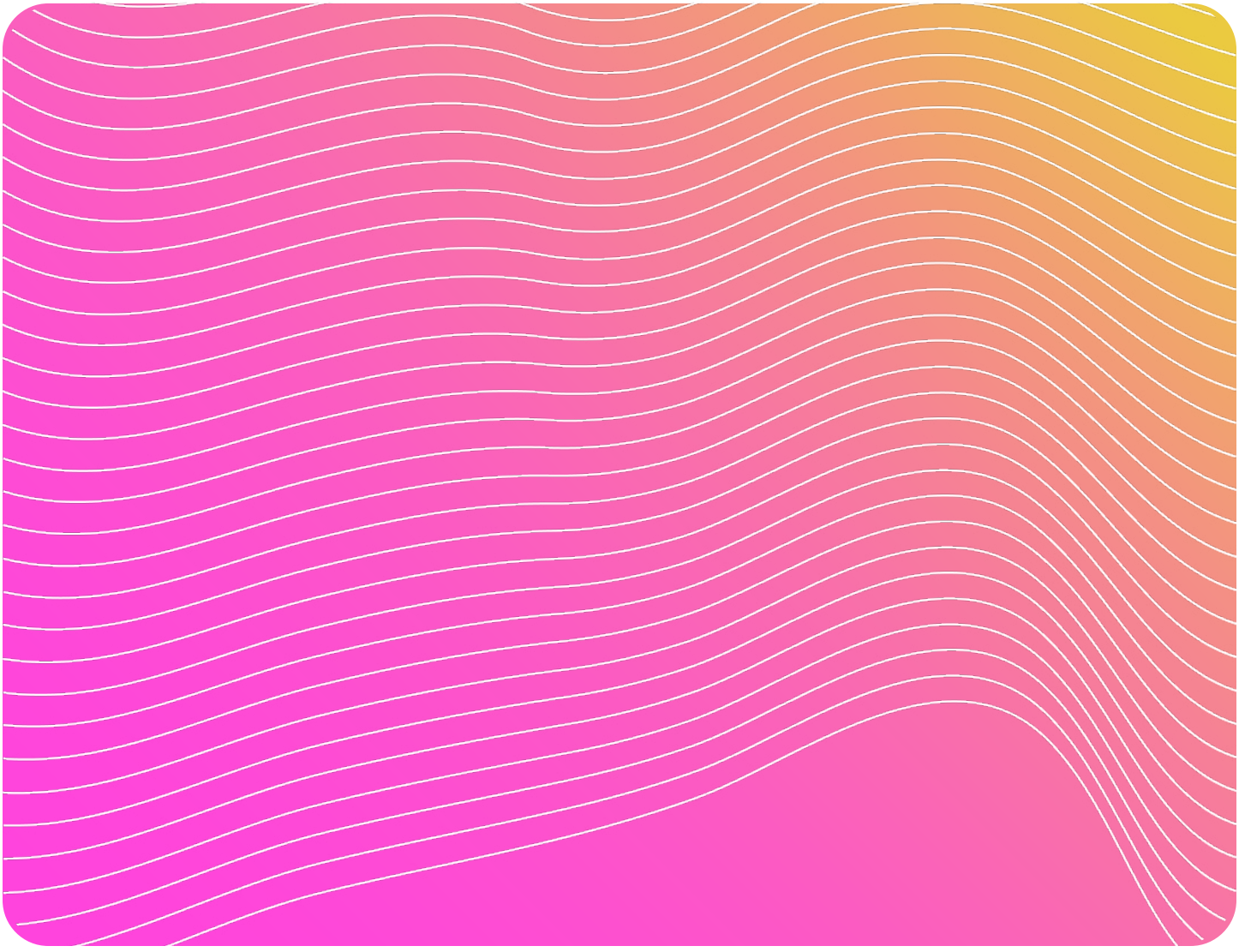
auth0

Mit CIAM bringen Sie Sicherheit und Kundenerlebnis unter einen Hut

Sicherheit ist ein bewegliches Ziel. Eine starke CIAM-Lösung kann Ihnen dabei helfen, Ihre Anforderungen mit denen Ihrer Kunden unter einen Hut zu bringen.



WHITEPAPER

auth0.com

Haben Sie Ihre Haustür abgeschlossen?

Es herrscht dort ein stetes Kommen und Gehen, und Sie haben genug zu tun mit Kaffee, Kindern, Taschen und der Katze, die versucht, durch die offene Haustür zu entwischen. Da kann man leicht etwas Wichtiges übersehen – beispielsweise die Tür abzuschließen. Das ist in der Alltagshektik schnell passiert.

Und auch im Geschäftsleben geht es oft hektisch zu. Das Telefon klingelt ununterbrochen, die neuesten Ergebnisse der Kundenfokusgruppen sind soeben eingetroffen, Ihr Projektmanager will unbedingt in der Mittagspause ein Meeting ansetzen, und für die tägliche Morgenbesprechung sind Sie ohnehin spät dran. Berücksichtigt man außerdem den rasanten digitalen Wandel in allen Sektoren und die Auswirkungen der Corona-Pandemie, kann einem schwindlig werden.

