KuppingerCole Report

Whitepaper

by Martin Kuppinger | August 2019

Identitäten richtig handhaben - damit Ihre digitale Geschäftsstrategie erfolgreich wird.

Registrierung und Authentifizierung sind die ersten Schritte, die erfolgen, wenn ein Nutzer Kunde digitaler Dienstleistungen werden möchte. Funktionieren diese Schritte nicht wie vom Nutzer erwartet, leidet die Akzeptanz solcher Dienste und damit ist der Erfolg digitaler Geschäftsstrategien in Gefahr. Identitäts-API-Plattformen helfen beim Aufbau von standardisierten Lösungsansätzen für die Bereitstellung von vereinheitlichten Identitätsdiensten für Unternehmen. Solche Plattformen sind unerlässlich für den Erfolg im digitalen Zeitalter.

von **Martin Kuppinger**
mk@kuppingercole.com
August 2019

Unterstützt von Auth0

Inhaltsverzeichnis

Abbildungen

Verwandte Dokumente

Leadership Compass: Identity API Platforms - 79012

Leadership Compass: IDaaS Access Management - 79016

Leadership Compass: CIAM Platforms - 79059

Executive View: Auth0 Authentication Service - 71325

Executive View: Auth0 Customer Identity Management - 71053

1 Einleitung

Seit mehr als zwei Jahrzehnten sind Unternehmen zunehmend digitaler geworden. Allen digitalen Diensten ist es dabei gemeinsam, dass sie als Schnittstellen zwischen Verbraucher und Unternehmen vermitteln. Ein wesentlicher Bestandteil dieser Beziehung ist, dass aus dem Verbraucher schließlich ein identifiziertes Individuum wird: Der digitale Kunde.

An diesem Punkt stehen Unternehmen vor der Herausforderung, die Identität ihrer zukünftigen Kunden zu überprüfen und einen Registrierungsprozess einzurichten, ohne hierbei den Verbraucher auf dem Weg zum (hoffentlich zahlenden) Kunden zu verlieren.

Der Hauptgrund dafür, dass Unternehmen mit komplexen und umständlichen Customer Journeys[1] über ihre verschiedenen Anwendungen und Services hinweg zu kämpfen haben, ist das Fehlen standardisierter Identitätsmanagement-Lösungen, die von Entwicklungsteams problemlos genutzt werden können. Wenn Entwickler den Registrierungsprozess beim Aufbau eines digitalen Dienstes "erfinden" müssen oder wenn sie eigenständig herausfinden müssen, wie sie einen notwendigen Prozess mit einer guten Customer Journey kombinieren können, werden die Ergebnisse kaum perfekt ausfallen.

Um diesen Prozess zu vereinfachen, setzen Unternehmen auf standardisierte Identitätsmanagement-Lösungen. Solche Service-Layer und Service-Systeme werden allgemein als Identitätsplattformen (Identity Platforms) oder Identitäts-API-Plattformen (Identity API Platforms) bezeichnet. API steht hierbei für Application Programming Interface, d.h. die technische Schnittstelle, mit der ein Entwickler zentrale Dienste aufrufen kann, wie sie etwa für die Authentifizierung von Benutzern, die Registrierung oder andere Aufgaben im Zusammenhang mit der Verwaltung von Identitäten und der Customer Journey erforderlich sind.

Auch wenn sich ihre Kern-Services nicht ausschließlich auf das Identitätsmanagement beschränken, sind Identity-API-Plattformen ein Eckpfeiler für die effiziente und zügige Bereitstellung digitaler Dienste. Identity-API-Plattformen bündeln IAM-, CIAM- und IDaaS-Funktionen und stellen sie über APIs zur Verfügung.

Die Vorteile, die aus dem Einsatz einer Identity API-Plattform entstehen, sind offensichtlich: Sie ermöglichen eine effiziente Implementierung und Wiederverwendung von Identity Services über alle in einem Unternehmen entwickelten digitalen Plattformen und Dienste hinweg. Aufgrund ihrer Entwicklerfreundlichkeit sind sie leicht zu erlernen und für digitale Dienste einzusetzen.

[1] „Customer Journey“ = Zusammenfassender Begriff für die einzelnen Phasen, die ein Kunde durchläuft, bis er sich für den Kauf eines Produktes oder einer Dienstleistung entscheidet. Oft wird hierbei auch die Gesamtheit der Kundenbeziehung über einen potentiell langen Zeitraum und damit über die erste Kaufentscheidung hinaus betrachtet.

Da Identität im Mittelpunkt der Beziehung zwischen Individuen und Unternehmen steht, ist der richtige Umgang mit Identitäten entscheidend für den Erfolg. Eine Identitäts-API-Plattform muss Teil der IT-Strategie eines Unternehmens werden, die die Authentifizierung von Kunden und anderen Subjekten vereinheitlicht. Die bloße Verwendung von Identitäten als isolierte Punktlösung in einer 1:1-Beziehung zu einem digitalen Dienst ist nicht gut genug. Der größtmögliche Wert kann nur erreicht werden, wenn alle digitalen Dienste die gleiche Identitätsplattform nutzen.

Auth0 zählt zu den führenden Anbietern von Identity-API-Plattformen mit Niederlassungen in Bellevue, WA (USA), London, Buenos Aires, Sydney und Tokio. Auth0 wurde von zwei Microsoft-Veteranen gegründet und ist ein Pionier auf dem Gebiet der API-orientierten Identitätsdienste. Auth0 kann eine Reihe von IAM-Anwendungsfällen unterstützen, darunter CIAM, B2B und B2E. Somit ist Auth0 bestens aufgestellt, um die Identitätsplattform für digitale Anwendungen für jede Art von Unternehmen zu werden.

