LERNEN LEICHT GEMACHT

Auth0-Sonderausgabe

Identity as a Service (IDaaS)

für dummies

Was ist Identity as a Service (IDaaS)?

Sicherheitsherausforderungen und Anwendungsbeispiele

Führen Sie moderne Identität ein

Präsentiert von

auth0

Lawrence C. Miller

Frederico Hakamine

Über Auth0

Auth0 bietet eine Plattform für die Authentifizierung, Autorisierung und Sicherung des Zugriffs für Anwendungen, Geräte und Benutzer. Sicherheits- und Anwendungsteams verlassen sich auf die Einfachheit, Erweiterbarkeit und das Know-how von Auth0, um Nutzen aus dem Identitätsmanagement zu ziehen. Auth0 sichert jeden Monat mehr als 4,5 Milliarden Anmeldetransaktionen und dadurch gleichzeitig auch Identitäten, damit sich Unternehmen auf Innovationen konzentrieren können. Zudem ermöglicht Auth0 es globalen Unternehmen, ihren Kunden weltweit zuverlässige, erstklassige digitale Erlebnisse zu bieten.

Identity as a Service (IDaaS)

Auth0-Sonderausgabe

Von Lawrence C. Miller und Frederico Hakamine

für dummies®

Identity as a Service (IDaaS) für Dummies®, Auth0-Sonderausgabe

Veröffentlicht von
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 070305774
www.wiley.com

ISBN 978-1-119-86665-7 (pbk); ISBN 978-1-119-86666-4 (ebk)

Hergestellt in den Vereinigten Staaten von Amerika.

10 9 8 7 6 5 4 3 2 1

Danksagung des Verlags

Wir sind stolz auf dieses Buch und die Personen, die daran mitgewirkt haben. Die folgenden Personen haben an der Erstellung dieses Buches mitgewirkt:

Project Editor: Martin V. Minner
Editorial Manager: Rev Mengle
Associate Publisher: Katie Mohr
Business Development Representative: Frazer Hossack, Karen Hattan
Production Editor: Mohammed Zafar Ali

Inhaltsverzeichnis

Einführung

Wenn Unternehmen expandieren und wachsen, passen sie die eingesetzten Anwendungen an, um ihre Netzwerke und Betriebsabläufe zu optimieren. Während Mitarbeiter früher vielleicht nur ein Passwort und einen Benutzernamen hatten, muss die IT heute Hunderte von Anmeldedaten für On-Premises- und Software as a Service-Apps (SaaS) verwalten, die auf unterschiedlichen Plattformen und Geräten laufen.

In ähnlicher Weise bieten viele Unternehmen jetzt Online-Produkte und -Dienstleistungen an, für die sich ihre Kunden bei einem sicheren Konto anmelden müssen. Die IT muss deshalb jetzt Millionen von Anmeldedaten für die weltweiten Kunden des Unternehmens verwalten.

Hinzu kommt, dass Benutzer eines der Hauptziele von Angriffen sind. Laut einem vor Kurzem von Verizon veröffentlichten „Data Breach Investigations Report (DBIR)" werden 81 % der Datenschutzverletzungen durch schwache oder gestohlene Anmeldedaten verursacht. Zur Verringerung dieser Bedrohungen brauchen Unternehmen unterschiedliche Methoden zur Authentifizierung einer Benutzeridentität. Passwörter allein sind nicht mehr ausreichend.

IT-Abteilungen wissen, dass schon ein einziger Ausrutscher in puncto Sicherheit das Aus für ein Unternehmen bedeuten kann. IAM-Lösungen ermöglichen ihnen den Ausbau ihres Identitäts- und Zugriffsmanagements, damit sie Hunderttausende Mitarbeiter ebenso schnell und verlässlich verwalten können wie nur zehn und damit die Verwaltung auch für Zehntausende oder Millionen Kunden einfach bleibt. Diese Lösungen schützen Anmeldedaten von Benutzern ebenso wie sensible Daten und befreien das Personal von zeitaufwendigen manuellen Aufgaben, wie etwa dem Zurücksetzen von Passwörtern und der Kontobereitstellung, so dass es sich auf anspruchsvollere und wertschaffende Projekte konzentrieren kann, die das Wachstum und die Rentabilität des Unternehmens fördern.

Um IAM-Dienste in großem Maßstab nutzen zu können, stellt die Mehrheit der Unternehmen auf moderne Identität aus der Cloud um – Identity as a Service (IDaaS). IDaaS stellt robuste und skalierbare Identität bereit, damit Unternehmen den Benutzer- und Kundenzugriff verwalten und gewährleisten können, dass der Zugriff auf ihre Anwendungen und Dienste an jedem Ort der Welt und an jedem Gerät sicher möglich ist. In diesem Buch erfahren Sie, worum es bei moderner Identität geht und wie IDaaS Ihrem Unternehmen helfen kann.

Über dieses Buch

Dieses Buch besteht aus fünf Kapiteln, die sich mit den folgenden Themen befassen:

- Die Bedeutung von Identität, was sie ist und wie sie sich entwickelt hat (Kapitel 1)
- Was moderne Identität (Identity as a Service) ist und wie sie Unternehmen hilft, Identitätsherausforderungen und unterschiedliche Anwendungsfälle anzusprechen (Kapitel 2)
- Die Komponenten einer modernen Identitätslösung (Kapitel 3)
- Neue Trends und Innovationen, die der Zukunft von Identität Rechnung tragen (Kapitel 4)
- Leistungspotentiale und Vorteile der modernen Identität (Kapitel 5)

Jedes Kapitel ist in sich selbst geschlossen. Sie können deshalb einfach zu einem Thema springen, das Sie interessiert.

In diesem Buch verwendete Symbole

In diesem Buch verwenden wir gelegentlich einige spezielle Symbole, um auf wichtige Informationen aufmerksam zu machen. Sie werden auf die folgenden Hinweise stoßen:


MERKEN

Dieses Symbol macht auf Informationen aufmerksam, die Sie in Ihrem nichtflüchtigen Speicher bzw. Ihren grauen Zellen ablegen sollten – zusammen mit allen Jahres- und Geburtstagen!


TECHNISCHES

Wenn Sie in Zukunft mit Fachbegriffen und -wissen prahlen möchten, sind Sie hier an der richtigen Stelle! Dieses Symbol erläutert das Fachchinesisch hinter dem Fachchinesisch und signalisiert, dass hier etwas näher auf technische Details eingegangen wird.


TIPP

Tipps sind meist unerwartet, aber willkommen. Wir haben auf jeden Fall die Hoffnung, dass die Tipps in diesem Buch nützlich für Sie sein werden.

IN DIESEM KAPITEL

- Grundlegende Informationen zur Identität und ihrer Bedeutung
- Einführung in die unterschiedlichen Identitätsdomänen
- Die Entwicklung von Identitätsdiensten

Kapitel 1
Was ist Identität?

In diesem Kapitel untersuchen wir, was Identität eigentlich ist und warum sie so wichtig ist, welche unterschiedlichen Domänen des Identitätsmanagements es gibt und wie sich Identität entwickelt hat.

Was ist Identität und warum ist sie so wichtig?

Informationstechnologie ist seit jeher eine wertvolle Ressource, für die schon immer ein gewisses Maß an Kontrolle darüber erforderlich war, wer auf was zugreifen darf.

Frühe LANs (Local Area Networks) wurden zunächst für die gemeinsame Nutzung von Dateien und Druckern in Unternehmen eingerichtet – aber die wirklich kritischen Dateien und teuren Farblaserdrucker wurden nur mit den Führungskräften und dem Marketing geteilt! Die IT-Abteilung musste diese Führungskräfte und Marketingleute identifizieren können, um sicherzustellen, dass niemand sonst im Unternehmen Einblick in die Vertriebsprognosen erhielt oder wirklich großartige Grafiken drucken konnte.

Wenn wir noch weiter zurückblicken, war der Zugriff auf Großrechner (ca. 1960er Jahre) auf eine Handvoll von Leuten im Unternehmen beschränkt. Natürlich war zur Kontrolle des Zugriffs auf den Großrechner nichts weiter erforderlich als ein verschlossener Raum, und mit der Identität verhielt es sich recht einfach – wer keine Hornbrille trug oder ein Kugelschreiberetui bei sich hatte, hatte auch keinen Zutritt.

Identität und IT sind seit jeher untrennbar verbunden (siehe Abbildung 1-1).

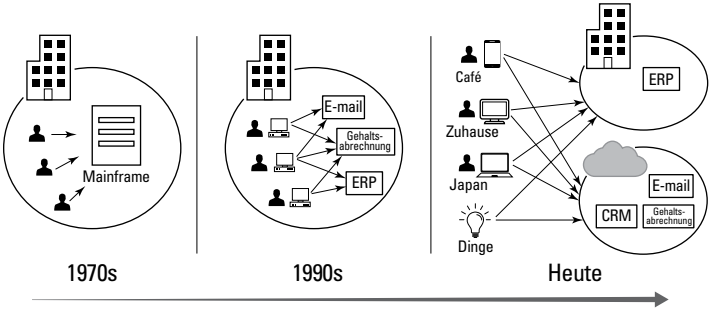

ABBILDUNG 1-1: Identität und IT sind seit jeher untrennbar verbunden. Mit der Weiterentwicklung der IT steigt auch die Nachfrage nach Lösungen, mit denen Personen und Dinge sicher mit Technologie verbunden werden können.

Bei jedem weiteren Entwicklungsschritt der IT gewinnen auch Identitäts- und Sicherheitslösungen an Bedeutung. Beispielsweise arbeiteten in den 1990er und frühen 2000er Jahren die Mitarbeiter eines Unternehmens in Bürogebäuden. Ihre Daten wurden durch eine zwischen dem Unternehmensnetzwerk und dem Internet erstellte Firewall geschützt. Mitarbeiter fuhren morgens ins Büro, stempelten an der Stechuhr ein und meldeten sich über ihre Rechner am Arbeitsplatz an. Am Ende des Tages meldeten sie sich an ihren Arbeitsplatzrechnern ab und gingen wieder nach Hause.

Dann kamen iPhones und Laptops in Mode und Mitarbeiter begannen, dynamischer zu arbeiten und mit Kollegen zu interagieren. Mitarbeiter lesen heute geschäftliche E-Mails auf ihren persönlichen Smartphones, chatten mit Freunden und senden Links aus sozialen Medien von ihren dienstlichen Laptops, die mit öffentlichen WLAN-Netzwerken in Cafés, Flughäfen und Hotellobbys verbunden sind. Die heutige Arbeitswelt – in der die Grenzen zwischen Privat- und Berufsleben zunehmend verschwimmen – hat mit der strikt getrennten, gut kontrollierten Arbeits- und Netzwerkumgebung der Vergangenheit rein gar nichts mehr gemeinsam.

Da Menschen mit der IT mittlerweile von jedem Gerät und jedem Ort aus interagieren und ihre Services nutzen, ist deren Schutz längst nicht mehr so einfach wie in Zeiten, als alle an ein Büro und an einen bestimmten Arbeitsplatzrechner gebunden waren und jedem, der sich innerhalb der Netzwerkabgrenzung befand, grundsätzlich vertraut werden konnte. Unternehmen müssen in der Lage sein, den Zugriff auf Apps für jeden Benutzer abzusichern und zugleich Sicherheitsfunktionen für unterschiedliche Netzwerk-, System- und Datenkontexte

durchzusetzen. Sie müssen zudem in der Lage sein, diese Identitäten über ein umfangreiches Ökosystem aus Mitarbeitern und Kunden hinweg auf einer Vielzahl von Systemen überall in der Welt skalierbar zu verwalten. Während sich die IT weiterentwickelt, werden Sie die Identität auch weiterhin als Schutzmaßnahme nutzen können.

MERKEN

Wann immer Sie gemeinsam genutzte Ressourcen oder vertrauliche Informationen besitzen, benötigen Sie eine Identität, um Personen sicher zu identifizieren, die diese Ressourcen nutzen oder einsehen. So können Sie einschränken, was eine Person tun darf (zum Beispiel, den Farblaserdrucker verwenden) oder verhindern, dass andere Personen Daten einsehen oder Dinge tun, die jemandem schaden könnten (zum Beispiel verbotenerweise deren Steuernummer auf der elektronischen Steuererklärung einsehen oder Waren bei Amazon mit der Kreditkarte einer anderen Person kaufen).

Unterscheidung der drei Identitätsdomänen

Identitätslösungen umfassen Technologien, die drei Probleme beheben sollen:

- Bestätigung und Verifizierung einer Identität
- Bestimmung der Zugriffsberechtigung und des Handlungsrahmens einer Identität
- Definition der Richtlinien und Prozesse, die zur Verwaltung von Identitäten innerhalb der Netzwerke und Systeme eines Unternehmens angewandt werden

Diese Technologien gehören drei Domänen an, die in Abbildung 1-2 dargestellt sind und in den folgenden drei Abschnitten beschrieben werden.

Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM)

Generell handelt es sich beim Identitäts- und Zugriffsmanagement bzw. IAM um Technologie für die Klassifizierung von Benutzern und Gruppen in einem Softwaresystem sowie der Ressourcen, auf die sie Zugriff erhalten, und der Funktionen, die sie ausführen können. IAM wird für die Adressenauthentifizierung, Kontoverwaltung und Zugriffskontrolle eingesetzt.

Die Lösung hilft Unternehmen zu kontrollieren, wer die Benutzer sind (hier kommt die Identität ins Spiel), auf welche Dienste sie zugreifen dürfen oder nicht und wie sie dies tun (Zugriffsmanagementkomponente).

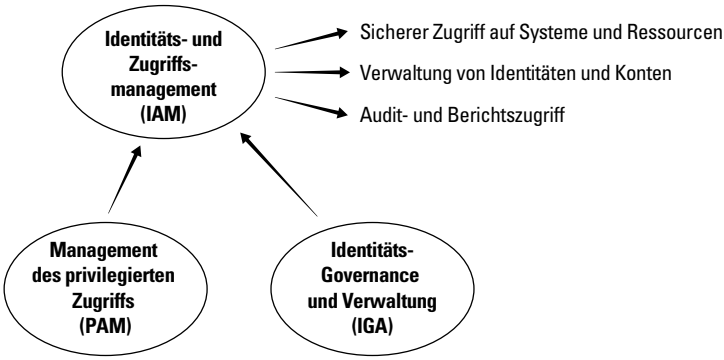

ABBILDUNG 1-2: Die drei Identitätsdomänen (IAM, PAM und IGA) und deren Interaktion.