Tatsächlich meldet Twilio, dass die potente Kombination aus bisherigen Bemühungen und pandemiebedingter Beschleunigung diesen Wandel in vielen Unternehmen **um durchschnittlich sechs Jahre beschleunigt hat**, in manchen Branchen sogar um fast zehn Jahre. Sage und schreibe 97 % der Entscheidungsträger in den befragten Unternehmen führen das stark angezogene Tempo auf die Pandemie zurück. Wenn Sie diese rasante Entwicklung auf allen Kanälen für Ihre Kunden angenehmer gestalten möchten, sollten Sie beim nächsten Release über ein zentrales, einheitliches Nutzermanagementsystem nachdenken.

> **„Kundenidentitäts- und -zugangsmanagement (Customer Identity and Access Management, CIAM) ist die zentrale Lösung für das Onboarding, die Organisation und das Management Ihrer Nutzerkonten und -daten von einem einzigen Ort aus.“**

Die Login-Seite ist die Eingangstür, durch die Sie Ihre Kunden hereinlassen. Sie ist das Erste, was Ihre Kunden sehen, also muss die Anmeldung unbedingt reibungslos ablaufen. Gleichzeitig ist dies aber auch der Ort, den viele Hacker ins

Visier nehmen, um nach Schwachstellen zu suchen und Ihre Daten zu stehlen. Also muss die Seite gut gesichert sein – und Sie müssen entscheiden, wie gut Sie sie sichern wollen und müssen. Lassen Sie sie einen Spalt offen stehen, um alle Besucher willkommen zu heißen? Oder versehen Sie sie mit einem Riegel, sodass jeder erst anklopfen und warten muss, bis jemand ihm die Tür öffnet? Ist die Sicherheit zu gering, kann jeder hereinkommen. Ist sie zu hoch, will niemand mehr hereinkommen. Ein ewiger Balanceakt zwischen Sicherheit und Kundenerlebnis.

Kundenidentitäts- und -zugangsmanagement (Customer Identity and Access Management, CIAM) ist die zentrale Lösung für das Onboarding, die Organisation und das Management Ihrer Nutzerkonten und -daten von einem einzigen Ort aus. Ein robustes CIAM-Tool ermöglicht Ihnen außerdem die Einrichtung angemessener Sicherheitsvorkehrungen, um die Daten Ihrer Kunden sicher zu speichern und gleichzeitig zu gewährleisten, dass Ihre Nutzer ein niedrigschwelliges, reibungsloses Erlebnis haben.

Einfach ausgedrückt führt zu viel Aufwand für den Kunden zu Konversionsverlusten – ob es sich um einen neuen Nutzer handelt, der aufgibt, wenn er zum dritten Mal aufgefordert wird, einen CAPTCHA-Code einzugeben, oder um einen langjährigen treuen Kunden, der es leid ist, sich durch einen umständlichen Passwort-Reset zu quälen. Ein hoher Aufwand beim Login-Prozess wie in diesen Beispielen kann dazu führen, dass Nutzer aufgeben und Ihrem Unternehmen den Rücken kehren. Und ihren Freunden davon erzählen, die es dann erst gar nicht versuchen, sodass Ihre Marke unbemerkt langfristig Schaden erleidet.

Als Ihre digitale Eingangstür ist Ihr CIAM die zentrale Schaltstelle für Sicherheit, Datenschutz und Komfort. Die richtige Kombination dieser drei elementaren Grundlagen für Ihr Produkt und Ihre Kunden zu finden, bringt uns zu einer möglichen Komplikation: Wenn Sie für die Entwicklung einer eigenen Lösung Mittel und Personal abstellen, fehlen diese an einer anderen, entscheidenden Stelle, nämlich beim Kernprodukt. Ihr Entwicklungsteam kann das am besten, wofür es da ist. Wenn es seine geballte Kompetenz darauf verwendet, das bestmögliche Kernprodukt für Sie zu entwickeln. Sollten Sie nicht das Login-Erlebnis und die Datensicherheit Ihrer Nutzer ähnlich behandeln und sich **beim Identitätsmanagement ebenfalls auf Experten verlassen**?

Wenn Sie sich für eine spezielle SaaS-Lösung für Ihr Identitätsmanagement entscheiden, können Ihre Entwickler nicht nur ihr Fachwissen auf Ihr Kernprodukt konzentrieren, Sie sorgen außerdem dafür, dass die Daten Ihrer Kunden bei Ihnen sicher sind – was erheblich dazu beiträgt, deren Vertrauen in Ihr Unternehmen zu stärken. Laut dem Trust Barometer Report 2020 von Edelman teilen sich **das Vertrauen und der Ruf der Marke** den zweiten Rang direkt hinter dem Preis, wenn es darum geht, wie die Menschen Kaufentscheidungen treffen.