2 Highlights

- Zentrale Rolle von Identitäten für den Erfolg von digitalen Unternehmensdienstleistungen und Unternehmensapplikationen
- Notwendigkeit, die Customer Journey zu vereinfachen, von der Registrierung über die Authentifizierung bis hin zur Profilanreicherung
- Identitäts-API-Plattformen können einen standardisierten Identitätsansatz für alle Anwendungen liefern
- Warum eine Identity API-Plattform ein strategischer Dienst in der digitalen Infrastruktur sein sollte
- Best Practice-Empfehlungen für die Auswahl einer Identity API-Plattform
- Vorteile von Identity-API-Plattformen auf einen Blick
- Der Auth0-Ansatz zur Bereitstellung einer Identitäts-API-Plattform
- Aktionsplan für den Übergang zu einem strategischen Identitätsansatz

3 Identitäten sind überall - in jedem einzelnen digitalen Dienst und in jeder App

Bei der Gestaltung digitaler Dienste geht es immer auch um die Verwaltung der digitalen Identitäten von Verbrauchern, Kunden und Geschäftspartnern. Die Fähigkeit, diese digitalen Identitäten bestmöglich zu verwalten, ist ein wichtiger Erfolgsfaktor für Unternehmen, denn dies erfolgt bereits beim ersten Zugang zu ihren Diensten.

Seit mehr als zwei Jahrzehnten sind Unternehmen zunehmend digitaler geworden. Diese digitale Transformation begann schon vor langer Zeit, weit bevor der Begriff allgemein verwendet wurde. Es liegt in der Natur eines jeden digitalen Dienstes, dass er Verbraucher, Kunden und Partner mit Unternehmen verbindet. Unternehmen versuchen, so eng wie möglich mit diesen Zielgruppen zu interagieren, indem sie ihnen digitale Dienstleistungen anbieten und somit ihre Erlöse von herkömmlichen, physikalischen Verkaufsstätten auf digital erzielte Erlöse verlagern.

Eine wesentliche Rahmenbedingung in dieser Beziehung ist, wenn der Konsument schließlich zu einer identifizierten Person wird, d.h. zu einem digitalen Kunden. Dies ist der Wendepunkt vom anonymen Verbraucher zum wohlbekannten Kunden, an dem der Lebenszyklus einer digitalen Identität ihren Anfang nimmt und die eigentliche Geschäftsbeziehung beginnt.

Die Registrierung ist der Wendepunkt vom anonymen Konsumenten zum Kunden - dort, wo der Lebenszyklus einer digitalen Identität beginnt.

Zu diesem Zeitpunkt stehen Unternehmen vor der Herausforderung, die Identität ihrer zukünftigen Kunden zu überprüfen und einen Registrierungsprozess durchzuführen, ohne dabei den Konsumenten auf dem Weg zum (hoffentlich zahlenden) Kunden zu verlieren. Unabhängig davon, ob Apps oder Browser verwendet werden, ist in der überwiegenden Mehrheit der Geschäftsfälle nach wie vor eine Identitätsprüfung und Registrierung erforderlich - auch wenn sie nur eine externe Identität auf ein internes Kundenkonto abbildet und einige Daten ergänzt, z.B. durch eine Profilanreicherung.

Für den einzelnen Kunden führt dies zu immer wiederkehrenden Registrierungen, in der Regel Dutzende davon innerhalb eines Jahres für alle möglichen digitalen Dienste, die er nutzen möchte. Es ist wahrscheinlich, dass keine einzige Person diesen an sich lästigen Ansatz wertschätzt, weshalb sich Unternehmen der Notwendigkeit einer guten Benutzererfahrung bewusst sein und auf eine solche konsequent hinarbeiten müssen.

Die Verringerung des Aufwands bei wiederkehrenden Registrierungen und die Vereinfachung des Onboardings von Kunden sind sehr aufwändig. Allerdings ist es nur ein Teil der Herausforderung. Denn zusätzlich neigen viele Unternehmen bei ihren Bemühungen, sich in Richtung Digitalisierung zu entwickeln, dazu, eine große Vielfalt an digitalen Diensten auf unkoordinierte Weise zu entwickeln. Es ist definitiv sinnvoll, die Anzahl der internen und externen Apps und webbasierten Dienste innerhalb des Unternehmens sowie die Anzahl der Benutzer solcher Dienste zu bestimmen.

Es könnte sich herausstellen, dass viele von ihnen nicht weit verbreitet sind. Schlimmer noch, es könnte sich herausstellen, dass der Zugriff aus ihnen heraus auf andere Anwendungen und Dienste des Unternehmens nicht ohne Bruch möglich ist, da der Kunde eine digitale Identität, die er bereits erworben hat, hierfür nicht nutzen kann.

Die Überzeugung vieler Unternehmen, dass sie die gesamte Customer Journey kontrollieren müssen, ist eine Illusion in den vernetzten, digitalen Ökosystemen von heute.

Der Weg vom anonymen Verbraucher zum bekannten, immer wiederkehrenden Kunden ist aus verschiedenen Gründen eine Herausforderung. Einer davon ist, dass viele Unternehmen glauben, dass sie die gesamte Customer Journey kontrollieren müssen, was in den heutigen vernetzten, digitalen Ökosystemen eine Fiktion ist.

Betrachten wir eine einfache Customer Journey: Zunächst authentifiziert sich eine Person gegenüber ihrem Gerät, wie beispielsweise einem Smartphone. Dieses Smartphone kann auch als Authentifikator für den Zugriff auf Apps und Dienste verwendet werden. Diese Authentifizierung wird von einem Identity Provider (IdP) verarbeitet, der ein internes Identifikationssystem sein kann, aber auch ein externer IdP wie Facebook oder Xing, ein regionaler IdP wie die Nordic Bank ID oder die deutschen Verimi und netID, oder etwas anderes sein kann. Wenn ein externer IdP verwendet wird, wird diese Identität einem vom Unternehmen verwalteten Identitätsdatensatz zugeordnet. Dieser kann beispielsweise zusätzliche Attribute oder Tracking-Daten beinhalten, um das Verhalten des Kunden besser zu verstehen. Schließlich existieren noch die Kundendatensätze in ERP- und CRM-Systemen.

