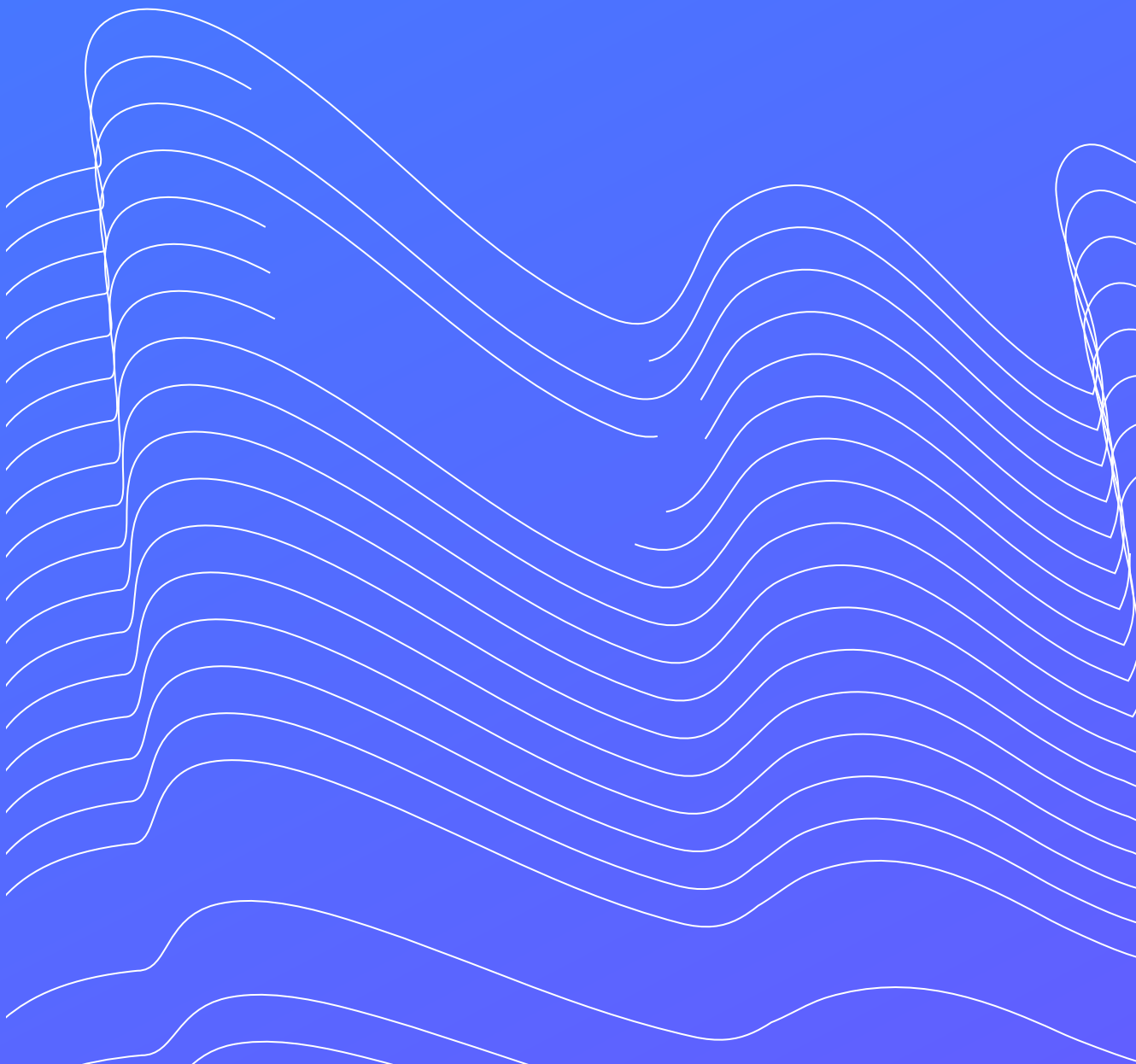
auth0

Passwortlose Authentifizierung

Maximierung von Conversions (und Verbesserung der Sicherheit) im Convenience-Zeitalter



EBOOK

auth0.com

Inhalt

Einleitung 05

Trugschluss 1: Es ist unmöglich, Komfort, Sicherheit und Datenschutz gleichzeitig zu bieten 06