MERKEN

IAM ist die grundlegende Identitätstechnologie und erfüllt die folgenden wichtigen Identitätsfunktionen:

- Speichern von Benutzerdaten, Richtlinien und Konfigurationen
- Verwaltung von Benutzerkonten und Anmeldedaten
- Bereitstellung und Entzug von Anwendungen und Ressourcen für Benutzer
- Authentifizierung von Benutzern
- Kontrolle des Zugriffs auf Anwendungen
- Prüfung von Identitäten, damit nachvollzogen werden kann, welche Person was und wann getan hat

Management des privilegierten Zugriffs (Privileged Access Management, PAM)

Mehrere Benutzer müssen sich häufig ein spezifisches Konto mit privilegiertem Zugriff teilen, um administrative Aufgaben zu erledigen. Bei Linux gibt es beispielsweise ein Superuser-Konto (root), das privilegierten Zugriff hat und auf einem Server alles Mögliche tun kann. Weitere Beispiele für Superuser-Konten sind das Windows-Administratorkonto und der Oracle Database SYS-Benutzer.

Da diese Konten nicht individualisiert sind, nutzen in vielen Unternehmen mehrere Benutzer dieselben Kontoanmeldedaten (das heißt, alle IT-Administratoren kennen das Root-Passwort), was gefährlich ist.

Zudem wird es schwierig, den Überblick zu behalten, welcher Benutzer zu einem bestimmten Zeitpunkt eine Aktion durchgeführt hat. Die Serverprotokolle zeigen zwar, dass der Root-Benutzer einen wichtigen Systemordner gelöscht hat, aber nicht, wer in diesem Moment das Root-Konto verwendet hat. Jeder IT-Administrator wird damit zum Verdächtigen.

PAM ergänzt IAM mit einem zwischengelagerten, als Vault bezeichneten Schutzmechanismus. In diesem Vault werden gemeinsam genutzte Konten mit Superuser-Berechtigungen durch ein zufälliges/geheimes Passwort gesichert, das niemand kennt. Jedes Mal, wenn Benutzer ein privilegiertes Konto verwenden müssen, wechseln sie zum PAM-System, um das Konto auszuchecken. Nach Erhalt einer Auscheckanforderung überprüft das PAM-System, wie lange ein Benutzer dieses Konto verwenden darf, protokolliert den Auscheckvorgang für Prüfungszwecke, ändert das Passwort für das Superuser-Konto und gibt es dann dem Benutzer bekannt, der das Konto ausgecheckt hat. Sobald die Nutzungsfrist abgelaufen ist, nimmt das PAM-System das Konto zurück (indem es das Passwort in einen anderen geheimen Wert ändert, den niemand kennt) und speichert es im Vault.

TIPP

Neben der Vergabe von individuellen Berechtigungen wird PAM auch zur Verwaltung spezieller Kontentypen wie Dienstkonten (zum Beispiel zur Interaktion mit einem Betriebssystem), Anwendungskonten (zum Beispiel zur Ausführung eines Stapelauftrags oder Skripts) sowie Datenbankkonten (zum Beispiel zum Ändern eines Datenbankschemas) verwendet.

Identity Governance und Administration (IGA)

Anfang der 2000er Jahre manipulierten Unternehmen wie Tyco, MCI WorldCom und Enron ihre IT-Systeme so, dass sie bessere Finanzergebnisse meldeten und ihre Aktienkurse erhöhten. Nach der Aufdeckung dieser Skandale verloren viele Aktionäre viel Geld.

Um weitere derartige Vorfälle zu verhindern, begann die Regierung, an der Börse notierte Unternehmen zur Kontrolle und besseren Prüfung von Konten in IT-Systemen zu verpflichten, die mit Unternehmensfinanzen zu tun hatten. Zu den Kontrollmaßnahmen gehörte die regelmäßige Überprüfung, wer worauf Zugriff hat (in einem als *Nachweis* bezeichneten Prozess), sowie die Implementierung von Anforderungsgenehmigungen und die Vermeidung von geheimen Absprachen (ein als *Funktionstrennung* bezeichneter Prozess).

Zur Unterstützung einiger dieser Anforderungen können Unternehmen ihr IAM mit Identity Governance and Administration (IGA) ausbauen.

MERKEN

Die Notwendigkeit für IGA entstand im Zuge von gesetzlichen Compliance-Auflagen wie dem Sarbanes-Oxley Act (SOX) und dem Health Insurance Portability and Accountability Act (HIPAA). IGA erzwingt den Nachweis und die Funktionstrennung und stellt auch Compliance-Berichte bereit.

Während IAM und PAM den technologischen Identitätsaspekt repräsentieren, kann man sich IGA als die Richtlinien- und Prozesskomponente der Identität vorstellen. IGA umfasst Richtlinien, die Folgendes definieren:

- Wer basierend auf seinen Rollen und Verantwortlichkeiten innerhalb des Unternehmens, Zugriff auf welche Netzwerkressourcen erhalten soll
- Die Prozesse für das Identitäts-Lebenszyklusmanagement im Unternehmen (etwa Zugriffsanforderungen und -genehmigungen und Kontobereitstellung und -stilllegung)
- Die fortlaufende Überprüfung der Einhaltung von Identitätsvorschriften im Unternehmen, einschließlich Protokollierung, Überwachung, Identitäts- und Zugriffsprüfung

TIPP

Viele IGA-Systeme übernehmen auch die Bereitstellung. In modernen Identitätslösungen sind diese Funktionen jedoch bereits nativ integriert (weitere Informationen finden Sie in Kapitel 2).

Ein Blick auf die Entwicklung der Identität

Wie jede andere Technologie hat sich Identität im Laufe der Zeit weiterentwickelt, um sich an neue Herausforderungen und Anforderungen anzupassen (siehe Abbildung 1-3).

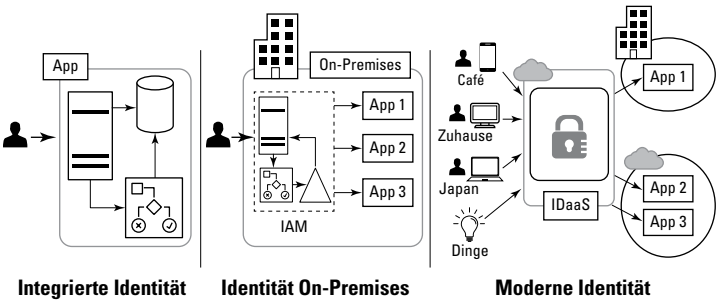

ABBILDUNG 1-3: Weiterentwicklung der Identität entsprechend neuen IT- und Sicherheitsherausforderungen.

Integrierte Identität

Am Anfang bestand der Identitätsnachweis in der lokalen Authentifizierung bei einem Großrechner oder einer Desktopanwendung. Zu dieser Zeit waren relativ wenige Computer miteinander verbunden, sodass sich Unternehmen hauptsächlich darauf konzentrierten, den lokalen Zugriff auf einen Arbeitsplatzrechner oder eine Anwendung zu beschränken und das Betriebssystem zu schützen. Deshalb waren in vielen Desktopbetriebssystemen und lokal installierten Anwendungen in der Regel einfache Authentifizierungsfunktionen integriert, die lediglich einen Benutzernamen und ein Passwort für die Anmeldung verlangten.

Identität On-Premises

Mitte bis Ende der 1990er Jahre begannen Unternehmen, Computer und Server zum Informationsaustausch in LANs zu verbinden. Mit der zunehmenden Einführung von Internet- und Webanwendungen (wie E-Mail, Intranet-Portale, Oracle und SAP) stieg auch der Bedarf an robusteren Identitätsfunktionen. Unternehmensnetzwerke wuchsen auf mehrere Tausend Computer an, die alle routinemäßig mit Millionen von Diensten im Internet verbunden waren. Und Unternehmen hatten plötzlich mit der Bedrohung zu kämpfen, dass Hacker in ihre Netzwerke eindringen. Gleichzeitig bereitete die Benutzerkontenverwaltung der IT-Abteilung zunehmend Kopfzerbrechen, da Benutzer sich an vielen verschiedenen Stellen anmelden müssen, etwa bei ihren Desktopcomputern, bei Dutzenden von Apps und ihren E-Mail-Clients. Die IT-Abteilung musste nun auch dort den Zugriff kontrollieren und – natürlich – vergessene Benutzerpasswörter zurücksetzen.

Um diese Herausforderungen zu meistern, begannen Unternehmen damit, die Identität auf dedizierten Systemen zu verwalten. Der Dienst Microsoft Active Directory (AD), der erstmals mit Windows 2000 Server veröffentlicht wurde, zentralisierte die Netzwerkkontenverwaltung und ermöglichte verzeichnisbasierte identitätsbezogene Dienste in Windows-Netzwerken und -Anwendungen. In ähnlicher Weise ermöglichten Novell eDirectory (jetzt NetIQ eDirectory) und Lightweight Directory Access Protocol (LDAP) verzeichnisbasierte identitätsbezogene Dienste sowohl in Windows- als auch in Nicht-Windows-Netzwerken. Und um den Zugriff auf Webanwendungen und E-Mails zu sichern, haben Unternehmen Web Single Sign-On-Lösungen – auch bekannt als SSO oder Web Access Management (WAM) – wie Oracle Access Manager, CA SiteMinder, PingAccess, Tivoli Access und Microsoft Active Directory Federation Services (ADFS) eingeführt.

Identity as a Service (IDaaS) – die moderne Identität

Der Bedarf an einem robusten Identitätsmanagement ist heute größer denn je. Das Risiko einer Sicherheitsverletzung oder eines Angriffs

besteht immer und die Angreifer, die böswillige Insider und Cyberkriminelle oder auch Hacktivisten und Cyberterroristen sein können – sind hoch motiviert und von Gier oder Ideologie getrieben.

Gleichzeitig gibt es mehr Anwendungen als je zuvor und sie werden zunehmend als SaaS-Angebote (Software as a Service) in der Cloud bereitgestellt (zum Beispiel Office 365, Slack und Zoom). Laut dem Okta-Bericht „Businesses @ Work" von 2020 liegt die durchschnittliche Anzahl der Apps pro Unternehmen derzeit bei 88 und die Wachstumsrate in den letzten 3 Jahren betrug 21 Prozent. Und die Vielzahl der unterschiedlichen Gerätetypen verschärft das Problem noch zusätzlich. Neben einem vom Unternehmen bereitgestellten Laptop hat praktisch jeder Benutzer zumindest ein zusätzliches mobiles Gerät und einen Computer oder ein iPad zu Hause. Diese Umgebungen haben viele Unternehmen nicht unbedingt im Blick – zum Beispiel hat AD keine Kontrolle über Anwendungen auf Android-, Mac- und anderen Nicht-Windows-Geräten. Und schließlich greifen Benutzer praktisch von überall auf Anwendungen und Daten zu, einschließlich öffentlicher (also nicht sicherer) WLAN-Netzwerke in Flughäfen und Cafés.


TIPP

Weitere Informationen darüber, wie Unternehmen heutzutage Apps nutzen, finden Sie im Bericht „Businesses @ Work" unter `https://www.okta.com/businesses-at-work/2020/` und im Businesses @ Work-Dashboard unter `https://www.okta.com/businesses-at-work/`. Diese Daten werden von Okta in Echtzeit und jährlich unter Verwendung anonymisierter Daten von Tausenden von Kundenorganisationen, Anwendungen, IT-Integrationen und täglichen Benutzeraktivitäten zusammengestellt.

Identität hat sich somit nicht nur weiterentwickelt, sondern sich vielmehr in eine hybride Realität verwandelt, in der die Anwendungen, auf die zugegriffen wird, das verwendete Gerät und der Netzwerkperimeter sich ständig ändern (stellen Sie sich eine Welt vor, in der Menschenaffen, Neandertaler und der Homo sapiens versuchen, bei Kaffee und Bananen zusammen auf ihren Computern und mobilen Geräten zu arbeiten).

Herkömmliche Identitätslösungen wie AD und lokales SSO können angesichts dieser Trends und Herausforderungen keine Konten verwalten und den Zugriff absichern. Und selbst wenn, würden Hunderte von Servern und Arbeitsstunden benötigt, um derartige Auslastungen und Anforderungen zu bewältigen. Mit herkömmlichen On-Premises-Identitätslösungen ist dies beinahe unmöglich.

Die Lösung ist Identity as a Service (IDaaS), eine moderne Identifizierungslösung, die alles unter einen Hut bringt. Im Rest dieses Buches erfahren Sie mehr über IDaaS.

ADOBE NUTZT OKTA, UM TAUSENDE MIT DER CLOUD ZU VERBINDEN

2012 führte Adobe Creative Cloud ein und veränderte die kreative Welt für immer. An diesem Punkt wurden alle Creative Suite-Produkte des Unternehmens in die Cloud verschoben. Mit der Creative Cloud-Mitgliedschaft können Benutzer jede Adobe Creative Suite-Anwendung herunterladen und installieren.

Die Auslagerung des gesamten kreativen Workflows in die Cloud hat das Geschäft von Adobe grundlegend verändert. Fast über Nacht wechselte Adobe von unbefristeten Produktlizenzen und 18-monatigen Veröffentlichungszyklen zu monatlichen und jährlichen Abonnements und regelmäßigen Produktaktualisierungen.

Damit änderten sich auch die Identitäts- und Zugriffsanforderungen bei Adobe. Die erste Veröffentlichung von Creative Cloud ermöglichte keine Verbindung mit den Corporate Identity-Systemen, die von vielen Adobe Enterprise-Kunden bereits verwendet wurden. IT-Administratoren mussten in Adobe Creative Cloud völlig neue Benutzeranmeldedaten erstellen und verwalten, was später zu Problemen führte, wenn Benutzer ein Passwort vergaßen oder ihre Anmeldedaten aktualisierten.

Für Adobe machte es keinen Sinn, eine individuelle Möglichkeit zur Einrichtung von Partnerverbindungen zwischen Creative Cloud und den Identitätssystemen von Unternehmenskunden zu schaffen. Technische Ressourcen lassen sich besser einsetzen, um die nächste kreative Funktion in Photoshop Creative Cloud zu entwickeln oder neue vernetzte kreative, mobile Apps auf den Markt zu bringen. „Ich möchte in unserem Identitätsstapel nicht unbedingt das Rad neuerfinden. Ich will die beste auf dem Markt erhältliche Lösung nutzen und dann die Adobe-spezifischen Anforderungen auf diesen Stapel anwenden, um unseren Kunden wirklich schnelle Lösungen anzubieten“, sagt Scott Castle, Produktmanager für Creative Cloud.