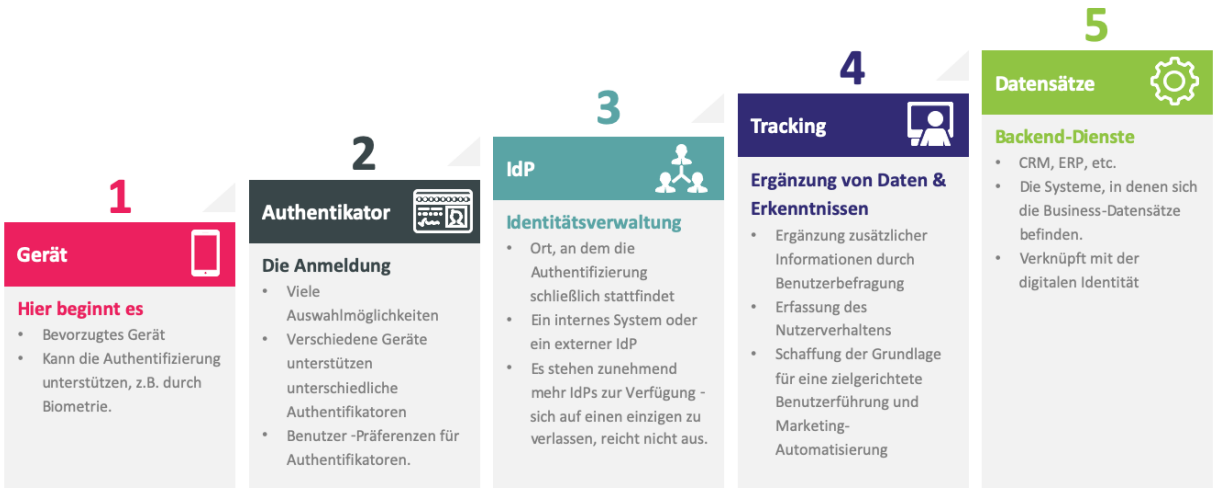

Abbildung 1: Authentifikatoren, Identitätsprovider (IdPs) und Kundendatensätze sollten gut voneinander abgegrenzt sein

Es gibt viele Arten, diese Customer Journey zu gestalten. Da Kunden Einzelpersonen sind, ist es ein Schlüssel zum Erfolg, ihnen die Wahl zu lassen, wie sie sich authentifizieren wollen. Wenn diese Reise zu umständlich ist, ist es eine erwiesene Tatsache, dass Menschen dazu neigen, diese abzubrechen. Die heutigen Standards und Serviceangebote ermöglichen eine Auswahl - die Wahl der Geräte, die Wahl der Authentifikatoren und die Wahl der IdPs.

Ein weiterer Grund dafür, dass Unternehmen zu komplexen und umständlichen Customer Journey über ihre verschiedenen Anwendungen und Dienste kommen, ist das Fehlen standardisierter Identitätsmanagement-Lösungen, die von Entwicklungsteams problemlos genutzt werden können. Wenn Entwickler den Registrierungsprozess beim Aufbau eines digitalen Dienstes "erfinden" müssen oder wenn sie herausfinden müssen, wie sie einen notwendigen Prozess mit einer guten Customer Journey kombinieren müssen, werden die Ergebnisse selten perfekt sein. Häufig sind Entwickler keine Experten für Identitäten, stehen aber unter dem Druck, etwas abzuliefern. Leider bedeutet dies, dass Sicherheit oder andere Schlüsselelemente einer guten Benutzererfahrung entweder übersehen oder aber geopfert werden, was das Unternehmen einem Risiko aussetzt. Wenn Entwickler nicht auch mit anderen Aspekten der Customer Journey verknüpft sind, was oft der Fall ist, werden Unternehmensteams zu isolierten Silos.

Identitäten sind eine Herausforderung für die agile Gestaltung digitaler Dienste, wenn es keine einheitliche, einfach zu bedienende Lösung gibt. Da Identität für jeden digitalen Dienst unerlässlich ist, ist die Bereitstellung von Identitätsdiensten, die auf einer standardisierten Plattform basieren, ein Muss für jedes digitale Unternehmen.

4 Umstieg von der Punktlösung zur strategischen Identitätsplattform

Identitäts-API-Plattformen sind ein unverzichtbarer, strategischer Service in modernen IT- und IAM-Infrastrukturen, die einen Grundumfang an Services über eine API-Schicht bereitstellen. Diese ermöglichen die Entkopplung von Identitäten von einzelnen Anwendungen.

Kernsysteme für das Identitätsmanagement werden allgemein als Identitätsplattformen oder Identitäts-API-Plattformen bezeichnet. API steht für Application Programming Interface, d.h. die technische Schnittstelle, mit der ein Entwickler Kern-Services aufrufen kann, wie sie für die Authentifizierung von Benutzern, die Registrierung oder andere Aufgaben rund um die Identitätsverwaltung und die Customer Journey erforderlich sind.

