White Paper

Finden Sie mit CIAM die richtige Balance zwischen Sicherheit und Customer Experience

Die Security entwickelt sich dynamisch weiter. Eine starke CIAM-Lösung kann Ihnen helfen, die richtige Balance zwischen den Anforderungen Ihres Unternehmens und Ihrer Kunden zu finden.

Haben Sie die Haustür abgeschlossen?

Sie haben viel um die Ohren: Sie versuchen, Ihren Kaffee, die Kinder, Taschen sowie die Ranzen im Blick und die Katze unter Kontrolle zu halten, die nach draußen will. Dabei ist es leicht, den Überblick zu verlieren – und einen wichtigen Schritt wie das Abschließen der Tür zu vergessen. Wir wissen, dass das Leben manchmal hektisch sein kann.

Das gilt im privaten Bereich ebenso wie auf Arbeit. Sie haben Zeitdruck, die neuesten Ergebnisse der Kundenfokusgruppe sind hereingekommen, Ihr Projektmanager hat ein Meeting während der Mittagspause angesetzt und Sie verpassen fast eine anstehende Deadline. Wenn dann auch noch die rasant voranschreitende Digitalisierung und die Folgen der COVID-19-Pandemie hinzukommen, geht die Dynamik auf Warp-Geschwindigkeit.

So meldet Twilio, dass die Kombination aus bereits initiierten und pandemiebedingt vorgezogenen Maßnahmen dazu geführt hat, dass viele Unternehmen ihre Digitalisierung im Durchschnitt um 6 Jahre beschleunigt haben – einige Branchen sogar um bis zu 10 Jahre. 97 % der Entscheidungsträger in den befragten Unternehmen sind der Meinung, dass die Pandemie für diese gestiegene Geschwindigkeit verantwortlich ist. Um diese hohe Umsetzungsgeschwindigkeit über alle Kanäle hinweg im Griff zu behalten, müssen Sie verstehen, dass ein zentrales und durchgängiges System für die Benutzerverwaltung ganz oben auf der Agenda stehen muss.

Mit einem CIAM-System (Customer Identity and Access Management) können Sie die Accounts und Daten Ihrer Benutzer an einem zentralen Ort importieren, organisieren und verwalten.

Die Anmeldeseite ist für Ihre Kunden die Eingangstür und das Erste, was sie sehen. Deshalb muss die Anmeldung so benutzerfreundlich wie möglich sein. Gleichzeitig setzen hier auch viele Hacker an, wenn sie nach einer Schwachstelle suchen, über die sie Ihre Daten stehlen können. Die zuverlässige Absicherung der Anmeldung ist also zwingend notwendig. Es liegt an Ihnen, wie viel Aufwand Sie hier betreiben wollen. Lassen Sie diese Tür offen, damit jeder Gast nach Belieben hereinspazieren kann? Oder setzen Sie noch eine zusätzliche Kette ein, damit jeder erst einmal klopfen und um Einlass bitten muss? Zu wenig Sicherheit, und jeder kann Zutritt erlangen – zu viel, und niemand wird hinein wollen. Diesen Balance-Akt zwischen Sicherheit und Customer Experience müssen Sie perfektionieren.

Mit einem CIAM-System (Customer Identity and Access Management) können Sie die Accounts und Daten Ihrer Benutzer an einem zentralen Ort importieren, organisieren und verwalten. Ein starkes CIAM-Tool ermöglicht es Ihnen, zuverlässige Sicherheitsmaßnahmen zu implementieren, die den Schutz Ihrer Kundendaten garantieren und gleichzeitig eine reibungslose Nutzung sicherstellen.

Einfach ausgedrückt: Mehraufwand bei der Anmeldung führt zu entgangenen Konversionen. Dabei kann es sich ebenso um neue Benutzer handeln, die nach der Eingabe des dritten CAPTCHA aufgeben, wie auch um jahrelange treue Kunden, die nach einer aufwändigen Passwortrücksetzung das Handtuch werfen. Mehraufwand bei der Anmeldung kann dazu führen, dass Benutzer den Prozess abbrechen – und Ihrem Unternehmen den Rücken kehren. Wenn sie dabei auch ihre Freunde mitnehmen, schadet das Ihrer Marke auf Dauer enorm.