Optimale Sicherheit, Datenschutz und Komfort dank CIAM

Leider geht mit dem zunehmenden Einsatz digitaler Technologien in sämtlichen Sektoren auch ein rapider Anstieg der Zahl der Cyberangriffe auf Ihren Perimeter einher, Ihre Schnittstelle zur Außenwelt. Dadurch rücken der Schutz der Integrität und des Rufs der Marke plötzlich viel stärker in den Fokus der Geschäftsleitungen. Mit anderen Worten: Ihren Perimeter einbruchsicher zu machen, muss Priorität im Unternehmen haben. **Datenschutzverletzungen** können nicht nur dem Ruf Ihrer Marke erheblich schaden, sondern auch das Finanzergebnis empfindlich trüben und möglicherweise noch Jahre nach dem eigentlichen Vorfall Auswirkungen nach sich ziehen. Die Angriffsfläche für Cyberkriminelle möglichst klein zu halten, ist also auch in geschäftlicher Hinsicht sinnvoll.

Für die meisten Unternehmen sind die Konversionsraten ausschlaggebend für ihr Geschäft. Und da ein zu großer Aufwand für die Kunden zu Konversionsverlusten führt, ist es nur logisch, dass alles, was Sie unternehmen, um Ihre Login-Seite so niedrigschwellig wie möglich zu gestalten, Ihrer Konversionsrate direkt zugutekommt. Ein CIAM gibt Ihnen die Möglichkeit, den reibungslosen Ablauf des Login-Erlebnisses Ihrer Kunden zu steuern und die Daten zu verwalten, die Sie für die kontinuierliche Weiterentwicklung angesichts sich verändernder Anforderungen benötigen. Indem Sie die Weichen für Sicherheit, Datenschutz und ein reibungsloses Kundenerlebnis optimal stellen, erhalten Sie die Sicherheit, die Sie brauchen, und das niedrigschwellige Erlebnis, das Ihre Kunden verlangen.

Ein CIAM bietet jedoch noch mehr als nur ein reibungsloses Login-Erlebnis. Eine gute CIAM-Lösung kombiniert das Nutzererlebnis mit Schutz vor Cyberangriffen, Schutz der Nutzerdaten und intuitiv gesteuertem Nutzerkontenmanagement.

CIAM als Schutz vor Angriffsvektoren und Verteidigung des Perimeters

Stellen Sie sich folgendes Szenario vor: Ihr Unternehmen erweitert seine Internetpräsenz. Sie haben vor Kurzem ein E-Commerce-Start-up-Unternehmen erworben UND die Entwicklung eines Portals für exklusive eintägige Deals nur für Mitglieder abgeschlossen, das Ihre vorhandenen Web-Apps und Stores ergänzen soll. Ihr Team soll all diese Elemente über eine neue Web-App in einer einheitlichen Benutzeroberfläche bündeln. Dies ist der ideale Zeitpunkt, eine erweiterungsfähige und skalierbare CIAM-Lösung zu integrieren, über die Ihre Kunden mit denselben Anmeldedaten auf alle Kanäle zugreifen können und die Cyberkriminellen möglichst wenig Angriffsfläche bietet.

Darüber hinaus tragen CIAM-Lösungen, die Funktionen wie Bot-Erkennung und -Abhilfe, Multi-Faktor-Authentifizierung (MFA) und Protokoll-Streaming unterstützen, weiter zur Verstärkung Ihrer Verteidigungslinien bei. In der verteilten Architektur von heute ist die Identität der Perimeter. Erweiterungsfähigkeit, Skalierbarkeit und Partnerintegrationen spielen eine große Rolle bei der Bewertung, ob eine CIAM-Lösung das Wachstum Ihres Unternehmens unterstützen und gleichzeitig Perimeter und Daten schützen kann.

> **„Durch die Durchsetzung von Mindestanforderungen für Passwörter (einschließlich Regeln zu deren Wiederverwendung), die Optimierung des Passwort-Resets und die Integration von MFA macht eine CIAM-Lösung Ihren Identitätsperimeter zum Schutzwall.“**

Ein Faktor, den viele Angriffsvektoren ausnutzen, ist die Tatsache, dass die Menschen ihre Passwörter wiederverwenden. Tatsächlich zeigt eine aktuelle Umfrage von LogMeIn, den Entwicklern des Passwort-Managers Lastpass, dass **zwar 91 % der Befragten** wissen, dass die Wiederverwendung von Passwörtern ein Sicherheitsrisiko darstellt, 66 % aber zugeben, es trotzdem zu tun. CIAM kann Ihnen dabei helfen, in diesem Bereich bewährte Best Practices durchzusetzen. Durch die Durchsetzung von Mindestanforderungen für Passwörter (einschließlich

Regeln zu deren Wiederverwendung), die Optimierung des Passwort-Resets und die Integration von MFA macht eine CIAM-Lösung Ihren Identitätsperimeter zum Schutzwall.