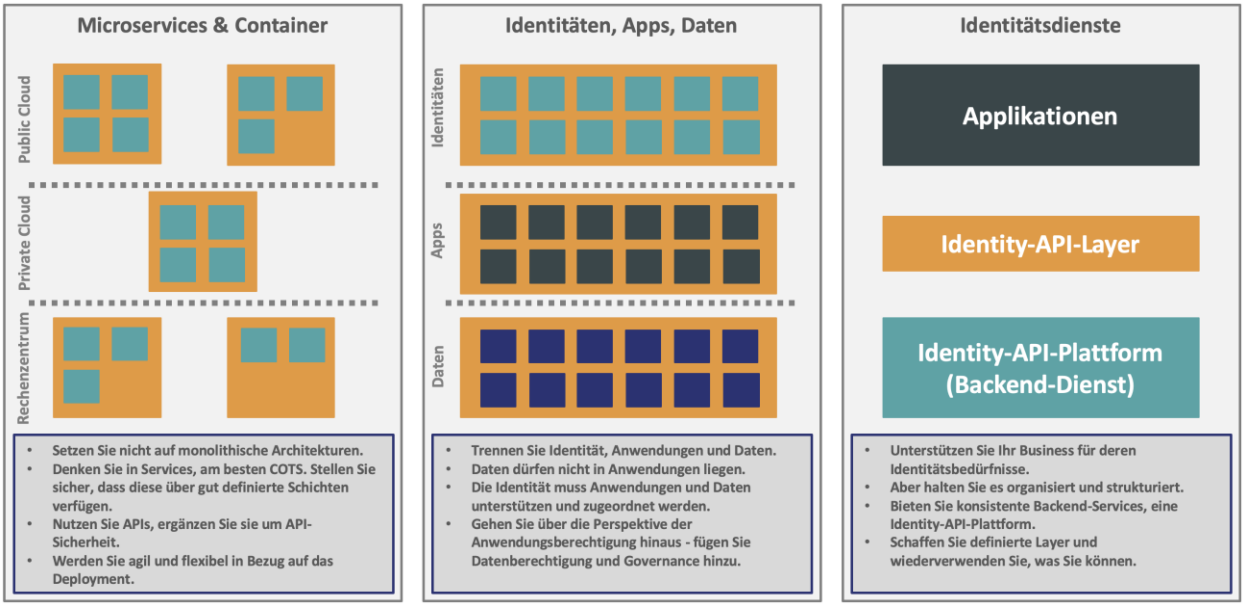

Abbildung 2: Ansätze für die richtige Umsetzung von Identitäten in modernen digitalen Diensten

Die folgenden Dienste sind Teil von drei grundlegenden Paradigmen bei der richtigen Ausgestaltung von Identitäten in modernen, digitalen Unternehmen:

1. **Mikroservices und Container:** Das heute etablierte Paradigma in der Softwarearchitektur konzentriert sich auf die Schaffung von Mikroservices mit gut abgegrenzten Funktionalitäten. Dazu gehören nicht nur Services für die Business-Funktionalitäten, sondern auch grundlegende Funktionen wie Authentifizierung, Benutzerverwaltung, Verschlüsselung oder andere Identitäts- und Sicherheitsdienste. Für moderne Anwendungen sind diese Dienste sorgfältig zu definieren und als Standardkomponente für eine Vielzahl von Anwendungen bereitzustellen. Das Setzen auf Mikroservices ermöglicht nicht nur die grundlegende Bereitstellung von Standard-Diensten etwa für Identitäten, sondern auch deren effiziente Bereitstellung in verschiedenen Implementierungsmodellen und deren Skalierung, basierend auf Container- oder auch serverlosen Infrastrukturen.
2. **Abgrenzung zwischen Applikationen, Identitäten und Daten:** Identitäten dürfen nicht nur einer einzigen Anwendung "gehören". Auch Daten sollten separiert werden, damit mehrere Anwendungen und Dienste diese Daten nutzen können. Eine solche Abgrenzung führt zwangsläufig zu eigenständigen Identitätsdiensten.
3. **Identity API Schichten und Plattformen:** Eine Konsequenz solcher Architekturen ist der Bedarf an Identitäts-Backend-Services, d.h. Identitäts-API-Plattformen, die ihre Dienste als Identitäts-API-Schicht darstellen. Anwendungen können dann diese Dienste nutzen, anstatt eigene, eingeschränkte Identitätsdienste neu zu schaffen.

Um digitale Dienste in einem agilen Ansatz bereitzustellen, müssen diese Paradigmen eingehalten werden. Agile Entwicklung erfordert eine robuste Anwendungsarchitektur und einen bewährten Rahmen durchdachter Core Services.

Agile Entwicklung erfordert eine solide Anwendungsarchitektur und einen bewährten Rahmen von gut ausgearbeiteten Core Services - mit Identitätslösungen im Mittelpunkt.

Obwohl sich diese Kerndienste nicht auf das Identitätsmanagement beschränken, sind Identity-API-Plattformen ein Eckpfeiler für die effiziente und zügige Erbringung digitaler Dienste. Daher sollte Identität als strategischer Service behandelt werden, der die gesamte IT-Infrastruktur unterstützt.

5 Die digitale Transformation und die Vorteile von Identity API-Plattformen

Identity-API-Plattformen richten sich an Entwickler, die Anwendungen entwickeln müssen, die gleichzeitig sicher sind und eine hervorragende Anwenderfreundlichkeit bieten. Daher müssen diese mit einer starken Developer-Unterstützung und ausgeklügelten APIs für die unterschiedlichen Bereiche der Verwaltung digitaler Identitäten für heutige digitale Diensten ausgestattet sein.

Eine Vielzahl von Faktoren treibt heute die digitale Transformation auf dem Markt voran. Einer dieser Faktoren ist die Veränderung der Art und Weise, wie Unternehmen mit ihren Verbrauchern interagieren, die wiederum eine Veränderung der von ihnen angebotenen Dienstleistungen erwarten. Ein weiterer Faktor ist eher technisch bedingt, wenn es um die Implementierung neuer digitaler Anwendungen und Dienste geht, die aufgrund der verschiedenen Umgebungen und der vielen zu berücksichtigenden Integrationspunkte komplexer geworden sind. Dies treibt die rasant wachsende Nachfrage nach der Bereitstellung und Nutzung von APIs voran. APIs befähigen Unternehmen, neue Geschäftsmodelle zu entwickeln, mit Partnern und Kunden in Kontakt zu treten und gleichzeitig ein durchgängiges Erlebnis zu schaffen, indem sie Systeme und Dienste miteinander vernetzen.

Infolgedessen wird es notwendig, die Verfügbarkeit von Identity-API-Plattformen zu beobachten. Dieser aufstrebende Markt wird durch die Herausforderung getrieben, die sich abzeichnenden IT-Anforderungen von digitalen Unternehmen zu erfüllen. Dazu gehört die Unterstützung der vielfältigen funktionalen Anforderungen an die Verwaltung von Identitäten, die Föderierung von und zu IdPs und die Unterstützung sämtlicher Benutzer, von Mitarbeitern und Geschäftspartnern bis hin zu Kunden und Konsumenten.