Ebenso wie bei einer digitalen Eingangstür dient ein CIAM-System als zentrale Schnittstelle zwischen Security, Datenschutz und Benutzerkomfort. Die Suche nach der richtigen Balance dieser drei Grundanforderungen – mit Blick auf Ihr Produkt und Ihre Kunden – ist nicht ohne Komplikationen: Die Entwicklung Ihrer eigenen Identity-Lösung zieht Ihre Entwickler und Ressourcen von Ihrem Kernprodukt ab. Ihr Entwicklerteam ist auf seinem Gebiet sehr erfahren und nutzt seine umfangreichen Kompetenzen, um Ihnen das bestmögliche Kernprodukt zu liefern. Warum sollten Sie der Anmeldung Ihrer Kunden und der Datensicherheit nicht die gleiche Aufmerksamkeit widmen, indem Sie Experten für Identitätsmanagement ins Boot holen?

Wenn Sie für das Identity-Management eine dedizierte SaaS-Lösung integrieren, können sich Ihre Entwickler ganz auf Ihr Kernprodukt konzentrieren. Die Lösung stellt überdies sicher, dass Ihre Kunden-informationen bestmöglich abgesichert sind, was das Vertrauen in Ihre Marke erheblich stärkt. Laut dem Edelman‘s 2020 Trust Barometer Report liegen bei Kaufentscheidungen Vertrauen und Markenreputation gleich an zweiter Stelle nach dem Preis.

Ein CIAM-System hilft Ihnen, die optimale Balance zwischen Security, Datenschutz und Komfort zu finden

Durch die zunehmende Geschwindigkeit der digitalen Anpassung in allen Sektoren gab es parallel eine sprunghafte Zunahme bei Cyberangriffen, die den kundenseitigen Perimeter ins Visier nehmen. Der Schutz der Markenintegrität und der Reputation hat deshalb für viele Führungskräfte einen hohen Stellenwert. Das bedeutet, dass die Absicherung des kundenseitigen Perimeters Priorität für Ihr Unternehmen haben muss. Verstöße gegen die Datensicherheit können nicht nur den Ruf Ihrer Marke schädigen, sondern auch zu Umsatzeinbußen führen – und die Auswirkungen wirken mitunter noch jahrelang nach. Sie sollten deshalb alles Erdenkliche tun, um erfolgreiche Angriffe zu verhindern.

Die meisten Unternehmen leben von Konversionen. Und da Reibungsverluste in der Kundenkommunikation zu verlorenen Konversionen führen, sollten Sie sich bemühen, die Anmeldeseite zu optimieren, um die Konversionsrate zu verbessern. Mit einem CIAM-System können Sie den Ablauf der Kundenanmeldungen sowie die benötigten Daten bestimmen, um den Anmeldeprozess an die aktuellen Erfordernisse anzupassen. Durch das Verschieben der symbolischen Regler für Sicherheit, Datenschutz und Kundenerlebnis zu einer optimalen Balance für Ihr Unternehmen und Ihre Kunden erhalten Sie die reibungslose Sicherheit, die sich Ihre Kunden wünschen.

CIAM bietet jedoch nicht nur reibungslose Anmeldeprozesse. Eine starke CIAM-Lösung vereint eine hochwertige User Experience mit zuverlässigem Schutz vor Cyberangriffen, der Absicherung von Benutzerdaten und einem intuitiven Management der User-Accounts.

CIAM stärkt den Perimeter und stoppt auf diese Weise viele gängige Angriffsvektoren

Theoretisches Anwendungsszenario: Ihr Unternehmen erweitert seine Web-Präsenz. Sie haben vor Kurzem ein E-Commerce-Startup übernommen UND ein exklusives Portal für 1-Tages-Angebote integriert, das Ihre bestehenden Webanwendungen und Shops ergänzt. Ihr Team soll all das in einer neuen Webanwendung mit einer einheitlichen Benutzeroberfläche zusammenführen. Für Sie ist das die ideale Gelegenheit, eine erweiterbare und skalierbare CIAM-Lösung zu integrieren. So werden Ihre Kunden mit einem Satz Anmeldedaten auf alle Angebote Ihres Unternehmens zugreifen können, während gleichzeitig die Angriffsfläche verringert wird.