Konsolidierte Nutzerdaten sind leichter zu schützen

Die sogenannte Single Source of Truth (SSoT), eine zentrale Datenquelle, ist ein Datenmanagement-Rahmenwerk, laut dem der ideale Zustand für ein Unternehmen darin besteht, einen zentralen Ort zu haben, an dem alle relevanten Daten gespeichert werden, anstatt sie an mehreren isolierten Orten aufzubewahren. Ihr CIAM übernimmt dieses Konzept und wendet es auf Ihre Nutzerdaten an, indem es alle Kontodaten an einem Ort bündelt. Egal, auf wie vielen Plattformen Ihre Apps letztendlich angesiedelt sind, können Sie mithilfe Ihres CIAMs Ihre Nutzerkonten verwalten und alle eingehenden Daten an dieselbe Identität-SSoT leiten.

So lassen sich diese Daten viel leichter schützen, da sie sich alle am selben Ort befinden. Ein zentralisiertes Nutzerkontenmanagement ist auch für die Einhaltung einschlägiger Datenschutzvorschriften wichtig. Sowohl die Datenschutz-Grundverordnung (DSGVO) als auch das California Consumer Privacy Act (CCPA) schreiben Unternehmen vor, Nutzern auf Anforderung Kopien ihrer Daten und Informationen über den Verwendungszweck dieser Daten zukommen zu lassen. Und da diese Vorgabe sich auch auf Partnersysteme und -daten bezieht, erleichtert ein CIAM den nötigen Zugriff, um die Vorschriften zu erfüllen und Ihre Kunden glücklich zu machen.

Eine Identitäts-SSoT trägt auch zur Verbesserung des Nutzererlebnisses bei. Ein Single Sign-on, das auf den Einträgen Ihrer SSoT basiert, bedeutet, dass Ihre Nutzer sich nur einen Satz von Anmeldedaten einprägen müssen. Die damit verbundene höhere Zufriedenheit verringert nicht nur die Wahrscheinlichkeit, dass ein Nutzer Ihre App aufgibt. Sie trägt auch dazu bei, dass es ein verwaistes Konto weniger gibt, das Angreifern eine Einstiegsmöglichkeit bieten könnte. Es ist nicht einfach, alle Beteiligten glücklich zu machen. Doch mit einem modularen CIAM-SaaS-Tool kommen Sie diesem Ideal immerhin einen Schritt näher.

Optimierte Prozesse für zufriedene Nutzer

Wenn ein Kunde ein Konto anlegt oder sich bei seinem Konto anmeldet, setzt er sein Vertrauen in Sie. Er vertraut auch darauf, dass Ihre User Story ein Kundenerlebnis nach sich zieht, bei dem man nicht entnervt aufgibt, anstatt den Prozess zu Ende zu führen. Wenn dieser Kunde sieht, dass Sie einen Prozess mit wenigen, intuitiven Schritten einsetzen, sodass sein Konto im Handumdrehen verifiziert und einsatzbereit ist, dann haben Sie ihm soeben bewiesen, dass sein Vertrauen in Sie gerechtfertigt ist.

Eine CIAM-Lösung sollte all diese Kriterien erfüllen und das Anlegen eines Konto so mühelos wie möglich machen, damit sich neue Nutzer willkommen fühlen. Gleichzeitig müssen Sie zeigen, dass Ihre Datenverarbeitungsverfahren sicher sind. Laut PwC **geben sage und schreibe 32 % der Kunden ein Unternehmen** nach einer einzigen schlechten Erfahrung auf. Nein, Sie haben sich nicht verlesen. Ein Drittel der Befragten gibt an, die Beziehungen zu einem Unternehmen nach nur einer unangenehmen Erfahrung sofort abzubrechen. Können Sie sich vorstellen, was diese Kunden ihren Freunden erzählen, wenn diese schlechte Erfahrung die erste Begegnung mit Ihrem Unternehmen war? Wie Sie im nächsten Kapitel sehen werden, kann eine gute CIAM-Lösung das Gleiche in positiver Hinsicht für alle Ihre Nutzerkontenprozesse und -abläufe bewirken.

Vereinfachte Nutzerlebenszyklen sind leichter zu schützen

Es kann auch andere Gründe dafür geben, dass ein Nutzer ein neues Konto anlegt. Vielleicht hat er sein Passwort vergessen und findet Ihren Passwort-Reset viel zu umständlich. Dies führt dazu, dass Sie ein zweites Konto verwalten müssen, weil Sie gar nicht wissen, dass es sich um ein Duplikat handelt. Eine vollständig integrierte CIAM-Lösung bietet an allen Punkten des Nutzerlebenszyklus Sicherheitsvorteile.

Kontoregistrierung

Um zu verhindern, dass Konten aufgegeben werden, ist es wichtig, dass der Registrierungsprozess so reibungslos wie möglich verläuft, ohne die Verifizierung der Identität des Nutzers zu vernachlässigen. CIAM-Lösungen mit Single Sign-on tun genau das. Wenn Sie einem Nutzer ermöglichen, sich über sein Konto aus den sozialen Medien bei Ihnen anzumelden, profitieren Sie davon, dass seine Identität bereits überprüft worden ist. Gleichzeitig ermöglichen Sie es dem Nutzer, sich in Sekundenschnelle bei Ihnen zu registrieren. Dieser intuitive Prozess verringert auch die Wahrscheinlichkeit, dass Passwörter wiederverwendet werden. Damit ist dieses Konto schwerer zu hacken und die Daten sind besser geschützt.