Durch die Bereitstellung von Schlüsselfunktionalitäten über APIs werden Workflow- und Orchestrierungsfunktionen über alle Umgebungen hinweg ermöglicht, ebenso wie eine bessere DevOps-Unterstützung durch Automatisierung. Ein weiteres kritisches Charakteristikum von Identity API-Plattformen ist der Fokus auf Entwicklerfreundlichkeit. Kurz gesagt, IAM entwickelt sich ständig weiter, um die ständig zunehmende Zahl von IAM-Anforderungen zu erfüllen.

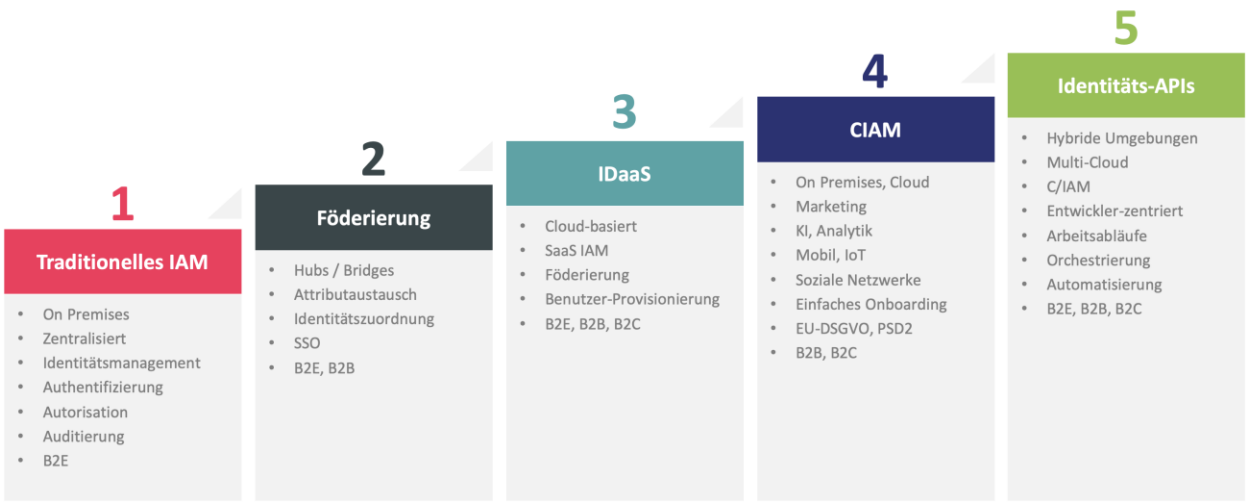

Abbildung 3: Entwicklung des IAM im Laufe der Zeit

Identitäts-API-Plattformen weisen viele Funktionalitäten auf, die in den Marktsegmenten IAM (Identity and Access Management), CIAM (Consumer IAM), IDaaS (Identity-as-a-Service) und Adaptive Authentication/Consumer Authentication zu finden sind. Tatsächlich bedienen viele der heute auf dem Markt erhältlichen Angebote mehrere dieser Segmente. Obwohl es zwischen diesen Segmenten Querschnittsfunktionen gibt, müssen Identity-API-Plattformen in jedem Fall die Grundfunktionen von Identitäts- und Benutzerverwaltung, Authentifizierung, Autorisierung und Unterstützung für das Auditing unterstützen. Die Identity API-Plattformen können auf der Grundlage der Anwendungsfallbeispiele für das Zielmarktumfeld um weitere Funktionen erweitert werden. Ein Anwendungsfall könnte beispielsweise ein Zustimmungsmanagement für Benutzer (wie im CIAM), eine Federation (wie bei IDaaS), eine intelligentere Authentifizierung (wie bei der Adaptiven Authentifizierung) sowie die Unterstützung von Compliance und Access Governance (wie bei IGA-Lösungen) erfordern. Über diese Fähigkeiten hinaus werden auch sich weiterentwickelnde Anforderungen wie IoT, Workflows und Orchestrierung, DevOps und API-Sicherheitsfunktionen berücksichtigt.

Die Unterschiede zwischen Identitäts-API-Plattformen und den in der Vergangenheit angebotenen COTS-Lösungen (Commercial off-the-shelf) ergeben sich aus ihren Anwendungsfällen. Die Anwendungsfälle der Identitäts-API-Plattform konzentrieren sich auf Anbieter, die es Kunden ermöglichen, ihre Identitätslösungen für definierte Dienste über APIs aufzubauen, sei es vor Ort im eigenen Rechenzentrum, in der Cloud oder in hybriden Umgebungen. Andere Anwendungsfälle der Identitäts-API-Plattform richten sich an Unternehmen, die aufgrund der Komplexität interner Prozesse und anderer betrieblicher Gründe eine eigene C/IAM-Plattform aufbauen, bestehende IAM-Funktionen automatisieren oder erweitern möchten. Auch wenn traditionelle schlüsselfertige COTS in erster Linie von der Benutzeroberfläche gesteuert werden, erfordern die Anwendungsfälle von Identitäts-API-Plattformen, dass die Lösung anpassbar ist und COTS API Toolkits wie Widgets und SDKs bereitstellen kann, die eine schnelle Entwicklung hin zu einer reinen API-Plattform ermöglichen.

Da Identity-API-Plattformen entwicklerfreundlich sind, sind praktische Online-Entwicklerportale mit der entsprechenden API-Dokumentation und Codebeispielen erforderlich, um ein gutes Entwickler-Ökosystem zu fördern.

Ein entscheidendes Merkmal von Identity API-Plattformen ist ihre Fokussierung auf Entwicklerfreundlichkeit.

Zu den wichtigsten Funktionen der Identitäts-API-Plattformen gehören:

Identitäts- und Benutzerverwaltungs-APIs	APIs, die die Verwaltung von Identitäten und Benutzerkonten ermöglichen, einschließlich der damit verbundenen Verzeichnisdienste und Datenbanken.
Authentifizierungs-APIs	Unterstützung von Authentifizierungsmethoden über APIs im Bereich von Benutzername/Passwort bis hin zu Biometrie und allem dazwischen. Außerdem Berücksichtigung von SSO und Bereitstellung von Session-Management.
Autorisierungs-APIs	APIs, die die Berechtigungen von Benutzern oder Administratoren auf Ressourcen steuern, wie z.B. Policy Management, rollenbasierte Zugriffskontrolle (RBAC) oder dynamische Berechtigungen.
Auditierungs- und Compliance-APIs	APIs, die die Überwachung des Zugriffs eines Benutzers auf Ressourcen oder die Änderungen eines Administrators am System unterstützen. APIs, die Audit- und forensische Funktionen bereitstellen, um beispielsweise bei branchenspezifischen Compliance-Anwendungsfällen und der Analyse von Sicherheitsvorfällen zu helfen.