Hinzu kommt, dass CIAM-Lösungen, die Funktionen wie Bot-Erkennung, Unterstützung bei der Behebung, Multi-Faktor-Authentifizierung (MFA) und Log-Streaming bieten, Ihren Schutz weiter stärken. In der heutigen Welt der verteilten Architekturen bildet Identität den Perimeter.

Eine CIAM-Lösung, die das Wachstum Ihres Unternehmens unterstützt und gleichzeitig Ihren Perimeter sowie Ihre Daten absichert, muss Erweiterbarkeit, Skalierbarkeit sowie Partnerintegrationen unterstützen.

> CIAM kann Mindestanforderungen für Passwörter (sowie Richtlinien zur Mehrfachnutzung) durchsetzen, die Ihre Password-Resets vereinfachen sowie MFA integrieren – und auf diese Weise Ihren Identity-Perimeter schützen.

Ein häufiges Thema, das viele Angriffsvektoren verbindet, ist die Mehrfachverwendung von Passwörtern. Nach einer Untersuchung von LogMeIn, dem Anbieter des Passwortmanagers Lastpass, wissen 91 % der Internetnutzer, dass die Mehrfachverwendung von Passwörtern ein Sicherheitsrisiko darstellt. Gleichzeitig geben 66 % zu, ihre Passwörter dennoch mehrmals zu verwenden. Ein CIAM-System kann Ihnen helfen, hier Best Practices durchzusetzen, CIAM kann Mindestanforderungen für Passwörter (sowie Richtlinien zur Mehrfachnutzung) durchsetzen, die Ihre Password-Resets vereinfachen sowie MFA integrieren – und auf diese Weise Ihren Identity-Perimeter schützen.

Konsolidierte Benutzerdaten lassen sich leichter schützen

Eine Single-Source-of-Truth (SSoT) ist ein Framework für die Datenverwaltung, das Unternehmen die Verwendung eines zentralen Datenspeichers anstatt mehrerer isolierter Speicherorte empfiehlt. CIAM erweitert dieses Konzept auf Ihre Benutzerdaten und führt alle Kontoinformationen an einem Ort zusammen. Unabhängig davon, auf wie vielen Plattformen Ihre Anwendungen betrieben werden, kann Ihr CIAM-System die Benutzerkonten verwalten und alle eingehenden Daten an die gleiche Identity-SSoT weiterleiten.

Dadurch wird die Absicherung dieser Daten erheblich einfacher, da nur ein Speicherort geschützt werden muss. Die zentralisierte Verwaltung der Benutzerkonten ist auch für die Einhaltung der wichtigsten Datenschutzbestimmungen relevant. Beispielsweise müssen Unternehmen laut DSGVO und CCPA auf Anfrage Benutzerdaten sowie Informationen zu ihrer Nutzung bereitstellen können.

Und da dies auch für die Systeme und Daten Ihrer Partner gilt, ermöglicht Ihnen Ihr CIAM den einfachen Zugriff, den Sie benötigen, um die Compliance-Vorgaben einzuhalten und Ihre Kunden zufriedenzustellen.

Ihr Identity-SSoT verbessert überdies auch die User Experience. Durch den Einsatz von Single Sign-On, das Datensätze aus Ihrem SSoT abruft, müssen Benutzer sich lediglich einen Satz Anmeldedaten merken. Das steigert deren Zufriedenheit, sodass die Wahrscheinlichkeit sinkt, dass sie Ihrer Anwendung den Rücken kehren. Gleichzeitig vermeiden Sie verwaiste Konten, die angegriffen werden können. Es ist nie einfach, alle Beteiligten zufriedenzustellen. Doch durch den Einsatz eines modularen CIAM-SaaS-Tools kommen Sie diesem Ziel einen Schritt näher.