Doppelte Cloud-Herausforderungen

Nicht nur das Adobe-Produktteam hatte mit Authentifizierungsproblemen zu kämpfen. Ende 2014 unterstützte das kleine interne IT-Team von Adobe rund 300 Cloud-Anwendungen mit einer Open-Source-SSO-Lösung, die es selbst entwickelt hatte. Noch im selben Jahr entschied sich das Unternehmen, Microsoft Office 365 für alle 13.500 Adobe-Mitarbeiter bereitzustellen und E-Mail-, Kalender- und SharePoint-Tools in die Cloud zu verschieben. Die alte Identitätsmanagementplattform, mit ihren gelegentlichen Macken und Ausfällen, war dieser Aufgabe jedoch nicht gewachsen.

Glücklicherweise, so Den Jones, leitender Manager von IT Services, wurde dem Team ungefähr zur gleichen Zeit Okta vorgestellt. Die Zusammenarbeit

(Fortsetzung)

(Fortsetzung)

mit einem externen Anbieter, der sich auf die Sicherung und Authentifizierung von Anwendungen in der Cloud konzentrierte, und nicht auf die Entwicklung brillanter, ausdrucksstarker Design-Tools, war sinnvoll.

Nach Betrachtung der Optionen und aufgrund von Oktas Ruf in der Branche beschloss die IT-Abteilung von Adobe, das interne Single Sign-on-System auszumustern und Office 365 mit Okta-Authentifizierung zu implementieren. Im Anschluss an dieses Rollout begann Adobe, seine verbleibenden Cloud-Anwendungen auf die Okta-Plattform auszulagern. Da die Wartung für die alte Plattform zur Erneuerung anstand, musste das Team in einem engen Zeitrahmen arbeiten und in drei Monaten 300 Anwendungen migrieren.

Der Zeitplan erwies sich sehr zur Freude von Jones und seinem Team als durchaus angemessen. Es dauerte etwa vier Wochen, um die ersten ca. 200 Anwendungen zu migrieren, sagt er. Die Bereitstellung der meisten Anwendungen erfolgt heute in Minutenschnelle, und nicht nach Wochen oder Monaten wie bisher. Seitdem hat Adobe mehrere Produkte aus der Okta Identity Cloud für seine wachsende Belegschaft bereitgestellt und zum Schutz und zur Verwaltung seiner 20.500 Mitarbeiter eingesetzt.

Identität für alle

Nach der Zusammenarbeit mit Okta an der Sicherung des Mitarbeiterzugriffs auf Cloud-Anwendungen gab es für die IT-Abteilung von Adobe wenig Zweifel, mit wem das Produktteam zusammenarbeiten musste, um Enterprise Identity in die Creative Cloud für Unternehmen zu integrieren. Bald darauf beauftragte Adobe Okta damit, Adobe-Produktingenieuren die gleichen leistungsstarken Identitätsdienste an die Hand zu geben.

Adobe nutzt Okta heute, um allen Unternehmenskunden eine umfassende Identitätsmanagementebene anzubieten, etwa für Adobe Marketing Cloud, Adobe Document Cloud oder Creative Cloud. Die vernetzte Lösung sichert Adobe Cloud-Anwendungen und ermöglicht Benutzern den Zugriff auf die innovativen Tools von Adobe mit ihren vorhandenen Unternehmensanmeldedaten – sicher, schnell und kostengünstig.

Um Creative Cloud-Benutzern zum Erfolg zu verhelfen (und die IT-Abteilungen von Kunden weiterhin zufriedenzustellen), erfüllt die Enterprise Identity-Plattform von Adobe einige sehr wichtige Funktionen:

- Verbindet Corporate Identity-Systeme von Kunden – wie AD oder LDAP –, damit IT-Administratoren keinen doppelten Managementaufwand mehr haben
- Integriert Okta-Funktionen in den vorhandenen Code der Adobe Creative Cloud
- Überzeugt durch Adobe-Branding
- Verbindet individuelle Benutzeridentitäten mit einzelnen Konten sowie mehreren Unternehmens- und Agenturkonten

IN DIESEM KAPITEL

- Einführung in Identity as a Service (IDaaS)
- Bewältigung moderner Identitätsherausforderungen mit IDaaS
- Einsatz von IDaaS für Menschen und Dinge

Kapitel 2
Definition von Identity as a Service (IDaaS) – die moderne Identität

In diesem Kapitel erfahren Sie, worum es bei IDaaS geht, wie es moderne Identitätsherausforderungen bewältigt, welche Vorteile es bietet und wie IDaaS Anwendungsfälle für Mitarbeiter, Auftragnehmer, Kunden und Dinge unterstützt.

Die Grundlagen von IDaaS

Identity as a Service (IDaaS) ist Identitäts- und Zugriffsmanagement (IAM), das von einem Service Provider in der Cloud erstellt und gehostet wird und Unternehmen über ein Software as a Service-Abonnement (SaaS) zur Verfügung steht. IDaaS bewältigt moderne Identitätsanforderungen ohne die Einschränkungen des On-Premises-IAM-Modells.

MERKEN

Die Einführung von SaaS-Lösungen wie IDaaS hat Unternehmen und IT-Administratoren folgende Vorteile gebracht:

- **Kurze Amortisierungszeit:** SaaS-Lösungen sind bereits bei der Anmeldung einsatzbereit, sodass Aufgaben wie die Beschaffung von Servern und die Installation von Software entfallen.

- **Geringerer Wartungsaufwand:** SaaS-Lösungen werden von ihren Anbietern ständig mit neuen Funktionen und Sicherheitsverbesserungen aktualisiert, ohne Ausfallzeiten zu verursachen, wodurch die Anzahl der Wartungsaufgaben reduziert wird, die von IT-Administratoren erledigt werden müssen.
- **Weniger manuelle Integrationen:** SaaS-Lösungen sind mit allem ausgestattet, was Sie für den Einsatz benötigen. Dadurch entfallen die Kosten der Integration interner Komponenten wie Server, Backup-Systeme und Netzwerke.
- **Kostenflexibilität:** Da SaaS-Lösungen in der Regel pro Benutzer und Monat berechnet werden, können Unternehmen ihre Ausgaben besser kontrollieren und müssen nur die von ihnen verwendeten Services bezahlen.

Diese Vorteile sind so groß, dass Unternehmen den Großteil ihres Kerngeschäfts in die Cloud verlagern. Wenn Sie heute eine neue IT-Lösung für Ihr Unternehmen suchen, ist es schwieriger, Ihre Vorgesetzten davon zu überzeugen, Server zu kaufen, Rechenzentren einzurichten, Software zu installieren und der IT die gesamte Wartung zu überlassen, als einen Cloud-Service zu abonnieren.

MERKEN

IDaaS hat dasselbe Ziel wie IAM: sicherzustellen, dass Benutzer die sind, die sie zu sein behaupten, und ihnen zur richtigen Zeit die richtigen Zugriffsmöglichkeiten auf Ressourcen zu geben. Der Hauptunterschied besteht darin, dass IDaaS Ihnen die Vorteile der Cloud bietet – ohne die Einschränkungen und Kosten von On-Premises-IAM.

Denken Sie beispielsweise darüber nach, wie Sie Single Sign-On (SSO) mit herkömmlichem On-Premises-IAM (zum Beispiel Microsoft Active Directory Federation Services (AD FS) oder Oracle Access Manager) im Vergleich zu IDaaS von Okta bereitstellen können. Sobald Sie IDaaS abonniert und Ihre Benutzer importiert haben, können sie die Vorteile des Service nutzen. Sie müssen Ihre Zeit und Ihr Geld nicht dafür aufwenden, Server und Betriebssysteme zu kaufen und zu installieren oder die Auslastung und Kapazität für den Service einzuschätzen.

Darüber hinaus werden neue Funktionen oder Updates automatisch bereitgestellt. Das kann eine neue Mobilgeräte-App sein, die den Zugriff auf Apple iOS und Android schützt, oder eine Sicherheitsverbesserung, die den Zugriff aus dem Darknet verhindert. Sie müssen nicht planen, testen, Wartungstermine festlegen und das System manuell aktualisieren. IDaaS verfügt bereits über alle Komponenten, die für die Verwaltung von Identitäten erforderlich sind, zum Beispiel Multi-Faktor-Authentifizierung (MFA) und Provisionierung. Daher ist die Verstärkung der Sicherheit ein Kinderspiel und Sie müssen keine separaten MFA- oder

Provisionierungslösungen von anderen Software-Anbietern beschaffen, manuell installieren und integrieren. Zudem hängen die Kosten für den Service davon ab, wie Sie ihn nutzen. Wenn Sie beispielsweise MFA nur für Manager implementieren möchten, entfallen die Kosten für die Einführung für Ihr ganzes Personal.

IDaaS kann zur Sicherung des Zugriffs und Verwaltung von Identitäten in unterschiedlichen Ressourcen verwendet werden – einschließlich APIs (Application Programming Interfaces), On-Premises, Cloud, mobilen Apps und Servern. Es bietet auch mehrere native Funktionen wie Adaptive MFA (in Kapitel 3 erläutert) zur Verbesserung von Authentifizierungssicherheit und SSO, das es Benutzern erlaubt, sich nur einmal am Netzwerk anzumelden, um Zugriff auf alle Anwendungen und Ressourcen zu erhalten, für die sie autorisiert sind.

In der On-Premises-Welt müssen Sie alle diese Funktionen (Adaptive MFA, SSO, Verzeichnisdienste, Provisioning usw.) für verschiedene Server, Anbieter (wie Oracle, RSA, Microsoft und Symantec) und manuelle Integrationen einrichten. Mit IDaaS ist alles in einem einzigen Angebot verfügbar und skalierbar – und das bei kurzer Amortisierungszeit (siehe Abbildung 2-1).

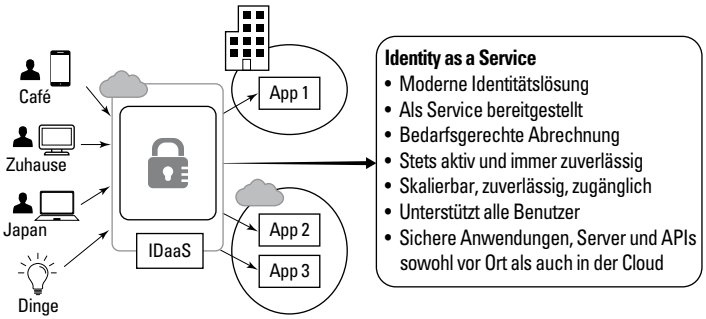

ABBILDUNG 2-1: Zusammenspiel von IDaaS mit moderner IT und die Vorteile, die sich daraus ergeben.

Bewältigung von Identitätsherausforderungen

IDaaS bewältigt viele Identitätsherausforderungen, die sich heutigen Unternehmen stellen. So ist mit IDaaS eine schnelle Integration in Cloud- und On-Premises-Anwendungen möglich, da offene Standards wie Security Assertion Markup Language (SAML) und OpenID Connect (OIDC) sowie Anwendungskataloge genutzt werden. IDaaS konsolidiert außerdem die Zugriffskontrolle unabhängig davon, wo eine Anwendung gehostet wird, und unterstützt Unternehmen mit hybrider

IT durch Systeme, die in mehreren lokalen, öffentlichen und privaten Cloud-Umgebungen gehostet werden.

IDaaS bietet die robuste Skalierbarkeit, Zuverlässigkeit und Zugänglichkeit, die moderne Unternehmen in einer „Always-on"-Welt benötigen, in der potenziell Hunderttausende (sogar Millionen) von Benutzern – darunter Mitarbeiter, Kunden und andere – jederzeit und von jedem Gerät aus Zugriff auf ihre Mobilgeräte-Apps, Websites, APIs und Portale benötigen.

MERKEN

IDaaS bietet Unternehmen zahlreiche Vorteile, darunter:

- Bessere Cybersicherheit für Unternehmen mit Funktionen wie Adaptive MFA (in Kapitel 3 erläutert) und zentralisiertem IAM.
- Höhere Benutzer- und IT-Produktivität. Benutzer können sich mit SSO schneller bei all ihren Anwendungen anmelden und der IT-Helpdesk benötigt weniger Zeit für das Zurücksetzen von Passwörtern. Egal, ob sich ein Benutzer von einem offenen WLAN an einem Flughafen oder von einem Firmenbüro aus anmeldet, der Prozess ist immer nahtlos und sicher.
- Möglichkeiten für Unternehmen, die IT-Kosten deutlich zu senken. Die Bereitstellung von Identitäten vor Ort (zum Beispiel mit Active Directory oder Oracle Identity Manager) kann mit einer Vielzahl von Kosten verbunden sein:
  - Kauf, Installation, Upgrade und Wartung von Serverhardware (oder virtuellen Softwarelizenzen) und Software
  - Hosting-Gebühren für Platz in einem Rechenzentrum, einer privaten oder öffentlichen Cloud
  - Konfiguration, Wartung und Überwachung von VPN-Verbindungen (virtuelles privates Netzwerk)

MERKEN

Mit IDaaS fallen nur die Kosten für das Abonnement und die IT-Administration zur Verwaltung Ihrer Benutzerkonten an. Ihre Benutzerlizenzen können zur Anpassung an die Anforderungen Ihres Unternehmens schnell und einfach herauf- oder herunterskaliert werden. IDaaS reduziert die wiederkehrenden Kosten für die Identitätshandhabung erheblich: von manuellen IT-Supportanfragen für die Bereitstellung und das Zurücksetzen von Benutzerkonten bis hin zu Professional Services für die Implementierung, das Patching und das Upgrade verschiedener Lösungen. Laut Forrester „liegt der größte Vorteil der Verwendung von IDaaS im Vergleich zu On-Premises-IAM-Lösungen in den um 30 bis 35 Prozent geringeren Kosten für Wartungsarbeiten".

Betrachtung von Anwendungsfällen

IDaaS unterstützt viele gängige geschäftliche Anwendungsfälle für das Identitätsmanagement (siehe Abbildung 2-2) wie zum Beispiel Mitarbeiter, Auftragnehmer, Partner, Kunden und Dinge.

ABBILDUNG 2-2: Die Anwendungsfälle (und Benutzer), die Identität erfordern.

Mitarbeiter

Mitarbeiter sind das wichtigste Kapital jedes Unternehmens und jeder Organisation. Es ist unabdingbar, dass Ihre Mitarbeiter sich auf sichere Weise mit den benötigten Technologien verbinden können. Mitarbeiter greifen heute von überall auf Systeme zu und arbeiten dezentral zusammen. Gleichzeitig werden Mitarbeiter zum Ziel von Angreifern, die nach Möglichkeiten suchen, ihren Zugriff zu missbrauchen.