Die Zukunft von Identity 06

Die Welt bewegt sich auf eine Zukunft ohne Login zu 06

Vertrauen bildet die Grundlage 08

Trugschluss 2: Loginless ist nicht sicher 09

Reibungslosigkeit als Imperativ 09

Reibungsverluste sind der natürliche Feind des Umsatzes (das ist der Tweet) 10

Die Reduzierung von Reibungsverlusten bietet einen Wettbewerbsvorteil 11

Reibungsverluste beeinträchtigen die Accessibility 12

Identity Flows sind grundlegende Elemente der Customer Journey 13

Trugschluss 3: Reibungsverluste sind ein technisches, kein betriebswirtschaftliches Problem 15

Inhalt

Das Wichtigste zuerst: Passwortlose Authentifizierung 15

Trugschluss 4: Sie haben noch keinen Passwordless Flow 17

Die passwortlose Authentifizierung kann Reibungsverluste minimieren und gleichzeitig die Sicherheit erhöhen 17

Die Loginless Roadmap 19

Trugschluss 5: Wir können aktuell keine nennenswerten Fortschritte machen (also warten wir ab) 20

Ändern Sie Ihre Einstellung in Bezug auf Identity Flows und Authentifizierung 20

Begnügen Sie sich nicht mit Passwörtern 20

Schaffen Sie Vertrauen 22

Trugschluss 6: Personenbezogene Daten sind mehr wert als Vertrauen 23

Fangen Sie an zu vertrauen 24

Trugschluss 7: Passwörter sind sicher; andere Authentifizierungsmethoden sind es nicht 25

Nutzen und fördern Sie biometrische Authentifizierung 25

Inhalt

Trugschluss 8: Biometrische Authentifizierung ist datenschutzrechtlich bedenklich 27

Priorisieren Sie Accessibility 27

Nutzen Sie Progressive Enrollment 29

Trugschluss 9: Sobald man eine bestimmte Authentifizierungsmethode anbietet, ist die Arbeit getan 31

Fazit 31

Trugschluss 10: Es ist zu schwierig, auf Passwordless umzustellen 33

Was Sie jetzt tun können 33

Erfahren Sie mehr über Identity Management mit Auth0 34

Einleitung

Identität befindet an der Schnittstelle zwischen:

- **Komfort:** Komfortable Experiences beeinflussen sowohl bewusste Entscheidungen als auch unterbewusste Präferenzen, und jede neue Interaktion wird mit der bislang komfortabelsten verglichen.
- **Sicherheit:** Ein einziger Breach kann Unternehmen ruinieren oder zumindest den Markenruf und Unternehmenswert nachhaltig schädigen – daher ist es von entscheidender Bedeutung, dass die von ihnen entwickelten Anwendungen den höchsten Sicherheitsstandards genügen.
- **Datenschutz:** Sowohl aus finanzieller Sicht als auch im Hinblick auf den Markenruf müssen Unternehmen sicherstellen, dass sie die sich ständig ändernden und anspruchsvollen Anforderungen an Datenschutz und Compliance erfüllen.

Von der Verbesserung der Customer Experience über nahtlosen Single Sign-On (SSO) bis hin zur schnellen und einfachen Multi-Faktor-Authentifizierung (MFA) – Ihre Login-Box muss das richtige Gleichgewicht zwischen Komfort, Sicherheit und Datenschutz finden.

Wir glauben, dass in den nächsten fünf Jahren diejenigen Unternehmen erfolgreich sein werden, die die ständig wachsenden Erwartungen der Verbraucher in Bezug auf diese drei Aspekte am besten abbilden können.

Doch wie wird diese Zukunft aussehen und wie können die Unternehmen von heute die Marktführer von morgen werden?

In diesem eBook geben wir Antworten auf diese Fragen und mehr.

Trugschluss 1: Es ist unmöglich, Komfort, Sicherheit und Datenschutz gleichzeitig zu bieten

Designer, Developer und IT-Experten, die digitale Experiences entwickeln, befinden sich stets in einem Spannungsfeld zwischen Sicherheit und Datenschutz auf der einen und Komfort für den User auf der anderen Seite.

In der Vergangenheit waren Unternehmen gezwungen, zu priorisieren und Kompromisse einzugehen. Unserer Meinung nach entsteht dieses Spannungsfeld jedoch nur aufgrund der Art und Weise, wie Infrastruktur und Systeme in der Vergangenheit konzipiert wurden.

Wie wir sehen werden, können innovative Lösungen alle drei Bereiche gleichzeitig abdecken.