Optimierung von Prozessen stellt Benutzer zufrieden

Wenn Kunden ein Konto anlegen oder sich bei einem bestehenden anmelden, setzen sie ihr Vertrauen in Sie. Sie vertrauen auch darauf, dass Ihre User Story eine Customer Journey umfasst, die keine unnötigen Hürden enthält und den Prozess behindert. Wenn sie feststellen, dass der Prozess lediglich einige wenige intuitive Schritte umfasst, sie im Handumdrehen verifiziert werden und mit ihrem Konto loslegen können – dann haben Sie ihnen bewiesen, dass dieses Vertrauen berechtigt war.

Eine CIAM-Lösung sollte all diese Aufgaben übernehmen und den Kontoerstellungsprozess optimieren, damit neue Benutzer sich willkommen fühlen – und sie sollte auch belegen, dass Sie die Daten sicher verarbeiten. Laut PwC kehren 32 % aller Kunden einem Unternehmen nach einem einzigen negativen Erlebnis den Rücken. Sie haben das richtig gelesen: Ein Drittel der befragten Benutzer beendet die Geschäftsbeziehung nach einem einzigen unfreundlichen Erlebnis. Was werden diese Menschen ihren Freunden sagen, wenn dieses negative Erlebnis ihr erstes Erlebnis mit Ihrem Unternehmen war? Wie Sie im nächsten Abschnitt sehen werden, kann CIAM alle Ihre Benutzerkontoprozesse und Workflows optimieren und damit Kundenabwanderungen verhindern.

Ein einfacher User-Lifecycle ist leichter zu schützen

Es gibt noch weitere Gründe dafür, dass Benutzer ein neues Konto erstellen. Beispielsweise könnten sie ihr Passwort vergessen haben und den Prozess für die Passwortzurücksetzung als unbequem empfinden. Das führt dazu, dass Sie anschließend zwei Konten verwalten müssen, weil Sie nicht wissen, dass es sich um ein Duplikat handelt. Eine nahtlos integrierte CIAM-Lösung bietet mit Blick auf die Security Vorteile für den gesamten User-Lifecycle.

Erstellung von Konten

Um die Zahl der Abbrüche bei der Anmeldung zu minimieren, muss der Kontoerstellungsprozess so reibungslos wie möglich sein, gleichzeitig jedoch zuverlässig die Benutzeridentität verifizieren. Diese Möglichkeit bieten CIAM-Lösungen mit Single Sign-On. Wenn sich Benutzer mit einem bestehenden Social-Media-Account bei Ihrer Website anmelden, können Sie von der bereits erfolgten Identitätsprüfung profitieren und die Erstellung eines neuen Kontos innerhalb weniger Sekunden ermöglichen. Dieser intuitive Prozess bedeutet auch, dass Benutzer seltener ein Passwort mehrfach verwenden, sodass ihr Konto schwieriger zu hacken ist – und ihre Daten besser geschützt sind.

Wartung der Accounts

Bei der allgemeinen Pflege von Benutzerkonten bietet Automatisierung erhebliche Vorteile. Ein CIAM-System sollte einen automatisierten Workflow für die Passwortrücksetzung bieten, damit diese möglichst reibungslos verläuft. Der nächste Schritt auf dem Weg zu einem durchgängigen Account-Management sind MFA-Optionen, die die Identität der sich anmeldenden Person zuverlässig bestätigen. Föderierte ID bedeutet dagegen, dass ein versehentlich erstelltes Duplikat eines Benutzerkontos von Ihrer Identity-SSoT-Lösung gefunden und mit dem anderen Konto kombiniert wird. Die zusätzliche Sicherheit durch diese MFA-Lösung und die Entfernung doppelter oder verwaister Konten verringern die Chancen einer erfolgreichen Kompromittierung.

