungs-Stack und Code-Schwachstellen. Da Entwicklungsteams selten über diese umfangreichen Sicherheitskenntnisse verfügen, erfahren sie erst nach einer Kompromittierung sensibler Daten, dass ihre Benutzersicherheit versagt hat. Zudem wissen sie oft nicht über neue Erkenntnisse Bescheid, z. B. über angreifbar gewordene Algorithmen oder neu entdeckte Angriffsvektoren. Ein gut gewählter Identitätsmanagement-Dienst schützt Ihre Benutzerdaten vor Angreifern, da das Entwicklungsteam aus Experten besteht, die sich ganz auf fortgeschrittene Sicherheitsmaßnahmen und den Schutz aller Angriffsvektoren konzentrieren. Zu den Sicherheitsmaßnahmen gehören leistungsstarke Verschlüsselung, API-Sicherheit, erweiterter Firewall-Schutz sowie robuste Verfahren für Datenverwaltung und Systemzugriffe. Dieselben Sicherheitsmaßnahmen und dieselbe Infrastruktur ermöglichen es Ihren Teams, die lokalen und branchenspezifischen Vorschriften wie HIPAA, FedRAMP und DSGVO einzuhalten.

„Okta hilft uns dabei, HIPAA-konform zu sein … vor allem, weil wir die Identität unserer Kunden nicht verwalten und aufrechterhalten müssen. Wir vertrauen dabei Okta."

– Rish Tandon, CTO, Heal

heal

### Gewährleistung besserer Benutzererfahrungen

Funktionen wie Kontoerstellung, Anmeldung, Passwortdurchsetzung und Sitzungsverwaltung bestimmen den ersten Eindruck des Benutzers von Ihrer Anwendung und damit auch von Ihrem Unternehmen. Wenn diese digitalen Interaktionen nicht perfekt sowie nahtlos sind, verlieren die Benutzer das Vertrauen und gehen lieber zur Konkurrenz. Ein vorgefertigter Identitätsdienst, der sich auf reibungslose Kundenerfahrungen in verschiedensten Anwendungsfällen konzentriert, bietet einen Vorsprung bei der Erstellung erfolgreicher Benutzererfahrungen. Führende Anbieter von Lösungen für Kundenidentitätsmanagement bieten Funktionen, die mit wenig oder komplett ohne benutzerdefinierten Code implementiert werden können. Diese reichen von sofort einsatzbereiten, anpassbaren und gehosteten Bildschirmen zur Selbstregistrierung bzw. Anmeldung über passwortlose Anmeldeprozesse bis hin zu Anmeldungen per Single Sign-On oder über Social-Media-Konten.

> „Die National Bank of Canada betreut Millionen von Kunden in Hunderten von Filialen in ganz Kanada. Wir haben unter anderem das klare Ziel, die Kundenerfahrung zu vereinfachen. Durch die intelligente Authentifizierung und die kontextbezogenen Funktionen von Okta können wir unseren Kunden eine nahtlose, sichere Online-Erfahrung bieten."
>
> – Alain Goffi, Vice President, IT Infrastructures, National Bank of Canada

NATIONAL BANK

### Motivierung der Entwickler

Trotz der Bedeutung des Identitätsmanagements für den Erfolg einer kundenorientierten Anwendung macht es Entwicklern in der Regel keinen Spaß, die Identitäts- und Sicherheitsinfrastruktur aufzubauen. Obwohl die Benutzerverwaltung mit vielen Risiken verbunden und häufig komplex ist, wird sie banal eingestuft. Stattdessen arbeiten die Entwickler lieber an Funktionen für die Differenzierung der Kernprodukte und für innovative Systeme. Der hohe Aufwand für die Implementierung der Benutzersicherheit kann besonders demotivierend wirken: Das Risiko ist hoch und es gibt viele widersprüchliche Anleitungen. Die Arbeit mit modernen REST-JSON API-Diensten empfinden Entwickler hingegen als interessant und zugänglich.