Die Zukunft von Identity

In naher Zukunft – vielleicht sogar noch in diesem Jahrzehnt – wird der traditionelle Login aussterben. An die Stelle der heute allgegenwärtigen Login-Boxes mit ihren User-ID- und Passwort-Feldern werden User-zentrierte Systeme treten, die auf Komfort (ohne Abstriche bei der Sicherheit oder dem Datenschutz) setzen und auf Vertrauen basieren.

Die Welt bewegt sich auf eine Zukunft ohne Login zu

Heutige Authentifizierungssysteme sind nicht intelligent und behandeln legitime User und Angreifer auf dieselbe Weise.

In Zukunft wird das anders sein: Die Beweislast wird sich vom User auf das Unternehmen verlagern. In dieser Welt ohne Login werden die User auf möglichst einfache Weise ihre Vertrauenswürdigkeit nachweisen. Sobald dies geschehen ist, werden weitere kontextbezogene Signale und Analysen zum Einsatz kommen, um die Vertrauenswürdigkeit aufrechtzuerhalten und zu erhöhen, anstatt den User zu zwingen, sich wiederholt einzuloggen.

Wie könnte diese Zukunft ohne Login aussehen?

Alex wird vom Wecker seines/ihres Smartphones geweckt. Nachdem er/sie kurz seinen/ihren personalisierten Newsfeed und die Entwicklung der internationalen Märkte gecheckt hat, geht er/sie ins Gästezimmer für einen morgendlichen Workout.

Die intelligenten Cardiogeräte erkennen Alex anhand einer Reihe von Faktoren – der Tageszeit, dem Druck auf den Touchscreen, seinem/ihrem Gewicht – und laden automatisch den richtigen User Account.

Nach einem kurzen HIT-Programm (Alex' bevorzugter morgendlicher Muntermacher) geht Alex ins Bad und stellt sich unter die Dusche. Wie die Fitnessgeräte erkennt auch das intelligente System der Dusche den User und sorgt für eine angenehme Experience.

Bereit für den Tag, klappt Alex seinen/ihren Laptop auf. Die integrierte Kamera und die biometrischen Daten authentifizieren Alex im Handumdrehen, ohne dass er/sie eingreifen muss. Obwohl Alex sich dessen nicht bewusst ist, ist dieselbe biometrische Identity der Grund dafür, dass der Zugriff auf Online-Anwendungen – sowohl auf berufliche Ressourcen als auch auf persönliche Services – so reibungslos funktioniert. Die einzige Ausnahme war ein Online-Arzttermin, für den Alex einige von einem virtuellen Assistenten gestellte Fragen mündlich beantworten musste, bevor er/sie autorisiert wurde.

Währenddessen versucht ein Angreifer am anderen Ende der Welt, auf Alex' Online Trading Account zuzugreifen. Hinter den Kulissen erkennt das System, dass die Zeitspanne zwischen dem morgendlichen Check der Märkte und dem jetzigen Zeitpunkt zu kurz ist, um den Standortwechsel plausibel zu erklären. Das System erkennt ein „unmögliches Reiseszenario" und konfrontiert den Angreifer mit einer MFA-Anfrage – und der Angriff wird gestoppt.

Der Schlüssel zu einem sicheren und komfortablen Betrieb eines solchen Systems ist Vertrauen.

Vertrauen bildet die Grundlage

Die Zukunft des Internets wird auf vertrauensvollen digitalen Beziehungen beruhen, wobei das Vertrauen in zwei Richtungen fließt:

- das Vertrauen, das ein User in ein Unternehmen setzt
- das intelligente Vertrauen, das ein Unternehmen einem User entgegenbringt

Auf den ersten Punkt werden wir später zurückkommen – jetzt wollen wir erst einmal den zweiten untersuchen.

Es stimmt zwar, dass Loginless auf einer Basis aus Vertrauen aufbaut, aber es ist wichtig zu verstehen, dass dieses Vertrauen nicht blind ist. Vielmehr wird das Customer Identity and Access Management (CIAM) von morgen eine Reihe von Technologien und Ansätzen verwenden, um eine sichere und komfortable Experience zu bieten. Im Kern müssen solche Systeme bei jeder User-Interaktion berücksichtigen:

- auf welche Funktionen, Daten und Ressourcen ein User zuzugreifen versucht
- wie es um die Vertrauenswürdigkeit des Users zu diesem Zeitpunkt bestellt ist

Durch das kontinuierliche Monitoring von Signalen (z. B. Standort des Users, Endgerät, Apps, Konsumverhalten, Tageszeit, Eingabeverhalten und so weiter) prüft das Authentifizierungssystem bei Bedarf ganz einfach, ob die Vertrauenswürdigkeit ausreicht, um dem User ungehinderten Zugriff auf eine bestimmte Ressource zu gewähren.