IDaaS unterstützt Mitarbeiter durch:

- Dynamische Integration und Änderung von Benutzerzugriffsrechten auf Basis von Benutzerdaten, die aus Personalverwaltungssystemen wie Workday und SuccessFactors bezogen werden
- Sichere Speicherung von Mitarbeiteridentitäten und -berechtigungen
- Sicherung des Mitarbeiterzugriffs auf alle Ressourcen, einschließlich Apps, Server und APIs sowohl vor Ort als auch in der Cloud, mit nur einem Satz starker Anmeldedaten
- Gewährleistung des sicheren Zugriffs unabhängig von Benutzerkontext, Gerät und Netzwerkstandort
- Steigerung der Mitarbeitereffizienz durch den mobilen Zugriff auf die Ressourcen des Unternehmens
- Änderung von Zugriffsvoraussetzungen auf Basis von Risiken bei dynamischer Verweigerung oder Anforderung von MFA für risikoreiche Zugriffe
- Belohnung von „Low-Risk"-Benutzern mit passwortlosem Zugriff

- Überwachung und Bereitstellung von Ereignisinformationen für das Sicherheitsteam

Auftragnehmer und Partner

Unternehmen arbeiten intensiv daran, Partnerschaften aufzubauen. Der effektiven Zusammenarbeit können jedoch schwerfällige Prozesse und Systeme im Wege stehen. Partner und Auftragnehmer bringen neue, dynamische Benutzertypen mit sich, was zu Komplexität für IT-Teams führt. Gleichzeitig setzt eine zu großzügige Zuweisung von Zugriffsberechtigungen für Partner wichtige Systeme unnötigen Sicherheitsrisiken aus.

Unternehmen haben den Zugriff durch Auftragnehmer und Partner bislang meist ermöglicht, indem sie entweder – bei kurzfristigen oder relativ überschaubaren Beziehungen – deren Identitäten mit derselben IAM-Lösung verwalten wie für ihre Mitarbeiter oder – bei umfangreicheren, langfristigen Partnerschaftsbeziehungen – indem sie sich in den IAM-Stack ihres Partners integrieren und so eine B2B-Integration (Business-to-Business) schaffen.

Der Aufbau von B2B-Integrationen ist ein kostspieliges und zeitaufwändiges Unterfangen. Im Durchschnitt betragen die Gesamtkosten für den Aufbau und die Wartung einer B2B-SAML-Integration in-house beispielsweise 20.000 US-Dollar pro Integration.

TIPP

IDaaS hilft, die Partnerintegration sowohl für kurzfristige als auch für langfristige B2B-Beziehungen zu optimieren. Die Vorteile sind unter anderem:

- **Nahtlose Benutzung:** Native Integration mit der IAM-Lösung des Partners, sodass Partner mit ihren vorhandenen Zugangsdaten auf Ihre Ressourcen zugreifen können
- **Förderung der Zusammenarbeit:** Optimierte Partnererfahrung durch Gewährung von sofortigem Zugriff auf die richtigen Ressourcen über ein personalisiertes und sicheres Portal
- **Automatisierung des Partner-Lebenszyklus:** Zentralisierte Benutzerverwaltung und automatisierte Bereitstellung von Partneridentitäten, um die administrativen Anforderungen an die IT zu reduzieren
- **Verbesserung der Sicherheit:** Volle Kontrolle über Authentifizierung, Identität, Anwendungen und Ressourcen und Automatisieren der Deprovisionierung, um weitere unerwünschte Zugriffe zu unterbinden

Kunden und Verbraucher

Heute betreibt jedes Unternehmen ein digitales Geschäft über Websites, APIs und Apps. Ob Sie Kunden zu gewinnen und ihren Lebenszeitwert maximieren können, hängt zunehmend davon ab, ob Sie deren hohe Erwartungen hinsichtlich technologisch fortgeschrittener, reibungsloser, kanalübergreifender und personalisierter digitaler Erfahrungen erfüllen können.

Nehmen wir an, Sie kaufen bei Amazon ein oder sehen Ihre Fotos auf Instagram durch. Sicherheit ist in beiden Beispielen entscheidend, denn Sie wollen die Gewissheit, dass niemand mit Ihrer Kreditkarte einkauft und dass Ihre Fotos und Kommentare sicher sind. Wenn die Bedienung dieser Websites jedoch unbequem und schwerfällig wäre, würden Sie diese wahrscheinlich nicht noch einmal verwenden. Sie erwarten außerdem, dass Sie dieselbe Anmeldung verwenden können und auf unterschiedlichen Geräten die gleiche Sicherheit und Benutzererfahrung erhalten. So könnten Sie zum Beispiel Instagram sowohl auf Ihrem Computer als auch Ihrem Smartphone verwenden, und Sie könnten sowohl auf der Amazon.de-Webseite als auch über Alexa einkaufen. Die reibungslose Bereitstellung ist in puncto Verbraucheridentität das A und O.

TIPP

IDaaS kann Unternehmen auf folgende Weise helfen, eine hervorragende Kundenerfahrung zu gewährleisten und anzubieten:

- **Verbesserte Kundenerfahrung bei der Registrierung und Anmeldung:** Bieten Sie auf allen Kanälen ansprechende, markenspezifische und personalisierte Erlebnisse an. Passen Sie den Registrierungs- und Anmeldeprozess problemlos über mehrere Anwendungen hinweg ohne kostspielige Programmier- und Entwicklungsarbeiten an.
- **Umfassender Blick auf Ihre Kunden:** Beseitigen Sie organisatorische Silos aufgrund unkoordinierter Konten. Die Verwendung einer einzigen Identität für jeden Kunden gibt Unternehmen Einblicke in seine Interessen und Vorlieben und steigert so seinen Lebenszeitwert.
- **Stärkung der Kundenbindung:** Verringern Sie Reibungspunkte beim Onboarding mit progressivem Profiling und passwortloser Authentifizierung. Integrieren Sie Apps nahtlos in das Kundenportal, damit Ihre Kunden sich nur einmal anmelden müssen.
- **Verwaltung von Einwilligungen:** Geben Sie Ihren Kunden die Kontrolle über ihre Daten und erfüllen Sie komplexe gesetzliche Compliance-Anforderungen wie den California Consumer Privacy Act (CCPA) und die EU-Datenschutz-Grundverordnung (DSGVO). Weitere Informationen zum Einwilligungsmanagement finden Sie in Kapitel 4.

Dinge

Das Internet der Dinge (IoT) und die Milliarden (bereits über 30 Milliarden im Jahr 2020) intelligenten, vernetzten Geräte stellen moderne Unternehmen vor neue Herausforderungen. Sicherheit im IoT – mit noch größeren Bedrohungen für das menschliche Leben und die öffentliche Sicherheit als andere Bereiche der Cybersicherheit – ist von höchster Bedeutung.

Intelligente Geräte wie Amazon Alexa, intelligente Glühbirnen und Smart TVs benötigen Identität, damit authentifiziert und kontrolliert werden kann, worauf sie zugreifen und was sie tun können – genau wie Menschen! Es gibt jedoch viel mehr intelligente Geräte als Menschen und im Gegensatz zu Menschen kommunizieren sie über APIs statt Browser und Apps.

MERKEN

IDaaS bietet die Identität und Skalierbarkeit, die erforderlich ist, um die Datenverkehrsanforderungen des IoT zu erfüllen. Darüber hinaus unterstützt IDaaS Protokolle wie Open Authorization (OAuth), die von intelligenten IoT-Geräten für den sicheren Zugriff auf APIs erwartet werden.

WAS IDAAS NICHT IST

In diesem Kapitel wird erläutert, was IDaaS ist. Kurz gefasst ist IDaaS eine Cloud-basierte IAM-Lösung, die den Zugriff auf Anwendungen und Systeme für die Benutzer eines Unternehmens absichert, einschließlich Mitarbeitern, Auftragnehmern, Partnern, Kunden und Dingen.

Was also ist IdaaS *nicht*? Nun, zunächst einmal: Eine On-Premises-Identitätsmanagementlösung, die mithilfe eines Infrastructure as a Service- (IaaS) oder Platform as a Service-Angebots (PaaS) in die Cloud migriert wurde, ist kein IDaaS. Auch nach der Auslagerung Ihrer lokalen Active Directory-Server in eine PaaS-Lösung oder selbst nach der Einführung einer modernen Container-Technologie wie Docker bleiben Sie weiterhin dafür verantwortlich, die Systeme manuell zu installieren und zu patchen, Kapazitätsplanungen durchzuführen und Integrationen in andere Module oder Anbieter manuell durchzuführen – und das alles ohne den Prepaid-Vorteil eines echten IDaaS. Das ist also nicht IdaaS. Auch wenn Container super cool sind (vor allem für die Entwicklung eigener Apps), haben Sie damit nur die Verlagerung Ihrer On-Premises-Herausforderungen in die Cloud erreicht!

IDaaS ist auch keine Managed Service Provider-Lösung (MSP). MSPs stellen in der Regel eine herkömmliche IAM-Lösung für Sie bereit und berechnen Ihnen dafür eine Abonnementgebühr. Auch wenn diese Lösungen Ihren Wartungsaufwand reduzieren, beseitigen sie nicht die wichtigsten Einschränkungen des traditionellen IAM, wie Echtzeit-Upgrades ohne geplante Ausfälle oder die Bereitstellung von Tausenden vorkonfigurierten Integrationen in Mobilgeräte-Apps, Cloud-Apps und APIs.

IN DIESEM KAPITEL

- Ein Blick auf die Bausteine von Identity as a Service
- Kontrolle des Zugriffs auf verschiedene Ressourcen
- Erwägungen zu Integrationen, Sicherheit und Datenschutz, Compliance und mehr

Kapitel 3
Die Bausteine von Identity as a Service

In diesem Kapitel erfahren Sie mehr über die wichtigsten Komponenten von Identity as a Service (IDaaS), die mit IDaaS abgesicherten Ressourcen sowie wichtige Überlegungen, die Sie bei der Einführung einer IDaaS-Lösung beachten müssen.

Die Bausteine

IDaaS-Lösungen haben in der Regel vier Hauptbausteine:

- Directory
- Single Sign-On (SSO)
- Multi-Faktor-Authentifizierung (MFA)
- Provisionierung und Workflows

Directory

Das Directory ist eine zentrale Komponente jeder Identitäts- und Zugriffsmanagementlösung (IAM). Es handelt sich hierbei um eine Datenbank von Entitäten (Benutzer, Gruppen und Ressourcen), Metadaten (Konfigurationen und Richtlinien) und Auditdaten, die IAM zur Erfüllung seiner Aufgabe benötigt.

Microsoft Active Directory (AD) ist ein typisches herkömmliches Directory, das in einer lokalen Umgebung installiert ist. Weitere Beispiele sind

Apache DS, NetIQ eDirectory, OpenLDAP und Oracle Internet Directory (OID).

Herkömmliche lokale Directorys wurden bereits entwickelt, als an Cloud, Telearbeiter, zunehmende Fusionen und Übernahmen (M&As) und Business-to-Business-Aktivitäten (B2B) sowie die Smartphone-/App-Revolution noch gar nicht zu denken war. Diese Directorys sind daher nicht vollständig für moderne Anforderungen optimiert. Wenn Unternehmen die Anpassung von lokalen Directorys an moderne Anforderungen erzwingen, um zum Beispiel Cloud-Anwendungen zu unterstützen oder Mobilgeräte zu verwalten, entsteht am Ende ein Dickicht von Verzeichnissen, Strukturbäumen, vertrauenswürdigen Domänen, Servern, selbst entwickelten Integrationen und PowerShell-/Bash-Skripten. Es werden also äußerst komplexe Umgebungen geschaffen, die letztlich ihren Anforderungen nicht gerecht werden.

MERKEN

Eine moderne Lösung muss moderne Anforderungen erfüllen und sich nahtlos in die Systeme einfügen, die das Directory verwenden, ohne dass Sie sich mit manuellen Integrationen und der Komplexität auseinandersetzen müssen.

IDaaS-Lösungen stellen ein integriertes Directory bereit, in dem die für alle modernen Anwendungsfälle erforderlichen Daten – von Mobil über M&A bis hin zur Cloud – sicher gespeichert werden, ohne dass Sie sich um die Infrastruktur kümmern oder benutzerdefinierte Setups, PowerShell- oder Bash-Skripte ausführen müssen. Das Directory ist nativ in alle Dienste integriert, die es nutzen (zum Beispiel SSO für die Authentifizierung von Benutzern), sodass manuelle Integrationsaufgaben entfallen.

TIPP

Bei der Einführung eines modernen IDaaS-Stacks ziehen viele Unternehmen in Betracht, ihre lokalen Directorys außer Betrieb zu nehmen. Bei Implementierungen, die ausschließlich für IAM verwendet werden, ist die Außerbetriebnahme von Legacy-Directorys ein Kinderspiel. Bei komplexen Umgebungen ist jedoch eine sorgfältige Planung erforderlich. In vielen Unternehmen wird Active Directory (AD) beispielsweise nicht nur zum Speichern der Identität, sondern auch für Dienste wie DNS-Auflösung (Domain Name System) und die Ausgabe von Zertifikaten für private Schlüssel verwendet. Darüber hinaus entwickeln einige Unternehmen eigene PowerShell-Integrationen oder „basteln“ Hunderte Domänencontroller zusammen, um ihre Daten zu speichern. Die Empfehlung für komplexe Bereitstellungen geht dahin, die Nutzung von Legacy-Directorys zu reduzieren, indem Dienste in moderne Lösungen ausgelagert werden und gleichzeitig die Komplexität reduziert wird.

Durch die Verwendung einer IDaaS-Lösung mit integriertem Directory und Provisioning können Sie beispielsweise auf benutzerdefinierte PowerShell-Skripte für identitätsbezogene Aktivitäten verzichten, zum

Beispiel für die Einbindung von Mitarbeitern im Zuge einer Fusion oder die Synchronisierung von E-Mail-Adressen über eine Vielzahl von Systemen. Die Übergabe dieser Aufgaben an IDaaS reduziert die Anzahl der Server und die Komplexität in Ihrem lokalen Directory erheblich.

Single Sign-On (SSO)

Anmeldedaten sind dazu gedacht, Konten zu schützen. Da Benutzer unterschiedliche Konten in Hunderten von Anwendungen haben, stellen sie jedoch eine Herausforderung dar. Um alle diese Anwendungen im Griff zu halten und gleichzeitig Passwortmüdigkeit und Produktivitätsverluste zu vermeiden, nehmen Benutzer gefährliche Abkürzungen: Sie verwenden die gleichen Anmeldedaten für verschiedene Anwendungen oder notieren Passwörter in Notizblöcken oder Tabellen. Verizon hat festgestellt, dass gestohlene Anmeldedaten die häufigste Ursache von Datenschutzverletzungen sind. Das liegt wahrscheinlich vor allem daran, dass Benutzer nur schwer einen Überblick über ihre vielen Anmeldedaten behalten.