Workflow- und Orchestrierungs-APIs	APIs, die die Automatisierung von Workflows wie z.B. Zugriffsanforderungen, Selbstregistrierung oder Einwilligung von Benutzern ermöglichen, darüber hinaus auch die Automatisierung der Orchestrierung von mehr als einem Workflow oder einer Aktivität.
API-Security	Die Funktionalität einer Anwendung, APIs gegen Cyberangriffe und andere Bedrohungen mithilfe von Methoden wie Verschlüsselung, Häufigkeitsbegrenzung, Inhaltsfilterung und Schemavalidierung zu schützen.
DevOps-APIs	APIs, die sowohl Entwicklern als auch dem Betriebsteam Unterstützungsoptionen für die jeweilige IT-Umgebung mit ihren Tools, der Automatisierung und der kontinuierlichen Integration bieten.
API-Entwicklerunterstützung	Die Fähigkeit des Herstellers, die Entwickler bei der Nutzung der Anwendungs-APIs durch Dokumentation, Tutorials und Tools sowie durch eine Wissensdatenbank und durch Community-Support / -Plattform für Entwickler zu unterstützen.

Die Vorteile, die sich aus dem Einsatz einer Identity API-Plattform ergeben, sind offensichtlich: Sie ermöglichen eine effiziente Implementierung und Wiederverwendung von Identitätsdiensten über alle digitalen Plattformen und Dienste hinweg, die ein Unternehmen entwickelt. Aufgrund ihrer Entwicklerfreundlichkeit sind sie leicht zu verstehen und können somit einfach in digitalen Diensten verwendet werden.

Auch hier ist es wichtig, dass eine Identitäts-API-Plattform Teil der IT-Strategie eines Unternehmens werden muss, um die Authentifizierung von Kunden und anderen Entitäten zu vereinheitlichen. Die bloße Verwendung von Identitäten als Punktlösung in einer 1:1-Beziehung mit nur einem digitalen Dienst ist nicht ausreichend. Nur wenn alle digitalen Dienste die gleiche Identitätsplattform nutzen, wird der größtmögliche Nutzen erzielt.

6 Der Auth0-Ansatz für Identity-API-Plattformen

Auth0 zählt mit einem Cloud-basierten Angebot, das umfangreiche API-Unterstützung speziell für die Authentifizierung und Autorisierung von Benutzern bietet, zu den führenden Anbietern von Identity-API-Plattformen.

Auth0 zählt zu den führenden Anbietern von Identity API Plattformen mit Niederlassungen in Bellevue, WA (USA), London, Buenos Aires, Sydney und Tokio. Auth0 wurde von zwei Microsoft-Veteranen gegründet und ist ein Pionier auf dem Gebiet der API-orientierten Identitätsdienste. Auth0 bietet Unterstützung für eine Vielzahl von IAM-Anwendungsfällen, darunter CIAM, B2B und B2E. Die Deployment-Modelle sind Cloud-basiert, hierzu gehören Public, Private und Managed Private Cloud-Angebote.

Von zwei Microsoft-Veteranen gegründet, ist Auth0 ein Pionier bei API-basierten Identitätsdiensten.

Die APIs von Auth0 sind in erster Linie als REST/JSON ausgelegt. Eine Besonderheit hierbei ist, dass Auth0 eine RESTful-Schnittstelle zu fast ihrem gesamten Management-Framework über ihre Management-APIs bietet, die es Kunden ermöglicht, verschiedene Aspekte ihres Auth0-Kontos zu verwalten. Die meisten Kunden greifen somit über DeployCLI auf die Management-API von Auth0 zu.

Standardmäßig speichert Auth0 die Zugangsdaten der Benutzer in einer Datenbank, wobei Kunden jedoch auch ihr eigenes Nutzerverwaltung verwenden können. Auth0 unterstützt out-of-the-box Microsoft Azure AD sowie die Möglichkeit der Authentifizierung gegenüber MS AD, LDAP und der integrierten Windows-Authentifizierung (Kerberos). Weiterhin kann Auth0 Benutzer über APIs gegenüber jedem Identity Provider authentifizieren.

Für die Föderierung von Identitäten werden eine Vielzahl von Identity Provider-Verbindungen standardmäßig bereitgestellt, inklusive Verbindungen zu social media, Unternehmens-IdPs, Datenbanken und passwortlose Verbindungen. Auth0 unterstützt OIDC, OAuth, SAML und WS-Federation. Deren föderierte Identitätsverbindungen bieten eine SSO-Funktionalität, die es Benutzern ermöglicht, sich zu authentifizieren. Provisionierung von und zu anderen Cloud-Diensten wird ausschliessliche über bestimmte Cloud-Service-APIs, wie z.B. Azure AD, bereitgestellt. Authentifizierungs-APIs werden mit den gängigsten Formularen und Standards weitgehend unterstützt, aber mit einigen Ausnahmen wie FIDO UAF & U2F. Auth0 unterstützt auch eine breite Palette von Anmeldungen über soziale Netzwerke zur föderierten Authentifizierung.

Die Auth0-Plattform verfügt über ein integriertes Werkzeug zur Erkennung von Anomalien zum Schutz vor Angriffen sowie die Möglichkeit, die Fähigkeiten des integrierten Tools durch eigene Regeln zu erweitern. Auth0 bietet darüber hinaus Schutz vor Brute-Force-Angriffen und die Erkennung von Passwortlecks. Eine der größten Stärken von Auth0 sind die Entwicklertools, der Online-Support und das umfassende Ökosystem.