### Hohe Skalierbarkeit und Zuverlässigkeit

Wenn die Benutzerverwaltung ausfällt, machen Sie quasi die Tür zu Ihrem Geschäft noch vor Ladenschluss dicht. Wenn die Anmeldung fehlschlägt, kennen die Endbenutzer den Grund nicht – und interessieren sich auch nicht dafür. Allerdings wird die Wahrnehmung Ihres Unternehmens und Ihrer Marke durch Ihre Kunden darunter leiden. Die Kundenauslastung ist nicht vorhersehbar und Marketing-Abteilungen wissen oder kommunizieren nicht immer, wann eine Werbeaktion einen Zustrom von Benutzern auslösen kann. Wenn Sie die Verwaltung selbst übernehmen, müssen Sie sich darauf verlassen können, dass Ihr Team maximale Verfügbarkeit und bei einer wachsenden Benutzerbasis problemlose Skalierbarkeit bieten kann. Sie müssen darauf vorbereitet sein, in Ihrem Rechenzentrum oder bei der Zusammenarbeit mit einem Infrastructure as a Service-Anbieter doppelte oder dreifache Redundanz bereitzustellen. Um die unterbrechungsfreie Verfügbarkeit des Dienstes zu gewährleisten, müssen Sie für nahtlose Upgrades und Wartung sorgen. Unternehmen, die diese alles andere als trivialen Aufgaben übernehmen, empfinden den Wartungsaufwand oft als unüberschaubar. Ein externer Benutzermanagement-Anbieter kann diese operativen Herausforderungen vollständig übernehmen.

„Wir legten großen Wert auf mehrere Punkte. Dazu gehörten die einfache Integration im gesamten Ökosystem, hohe Zuverlässigkeit und Verfügbarkeit. Außerdem wollten wir Identität für alle Systeme und als zentrales Element unserer Beziehung zum Kunden nutzen können.“

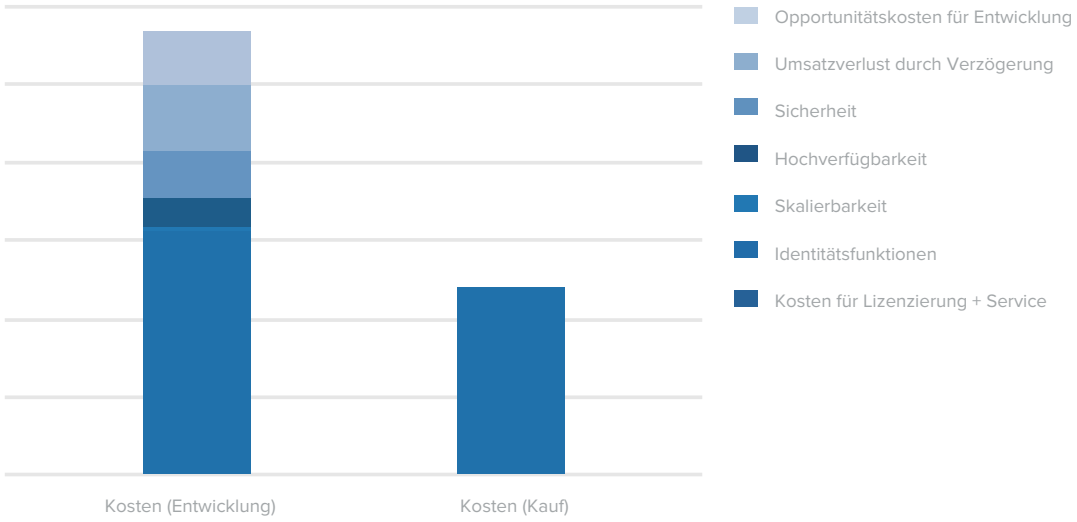
– James Fairweather, Senior Vice President of E-Commerce and Technology, Pitney Bowes

**Zusammenfassung**

Entwicklungsteams setzen zunehmend auf vorgefertigte Tools, um sich der Last der Anwendungsentwicklung zum Teil zu entledigen. Das Identitäts- und Zugriffsmanagement stellt Entwickler vor eine Vielzahl von Herausforderungen, die sich mit einer vertrauenswürdigen Identitätsschicht leicht beheben lassen. Diese Strategie eignet sich für alle Unternehmen, die die Markteinführung beschleunigen, die Kosten senken, die Entwicklungsteams auf die Kernfunktion konzentrieren und eine Reihe weiterer Vorteile nutzen möchten. Einige Unternehmen zögern noch, API-Dienste zu nutzen. Das liegt häufig an Missverständnissen, die bei der Ausgliederung eines Projekts leicht widerlegt werden können. Während Entwickler in der Vergangenheit davor zurückschreckten, Teile des Stacks auszulagern, werden sie dies bei bewährten Lösungen wie Twilio für die Kommunikation und Stripe für die Zahlungen nun gern tun.