Diese „kontinuierliche Authentifizierung“ ist außerordentlich leistungsstark, da sie sowohl die Sicherheit als auch die User Experience verbessert – und das Vertrauen, das diese liefert, geht weit über alles hinaus, was ein Passwort allein bieten kann.[1]

Nachdem wir nun einen Blick auf das „Was“ der Zukunft geworfen haben, wollen wir uns nun mit dem „Warum“ beschäftigen.

Trugschluss 2: Loginless ist nicht sicher

Ohne die Details darüber zu kennen, wie solche Systeme implementiert werden, ist es fast natürlich, den Begriff „Loginless“ zu betrachten und daraus zu schließen, dass dieser Ansatz Sicherheit zugunsten von Komfort opfert. Das ist jedoch nicht der Fall: Methoden mit geringerem Reibungsverlust können immer noch sicher gegenüber den häufigsten Angriffsvektoren sein.

Einfachheit als Imperativ

In der physischen Welt ist Reibung die Kraft, die der relativen Bewegung von aneinander gleitenden festen Oberflächen, flüssigen Schichten und Material entgegenwirkt.

Im Privatkundengeschäft **bezieht sich Reibung auf alles, was die Interaktion einer Person mit Ihrem Service verlangsamt**. Zu solchen Interaktionen gehören beispielsweise (aber nicht ausschließlich):

- ein User, der sich für Ihren Service anmeldet
- ein User, der sich in seinen bestehenden Account einloggt

1. Kontinuierliche Authentifizierung kann als ein wesentliches Element des strategischen Ansatzes betrachtet werden, den Gartner als Continuous Adaptive Risk and Trust Assessment (CARTA) bezeichnet.

   Gartner ®, “Secure Application Access by Applying the Imperatives of CARTA Access Management”, Michael Kelley, Abhyuday Data, Henrique Teixeira, Refreshed 12 August 2021, Published 25 February 2020. GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. und/oder seinen Tochtergesellschaften in den USA und international und wird hier mit Genehmigung verwendet. Alle Rechte vorbehalten.

- ein User, der verlorene Account-Informationen wiederherstellt
- ein User, der einen Kauf abschließt

Obwohl ein gewisses Maß an Reibung während dieser Interaktionen notwendig ist, um Vertrauen zu etablieren und Sicherheitskontrollen zu bieten, die die sensiblen Daten eines Users schützen und Betrug vorbeugen, gilt: Je mehr Reibungsverlust auftritt (z. B. mehr Schritte, mehr benötigte Informationen und so weiter), desto größer ist die Frustration des Users – und desto wahrscheinlicher ist es, dass er die Experience abbricht.

Reibungsverluste sind der natürliche Feind des Umsatzes (das ist der Tweet)

Im Privatkundengeschäft sind Reibungsverluste ein Haupthindernis für Conversions und damit auch für den Umsatz. Je mehr Reibungsverluste es bei jeder einzelnen Kundeninteraktion gibt, desto niedriger ist Ihre Conversion-Rate, und desto weniger Umsatz erzielen Sie kurz- und langfristig:

- Werden bei der Einrichtung eines Accounts zu viele Informationen abgefragt oder sind zu viele Schritte erforderlich? Dann werden sich weniger Kunden anmelden.
- Ist der Sign-In zu umständlich? Dann werden weniger Kunden Ihren Service nutzen.[2]

2. Eine FICO-**Studie zum digitalen Banking** [FICO] aus dem Jahr 2020 ergab, dass 28 Prozent der Amerikaner einen Onlinekauf abbrechen, weil sie ihre Login-Daten vergessen haben.

- Ist das Zurücksetzen des Passworts zu umständlich? Kurzfristig brechen Kunden, die während des Checkouts mit diesem Problem konfrontiert werden, ihre Einkäufe ab;[3] langfristig können zähe Abläufe beim Zurücksetzen von Passwörtern dazu führen, dass Kunden Ihren Service überhaupt nicht mehr nutzen.
- Ist der Checkout zu kompliziert? Dann bleiben Artikel im Einkaufswagen liegen – möglicherweise für immer.