Kontopflege

Wenn es um die allgemeine Pflege Ihrer Nutzerkonten geht, ist die Automatisierung Ihr bester Freund. Ihr CIAM sollte einen automatisierten Ablauf für den Passwort-Reset bieten, um diesen häufig genutzten Schritt möglichst reibungslos zu gestalten. MFA-Optionen, die Bedenken hinsichtlich der Echtheit der Identität der Person ausräumen, sind der nächste Schritt auf einer umfassenden Kontomanagementplattform, während eine föderierte Identität bedeutet, dass, wenn ein Nutzer versehentlich ein zweites Konto anlegt, dieses erkannt und in Ihrer Identitäts-SSoT mit dem bestehenden Konto kombiniert wird. Die zusätzliche Sicherheit, die diese MFA bietet, und die Eliminierung doppelter oder verwaister Konten mindern die Wahrscheinlichkeit eines erfolgreichen Übergriffs.

Kontoaufgabe

Was geschieht, wenn ein Nutzer sein Konto schlicht vergessen hat? Oder zu einer anderen Firma abwandert und sein Konto aufgibt? In vielen Fällen lautet die Antwort vermutlich – nichts. Wenn die Kontopflege nicht nachgehalten wird, füllt sich Ihre Identitäts-SSoT im Laufe der Zeit mit aufgegebenen, ungenutzten

und redundanten Konten. Dies ist nicht nur ein Wartungsproblem. Auch die Sicherheit ist dadurch gefährdet, da die Anmeldedaten solcher Konten anfälliger für Datenschutzverletzungen sind und möglicherweise für Angriffe auf Ihre Systeme verwendet werden könnten. Automatisierte Kontofunktionen wie der Versand von E-Mails an Inhaber von Konten, bei denen für einen voreingestellten Zeitraum keine Aktivität festgestellt wurde, automatische Kontodeaktivierung und schließlich die Löschung solcher Konten blockieren diese beliebte Einfallschneise für Angreifer.

Zahlreiche Angriffsmöglichkeiten durch Anmeldedatenlecks

Werden bei einer Datenschutzverletzung Anmeldedaten von Nutzern gestohlen, können sie häufig aufgrund schlechter Passworthygiene wieder und wieder verwendet werden, um sich Zugang zu unzähligen anderen Websites zu verschaffen. Für Cyberkriminelle ist es kein Problem, sich Nutzernamen und Passwörter zu beschaffen, auch wenn sie technisch nicht versiert genug sind, um selbst eine Datenbank zu hacken. Diese sogenannten „Script Kiddies“ können eine „Combo List“ mit Anmeldedaten im Darknet kaufen und dann dort ebenfalls erhältliche Scripts oder komplette Anwendungen nutzen, um mit Credential Stuffing oder anderen Brute-Force-Methoden einen Übergriff zu starten. Diese Angriffsvektoren sollten Sie kennen, wenn Sie Ihr CIAM auf optimale Weise in Ihr individuelles Anwendungsszenario integrieren wollen.

Credential Stuffing

Einer der gängigsten aktuellen Vektoren für Brute-Force-Angriffe ist unter der Bezeichnung **Credential Stuffing** bekannt. Dabei übernimmt ein Angreifer eine Liste mit Nutzernamen und Passwörtern und lässt sie durch den Login-Prozess einer anderen Website laufen. Weil viele Nutzer ihre Passwörter wiederverwenden, ist dieser Vektor für Angreifer so interessant, denn die Wahrscheinlichkeit, dass die vom Angreifer ausprobierten Anmeldedaten funktionieren, ist immerhin so hoch, dass sich der Aufwand für ihn lohnt. Solche Angriffe basieren in erster Linie darauf, dass die Menschen bequem sind und einfache, leicht zu knackende Passwörter verwenden (das **belieb teste Passwort** ist tatsächlich immer noch „123456“, dicht gefolgt von „password“).

Kompromittierte geschäftliche E-Mail

Passwortlecks sind auch die Grundlage für andere Angriffe. So kann ein Hacker beispielsweise eine Combo List kaufen, die sich auf ein bestimmtes Unternehmen bezieht, das er angreifen will. Durch Herausziehen der Netzwerk-Anmeldedaten hochrangiger Führungskräfte und durch Spoofing kann der Angreifer nun gezielte Phishing-E-Mails versenden (auch Spear Phishing genannt), die scheinbar von dieser Führungskraft stammen. Die Häufigkeit solcher Angriffe nimmt mithilfe von Bots zu, doch handelt es sich in erster Linie um einen auf Social Engineering beruhenden Vektor, dessen Erfolg auf dem menschlichen Sicherheitsfaktor (oder dessen Fehlen) basiert.