SSO löst dieses Problem, indem es den Zugriff auf alle Anwendungen mit einer einzigen Anmeldung ermöglicht. Um dies zu erreichen und Benutzer mit Systemen und Anwendungen von Drittanbietern zu verbinden, setzt SSO auf offene Standards wie Security Assertion Markup Language (SAML) und OpenID Connect (OIDC).


TIPP

SSO-Lösungen werden gelegentlich dafür kritisiert, dass sie einen Single Point of Failure in den Authentifizierungsprozess einführen, was manche als „Schlüssel zum Himmelreich" bezeichnen. Es gibt jedoch wichtige Funktionsmerkmale und bewährte Methoden, die diese Bedenken nicht nur angehen, sondern auch die Sicherheit und Produktivität verbessern. Hier einige Beispiele:

- **MFA:** MFA gilt als der beste Freund von SSO. Die Verwendung von MFA erhöht die SSO-Sicherheit mithilfe von Authentifizierung und zusätzlichen Faktoren wie biometrischen Benutzerdaten, die sicherer sind als herkömmliche Passwörter.
- **Adaptiver Zugriff:** Eine gute Methode zur Erhöhung der SSO-Sicherheit ist der Einsatz von Lösungen, die den Benutzerzugriff auf Basis von Kontext, Netzwerk, Gerät und Standort neu bewerten und intelligente Bedrohungs-Feeds nutzen. Dadurch ändert SSO automatisch die Anmeldeanforderung, sperrt den Zugriff und löst Sicherheitswarnungen aus, wenn verdächtige Ereignisse auftreten.

SSO ist eine großartige Möglichkeit, robuste Passwortpraktiken für Ihre Benutzer durchzusetzen. Bei nur einem zu kontrollierenden Passwort kann die IT-Abteilung mithilfe von Richtlinien sicherstellen, dass dieses

Passwort so sicher wie möglich ist. Passwörter müssen des Weiteren die folgenden Anforderungen erfüllen:

- Sie müssen nach einer bestimmten Zeit ungültig werden.
- Sie müssen sich von bereits verwendeten Passwörtern unterscheiden, um eine Wiederverwendung zu verhindern.
- Sie dürfen auf keiner vorhandenen Liste von gehackten Anmeldedaten erscheinen.
- Nach einer bestimmten Anzahl von erfolglosen Versuchen zum Schutz vor Brute-Force-Angriffen muss eine Sperrung ausgelöst werden.

TIPP

Auch Passwortmanager können Endbenutzern den Zugriff erleichtern. Sie sind jedoch hauptsächlich auf den Schutz von Anmeldedaten in einer Art Tresor ausgerichtet (anstatt Passwörter überflüssig zu machen). Darüber hinaus bieten Passwortmanager keine wichtigen Sicherheitsfunktionen wie die Möglichkeit, den Kontext des Benutzers zu betrachten oder den Zugriff aus gefährlichen Netzwerken zu verhindern.

Anhand dieser Funktionen kann einem Benutzer, selbst wenn er die korrekten Anmeldedaten angibt, ein begrenzter Zugang (mit einer Zeitbegrenzung von Minuten statt Stunden) gewährt werden. Er kann auch zu einer zusätzlichen Authentifizierung aufgefordert werden oder der Zugriff wird ihm vollständig verweigert. Wenn ein Benutzer beispielsweise einen Tor-Anonymizer verwendet, um sich bei einem sensiblen System anzumelden, kann der Zugriff vollständig verweigert werden. SSO gibt Administratoren mehr und präzisere Kontrolle darüber, wie Benutzern Zugriff auf Unternehmensressourcen gewährt wird.

TIPP

In unserem Blog unter `https://okta.com/blog`, der mit einigen Mythen aufräumt, erfahren Sie mehr über SSO.

Adaptive Multi-Faktor-Authentifizierung (MFA)

Bei der Authentifizierung eines Benutzers wird typischerweise ein Identitätsanspruch (zum Beispiel ein Benutzername) mit einem sogenannten *Faktor* validiert. Authentifizierungsfaktoren sind im Allgemeinen einer von drei Typen:

- **Etwas, das Sie wissen** – wie eine persönliche Identifikationsnummer (PIN), ein Passwort oder der Mädchenname Ihrer Mutter
- **Etwas, das Sie haben oder besitzen** – wie ein Smartphone, Ihr Betriebsausweis oder ein FIDO U2F-Schlüssel (Fast ID Online Universal Second Factor)
- **Etwas, das Sie sind** – eine eindeutige biometrische Kennung wie Fingerabdruck, Netzhaut- oder Irismuster

Die meisten Anwendungen authentifizieren Benutzer anhand eines einzigen Faktors, in der Regel anhand eines Passworts. Die Verwendung von Passwörtern, obwohl einfach und unkompliziert, hat viele Nachteile. Passwörter bieten die einfachste Möglichkeit, in Ihre Systeme einzudringen, und Hacker können sie auf vielfältige Weise nutzen.

TIPP

Die fünf häufigsten Passwortattacken sind: breitangelegtes Phishing, gezieltes Spear-Phishing, Credential Stuffing, Password Spraying und Man-in-the-Middle. Unter `https://www.okta.com/resources/whitepaper/5-identity-attacks-that-exploit-your-broken-authentication/` erfahren Sie, wie diese Attacken ausgeführt werden.

TIPP

Nutzen Sie kostenlose Ressourcen wie `https://haveibeenpwned.com/` und das PassProtect-Plug-In für den Google Chrome-Browser, um zu sehen, ob Ihre Passwörter und Konten kompromittiert wurden.

TECHNISCHES

Passwörter sind außerdem anfällig für Brute-Force-Angriffe. Die meisten Systeme können diese Angriffe jedoch blockieren, indem sie nach einer bestimmten Anzahl fehlgeschlagener Anmeldeversuche eine Kontosperrung vornehmen.

Die Lösung für die inhärenten Schwächen und Herausforderungen bei Passwörtern und Einzelfaktor-Authentifizierung ist die Multi-Faktor-Authentifizierung (MFA)!

MFA erfordert zwei oder mehr Faktoren, um eine Identität zu authentifizieren. Beispielsweise kann MFA verlangen, dass sich ein Benutzer mit einem Passwort bei einer Website anmeldet und dann eine einmalige Kennung eingibt, die an sein Smartphone gesendet wird. Die Kennung bleibt für eine begrenzte Zeit (in der Regel drei bis fünf Minuten) gültig und kann nur für einen Anmeldeversuch verwendet werden. Wenn die Kennung falsch eingegeben wurde oder sich der Benutzer von der Sitzung abmeldet und versucht, sich erneut mit derselben Kennung anzumelden, schlägt der Anmeldeversuch fehl.

Der Nachteil von MFA ist, dass sie bei jeder Anmeldung eines Benutzers erforderlich ist und so MFA-Ermüdung verursachen kann. MFA birgt Reibungspunkte für Endbenutzer, die sich während ihres Arbeitstages erneut authentifizieren oder eine Kombination aus Hardware- und Software-Token verwenden müssen, um Zugriff zu erhalten. Jeder zusätzliche Authentifizierungsfaktor verbessert zwar die Zugriffskontrolle, tut dies aber auf Kosten der Benutzerfreundlichkeit. MFA-Ärgernisse können jedoch verringert werden, indem die Anzahl der Anmeldungen für Benutzer reduziert wird (mit – Sie haben es erraten – SSO!), nahtlose und intuitive Faktoren verwendet werden und Ihre MFA an unterschiedliche Kontexte und Risikoprofile angepasst wird.

IDaaS bietet eine umfassende Unterstützung für verschiedene MFA-Faktoren, um ein ausgewogenes Verhältnis von Sicherheit, Kosten und Benutzerfreundlichkeit zu schaffen. Diese Faktoren reichen von geringer Sicherheit (wie Sicherheitsfragen und SMS-Textcodes) bis hin zu hoher Sicherheit (wie Push-Benachrichtigungen, Biometrie und Hardwaretoken).

TIPP

Viele Unternehmen verlassen sich nach wie vor auf Faktoren mit geringer Sicherheit wie Sicherheitsfragen und SMS-Textcodes. Sicherheitsfragen sind heute der beliebteste Faktor und finden zunehmend breitere Verwendung. Laut einer Studie von Okta verwenden heute 38 Prozent der MFA-Benutzer Sicherheitsfragen als zweiten Faktor, verglichen mit 30 Prozent im Vorjahr. Das Problem bei Sicherheitsfragen ist, dass die Antworten auf diese Fragen (zum Beispiel der Mädchenname Ihrer Mutter oder der Name Ihres Ehepartners) oft in öffentlichen Aufzeichnungen und in sozialen Medien zu finden sind. Auch die Verwendung von SMS-Textnachrichten als einziger zweiter Faktor birgt Risiken. Für Unternehmen, die Vorschriften wie DFARS (Defense Federal Acquisition Regulation Supplement) einhalten müssen, erlauben die Richtlinien des US-amerikanischen National Institute of Standards and Technologies (NIST) keine SMS-basierte Zwei-Faktor-Authentifizierung mehr, da die Gefahr besteht, dass Codes abgefangen werden. Dies bedeutet nicht, dass diese Faktoren in einer MFA-Lösung ineffektiv sind. Es kommt darauf an, die richtigen Faktoren für das richtige Risikoniveau zu verwenden.

IDaaS implementiert adaptive MFA, um die Sicherheit zu verbessern, ohne dass die Benutzerfreundlichkeit leidet. Adaptive MFA analysiert individuelle Anmeldeanforderungen mithilfe von Backend-Analysen, um festzustellen, wie viele Faktoren erforderlich sind und wie viel Zugriff gewährt werden soll. Wenn ein Mitarbeiter beispielsweise auf dem Firmengelände arbeitet und einen Smart-Ausweis verwendet, um durch die Sicherheitskontrolle in sein Büro zu gelangen, erkennt adaptive MFA, dass er sich an einem vertrauenswürdigen Ort befindet und möglicherweise nur seinen Fingerabdruck benötigt, um sich beim System anzumelden. Wenn der gleiche Mitarbeiter jedoch an einem privaten Gerät in einem Café arbeitet, fordert ihn adaptive MFA möglicherweise zur Eingabe eines zusätzlichen Authentifizierungsfaktors auf.

Provisionierung und Workflows

Bis zu diesem Punkt haben Sie drei Bausteine von IDaaS kennengelernt: Das Directory hält Benutzerdaten und -konfigurationen fest, SSO reduziert Reibungspunkte für Benutzer beim Zugriff auf Hunderte von Systemen und Anwendungen und adaptive MFA verbessert die Benutzersicherheit für den Zugriff auf alle Anwendungen auf Basis ihrer jeweiligen Risikostufe. Aber es gibt noch eine letzte Herausforderung: Wie stellen Sie sicher, dass Ihre Benutzer korrekt in Ihr IDaaS-Directory

aufgenommen und den Systemen zugeordnet werden, die sie für die Anmeldung benötigen? Provisionierung und Workflows lösen dieses Problem.

Mit Provisionierung können Unternehmen IDaaS nicht nur zur Kontrolle des Zugriffs auf Systeme verwenden, sondern auch, um Konten und Berechtigungen basierend auf dem Status ihrer Benutzer zu erstellen, zu aktualisieren und zu löschen. Der Benutzerstatus kann direkt im IDaaS-Directory oder in wichtigen Drittanbietersystemen definiert werden, die als verlässliche Informationsquelle für das Unternehmen gelten (die verlässliche Informationsquelle für Mitarbeiter im Unternehmen könnte beispielsweise das Personalsystem sein).

Provisionierung automatisiert die Konto- und Berechtigungsverwaltung interner und externer Konten und spart so Zeit und Geld. Im Durchschnitt sparen Unternehmen 30 Minuten bei jeder Anforderung zur Anwendungsbereitstellung, 30 Minuten beim Festlegen und Konfigurieren von Gruppen und Berechtigungen sowie 20 US-Dollar pro Benutzer bei der jährlichen Vorbereitung auf Audits. Multipliziert mit den Tausenden Bereitstellungsanforderungen und diversen Audits, mit denen sich ein typisches Unternehmen jedes Jahr befassen muss, können die Zeit- und Kosteneinsparungen erheblich sein.

Aufgrund von Identitätsänderungen müssen jedoch auch andere Prozesse in Drittsystemen ausgelöst werden, die über die Kontenverwaltung hinausgehen. Zum Beispiel:

- Martin tritt dem Sicherheitsteam bei. Er erhält Zugriff auf die Sicherheitssysteme und muss zusätzlich eine Sicherheitsschulung absolvieren (zum Beispiel bei Udemy) sowie ein Dokument unterschreiben (zum Beispiel in Adobe Sign oder DocuSign), in dem er bestätigt, dass er den Kurs verstanden und abgeschlossen hat.
- Lara, eine in Deutschland lebende Kundin, greift auf die Shopping-App Ihres Unternehmens zu und fordert eine Kopie aller von Ihrem Unternehmen erhobenen personenbezogenen Daten an. Die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) verlangt von Ihrem Unternehmen, Lara innerhalb von 30 Tagen eine Kopie ihrer Daten zur Verfügung zu stellen.

Workflows sind eine IDaaS-Funktion, die Automatisierung über die Kontobereitstellung hinaus ermöglichen, sodass Sie diese Art von Prozessen automatisieren und orchestrieren können, ohne dass zusätzlicher Code geschrieben werden muss.

MERKEN

IDaaS bietet alle Bausteine des IAM – Directory, SSO, adaptive MFA sowie Provisionierung und Workflows – in einem einzigen zusammenhängenden Paket, das für Sie einsatzbereit ist, sobald Sie den Service

abonnieren. Dies ermöglicht die kürzeste Amortisierungszeit, sodass Sie sich auf wichtige Dinge wie das Einrichten von Sicherheit und Verbessern der Benutzererfahrung konzentrieren können. Parallel dazu sparen Sie Zeit und Geld, da Sie keine separaten Lösungen installieren, patchen und integrieren müssen.

Ressourcen

In diesem Abschnitt werden einige der wichtigsten Arten von Ressourcen beschrieben, für die Sie mithilfe von IDaaS-Directory, SSO, adaptiver MFA, Provisionierung und Workflows den Zugriff absichern und die Identität verwalten können.