Zu wenige Unternehmen sind sich dieser simplen Wahrheit bewusst – weshalb es sich lohnt, sie zu wiederholen: **Je höher der Reibungsverlust, desto geringer der Umsatz und Gewinn.**

Die Reduzierung von Reibungsverlusten bietet einen Wettbewerbsvorteil

Die Reduzierung von Reibungsverlusten trägt auch dadurch zu einem besseren Outcome, sprich höheren Conversions und Umsatz, bei, dass sie einen Wettbewerbsvorteil gegenüber weniger userfreundlichen Alternativen schafft.

Viele Dienstleistungsbranchen und E-Commerce-Websites haben diese Tatsache bereits erkannt und Benutzerkomfort als Hauptunterscheidungsmerkmal positioniert.

Während es in der digitalen Welt Funktionen wie „Jetzt kaufen“ und „Nochmals kaufen“ gibt, hat die physische Welt viele eigene Beispiele.

3. Eine gemeinsam von MasterCard und der University of Oxford durchgeführte Studie (**Mobile Biometrics in Financial Services: A Five Factor Framework**) [University of Oxford] kommt zu dem Ergebnis, dass „etwa ein Drittel der Onlinekäufe beim Checkout abgebrochen wird, weil sich die Verbraucher nicht an ihre Passwörter erinnern können“.

So war die Mobile App eines Hotels selten mehr als eine Möglichkeit, Buchungen und Prämienpunkte zu managen – bis Marriott und Hilton die App nutzten, um Smartphones sowohl zum Check-in-Schalter als auch zum Zimmerschlüssel zu machen. Geschäftsreisende – ein lukratives Segment in der Hotelbranche – schätzten die Möglichkeit, Check-in-Schlangen umgehen zu können, und sich nicht mehr mit dem Ärger herumschlagen müssen, der mit dem Verlust eines Zimmerschlüssels einhergeht.

Oder denken Sie an die Autovermietung National Car Rental, die ihren Emerald-Club-Mitgliedern den Zusatzservice „Wählen Sie ein beliebiges Fahrzeug aus dem Fuhrpark und fahren Sie los“ bietet.

Eine hochwertige Experience kann Ihren Brand von allen anderen abheben, die Erwartungen der Kunden auf dem Markt insgesamt erhöhen und die Konkurrenz zwingen, aufzuschließen.

Und bis sie das tut, bedeutet das mehr Kunden und höhere Umsätze für Sie.

Reibungsverluste beeinträchtigen die Accessibility

Während Reibungsverluste für die meisten User eine Unannehmlichkeit sind, können sie für manche eine erhebliche Hürde darstellen, die sie daran hindert, Ihre Services in Anspruch zu nehmen.

Leider steht das Thema Accessibility (wenn es überhaupt berücksichtigt wird) oft weit hinter anderen Faktoren auf der Prioritätenliste, was zu Designs führt, die zwar schick aussehen, aber für manche Kunden nur schwer zu navigieren sind. Die COVID-19-Pandemie hat viele dieser Usability-Mängel deutlich gemacht, da sie dazu führte, dass viel mehr Interaktionen online stattfanden.

Denken Sie an Behinderungen wie Sehstörungen, kognitive Beeinträchtigungen oder eingeschränkte Motorik und stellen Sie sich vor, wie Sie versuchen, durch einen umständlichen Authentifizierungsprozess zu navigieren, bei dem der User sich ein langes, komplexes Passwort merken und dann eingeben muss.

Oder denken Sie darüber nach, wie ein User, der mit der Technik nicht vertraut ist, auf eine Nachricht reagieren würde, in der er aufgefordert wird, eine App herunterzuladen und Push-Benachrichtigungen zu konfigurieren.

Solange Designer und Developer – die selbst technisch versiert sind – für die Experience verantwortlich sind, kann es die Tendenz geben, sich unverhältnismäßig stark auf ähnlich kompetente User zu konzentrieren („Wie bitte, benutzt heutzutage nicht jeder einen Passwortmanager?!“[4]), aber man muss darauf achten, dass andere nicht abgehängt werden.