Accounts am End-of-Life

Was geschieht, wenn Benutzer vergessen, dass ihr Konto existiert, oder wenn sie zu einem anderen Produkt wechseln und ihr Konto gänzlich aufgeben? In vielen Fällen lautet die Antwort wahrscheinlich: nichts. Wenn Sie nichts für die Konto-Hygiene tun, wird sich Ihre Identity-SSoT im Laufe der Zeit mit zahllosen verwaisten, ungenutzten und redundanten Konten füllen. Das erschwert nicht nur die Wartung, sondern ist auch mit Blick auf Sicherheit problematisch, da auch solche Zugangsdaten für Daten-Breaches und Angriffe missbraucht werden könnten.
Dieser typische Angriffsvektor lässt sich mithilfe automatisierter Account-Features wie E-Mails, die nach einer festgelegten Zeit an ruhende Konten gesendet werden, automatischer Kontodeaktivierung und letztendlicher Löschung blockieren.

Kompromittierte Zugangsdaten öffnen eine Vielzahl von Angriffs-vektoren

Wenn Benutzeranmeldedaten bei einem Daten-Breach gestohlen werden, können sie bei schlechter Passworthygiene mehrfach für verschiedene Websites verwendet werden. Cyberkriminelle haben kein Problem damit, an Benutzernamen und Passwörter zu gelangen, selbst wenn sie nicht technisch versiert genug sind, um selbst in eine Datenbank einzubrechen.

Diese so genannten „Skript-Kiddies“ können im Dark Web eine „Combo-Liste“ mit Anmeldedaten kaufen und mit bereits vorhandenen Skripten oder kompletten Anwendungen aus dem Dark Web einen Angriff starten. Dabei kommt Credential Stuffing oder eine andere Brute-Force-Angriffstechnik zum Einsatz. Sie müssen diese Angriffsvektoren und ihre Nutzung im Blick behalten, wenn Sie Ihr CIAM-System für Ihren Anwendungsfall optimal integrieren möchten.

Credential Stuffing

Einer der aktuell am häufigsten ausgenutzten Vektoren sind Brute-Force-Angriffe, die als Credential Stuffing bezeichnet werden. Dabei nutzt der Angreifer eine Liste mit Benutzernamen und Passwörtern und versucht, sich damit bei einer Website anzumelden. Die Angriffsmethode ist bei Kriminellen so beliebt, weil Passwörter häufig mehrfach verwendet werden. Die Wahrscheinlichkeit ist also groß, dass die ausprobierten Anmeldedaten häufig genug funktionieren, dass sich der Aufwand lohnt. Diese Angriffe nutzen in erster Linie den Umstand aus, dass Benutzer bequem sind und einfache sowie leicht zu erratende Passwörter verwenden (das am häufigsten verwendete Passwort ist derzeit „123456“, dicht gefolgt von „password“).

Business Email Compromise (BEC)

Kompromittierte Passwortdaten können auch als Basis für weitere Angriffe dienen. Beispielsweise können Hacker eine Combo-Liste für ein bestimmtes Unternehmen kaufen, das sie angreifen möchten. Wenn sie an die Netzwerk-Zugangsdaten ausgewählter Führungskräfte gelangen, können sie per Spoofing in ihrem Namen gezielte Phishing-E-Mails versenden (was auch als Spear Phishing bezeichnet wird). Durch den Einsatz von Bots werden diese Angriffe immer häufiger. Sie sind jedoch in erster Linie ein Social-Engineering-basierter Vektor, der sich fehlende Security-Awareness aufseiten der Mitarbeiter zunutze macht.

Bot-Attacken

Einige Hacker wollen einfach nur die Systeme des Zielunternehmens sabotieren und nichts stehlen. Stattdessen möchten sie ein Statement setzen, indem sie Geschäftsprozesse blockieren und das Zielunternehmen dabei beobachten, wie es wieder auf die Beine zu kommen versucht. Hierfür sind DDoS-Attacken (Distributed Denial of Service) das häufigste Beispiel. In diesem Fall nutzen Hacker Bots, um eine Website mit Datenverkehr zu überfluten und sie über einen gewissen Zeitraum hinweg für legitime Besucher unzugänglich zu machen. Diese Angriffe schädigen den Ruf des betroffenen Unternehmens und verursachen wegen der Ausfallzeit zudem finanziellen Schaden.