Bot-Angriffe

Manche Hacker wollen auch „lediglich“ die Systeme des von ihnen ins Visier genommenen Unternehmens lahmlegen. Sie wollen gar nichts stehlen, sondern den Geschäftsbetrieb zum Stillstand bringen und beobachten, wie das Angriffsopfer verzweifelt versucht, den Übergriff abzuwehren und wieder auf die Beine zu kommen. Ein gängiges Beispiel sind sogenannte „Distributed Denial of Service“-Angriffe (DDoS-Angriffe), bei denen Hacker Bots einsetzen, um eine Website mit Verkehr zu überschwemmen, sodass diese den legitimen Besuchern für den betreffenden Zeitraum nicht zur Verfügung steht. Diese Angriffe beschädigen nicht nur den Ruf des angegriffenen Unternehmens, sie resultieren aufgrund der Ausfallzeit auch in finanziellen Verlusten.

Ein weiterer beliebter Bot-Angriff ist die „Flutung“ des Login-Ablaufs einer E-Commerce-Website, um begehrte Artikel aufzukaufen. Solche Bot Swarms waren kürzlich noch zu beobachten, als **Nvidia eine neue Grafikkarte herausbrachte**, die von Gamern auf der ganzen Welt mit Spannung erwartet wurde. Gleiches geschah, als Microsoft die X-Box X und Sony die heiß begehrte Playstation 5 auf den Markt brachte. Websites wie Walmart und Amazon waren dem Ansturm von Hunderttausenden von Bots erstellten Konten ausgesetzt, die dazu verwendet wurden, sich **alle verfügbaren Lagerbestände einzuverleiben**,

um die Preise auf dem Sekundärmarkt hochzutreiben. Diese Schwarmangriffe verknappen nicht nur die Verfügbarkeit begehrter Waren, sie hindern auch legitime Nutzer daran, die Website zu nutzen, bis der Angriff abgewehrt worden ist. Für das betroffene Unternehmen ist dies mit Umsatzverlusten und Rufschäden verbunden.

Wie Auth0 CIAM sicher macht

„Wenn Sie über Sicherheit nachdenken, müssen Sie über Ihre Risiken nachdenken. Es gibt keine für alle passende Sicherheitslösung. Ihre Lösung sollten Sie unter Berücksichtigung der Risiken auswählen, die speziell für Ihr Unternehmen, Ihre Kunden und Ihre Nutzer gelten. Sie können Ihre Sicherheitskontrollen entsprechend hoch oder tief ansetzen. Und das wird Ihnen dabei helfen, in puncto Sicherheit nicht über das Ziel hinauszuschießen und Ihr Produkt nicht so zu verbarrikadieren, dass das Nutzererlebnis beeinträchtigt wird.“

DUNCAN GODFREY, SENIOR DIRECTOR SECURITY ENGINEERING, AUTH0

Duncan Godfrey spricht die Tatsache an, dass Sicherheit an die Gegebenheiten angepasst werden muss. Um die hier erwähnten Sicherheitsbedrohungen erfolgreich einzudämmen und für die Dinge, die Hacker demnächst noch auf die Internetgemeinde loslassen werden, gerüstet zu sein, ist eine kombinierte Anstrengung erforderlich, die eine solide CIAM-Lösung beinhaltet, die skalierbar und erweiterungsfähig ist, sodass Sie ein gutes Gleichgewicht aus Sicherheit, Datenschutz und Kundenerlebnis gewährleisten können.

Aufgrund der exponierten Position als „digitale Eingangstür“ Ihres Unternehmens ist Ihr CIAM die erste Verteidigungslinie Ihres Perimeters. Das ist genau der Punkt, auf den Angreifer ihre Bemühungen fokussieren und den Ihre Kunden als Erstes

sehen, wenn sie mit Ihnen interagieren oder Ihr Produkt kaufen wollen. Es ist auch der Punkt, an dem Sie die Daten dieser Kunden verwalten, analysieren und sicher speichern.

Die modulare Bauweise hat sich mittlerweile als Norm bei der App-Entwicklung etabliert. Zahlungs-, Mitteilungs- und Authentifizierungssysteme zählen zu den führenden SaaS-Tools, die integriert werden. Marktforschungen von Auth0 haben ergeben, dass **83 % der Apps, die heute entwickelt werden, eine Authentifizierung erfordern**, allerdings gaben nur 58 % der Befragten an, ein externes SaaS-Tool zu verwenden. Während Ihr Bereitstellungsteam damit beschäftigt ist, das bestmögliche Kernprodukt zu liefern, gibt es viele gute Gründe dafür, die bestmögliche und sicherste CIAM-Lösung von unserem Team entwickeln zu lassen.