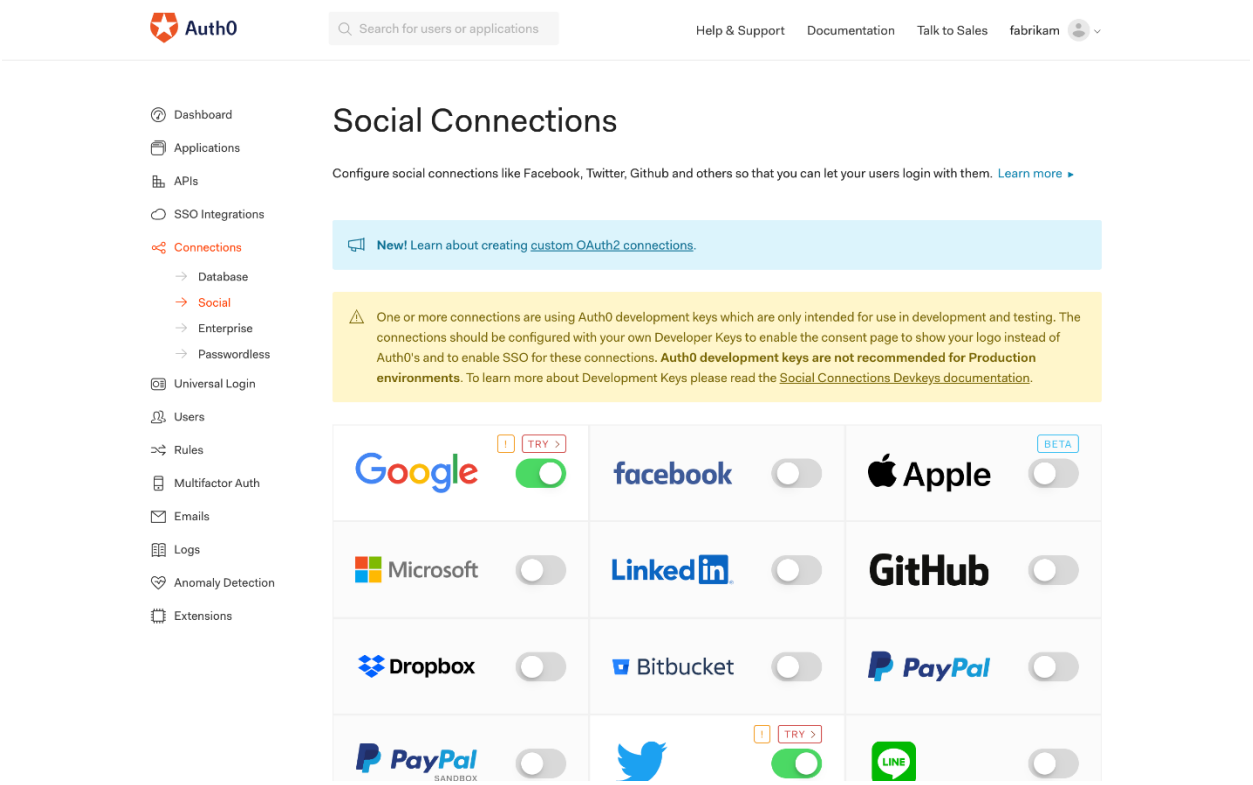

Abbildung 4: Eine gut durchdachte Benutzeroberfläche für die Verwaltung der Identity-APIs.

Zu den wichtigsten Funktionen der Auth0-Plattform gehören:

- Single Sign On: Ermöglichung von Single Sign On (SSO) für alle Dienste und Anwendungen, die die Auth0-Plattform nutzen.
- Universelles Login: Auth0's neueste Implementierung des Login-Workflows, die es Entwicklern ermöglicht, ihre markenspezifische Authentifizierungserfahrung schnell und zentral vollständig anzupassen, ungeachtet der Authentifizierungs- und Autorisierungsfunktionen, von denen sie abhängen, wie soziale Netzwerke, Multifaktor-Authentifizierung (MFA), Anomalie-Erkennung, etc.
- Passwortsicherheit & Passwordless: Während Passwörter unterstützt und geschützt werden, gibt es auch eine breite Unterstützung für eine passwortlose Authentifizierung
- Multi-Faktor-Authentifizierung: Abhängig von den Anforderungen aus Risiko- und Sicherheitssicht wird MFA durch eine Vielzahl von Methoden unterstützt, darunter SMS, Einmalpasswort, Authentifikatoren von Drittanbietern und Push-Benachrichtigungen. Dies ermöglicht es Unternehmen, die geforderte Authentifizierungsstärke für kritische Dienste zu steigern.

- API-basierter Zugriff: Auch wenn immer noch ein Großteil des Zugriffs von Menschen über Websites erfolgt, so geschieht doch immer mehr Zugriff aus Anwendungen, Apps oder Diensten über APIs. Dies wird von Auth0 gut unterstützt.
- Benutzerverwaltung: Letztlich stehen Funktionen zur Verwaltung des Benutzers und seiner Customer Journey zur Verfügung, einschließlich progressiver Profilerstellung, Kontoverknüpfungen und Profilanreicherung durch Drittanbieterintegration.

Der Schwerpunkt von Auth0 liegt auf dem Registrierungs- und Authentisierungsprozess der Benutzer, dem wesentlichen Element auf jeder Customer Journey. Damit ist Auth0 gut positioniert, die Identitätsplattform für digitale Anwendungen, für jede erdenkliche Art von Unternehmen zu werden. Insbesondere sollten Ansätze wie der von Auth0 als strategische Plattform positioniert werden, um Identitätsdienste nicht nur für einzelne Anwendungen bereitzustellen. Der Nutzen von Auth0 ergibt sich insbesondere erst aus der Nutzung dieser Plattform als Standardansatz für Identitäten.