Bei der anderen – häufigen Bot-basierten – Angriffsmethode wird der Anmeldevorgang einer E-Commerce-Website überrannt, um Bestände nachgefragter Produkte aufzukaufen. Solche Bot-Schwärme wurden erst vor Kurzem gesehen, als Nvidia eine neue Grafikkarte veröffentlichte, die von Gamern auf der ganzen Welt sehnsüchtig erwartet wurde. Dergleichen geschah auch, als Microsoft die X-Box X und Sony die begehrte Playstation 5 auf den Markt brachten. Die Verarbeitungskapazitäten von Websites wie Walmart und Amazon wurden von hunderttausenden Konten, die von Bots erstellt wurden, an ihre Grenzen gebracht. Das Ziel war, den gesamten verfügbaren Bestand aufzukaufen, um die Preise auf dem Gebrauchtmarkt in die Höhe zu treiben. Diese Schwarm-Aktionen führen nicht nur dazu, dass stark nachgefragte Produkte kaum noch verfügbar sind, sie verhindern auch, dass legitime Benutzer die Website bis zur Behebung des Angriffs nutzen können. Das kostet das Unternehmen Geld und schädigt seinen Ruf.

Wie Okta Ihr CIAM schützt

„Bei der Betrachtung der Sicherheit sollten Sie stets das Risiko im Blick behalten. Es gibt keine Lösung von der Stange und Sie möchten die richtigen Sicherheitsentscheidungen für Ihr Unternehmen, Ihre Kunden und Ihre Benutzer treffen. Dementsprechend können Sie Ihre Security bei Bedarf jederzeit verstärken oder zurückfahren – was enorm dabei hilft, es mit der Sicherheit in Ihrem Produkt nicht vollkommen zu übertreiben und am Ende die Benutzerfreundlichkeit zu beeinträchtigen."

Duncan Godfrey
Vice President, Security Engineering, Okta

Duncan Godfrey erklärt, warum sich Security dynamisch weiterentwickelt. Um die oben angesprochenen Sicherheitsbedrohungen sowie weitere böse Überraschungen von Hackern erfolgreich abwehren zu können, ist ein kombinierter Ansatz mit einer skalierbaren und erweiterbaren CIAM-Lösung nötig. Damit können Sie die richtige Balance aus Sicherheit, Datenschutz und Kundenerlebnis finden.

CIAM ist optimal an der digitalen Eingangstür Ihres Unternehmens platziert – und damit auch ein Dreh- und Angelpunkt in Ihrer Perimeter-Security. Einerseits setzen Cyberkriminelle hier als Erstes an, andererseits kommen Ihre Kunden hier zum ersten Mal mit Ihrem Unternehmen in Berührung, wenn sie Ihre Website für Interaktionen oder Käufe aufsuchen. Außerdem werden hier die Daten dieser Kunden kontrolliert, analysiert und sicher gespeichert.

Modularität ist bei der Anwendungsentwicklung mittlerweile die Norm: Funktionen für Bezahlung, Messaging und Authentifizierung werden am häufigsten als SaaS-Tools integriert. Eine Untersuchung von Auth0 ergab, dass 83 % aller aktuellen Anwendungen Authentifizierung verlangen, aber nur 58 % ein externes SaaS-Tool nutzen. Ihr Entwicklungsteam ist in der Lage, Ihnen das bestmögliche Kernprodukt zu liefern, doch es gibt gute Gründe dafür, die Entwicklung der besten und sichersten CIAM-Lösung an unser Team zu übertragen.

Wenn Ihr Security-Team über brandaktuelle Informationen verfügt, kann es Angriffe schon frühzeitig erkennen, die Reaktion beschleunigen und potenziell schwerwiegende Schäden durch Sicherheitsverletzungen verhindern.

Offene Standards

Wie jedes andere Cybersecurity-Tool auch kann eine CIAM-Lösung auf offenen Standards aufbauen oder als Black Box ausgeführt sein. Letzteres bedeutet, dass Sie sich an diesen Anbieter binden, da nur er Zugriff auf sein Backend-System hat. Diesen so genannten „Vendor Lock“ sollten Sie vermeiden, um die nötige Flexibilität bei Ihren Sicherheitsimplementierungen zu bewahren und Ihre Sicherheitsmaßnahmen leicht erweitern zu können (siehe unten).