> **Zu gewährleisten, dass das Sicherheitsteam minutengenaue Informationen zur Verfügung hat, kann dazu beitragen, Angriffe bereits im Frühstadium zu erkennen, die Reaktionszeit zu verkürzen und möglicherweise gravierende Schäden im Nachgang einer Datenschutzverletzung abzuwehren.**

Offene Standards

Wie bei jedem Cybersicherheits-Tool gibt es auch bei der CIAM-Lösung offene Standards, oder aber sogenannte „Black Box“-Lösungen. Der letztgenannte Begriff bezeichnet den Umstand, dass Sie an einen bestimmten Anbieter gebunden sind, da nur er Zugriff auf das Backend seines Systems hat. Damit sind Sie von diesem Anbieter abhängig, ein Zustand, den es zu vermeiden gilt, wenn Sie sich die Agilität Ihrer Implementierungen und die problemlose Erweiterungsfähigkeit erhalten möchten (siehe unten).

Offene Standards wie OAuth2, OpenIDConnect und SAML sind maßgeblich dafür, wie wir das Kundenerlebnis in den Mittelpunkt rücken und dabei gleichzeitig unseren Entwicklerfokus behalten. Wenn ein Besucher sich innerhalb weniger Augenblicke registrieren kann, weil er Anmeldedaten nutzen kann, die er bereits hat, verbessert sich sein Nutzererlebnis drastisch. So ist er in der Lage, weniger,

aber dafür stärkere Passwörter zu verwenden, womit allen geholfen ist, denn die Daten sind sicher bei seinem Identitätsanbieter hinterlegt und nicht auf viele verschiedene Systeme verteilt.

Erweiterungsfähigkeit

Ein ausschlaggebendes Kriterium für eine flexible Lösung, die sich zusammen mit den Geschäftsanforderungen Ihrer Kunden weiterentwickeln kann, ist die Fähigkeit, Funktionen schnell und nahtlos hinzufügen und individuell anpassen zu können. Eine der Methoden, mithilfe derer Auth0 dies sicherstellt und Ihren Nutzern dabei die Möglichkeit lässt, das gewünschte Gleichgewicht zu finden, sind Regeln. Regeln ermöglichen es zum Beispiel, einen Trigger für „unmögliche Reiseszenarien“ zu erstellen. Wenn ein Nutzer in Chicago sich anscheinend von Brasilien aus anzumelden versucht, erhält der Nutzer, der den Zugriff in Brasilien versucht, eine MFA-Aufforderung, während der Nutzer in Chicago, der seine Identität bereits verifiziert hat, keine solche Aufforderung erhält. Regeln können auch dazu eingesetzt werden, andere Systeme über Login-Ereignisse zu benachrichtigen, zwecks Ereignisüberwachung oder Kundenservice.

Für Ihre Entwickler ist das Partner-Ökosystem von Auth0 der Schlüssel zur Erweiterungsfähigkeit. Wenn Sie eine Funktion benötigen, die in unserem Kernangebot nicht enthalten ist, ist dies sehr wahrscheinlich darauf zurückzuführen, dass es dafür eine Integration in ein Produkt eines branchenführenden Unternehmens gibt. Wenn Sie beispielsweise Consent-Management benötigen, um neue Vorschriften zu erfüllen, haben wir dafür eine Integration.

Protokoll-Streaming

Ein Merkmal einer starken Sicherheitsarchitektur ist die Fähigkeit, die von Ihren Cybersicherheits-Tools generierten Daten überhaupt nutzen zu können. Für Unternehmen mit eigener Dateninfrastruktur sendet Protokoll-Streaming Echtzeitdaten aus dem CIAM-System direkt an vorhandene Sicherheitsinformations- und -Ereignismanagementlösungen (SIEM) oder Sicherheitsorchestrierungs-, -automatisierungs- und Response-Lösungen (SOAR). Dies ist auch ein wichtiger Aspekt für die Einhaltung der Vorschriften in Bezug auf die Meldung und Löschung von Daten im Rahmen der oben erwähnten Datenschutzgesetze.

Auth0 Marketplace beinhaltet Integrationen in Splunk, Sumo Logic, Datadog und andere. Alternativ kann Ihr Team eine kundenspezifische Integration vornehmen oder unsere umfassenden APIs sowie unsere SKD-Bibliothek nutzen. Zu gewährleisten, dass das Sicherheitsteam minutengenaue Informationen zur Verfügung hat, kann dazu beitragen, Angriffe bereits im Frühstadium zu erkennen, die Reaktionszeit zu verkürzen und möglicherweise gravierende Schäden im Nachgang einer Datenschutzverletzung abzuwehren.

Brute-Force-Schutz

In ihrer einfachsten Form sind Brute-Force-Angriffe damit verbunden, dass ein Angreifer mehrere gängige Passwörter ausprobiert, um sich Zugang zu einem einzelnen Benutzerkonto zu verschaffen. Dieser auf den ersten Blick unbedarfte Angriffsversuch mag zwar ineffizient erscheinen, hat jedoch häufig genug Erfolg und erfreut sich daher nach wie vor großer Beliebtheit. Sollte Auth0 mehr als 10 Login-Versuche von derselben IP-Adresse bei einem Konto bemerken, blockiert der Brute-Force-Schutz diese IP für das betroffene Nutzerkonto (bei anderen Konten am gleichen Ort besteht weiterhin Zugriff), und der Nutzer wird per E-Mail benachrichtigt. Der betroffene Nutzer kann die IP-Adresse aus der E-Mail freischalten, oder sie wird automatisch wieder freigegeben, wenn er sein Passwort ändert.