Cloud-Anwendungen

Es gibt eine Vielzahl von Cloud-Anwendungen wie Office 365, Salesforce, Amazon Web Services und Slack. Tatsächlich entwickelt sich die Cloud zum vorherrschenden Bereitstellungsmodell für Anwendungen und ersetzt schnell lokal installierte Software als bevorzugte Methode. Moderne IDaaS-Lösungen bieten Ihnen einen Katalog vorgefertigter Anwendungsintegrationen. Sie können diesen Katalog für die minutenschnelle Integration in Ihre Cloud-Anwendungen verwenden.


TIPP

Die Integration zwischen IDaaS-Lösungen und Cloud-Anwendungen erfolgt über offene Standards wie SAML für die Föderierung und SCIM (System for Cross-domain Identity Management) für die Provisionierung.


TIPP

Okta verfügt derzeit über mehr als 6.000 vorgefertigte Anwendungsintegrationen.

On-Premises-Anwendungen

Obwohl Unternehmen immer mehr Cloud-Anwendungen und -Services einführen, laufen in den meisten Unternehmen zumindest einige der Systeme vor Ort. Moderne IDaaS-Lösungen bieten Funktionen für den sicheren Zugriff auf lokale Webanwendungen, wobei herkömmliche Integrationsmuster und Standards wie LDAP (Lightweight Directory Access Protocol), RADIUS (Remote Authentication Dial-in User Service), Kerberos und Header-basierte Authentifizierung verwendet werden, ohne dass Änderungen am Anwendungsquellcode erforderlich sind.


TIPP

Sie können mit der gleichen IDaaS-Lösung alle Ihre Systeme – von der lokalen Umgebung bis zur Cloud – mit denselben Sicherheitsrichtlinien schützen. So sparen Sie Zeit und Geld und nutzen stets die neuesten Sicherheitsfunktionen.

Selbst entwickelte Apps

Mark Andreessen, Gründer von Netscape, schrieb vor fast einem Jahrzehnt: „Software frisst die Welt auf." Jedes Unternehmen ist heute zu einem gewissen Grad ein „Tech-Unternehmen", das eine digitale Präsenz für sich selbst aufbaut, sei es E-Shopping, eine Ride-Sharing-App oder der nächste große Trend. Für Unternehmen ist Software-Innovation das „Tischgeld" für das Überleben in der heutigen extrem wettbewerbsorientierten globalen Wirtschaft.

Schauen Sie sich in Ihrem eigenen Unternehmen um. Wie viele App-Entwickler haben Sie heute, verglichen mit vor nur fünf Jahren? Wenn Sie in einem wirklich innovativen, führenden Unternehmen arbeiten, haben Sie wahrscheinlich nicht nur mehr Entwickler – Sie haben mehr *Arten* von Entwicklern, darunter Mobilgeräte-App-Entwickler, Datenwissenschaftler und Machine Learning-Ingenieure. All diese Leute entwickeln spezialisierte Anwendungen, die Sicherheit erfordern, aber sie sind nicht unbedingt (oder wahrscheinlich keine) Sicherheitsexperten. Die Bereitstellung einer unsicheren App, die für Kontoübernahmen oder Anmeldedaten-Kompromittierung anfällig ist, kann ein Unternehmen teuer zu stehen kommen und zu Rechtsstreitigkeiten, Bußgeldern und Strafen, schlechter Publicity, Reputationsschäden für die Marke sowie zum Verlust von Kundenvertrauen und Geschäftsmöglichkeiten führen.

IDaaS bietet integrierte SSO- und MFA-Funktionen in Form von SDKs (Software Development Kits) und APIs, die Entwickler schnell und einfach zu ihren Anwendungen hinzufügen können, damit sie sich auf das konzentrieren können, was sie am besten können – die Entwicklung von Apps – mit erstklassiger Sicherheit für Directory, SSO, MFA, Provisionierung und Workflows.

Server

Software muss irgendwo ausgeführt werden und zwar in der Regel auf Servern, die an mehreren Orten gehostet werden können – einschließlich eines lokalen Rechenzentrums, einer privaten Cloud oder einer öffentlichen Cloud wie Amazon Web Services (AWS), Google Cloud Platform (GCP) oder Microsoft Azure. Mit modernen Architekturen und App-Entwicklungstools wie Microservices, Containern, Serverless, Kubernetes und DevOps kann die Anzahl der Instanzen, auf denen Ihre Anwendung ausgeführt wird, je nach Auslastung dynamisch variieren. So könnte beispielsweise eine neue App auf nur zehn Servern in einer öffentlichen Cloud gestartet werden und wenn sie innerhalb weniger Stunden viral wird, haben Sie in Ihrer Cloud-Infrastruktur möglicherweise mehr als 1.000 Server, die zur Bewältigung der Last bereitgestellt wurden. Stellen Sie sich vor, Sie versuchen, alle diese Server selbst zu sichern, während sie mit enormer Geschwindigkeit herauf- oder

herunterskaliert werden. Moderne IDaaS-Lösungen bieten Ihnen die Möglichkeit, den Zugriff auf alle Ihre Server und Anwendungsinstanzen automatisch zu sichern.

Application Programming Interface (API)

APIs sind der Antrieb für all die Software, die die Welt auffrisst. Man kann sich APIs als eine App vorstellen, die von anderen Apps und intelligenten Geräten des Internet der Dinge (IoT) genutzt werden kann. Mit APIs sparen Entwickler Zeit, da sie keine Funktionen erstellen müssen, die bereits von einem anderen Benutzer erstellt wurden. Einige Beispiele für Verwendungsmöglichkeiten von APIs:

- Twilio zum Senden von SMS-Nachrichten an ein Smartphone
- Stripe zum Verarbeiten von Kreditkartenzahlungen
- Google Analytics zum Verfolgen von Besuchen auf Ihrer Website

Darüber hinaus können Sie als Unternehmen Teil der API-Wirtschaft werden: Erstellen Sie eigene APIs, bieten Sie sie anderen Unternehmen für deren Anwendungen an und generieren Sie Einnahmen aus Anfragen. Wenn Sie zum Beispiel ein Frachtunternehmen betreiben, können Sie eine API anbieten, die Lieferzeiten und Versandkosten berechnet oder Versandetiketten anfordert.

Moderne IDaaS-Lösungen sichern und autorisieren den Zugriff auf APIs und nutzen API-Sicherheitsstandards wie Open Authorization (OAuth).

Und vieles mehr ...

Gelegentlich haben Sie IT-Ressourcen, die zwar Identität erfordern, aber nicht als Cloud-App, On-Premises-App, Server, selbst entwickelte App oder API klassifiziert sind. Auch in diesen Situationen können Sie die Identitätssicherheit von IDaaS durch offene Standards nutzen. Offene Standards und Muster werden in vielen Branchen (einschließlich IT) verwendet, um eine nahtlose Integration zwischen Systemen zu ermöglichen.

Ohne Standards wäre beinahe alles auf der Welt schwieriger. Wie wäre es, eine Lampe zu kaufen, wenn jeder Hersteller seine eigenen Glüh-birnen verwendet, die nur in seinen Lampen funktionieren, oder ein Telefon zu benutzen, wenn jeder Ihrer Kontakte eine unterschiedlich lange Telefonnummer hat – 22 Ziffern, 15 Ziffern, 11 Ziffern oder nur eine Ziffer!

Identität verwendet, wie jede andere Branche, Standards. Es gibt Identitätsstandards für alles: von Verzeichnissen (wie LDAP) über Authentifizierung und SSO (wie SAML, RADIUS und OIDC) bis hin zu Provisionierung und Workflows (wie SCIM und Representational State

Transfer [REST] und Webhooks). IDaaS nutzt diese Standards zur Unterstützung einer Vielzahl von Systemen.

MERKEN

Standards erlauben Ihnen, branchenführende Lösungen zu implementieren und eine Bindung an anbietereigene Lösungen zu vermeiden. Die Bindung an einen Anbieter schränkt die Flexibilität Ihres Unternehmens ein, da dieser Anbieter die Preise für laufende Wartung und Support diktieren kann. Zudem sind Sie auf das Funktionsangebot beschränkt, das er in seinem Produktentwicklungsplan vorsieht (sofern er *überhaupt* einen Entwicklungsplan hat). Wenn Sie genug von diesem Anbieter haben, kann der Wechsel zu einer anderen Lösung sehr teuer sein (zum Beispiel: Wie bekommen Sie Ihre Daten aus dem alten System in das neue?).

TIPP

Laden Sie das E-Book zu Integrationsmustern für Legacy-Anwendungen unter `https://okta.com/resources/whitepaper-integration-patterns-for-legacy-applications` herunter und lesen Sie den Okta-Blog unter `https://okta.com/blog`, um mehr über Standards und Integration zu erfahren.

Weitere wichtige Überlegungen

Identität ist eine geschäftskritische Komponente Ihrer IT. Wenn Ihr Identitätssystem nicht läuft, verlieren Benutzer den Zugriff auf mehrere Ressourcen. Wenn Ihre Identitätslösung nicht sicher ist, ist Ihr gesamtes Unternehmen erheblich gefährdet. Um eine IDaaS-Lösung zu wählen, die Sie nicht im Stich lässt oder bindet, müssen Sie zusätzliche Faktoren berücksichtigen. Dazu gehören Integrationen, Neutralität, Sicherheit und Datenschutz, Compliance und Verfügbarkeit.

Integrationen

Integrationen von Drittanbietern sind ein maßgeblicher Aspekt für Unternehmen, die IDaaS in Betracht ziehen. Ein breites Ökosystem an Integrationen hilft Ihnen bei der nahtlosen Umsetzung von SSO, der Vermeidung einer Anbieterbindung und dem Erschließen neuer Wertangebote aus vorhandenen Anwendungen und IT-Systemen. Eine IDaaS-Lösung sollte anhand eines Integrationskatalogs die Anwendungen unterstützen, die Sie heute nutzen bzw. deren zukünftige Nutzung Sie erwägen. Darüber hinaus sollte die Lösung eine umfassende Auswahl an Integrationen über SSO hinaus bieten, darunter:

- **Anmeldung und Provisionierung:** Ermöglicht es Ihnen, Zugriff und Provisionierung für Anwendungen wie Box, Office 365, Salesforce, ServiceNow, Slack und Zoom innerhalb von Minuten zu steuern. Die Integration sollte über SSO hinausgehen und

Benutzer-Provisionierung, Offboarding und erweiterte Integrationen über Workflow-, Geräte- und Lizenzverwaltungsoptionen unterstützen.

- **Personalinformationssysteme (HRIS):** Stellen Sie eine Verbindung zu Personalverwaltungssystemen wie Workday und SuccessFactors her, um den Neuzugang und das Ausscheiden von Mitarbeitern zu automatisieren.
- **Application Delivery Controller (ADC):** Verbinden Sie externe Benutzer mit lokalen ADCs wie Citrix, F5 und Akamai.
- **Netzwerksicherheit:** Implementieren Sie SSO und MFA in Sicherheitslösungen für Unternehmensnetzwerke wie Cisco, Check Point, Palo Alto Networks und Zscaler.
- **Sicherheitsanalyse:** Erweitern Sie Ihre Sicht auf Cloud-, mobile und lokale Systeme zur Stärkung von Korrelations- und Durchsetzungsmöglichkeiten. Beispiele sind LogRhythm, Rapid7, QRadar und Splunk.

TIPP

Okta veröffentlicht seinen Anwendungskatalog unter `https://www.okta.com/okta-integration-network/`.

Neutralität

Die Verwendung offener Standards und die Bereitstellung von Integrationen – beide in den vorherigen Abschnitten erörtert – in einer modernen IDaaS-Lösung sind wichtig, reichen aber nicht aus. Ein IDaaS-Service-Provider muss neutral sein. Das heißt, Ihr Service-Provider muss den klaren Nachweis erbringen, dass er keine Favoriten unter den Lösungen wählt, mit denen er arbeitet, und Sie so indirekt an den einen oder anderen Anbieter bindet. Zum Beispiel bieten Microsoft, NetSuite, Salesforce und Zoho (beachten Sie, dass wir keine Favoriten nennen und sie in alphabetischer Reihenfolge auflisten!) durchweg hervorragende CRM-Software (Customer Relationship Management), und sie alle stehen im wechselseitigen Wettbewerb. Eine moderne IDaaS-Lösung muss innerhalb einer gegebenen Kategorie so viele gängige Software-Optionen wie möglich unterstützen.

TIPP

Achten Sie bei einem modernen IDaaS-Anbieter auf folgende Neutralitätszeichen:

- Ein breites Ökosystem mit (mindestens 5.000) nativen Integrationen in IT-Systeme und Software
- Tiefgreifende Integrationen, auch mit Konkurrenzprodukten von den Anbietern, die eine bestimmte Lösung anpreisen
- Breite Unterstützung für offene Industriestandards

TIPP

Okta unterstützt eine große Auswahl an Anbietern und Lösungen, die unter `https://www.okta.com/oin/` aufgelistet sind.

Sicherheit und Datenschutz

Sicherheit und Datenschutz sind heute für jedes Unternehmen von größter Bedeutung, und bei Ihrem Anbieter von modernem IDaaS ist es nicht anders. Achten Sie bei Ihrem IDaaS-Anbieter auf die folgenden Sicherheits- und Datenschutzzusicherungen:

- Dokumentation seiner Sicherheitskontrollen (das heißt Vertraulichkeit, Integrität und Verfügbarkeit).
- Unterstützung des Modells der geteilten Verantwortung für Cloud-Sicherheit, das klar umreißt, wofür jeweils er und Sie verantwortlich sind.
- Dokumentation, Best Practices und Produktfunktionen, die Ihnen helfen, Ihre Service-Instanz zu sichern.
- Nachweis einer soliden Erfolgsbilanz in puncto Sicherheit und Privatsphäre. Ihr IDaaS-Anbieter sollte Tools und Nachweise wie Trust Portals, öffentliche Bug-Bounty-Programme und automatisierte Sicherheitstests bereitstellen.
- Das Recht, die Sicherheit seiner IDaaS-Plattform und -Lösung zu testen.
- Zertifizierungen wie Security Trust Assurance and Risk (STAR) derCloud Security Alliance (CSA), Federal Risk and Authorization Management Program (FedRAMP), International Organization of Standardization (ISO) 27001 und System and Organization Controls (SOC) 2 Typ 2.

TIPP

In diesem Whitepaper finden Sie weitere Informationen über die Okta-Servicesicherheit: `https://www.okta.com/resources/whitepaper-okta-security-technical-white-paper`.