Offene Standards wie OAuth2, OpenIDConnect und SAML stehen für uns einerseits im Zentrum der Customer Experience, tragen aber auch den Anforderungen der Entwickler Rechnung. Wenn Besucher innerhalb weniger Augenblicke ein neues Konto mit ihren bereits vorhandenen Anmeldedaten erstellen können, verbessert das ihre User Experience erheblich. Dadurch können sie weniger, aber dafür stärkere Passwörter nutzen und haben gleichzeitig die Sicherheit, dass ihre Daten sicher beim Identity Provider liegen, anstatt über mehrere Systeme verteilt zu sein.

Erweiterbarkeit

Eine Lösung, die sich flexibel an die geschäftlichen Anforderungen Ihrer Kunden anpassen kann, muss das schnelle und nahtlose Hinzufügen oder Ändern von Funktionen unterstützen. Hierfür ermöglicht es Okta Ihren Benutzern, regelbasiert die für sie richtige Balance zu finden. Mithilfe von Regeln lassen sich beispielsweise Trigger für nicht plausible Ortsveränderungen erstellen. Wenn ein Benutzer aus Chicago sich scheinbar in Brasilien anmeldet, kann er zur MFA aufgefordert werden, während der bereits verifizierte Benutzer aus Chicago seine Identität nicht überprüfen lassen muss. Anhand von Regeln lassen sich auch weitere Systeme wie die Ereignisüberwachung oder der Kundenservice über Anmeldeereignisse informieren.

Für Ihre Entwickler ist das Partner-Ökosystem von Okta der Schlüssel zu unserer Erweiterbarkeit. Wenn Sie eine Funktion benötigen, die noch nicht in unserem Kernangebot enthalten ist, steht sie wahrscheinlich in unserem Marktplatz über die Integration mit einem Branchenführer zur Verfügung. Falls Sie zur Einhaltung neuer Compliance-Vorschriften Einwilligungen verwalten müssen, gibt es dafür bereits eine Integration.

Log-Streaming

Unverzichtbar für ein starkes Security-Standing ist die Möglichkeit, die von Ihren Cybersecurity-Tools generierten Daten nutzen zu können. Wenn im Unternehmen eine Dateninfrastruktur vorhanden ist, kann Log-Streaming Daten in Echtzeit aus dem CIAM-System direkt an SIEM-Lösungen (Security Information and Event Management) oder SOAR-Lösungen (Security Orchestration, Automation, and Response) senden. Dies spielt auch für die Einhaltung der Reporting- und Löschvorschriften der oben erwähnten Datenschutzregularien eine wichtige Rolle.

Der Okta-Marktplatz umfasst Integrationen mit Splunk, Sumo Logic, Datadog und anderen. Ihr Team kann aber auch selbst eine benutzerdefinierte Integration mithilfe unserer umfangreichen APIs sowie unserer SDK-Bibliothek entwickeln. Wenn Ihr Sicherheitsteam über brandaktuelle Informationen verfügt, kann es Angriffe schon frühzeitig erkennen, die Reaktion beschleunigen und potenziell schwerwiegende Schäden durch Sicherheitsverletzungen verhindern.

Schutz vor Brute-Force-Angriffen

Im einfachsten Fall probieren Angreifer bei einem Brute-Force-Angriff mehrere typische Passwörter aus, um Zugriff auf ein bestimmtes Benutzerkonto zu erlangen. Diese scheinbar wenig raffinierte Angriffsmethode kann – obwohl wenig effizient – durchaus erfolgreich sein, was ihren anhaltenden Erfolg begründet. Falls Okta mehr als zehn Anmeldeversuche für ein bestimmtes Konto von derselben IP-Adresse registriert, blockiert der Brute-Force-Schutz diese Adresse für das betroffene Benutzerkonto. Außerdem wird eine Warnungs-E-Mail an den entsprechenden Benutzer gesendet. Alle weiteren Konten am gleichen Ort haben jedoch weiterhin Zugriff. Der betroffene Benutzer kann die Blockierung der IP-Adresse mithilfe dieser E-Mail aufheben, sie wird aber auch dann entsperrt, wenn er sein Passwort ändert.