Es ist nicht nur eine moralische Verpflichtung, das Thema Accessibility während des Design- und Entwicklungsprozesses zu berücksichtigen, sondern es gibt auch einen handfesten finanziellen Anreiz: Wenn Sie Anwendungen entwickeln, die von allen genutzt werden können, maximieren Sie Ihre Marktreichweite.

Identity Flows sind grundlegende Elemente der Customer Journey

Sobald Sie die Gefahren von Reibungsverlusten und deren Ausprägungen erkannt haben, wird klar, dass:

- Identity Flows (in Abbildung 1 blau dargestellt) im Online-Privatkundengeschäft grundlegender Bestandteil der Customer Journey sind.

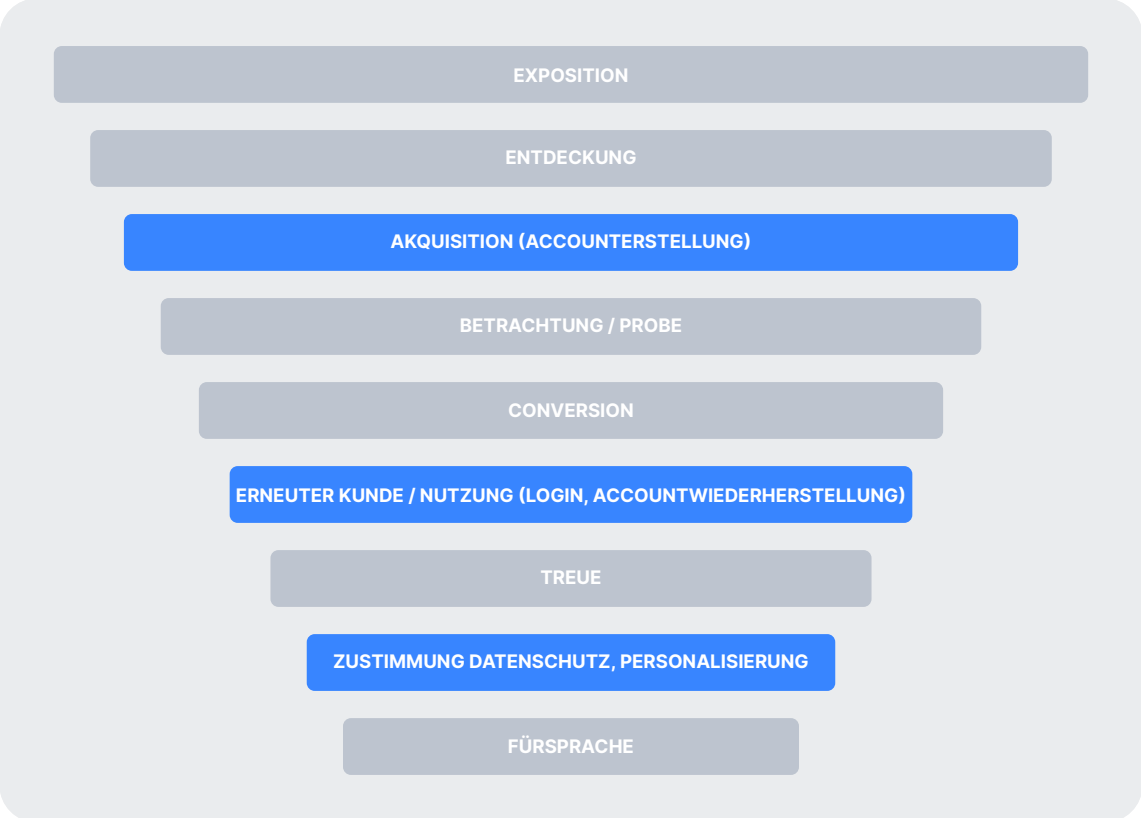
4. Dieselbe bereits zitierte FICO-Studie ergab, dass weniger als 23 Prozent der Amerikaner einen Passwortmanager verwenden.

- Reibungsverluste den Unterschied ausmachen können zwischen dem Erreichen oder Verfehlen Ihrer Conversion- und Umsatz-Ziele. Von dieser Warte aus betrachtet, werden die Kosten von Reibungsverlusten innerhalb der Identity Flows viel deutlicher. Zum Beispiel könnte eine abgebrochene Accounterstellung einem entgangenen Gesamtumsatz von 1.000 US-Dollar entsprechen, und jeder fehlgeschlagene Login könnte Sie 100 US-Dollar an entgangenem Umsatz kosten.