In vielerlei Hinsicht sollte die Identität wie eine Tätowierung behandelt werden. Mit einer DIY-Lösung schränken Sie Ihren Möglichkeiten zur zukünftigen Skalierung ein. Da die Identität für Ihren Anwendungs-Stack so wichtig ist, gilt es von Anfang an die richtige Lösung zu wählen.

Vergleich der Gesamtbetriebskosten: Entwickeln oder kaufen?



## Die Okta Identity Cloud

Die Okta Identity Cloud wurde speziell für das moderne Identitätsmanagement entwickelt und ermöglicht es Unternehmen, ihren Mitarbeitern, Partnern, Lieferanten und Kunden sichere und reibungslose digitale Erfahrungen zu bieten. Die moderne, sichere Identitätsschicht kann als Identitätsbaustein für Ihre mobilen oder Web-Anwendungen dienen und die Markteinführung Ihrer digitalen Projekte beschleunigen:

- **Eingebettete Authentifizierung:** Bieten Sie Ihren Anwendern reibungslose, sichere Erfahrungen. Nutzen Sie die von Okta vorgefertigten UI-Widgets für gängige Benutzeraktionen wie Anmeldung, Registrierung und Passwortrücksetzung oder bauen Sie mit den Okta-APIs eine vollständig angepasste Erfahrung auf.
- **Eingebettete Autorisierung:** Kontrollieren Sie mit der API-Zugriffsverwaltung von Okta, auf welche APIs Ihre Benutzer und Entwickler zugreifen können. Passen Sie Ansprüche und Bereiche an und fügen Sie über Okta-Token externe Attribute ein.
- **Benutzer- und Richtlinienverwaltung:** Verwalten Sie Ihre Benutzer und Sicherheitsrichtlinien programmgesteuert über APIs oder über unsere benutzerfreundliche Administrationskonsole. Erstellen Sie Single Sign-On-Erfahrungen (SSO) und verwalten Sie den Benutzerlebenszyklus mit automatisiertem Onboarding und Offboarding.
- **Effiziente Entwicklerprozesse:** Von „No-Code“ bis „Pro-Code“: Nutzen Sie die von Okta gehosteten Anpassungstools, um mit minimalen Entwicklungsressourcen zu beginnen. Alternativ können Sie mit dem Okta-SDK und REST API die Programmiersprache und das Framework Ihrer Wahl nutzen.
- **Produktionsbereit:** Vertrauen Sie auf das SLA, das zuverlässige Skalierung mit garantierter 99,9%iger Betriebszeit verspricht. Mit dem Administrator-Systemprotokoll können Sie potenzielle Sicherheitsbedrohungen in Echtzeit überwachen. HIPAA-, FedRAMP-, DSGVO- und PSD2-konform.
- Okta Integration Network: Ein komplettes Ökosystem zur Unterstützung Ihrer Entwicklungsmaßnahmen. Die Integrationen umfassen mehr als 5.000 vorgefertigte Konnektoren für SSO zu Anwendungen, API-Gateways, IaaS, Identitätsprüfung und Controllern für die Anwendungsbereitstellung.

## Über Okta

Okta ist ein führender unabhängiger Identitätsanbieter für Entwickler und Unternehmen. Die Okta Identity Cloud verbindet Unternehmen sicher mit ihren Kunden, Partnern und Mitarbeitern. Durch die nahtlose Einbindung in über 5.000 Anwendungen ermöglicht die Okta Identity Cloud jedem Benutzer einfachen und sicheren Zugriff von jedem Gerät aus.

Tausende von Kunden, darunter 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn und News Corp, verlassen sich auf Okta, um schneller zu arbeiten, ihren Umsatz zu steigern und ihre Sicherheit zu wahren. Mit Okta kommen Kunden schneller ans Ziel, denn Okta macht den Zugang zu Technologien, die Kunden für ihre Arbeit unbedingt benötigen, sicher und benutzerfreundlich.

Weitere Informationen dazu finden Sie unter www.okta.com/de.


okta