Bot-Erkennung

Bei der Abwehr komplexerer Credential-Stuffing-Angriffe ist die Bot-Erkennung häufig die entscheidende Komponente. Anhand unserer Daten zu 4,5 Milliarden monatlichen Anmeldungen – in Kombination mit der Analyse von Risikoindikatoren – kann die Bot-Erkennung von Okta feststellen, ob Anmeldeversuche von einem Bot bzw. Skript durchgeführt werden und einen CAPTCHA-Schritt in den Ablauf einbinden. Laut einer Untersuchung von Auth0 kann das die Effektivität eines Credential-Stuffing-Angriffs um bis zu 85 % verringern. Für legitime Benutzer, die sich von bekannt sicheren IP-Adressen anmelden, ist dieser zusätzliche Sicherheitsschritt nicht nötig.

Echte Kunden müssen also keinen Mehraufwand befürchten. Die Minimierung von Risiken, während gleichzeitig legitime Benutzer von reibungslosen Abläufen profitieren, folgt dem Konzept, die richtige Balance zwischen Sicherheit und Customer Experience für Sie und Ihre Kunden zu finden.

Adaptive MFA

Das NIST (National Institute of Standards and Technology) betrachtet MFA als Best Practice und empfiehlt die ständige Nutzung. Und laut OWASP (Open Web Application Security Project) ist MFA der bei weitem beste Schutz vor den meisten Passwort-Angriffen. Okta Adaptive MFA ermöglicht MFA mit erheblich verbessertem Benutzererlebnis und optimierter Datensicherheit. Adaptive MFA wertet kontextabhängige Attribute wie Standort, Unique Device Identifier, Zeit seit der letzten Anmeldung u. a. aus und erstellt eine Risikoanalyse für jede Benutzeranmeldung. Weitere Faktoren für die Anmeldung werden nur abgefragt, wenn dies als notwendig erachtet wird (siehe unser Beispiel mit der nicht plausiblen Ortsveränderung oben).

Passwortlose Authentifizierung

Angesichts der mit Passwörtern verbundenen Schwierigkeiten wäre es vielleicht am besten, wenn sie gänzlich aus dem Anmeldevorgang verschwinden würden. Mit der passwortlosen Authentifizierung von Okta ist das möglich. Stattdessen wird ein One-Time-Code genutzt, den die Benutzer per E-Mail oder SMS erhalten. Durch den Verzicht auf Passwörter haben Credential-Stuffing-Angriffe und andere Formen der Kontenkompromittierung keine Chance mehr. Und dank einer öffentlichen API, die das Festlegen von Bandbreiten-Limits ermöglicht, sind die Benutzerdaten auch vor automatisierten oder Bot-Attacken geschützt.

CIAM vereint Security und Bedienkomfort

Sie und Ihr Team haben schon genug zu tun. Wenn Sie dem Trend der Modularisierung folgen und – wo es sinnvoll ist – externe SaaS-Lösungen integrieren, können Sie CIAM schnell und sicher implementieren. Um ein Höchstmaß an Sicherheit und Kundenzufriedenheit zu gewährleisten, ist es wichtig zu verstehen, dass mit der Zunahme legitimer Benutzer auch die Zahl von Cyberkriminellen wächst, die es auf Ihre Daten abgesehen haben. Eine CIAM-Lösung, die dieser Dynamik Rechnung trägt, kann den Schutz dynamisch an die Benutzerzahlen anpassen.

Unternehmen achten immer mehr darauf, wie sie mit den digitalen Identities ihrer Kunden umgehen – und eine hochwertige Customer Experience beim Login ist unverzichtbar, um das Vertrauen der Kunden zu gewinnen.

Unser ROI-Kalkulator zeigt Ihnen, wie Ihr Unternehmen von Okta Customer Identity profitieren kann.