Compliance

Unternehmen in unterschiedlichen Branchen müssen unterschiedliche Anforderungen hinsichtlich der Einhaltung gesetzlicher Vorschriften erfüllen. Stellen Sie sicher, dass Ihre IDaaS-Lösung alle behördlichen Anforderungen bzw. Branchenstandards erfüllt, die möglicherweise für Ihr Unternehmen gelten. Dazu gehören beispielsweise die Datenschutz-Grundverordnung (DSGVO), der California Consumer Privacy Act (CCPA), Sarbanes-Oxley (SOX), der Health Insurance Portability and Accountability Act (HIPAA) und andere. Relevante Standards könnten zum Beispiel die Payment Card Industry (PCI) Data Security Standards

(DSS) und die Standards der Internationalen Organisation für Normung (ISO) 27001 sein.

TIPP

Unter `https://trust.okta.com/compliance` erfahren Sie mehr über den Compliance-Ansatz und die Zertifizierungen von Okta.

EIN IDAAS-BEISPIEL: WIE ES OKTA MACHT

Die Okta Identity Cloud ist die von Okta entwickelte und verwaltete IDaaS-Plattform. Als echter Cloud-nativer Service – zu 100 Prozent in der Cloud entwickelt und aufgebaut – bietet die Okta-Plattform wichtige Vorteile:

- Sie ist weltweit verfügbar, 100 Prozent mandantenfähig, zustandslos und redundant.
- Sie wird regelmäßig mit Sicherheitsverbesserungen und neuen Funktionen aktualisiert.
- Sie hat keine geplante Ausfallzeit: Okta aktualisiert die Plattform dynamisch und benötigt keine Ausfallzeit für die Wartung.
- Sie reduziert die operativen Aufgaben sowie Setup- und Wartungskosten drastisch.
- Sie ist abonnementbasiert und kostenflexibel.

Diese Vorteile sind nur selten bei On-Premises-Software, Managed Cloud Services oder bei Anbietern zu finden, die ältere On-Premises-Software in die Cloud portiert haben.

Das Funktionsangebot der Identity Cloud Platform umfasst Produkte für Mitarbeiter- und Kundenidentität.

Mitarbeiteridentität

Workforce Identity-Produkte sind für IT- und Sicherheitsverantwortliche gedacht. Vereinfacht ausgedrückt erleichtern sie Benutzern das Verbinden mit Unternehmenstechnologie, erhöhen gleichzeitig die Effizienz und tragen dazu bei, dass IT-Umgebungen sicher bleiben. Zu diesen Lösungen gehören:

- **Universal Directory:** Mit diesem flexiblen, Cloud-basierten Benutzerspeicher können Sie beliebige Benutzerattribute aus mehreren Identitätsquellen anpassen, organisieren und verwalten.
- **Single Sign-On:** Befreien Sie Ihre Mitarbeiter von der Mühsal unterschiedlicher Passwörter. Ein einziger Satz von Anmeldedaten gewährt

ihnen Zugriff auf Unternehmensanwendungen in der Cloud, am Arbeitsplatz und auf mobilen Geräten.

- **Lifecycle Management:** Automatisieren Sie das Onboarding und Offboarding von Benutzern, indem Sie die nahtlose Kommunikation zwischen Verzeichnissen wie Active Directory und LDAP sowie Cloud-Anwendungen wie Workday, SuccessFactors, Office 365 und RingCentral gewährleisten.
- **Adaptive Multi-Factor Authentication:** Sichern Sie Ihre Anwendungen und Ihr virtuelles privates Netzwerk (VPN) mit einem robusten Policy-Framework, einer umfassenden Reihe moderner Verifizierungsfaktoren und einer adaptiven, risikobasierten Authentifizierung ab, die sich in alle Ihre Anwendungen und Infrastrukturen integrieren lässt.

Mit Workforce Identity verfügt die IT über eine zentrale Stelle für eine richtlinienbasierte Verwaltung, an der festgelegt wird, welche Benutzer Zugriff auf die geschäftskritischen Anwendungen und Daten erhalten, die die wichtigsten Geschäftsprozesse steuern.

Mitarbeiter profitieren von einer Single Sign-On-Startseite, die ihr Leben vereinfacht und durch „Passwortmüdigkeit" verursachte Sicherheitsrisiken reduziert. Mit Okta greifen sie nicht mehr auf riskante Methoden zum Speichern von Passwörtern zurück – zum Beispiel durch die Auswahl offensichtlicher oder wiederverwendeter Passwörter, das Aufschreiben von Passwörtern auf Post-it-Notizen oder das Speichern in Excel-Dateien auf ihren Laptops.

Kundenidentität

Mit Customer Identity-Produkten können Sie Okta als Identitätsebene in Ihre Anwendungen einbetten oder Okta für die folgenden Zwecke anpassen:

- **Stellen Sie eine anpassbare Benutzererfahrung bereit:** Nutzen Sie Okta-APIs und -Widgets, um vollständig markenspezifische Anmeldeabläufe oder Endbenutzerportale zu erstellen. Sie können mithilfe von Okta-APIs sogar eigene Administrationsprozesse erstellen, in deren Rahmen Kunden oder Abteilungsleiter ihre Benutzer verwalten können.
- **Nutzen Sie Okta für jeden Anwendungsfall:** Bewältigen Sie jede komplexe Problemstellung bei der Identitätsintegration, bei Daten oder der Automatisierung durch die Nutzung der umfassenden APIs von Okta. Führen Sie Skripte zum Ändern von Benutzerdaten, zur automatischen Integration von Anwendungen oder zur Integration in unternehmensspezifische Workflows aus.

(Fortsetzung)

(Fortsetzung)

- **Nutzen Sie die branchenbeste Customer IAM (CIAM)-Lösung:** Geben Sie Ihren Entwicklern die Freiheit, sich auf die Kundenerfahrung zu konzentrieren, und überlassen Sie Okta die Identität. Nutzen Sie Okta als „Identitäts-API" für alle Ihre Anwendungsentwicklungsprojekte und überlassen Sie Okta die Authentifizierung, Autorisierung und Benutzerverwaltung.

Customer Identity-Produkte bieten programmatischen Zugriff auf die Okta Identity Cloud, sodass Ihre Entwickler erstklassige Benutzererlebnisse aufbauen und Okta auf jede vorstellbare Weise erweitern können. Mit der Unterstützung der Kundenidentität für Ihr digitales Unternehmen kann Okta Ihre komplexesten Herausforderungen in der Unternehmensarchitektur bewältigen.

Unternehmen, die den Okta-Service nutzen, verzeichnen eine dramatische Verbesserung bei der Sicherheit und den Erfahrungen von Benutzern bei der Interaktion mit ihren Anwendungen – ob Mitarbeiter, Auftragnehmer oder Kunden, die einen Cloud-Dienst, eine On-Premises-Anwendung, VPN, eine Firewall oder eine selbst entwickelte Anwendung nutzen.

Verfügbarkeit

Ein IDaaS-Anbieter muss sicherstellen, dass der Service immer verfügbar ist, damit sich Mitarbeiter und Kunden in Ihrem Unternehmen jederzeit von überall und von jedem Gerät anmelden können.

Suchen Sie nach einem IDaaS-Anbieter mit einer robusten Cloud-Architektur, umfassenden Service Level Agreements (SLAs), die Ihre geschäftlichen Anforderungen erfüllen, und einem öffentlichen Dashboard mit Echtzeitüberwachung und Statusinformationen zum Service.

TIPP

Okta veröffentlicht seine Serviceverfügbarkeit in Echtzeit unter `https://trust.okta.com`.

IN DIESEM KAPITEL

- Von Null auf Zero Trust
- Nutzung der Blockchain-Technologie
- Betrachtung von Identitätsherausforderungen und Lösungen im Internet der Dinge (IoT)
- Ansätze für Datenschutzbelange
- Ein Blick auf führende Anwendungen

Kapitel 4
Ein Blick in die nahe Zukunft von Identität

In diesem Kapitel erfahren Sie, was die nahe Zukunft für Identität bereithält und wie moderne Identität Ihnen hilft, mit kommenden Innovationen auf dem neuesten Stand zu bleiben.

Zero Trust

Aufgrund der Allgegenwart von Mobile- und Cloud-Computing ist das Konzept eines Netzwerk-Perimeters – mit einem „vertrauenswürdigen" internen Netzwerk und einem „nicht vertrauenswürdigen" externen Netzwerk – praktisch überholt. In dieser neuen Realität müssen Unternehmen ihren Benutzern sicheren Zugriff ermöglichen, unabhängig von Standort, Gerät oder Netzwerk.

Um diesen Herausforderungen zu begegnen, hat John Kindervag 2010 bei Forrester Research das Zero-Trust-Security-Framework geschaffen. Zero Trust basiert auf dem Prinzip „Vertrauen ist gut, Kontrolle ist besser", das heißt, die richtigen Personen haben die richtigen Zugriffsrechte auf die richtigen Ressourcen im richtigen Kontext, und dieser Zugriff wird kontinuierlich bewertet. Das Identitäts- und Zugriffsmanagement (IAM) ist somit eine Kerntechnologie und ein Dreh- und Angelpunkt im Zero-Trust-Framework und sollte der Ausgangspunkt für Unternehmen sein, die eine Zero-Trust-Architektur implementieren.

TIPP

Forrester Research hat Okta in seinem Bericht „The Forrester Wave: Zero Trust Extended Ecosystem Platform Providers, Q4 2019“ als einen führenden Anbieter eingestuft. Okta erzielte die höchstmögliche Punktezahl in der Hälfte der Bewertungskriterien.

Dezentralisierte/selbstsouveräne Identität

In einem dezentralen oder selbstsouveränen Identitätsmodell verwalten Einzelpersonen ihre digitalen Identitäten selbst. Dieses Modell gibt dem Einzelnen eine größere Kontrolle über seine Konten und Daten. Eine selbstsouveräne Identität besteht aus drei Komponenten: Einem *Anspruch*, in dem die Person ihre Identität geltend macht; *Nachweisen* – wie etwa einem Block in einer Blockchain – als Beleg der Gültigkeit eines Anspruchs; und einer *Bescheinigung*, in der ein System den Anspruch auf der Grundlage des vorgelegten Nachweises validiert.

Ein häufiges Beispiel für aktuelle selbstsouveräne Identität ist Apple FaceID, das auf iPhones zum Zugreifen auf das Telefon, für Online-Einkäufe sowie für die Anmeldung bei verschiedenen Apps verwendet wird. Der Anspruch wird lokal auf dem Gerät gespeichert, wenn FaceID für den iPhone-Benutzer eingerichtet wurde. Der Nachweis ist der Satz von einzigartigen Gesichtsmerkmalen des Benutzers, die zuvor im Rahmen des Einrichtungsprozesses zusammen mit dem Anspruch registriert wurden, und die Bescheinigung ist die automatische Verifizierung des Anspruchs und des Nachweises durch die FaceID-Software.

Internet of Things (IoT)

Als Internet der Dinge (Internet of Things, IoT) wird das Netzwerk „intelligenter“ Geräte bezeichnet, in die Elektronik, Software, Sensoren und Netzwerkkonnektivität eingebettet sind, um erweiterte Fähigkeiten und Funktionen bereitzustellen. Obwohl das IoT viele Innovationen bietet, birgt es auch ein viel größeres Risiko für Zugriffskontrolle und Daten.

Was bedeutet das IoT für IAM? IoT-Geräte müssen ordnungsgemäß identifiziert und authentifiziert werden, und die Cloud ist die einzige Plattform, die die zuverlässige Skalierbarkeit bietet, um Verzeichnisdienste und Zugriffskontrolle für mehrere Milliarden von Geräten weltweit unterstützen zu können.

TIPP

Es hat sich auch gezeigt, dass das IoT Teil der Lösung sein kann. IDaaS-Lösungen können Wearables wie die Apple Watch als Faktor für die adaptive Multi-Faktor-Authentifizierung (MFA) nutzen und Push-Benachrichtigungen zur Authentifizierung von Zugriffsanfragen bereitstellen.

Datenschutz auf globaler Ebene

Datenschutzvorschriften wie die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU), der California Consumer Privacy Act (CCPA) und die Australian Privacy Principles (APP) haben umfassendere Datenschutzrechte für Einzelpersonen definiert und stellen Unternehmen weltweit vor wachsende rechtliche und Compliance-Herausforderungen.

Ein Aspekt vieler Datenschutzbestimmungen ist die Anforderung, dass Einwilligungsdaten (wie zum Beispiel gesetzliche Vereinbarungen und Marketinginformationen) erfasst, regelmäßig überprüft, von Verbrauchern erneut bestätigt und für einen konkreten Verarbeitungszweck bereitgestellt werden. Darüber hinaus müssen Unternehmen bei Einwilligungen sicherstellen, dass nur die erforderlichen Mindestdaten erfasst und diese nur für rechtmäßige und autorisierte Verarbeitungszwecke verwendet werden. Hinzu kommt, dass einige Einwilligungen (zum Beispiel Marketinganfragen) vom Nutzer widerrufen werden können, während dies bei anderen (zum Beispiel rechtlichen Vereinbarungen) nicht möglich ist.

Für das Management von Einwilligungen müssen Unternehmen zahlreiche Vorschriften und Kundendaten im Blick behalten, die in mehreren Systemen und Datenbanken aufgezeichnet sind. Lösungen wie Customer Data Platforms (CDP) und IDaaS helfen, Kundendaten zu aggregieren und die Verarbeitung von Einwilligungen über mehrere Datenunterverarbeiter und Systeme hinweg zu vereinfachen.

TIPP

Da immer mehr Länder ihre Einwilligungsanforderungen erweitern, werden für das Einwilligungsmanagement Lösungen für die Unterstützung von Datenschutz auf globaler Ebene benötigt.

Identitätsfreiheit

Angesichts des Wachstums und der zunehmenden Heterogenität des Unternehmenssoftware-Ökosystems suchen Unternehmen nach den besten Anwendungen, die ihre Mitarbeiter unterstützen und die Effizienz bei gleichzeitiger Wahrung der Kontrolle und Sicherheit steigern. Unternehmen stellen zunehmend branchenführende, sogenannte Best-of-Breed-Anwendungen wie Slack und Zoom sowie komplette Anwendungssuiten wie Office 365 bereit – selbst wenn sich ihre Funktionen überschneiden.

TIPP

Mit Stand vom Juni 2019 hatten mehr als 77 Prozent der Okta-Kunden mit Office 365 zusätzlich auch Best-of-Breed-Anwendungen wie Slack, Zoom, Box, AWS, Salesforce oder G-Suite eingeführt – und diese Zahl

wächst weiter. Zwischen Oktober 2018 und Juni 2019 verzeichnete Zoom eine 25-prozentige Zunahme der Office 365-Kunden, die seine Lösung einführten. Das ist mehr als bei jeder anderen innerhalb der Okta-Kundenbasis analysierten Best-of-Breed-Anwendung. Das Wachstum von Slack unter Office 365-Kunden lag ebenfalls im zweistelligen Bereich und stieg von 11 auf 31 Prozent, was bedeutet, dass der Startschuss im Wettlauf um Best-of-Breed-Collaboration-Apps im Enterprise-Bereich gefallen ist.