Bot-Erkennung

Wenn es darum geht, komplexere Credential-Stuffing-Angriffe zu stoppen, ist die Bot-Erkennung häufig das fehlende Glied in der Kette. Mithilfe der Daten aus unseren 4,5 Milliarden Logins pro Monat in Kombination mit einer Risikosignalanalyse erkennt die Auth0 Bot-Erkennung, wenn Login-Versuche wahrscheinlich von einem Botnet oder Script stammen, und fügt einen CAPTCHA-Schritt zum Ablauf hinzu. Auth0-Forschungen haben ergeben, dass dies die **Effektivität eines Credential-Stuffing-Angriffs um ganze 85 % verringern kann**. Bei legitimen Nutzern, die sich über bekannte gute IP-Adressen anmelden, ist dieser zusätzliche Sicherheitsschritt nicht notwendig. So bleibt der Ablauf für echte Kunden niedrigschwellig. Risiken mindern und gleichzeitig das Angebot für echte Nutzer niederschwellig zu halten, entspricht dem Konzept, Sicherheit und Kundenerlebnis unter einen Hut zu bringen.

Adaptive MFA

Laut dem National Institute of Standards and Technology (**NIST**) entspricht MFA Best Practice und ist **daher immer zu empfehlen**. Und laut The Open Web Application Security Project (**OWASP**) ist MFA „bei Weitem der beste Schutz vor den meisten passwortbezogenen Angriffen.“ **Auth0 Adaptive MFA** setzt neue Maßstäbe für Nutzererlebnis und Datensicherheit. Durch die Anwendung von Kontexthinweisen wie Standort, Unique Device Identifier, Zeit seit dem letzten Login usw. unterzieht die adaptive MFA jede Benutzeranmeldung einer Risikoanalyse und fordert nur dann zur Angabe weiterer Faktoren auf, wenn dies erforderlich erscheint, wie in unserem unmöglichen Reisebeispiel oben.

Authentifizierung ohne Passwort

Wenn man überlegt, wie problematisch Passwörter sein können, ist es vielleicht an der Zeit, Ihren Kunden zu erlauben, bei ihrem Anmeldevorgang komplett darauf zu verzichten. Mit Auth0 Passwordless können Sie genau das tun und stattdessen

einen einmaligen Passcode verwenden, der dem Nutzer per E-Mail oder SMS zugesandt wird. Ohne Passwörter wird das Risiko für Credential-Stuffing-Angriffe und andere Formen von Kontokompromittierung erheblich gemindert. Und mit einer öffentlichen API, die eine Durchsatzbeschränkung beinhaltet, sind Nutzerdaten auch vor automatisierten Attacken oder Bot-Angriffen geschützt.

Sicherheit durch CIAM trotz niederschwelligem Login

Sie und Ihr Team haben mit Ihren eigentlichen Aufgaben alle Hände voll zu tun. Wenn Sie dem Trend zur Modularisierung und zur Integration von SaaS-Lösungen von Drittanbietern folgen, können Sie Ihr CIAM schnell und sicher implementieren. Um diese Sicherheit zu gewährleisten und gleichzeitig die Kundenzufriedenheit zu erhalten, muss Ihnen klar sein, dass jede Zunahme der Anzahl legitimer Kunden immer auch eine Zunahme von Angreifern bedingt, die es auf Ihre Daten abgesehen haben. Eine CIAM-Lösung, die diese Dynamik berücksichtigt, skaliert den Schutz in Übereinstimmung mit den Nutzerzahlen.

Unternehmen achten immer stärker darauf, wie sie ihre digitalen Identitäten gestalten. Die Schaffung eines angenehmen Kundenerlebnisses direkt ab der Login-Seite ist für den Aufbau vertrauensvoller Geschäftsbeziehungen unverzichtbar. Wenn Sie finden, dass Ihr Unternehmen seiner Zugangsmanagementlösung mehr Aufmerksamkeit schenken sollte, **setzen Sie sich am besten noch heute mit unseren Identitätsfachleuten in Verbindung**, um Ihre Anforderungen zu besprechen.

Über Auth0

Auth0, eine Produkteinheit von Okta, verfolgt einen modernen Ansatz zum Thema Identitätsmanagement und ermöglicht es Organisationen, jedem Benutzer sicheren Zugang zu jeder Anwendung zu gewähren. Die Auth0-Plattform ist eine hochgradig anpassbare Plattform, die so einfach zu bedienen ist, wie Entwicklungsteams es sich wünschen und so flexibel, wie sie es benötigen. Auth0 sichert jeden Monat Milliarden von Login-Transaktionen und bietet Komfort, Datenschutz und Sicherheit, damit sich Kunden auf Innovationen konzentrieren können.

Weitere Informationen finden Sie unter **https://auth0.com/de**