Auth0 ist ein globales Unternehmen mit Kunden in über 70 Ländern in Nordamerika, Lateinamerika, EMEA und dem asiatisch-pazifischen Raum. Ein gutes weltweites Netzwerk von Systemintegrator-Partnern steht den Kunden ebenfalls zur Verfügung. Mit dem Fokus von Auth0 auf gute Entwicklerunterstützung und ein Ökosystem zum schnellen Aufbau von Identitätsdiensten positioniert sich Auth0 als einer der Marktführer im aufstrebenden Markt für Identitäts-API-Plattformen. KuppingerCole hat das Unternehmen auch als Branchen- und Technologieführer bei CIAM-, IDaaS- und Identitäts-API-Plattformen in jeder unserer jeweiligen Leadership Compass-Studien anerkannt.

7 Maßnahmenplan für die Implementierung von Identity-API-Plattformen

Bei der Entscheidung für eine Identity API-Plattform hängt der Ansatz stark von der bestehenden IAM-Infrastruktur ab. Es ist einfacher, von oben nach unten zu beginnen, als verschiedene bestehende Lösungen zu konsolidieren. Beides ist jedoch mit Identity-API-Plattformen möglich.

Wie in diesem Dokument erläutert, gibt es einen konkreten, unternehmerischen Bedarf an Identity-API-Plattformen. Sie sind der Grundbaustein jeder Infrastruktur für die agile Entwicklung und Bereitstellung digitaler Anwendungen und Dienste und unterstützen sowohl die Interaktion mit Geschäftspartnern als auch mit Kunden.

Viele Unternehmen nutzen bereits spezifische Lösungen für die Verwaltung ihrer Partner- und Kundenidentitäten. Allerdings werden die meisten Implementierungen solcher Lösungen nicht strategisch vom Unternehmen gesteuert, sondern "passieren", wenn Entwickler selbst ihre Identitäten gestalten oder nach einer schnellen Lösung suchen.

Bei der Erstellung eines Maßnahmenplans sind verschiedene Gesichtspunkte zu berücksichtigen, je nachdem, ob das Unternehmen die Aktivitäten zunächst in einer einheitlichen Strategie für Identity-API-Plattformen koordinieren und bündeln muss oder ob es top-down beginnen kann.

Von der Taktik zur Strategie:

1. Untersuchen Sie, welche Ansätze und Tools/Dienstleistungen es bereits gibt, um die Identitäten von Verbrauchern, Kunden und Geschäftspartnern zu verwalten.
2. Holen Sie Ihre Architekten, Entwickler, das Produktmanagement, die IT-Sicherheit, Ihr IAM-Team und auch Ihr Marketing-Team mit an Bord - diese müssen Hand in Hand an einem strategischen Ansatz arbeiten.
3. Konzentrieren Sie sich auf die neuen Lösungen, die auf der Grundlage der Anforderungen an Identitäten konsolidiert und durch zusätzliche Komponenten für gemeinsame Erfordernisse wie Benutzerregistrierung oder Passwortrücksetzung unterstützt werden sollen.
4. Definieren Sie Ihre Strategie für die Integration mit bestehenden Lösungen oder migrieren Sie diese auf Ihre zukünftige Plattform. Die Herausforderung bei einer solchen Vorgehensweise besteht immer darin, Benutzer auf eine neue digitale Identität umzustellen - vermeiden Sie dies, wo immer möglich, aber tun Sie es frühzeitig, wenn Sie müssen.
5. Fügen Sie alles aus dem strategischen Ansatz (unten) hinzu, was fehlt.
6. Die Verwendung einer strategischen Identity-API-Plattform muss konsequent forciert werden.

Wie immer ist es problematischer, unterschiedliche Versionen zu konsolidieren - aber wenn man es nicht tut, wird die Situation mit der Zeit nur noch schlimmer.

Von der Strategie zur Taktik:

1. Holen Sie Ihre Architekten, Entwickler, das Produktmanagement, die IT-Sicherheit, Ihr IAM-Team und auch Ihr Marketing-Team mit an Bord - diese müssen Hand in Hand an einem strategischen Ansatz arbeiten.
2. Definieren Sie Ihren Ansatz für die Verwendung einer Identitäts-API-Plattform, z.B. wann APIs verwendet werden sollen, wo Widgets wie Registrierung oder Passwort-Rücksetzung erforderlich sind, wer die Verantwortung übernimmt, welche Integrationen erforderlich sind, etc.
3. Erarbeiten Sie Ihre Anforderungen und selektieren Sie die optimale Lösung.
4. Implementieren Sie diese Lösung und harmonisieren Sie sie sorgfältig mit Ihrem DevOps-Ansatz und Ihrer Customer Journey.
5. Die Verwendung einer strategischen Identity-API-Plattform muss konsequent forciert werden.

8 Urheberrechte

Die Zukunft der Informationssicherheit – Heute

KuppingerCole Analysts unterstützt IT-Fachleute mit herausragendem Fachwissen bei der Ausarbeitung von IT-Strategien und damit verbundenen Entscheidungsprozessen. Als führende Analysefirma bietet KuppingerCole Analysts anbieterneutrale Informationen aus erster Hand. Mit unseren Dienstleistungen haben Sie einen sicheren und zuverlässigen Partner an Ihrer Seite, um essentielle Entscheidungen für Ihr Unternehmen zu treffen.

KuppingerCole Analysts ist seit seiner Gründung im Jahr 2004 eine in Europa ansässige Analysefirma mit Fokus auf Informationssicherheit und Identity- and Access Management (IAM). KuppingerCole Analysts steht für Fachwissen, Vordenken, herausragende praktische Relevanz und eine anbieterneutrale Sicht auf die Marksegmente der Informationssicherheit. Alle wichtigen Aspekte werden abgedeckt: Identity and Access Management (IAM), Unternehmensverfassung und Abschlussprüfung, Sicherheit in der Cloud und in virtuellen Umgebungen, Informationsschutz, Mobilfunk- und Softwaresicherheit, System- und Netzwerksicherheit, Sicherheitskontrolle, Analyse und Berichterstattung, Unternehmensführung, Organisation und Richtlinien.

Für weitere Informationen kontaktieren Sie bitte clients@kuppingercole.com

KuppingerCole Analysts AG
Wilhelmstrasse 20 - 22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com