Obwohl Benutzer innerhalb eines Unternehmens oftmals schnell Best-of-Breed-Anwendungen einführen, können sich Identität und Zugriff als wichtiger Hemmschuh erweisen. Um Best-of-Breed zu fördern und Anbieterbindung zu vermeiden, benötigen Benutzer eine IDaaS-Lösung, die den Zugriff für jede Anwendung unabhängig vom Hersteller oder Anbieter gewährleistet.

Wie IDaaS mit diesen Trends korreliert

Die Welt durchläuft einen ständigen Wandel. Eines bleibt jedoch sicher: Neue IT-Innovationen, Bedrohungen und Möglichkeiten zur Identitätssicherung werden sich kontinuierlich weiterentwickeln. IDaaS wurde von Anfang an dafür konzipiert, Veränderungen heute und in Zukunft zu unterstützen. Im Gegensatz zu herkömmlichen Identitäts- und Zugriffsmanagementlösungen bietet IDaaS die folgenden Vorteile:

- Ermöglicht Zero Trust durch die Sicherung des Zugriffs für Benutzer unabhängig von Standort, Gerät oder Netzwerk.
- Unterstützt offene Standards und Konnektivität mit Systemen, die selbstsouveräne Identität bereitstellen.
- Sichert und autorisiert den Zugriff auf Anwendungsprogrammierschnittstellen (APIs), die von intelligenten Geräten verwendet werden, und ist entsprechend den Anforderungen des IoT skalierbar.
- Aggregiert Kundendaten und vereinfacht die Handhabung von Einwilligungen für verschiedene Datenunterverarbeiter und Systeme.
- Bietet Identitätsfreiheit, damit Unternehmen Best-of-Breed-Technologien einführen und eine Herstellerbindung vermeiden können.

MERKEN

Mit IDaaS erhalten Sie einen flexiblen Dreh- und Angelpunkt, mit dem Sie für Ihr Unternehmen heute und in Zukunft problemlos neue Innovationen verbinden und implementieren können.

PERSONAL CAPITAL VERWALTET SEINE CLOUD-UMGEBUNG

Personal Capital bietet einen „High-Tech-, High-Touch-Ansatz für persönliche Investitionen" und bringt finanzielle Klarheit und Vertrauen durch die kombinierte Kraft von intelligenter Technologie und intelligenten Menschen. Im Februar 2019 verwaltete das Unternehmen mehr als 9 Milliarden US-Dollar an Vermögenswerten und mehr als zwei Millionen Kundenkonten.

Personal Capital betreibt eine robuste Cloud-Architektur zur Unterstützung des Wachstums und der Größe des Unternehmens und zur gleichzeitigen Gewährleistung der Sicherheit der Finanzdaten. „Die Identitätsmanagementstrategie des Unternehmens war anfangs zu komplex", sagte Maxime Rousseau, Chief Information Security Officer.

Lösung für den Zero-Trust-Infrastrukturzugriff

Personal Capital betreibt sowohl kundenorientierte Anwendungen als auch Backend-Dienste auf Amazon Web Services (AWS). Nach der erfolgreichen Implementierung von Okta bestand der nächste Schritt darin, den Zugriff auf die Cloud-Infrastruktur zu sichern.

Das Team entschied sich für das Zero-Trust-Modell von Forrester, bei dem der Zugriff entsprechend dynamischer Benutzer- und Gerätebedingungen in Echtzeit gewährt wird. „Wir sind ein modernes Cloud-First-Unternehmen ohne herkömmlichen Perimeter und so sollte Sicherheit nach unserer Auffassung funktionieren", betonte Rousseau.

Die Implementierung eines derartigen Kontrollniveaus war jedoch keine leichte Aufgabe. „Es war eine Herausforderung, die richtigen Identitäten, Rollen, Gruppen und die zugehörigen öffentlichen Secure Shell (SSH)-Schlüssel dynamisch bereitzustellen, während die unveränderliche Infrastruktur herauf- und herunterskaliert wird", erklärte Rousseau. Ohne eine einheitliche Ebene für die Zugriffskontrolle musste das Team entweder eine eigene Vernetzungslösung aufbauen oder zusätzliche Zugangstechnologien integrieren, was zu Problemen bei der Akzeptanz, Kompatibilität und Skalierung führen würde.

Eine vielversprechende und zeitnahe Akquisition

Um den Authentifizierungs-Stack von Okta zu nutzen, entschied sich das Personal Capital-Team für ScaleFT und deren Produkt Zero Trust Server Access, das mit Okta integriert wurde und dynamische Provisionierungsfunktionen bietet. ScaleFT gab den Personal Capital-Teams für operative Abläufe, Sicherheit, Data Science und Technik eine nahtlose, sichere Möglichkeit für den Zugriff auf kritische AWS-Infrastruktur.

(Fortsetzung)

(Fortsetzung)

Zum damaligen Zeitpunkt durchlief ScaleFT den formalen Prozess der Verifizierung seiner Okta-Integration. Deshalb benötigte das Unternehmen einen gemeinsamen Okta- und ScaleFT-Kunden, um zu bestätigen, dass die Integration wie dokumentiert verlief. Personal Capital erklärte sich bereit, dieser gemeinsame Kunde zu sein, und half beim Abschluss der Okta-Verifizierung von ScaleFT. „Wir waren eine der ersten Kundenbrücken zwischen den Parteien", sagte Rousseau.

Im Anschluss an die Verifizierung baute Okta die Partnerschaft weiter aus und kündigte im Juli 2018 an, dass das Unternehmen ScaleFT übernehmen werde, um Identität auf Infrastrukturressourcen auszuweiten und die weitere Entwicklung seiner Zero-Trust-Plattform zu beschleunigen.

Diese Ankündigung war eine großartige Nachricht für das Team von Personal Capital. Heute trägt das Produkt ScaleFT Server Access den Namen Okta Advanced Server Access. Es optimiert zentrale Okta-Authentifizierungs-Workflows auf Linux- und Windows-Servern über SSH und Microsofts Remote Desktop Protocol (RDP).

Zero Trust – benutzerfreundlich und sicher

„Okta Advanced Server Access war die richtige Wahl für Personal Capital, da diese Lösung den sicheren Serverzugriff vereinfacht und gleichzeitig zusätzliche Technologien, manuelle Integrationen und statische Schlüssel überflüssig macht", so Rousseau. Durch die Lösung aller Richtlinienanforderungen mit einer einzigen Technologie vermeidet Personal Capital fehleranfällige manuelle Integrationen.

Advanced Server Access bietet eine Zero-Trust-Architektur, die die kritische Infrastruktur von Personal Capital schützt. „Wie Personal Capital bindet Okta alles an Identität", sagte Rousseau. „Advanced Server Access bindet Benutzergeräte an authentifizierte Sitzungen, so dass wir nun zusätzliche Gewissheit haben, dass jedem Gerät und jedem Mitarbeiter zu jedem Zeitpunkt vertraut werden kann."

Advanced Server Access beseitigt einen Großteil des üblicherweise mit Infrastruktur verbundenen Aufwands. „Wir müssen uns keine Sorgen mehr um Kontensynchronisation oder statische Anmeldeinformationen machen, die gestohlen bzw. missbraucht werden können", sagte Rousseau. „Wir können sehen, wer worauf zugegriffen hat, mit welchem Gerät und wann."

Dank fortschrittlichen Technologien bleibt Personal Capital ein führender Anbieter im Bereich Digital Wealth Management. Rousseau ist zuversichtlich, dass die Infrastruktur des Unternehmens bereit ist. „Da Okta das Identitäts- und Zugriffsmanagement übernimmt, haben wir eine sichere, skalierbare Grundlage, auf der wir wachsen können", betonte er. „Okta war die richtige Wahl für uns."

IN DIESEM KAPITEL

- **Identität einfach halten… und anbieterneutral**
- **Mehr als nur Zugriffskontrolle für jeden Benutzer**
- **Nutzung eines Cloud-Service-Modells**
- **Legacy-Produkte durch eine skalierbare, sichere und benutzerfreundliche Lösung ersetzen**
- **Vorbereitung auf die Zukunft**

Kapitel 5
Zehn Schlüsselfunktionen moderner IDaaS (Identity as a Service)

Hier sind zehn wichtige Funktionen und Geschäftsvorteile einer IDaaS-Lösung (Identity as a Service):

- **Sie lässt sich einfach implementieren und nutzen.** Mit einer Cloud-basierten IDaaS-Lösung (Identity as a Service) können Sie Identitäts- und Zugriffsmanagement (IAM) innerhalb von Stunden bereitstellen und die Integration in Anwendungen innerhalb von Minuten statt Wochen durchführen. Wenn Sie den Service abonnieren, ist die Lösung bereits einsatzbereit. Es ist keine Serverinstallation erforderlich.
- **Sie ist anbieterneutral.** IDaaS lässt sich universell in Anwendungen integrieren. Unterstützt werden Cloud- und On-Premises-Apps, von Unternehmen selbst entwickelte Apps, Mobilgeräte-Apps, Server und APIs über einen Katalog mit mehr als 6.000 vorgefertigten Integrationen, wodurch eine Anbieterbindung verhindert wird.
- **Sie geht über Zugriffskontrolle hinaus.** IDaaS bietet mehrere Services in einer Lösung. Dazu gehören die Speicherung von Benutzerdaten, die Bereitstellung von Self-Service-Funktionen

für Kontowiederherstellung und Zugriffsanforderungen, die Automatisierung der Kontenbereitstellung und -abschaltung, die Implementierung von Workflows und die Vereinfachung der Sicherheitsüberwachung. Diese Funktionen machen manuelle, von der IT ausgeführte Aufgaben überflüssig und senken die Gesamtkosten.

- **Sie unterstützt alle Benutzer.** IDaaS kann alle Benutzer in einer einzigen Plattform verwalten. Das reduziert die Systeme und Anbieter, die zum Schutz von Identitäten erforderlich sind, sowie die Anzahl der Integrationen, die eine App zur Unterstützung aller Benutzer benötigt.
- **Sie ermöglicht bedarfsgerechte Abrechnung.** IDaaS ist abonnementbasiert. Sie zahlen entsprechend Ihrem Wachstum. Wenn sich Ihr Unternehmen verändert, können Sie die Anzahl der benötigten Lizenzen schnell ändern und bleiben damit kostenflexibel.
- **Sie ist stets aktiv und auf dem neuesten Stand.** IDaaS wird vom Service Provider regelmäßig mit Sicherheitsverbesserungen und neuen Funktionen aktualisiert, ohne dass es zu Ausfällen oder geplanten Ausfallzeiten kommt. Der Service bietet auch Echtzeit-Verfügbarkeit über ein Live-Dashboard, sodass Sie sich auf strategische Projekte konzentrieren können, anstatt Systeme manuell zu patchen.
- **Sie ist ein Ausweg aus Legacy-Lösungen.** IDaaS ersetzt mehrere Legacy-Identitätslösungen von LDAP, Microsoft Active Directory und Active Directory Federation Services (AD FS) bis hin zu lokalen SSO- und MFA-Servern. Indem Sie diese Systeme durch einen einheitlichen Service ersetzen, sparen Sie Zeit und Geld bei Anbietermanagement, Beschaffung, manueller Integration, Patches, Wartung und Support.
- **Sie ist skalierbar und flexibel.** IDaaS skaliert dynamisch nach Bedarf, sodass Sie die Infrastruktur für das Wachstum Ihres Unternehmens in den kommenden Jahren nicht prognostizieren, installieren und patchen müssen.
- **Sie ist benutzerfreundlich.** Benutzer können ausgehend von einem einzigen Dashboard über Browser oder Mobilgeräte-Apps auf Systeme zugreifen, ohne mehrere Anmeldeinformationen oder zusätzliche Systeme wie virtuelle private Netzwerke (VPNs) verwenden zu müssen.
- **Sie ist zukunftssicher.** Identität ist ein wichtiger Bestandteil vieler Innovationen, darunter Zero Trust, das Internet der Dinge (IoT), Privatsphäre und Freiheit und viele andere (mehr dazu in Kapitel 4). Ohne eine IDaaS-Plattform, die sich weiterentwickelt, um möglicherweise im Hinblick auf die Zukunft bestehende Ungewissheiten auszuräumen, kann Ihr Unternehmen keine dieser Initiativen beginnen.

Das letzte Wort beim Identitäts- und Zugriffsmanagement

okta

okta.com/de

Läuten Sie die Zukunft des Identitätsmanagements ein

Mit Identitäts- und Zugriffsmanagementlösungen (IAM) kann Ihr Unternehmen die Sicherheit erhöhen und Identität sowie Zugriff schnell und zuverlässig verwalten. Zur Nutzung von IAM-Diensten und Sicherheit in großem Maßstab vollzieht die Mehrheit der Unternehmen eine Umstellung auf moderne Identität aus der Cloud – Identity as a Service (IDaaS). IDaaS bietet Unternehmen robustes und skalierbares IAM für die Sicherung und Verwaltung des Zugriffs jedes Benutzers von jedem Ort der Welt und jedem Gerät. In diesem Buch erfahren Sie, worum es bei moderner Identität geht und wie IDaaS Ihrem Unternehmen helfen kann.

Sie erfahren:

- Wie Sie moderne Identitätsherausforderungen bewältigen
- Wie Sie den Zugriff mit Single Sign-On (SSO) und Multi-Faktor-Authentifizierung (MFA) sichern
- Wie Sie die Kontobereitstellung automatisieren
- Wie Sie Cloud- und On-Premises-Apps, mobile und benutzerdefinierte Apps, Server und APIs sichern
- Wie Sie Herausforderungen mit Datensicherheit und Compliance bewältigen
- Wie Sie eine Zero-Trust-Architektur einführen

auth0

Lawrence C. Miller ist seit mehr als 25 Jahren im IT-Bereich tätig und hat beinahe 200 „Für Dummies"-Bücher verfasst.

Frederico Hakamine ist technischer Produktmanager bei Okta. Seine Hauptbeschäftigung sind die Entwicklung von Code und Werbung für die Okta-Plattform und APIs.

ISBN: 978-1-119-86665-7
Nicht für den Wiederverkauf

für dummies®

WILEY END USER LICENSE AGREEMENT

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