Setzen Sie Ihre eigenen Zahlen ein und multiplizieren Sie sie mit Ihrem Kundenstamm, und Sie erhalten eine ungefähre Vorstellung von den Kosten von Reibungsverlusten für Ihr Unternehmen.

Jetzt, da die Auswirkungen von Reibungsverlusten deutlich werden, stellt sich die Frage, wie Sie diese minimieren können.

Abbildung 1: Identity Flows sind grundlegende Elemente der Customer Journey und haben großen Einfluss auf Conversion Rates



Trugschluss 3: Reibungsverluste sind ein technisches, kein betriebswirtschaftliches Problem

Wenn mehr Unternehmen den Zusammenhang zwischen Identity Management und realen Geschäftsergebnissen verstehen würden, würden die Alarmglocken schrillen: Wenn Sie es nicht schaffen, eine reibungsarme Experience zu bieten, dann entgehen Ihnen buchstäblich Kunden und Einnahmen.

Leider betrachten zu viele Unternehmen Reibungsverluste innerhalb von Identity Flows als ein technisches Problem.

Woher wir das wissen? Weil an den meisten unserer Gespräche mit Unternehmen Mitarbeiter aus den Bereichen Identity und Security beteiligt sind. Finance, Product Management, Product Marketing, Customer Experience oder andere kundenorientierte Funktionen sind vergleichsweise selten involviert – und wenn, dann ist das ein deutliches Zeichen dafür, dass das Unternehmen verstanden hat, was tatsächlich auf dem Spiel steht.

Das Wichtigste zuerst: Passwortlose Authentifizierung

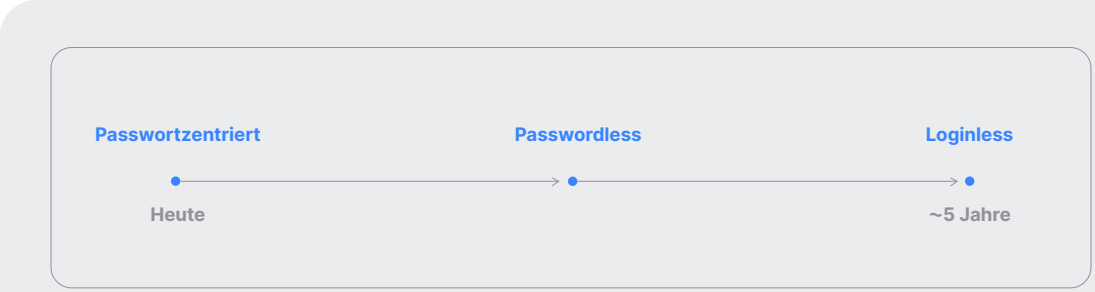
Es ist kein Geheimnis, dass Passwörter eine vergleichsweise schlechte Lösung sind, wenn es darum geht, User zu authentifizieren. Sie haben unter anderem den Nachteil, dass sie für die User umständlich zu erstellen und zu merken sind (ein Grund, warum Passwörter so häufig wiederverwendet werden) und dass sie für eine Reihe von Cyberangriffen anfällig sind.[5]

Glücklicherweise gibt es bessere Alternativen.

Die passwortlose Authentifizierung (oft einfach mit „Passwordless“ abgekürzt) bezieht sich auf jeden Mechanismus – und es gibt mehrere, wie wir noch sehen werden –, der einen User authentifiziert, ohne dass dieser sein Passwort eingeben muss.

5. Unser **State of Secure Identity Report** untersucht die neuesten Threats, darunter Credential Stuffing, Injection-Angriffe, die Erstellung von Fake-Accounts und MFA-Bypass-Angriffe, sowie die verfügbaren Abwehrmaßnahmen zur Bekämpfung dieser Angriffe.

Abbildung 2: Die drei Authentifizierungsparadigmen – Passwordless ist der Zwischenschritt auf dem Weg zu Loginless



Auch wenn die meisten von uns Passwörter nicht vermissen würden, ist das Wort „Passwordless“ doch etwas irreführend, denn Passwörter wird es weiterhin geben – zumindest in absehbarer Zukunft –, selbst wenn die passwortlose Authentifizierung weit verbreitet ist.

Der Hauptunterschied besteht darin, dass im passwortlosen Paradigma andere Authentifizierungsmethoden Vorrang haben werden – wobei Passwörter wahrscheinlich als letzter Faktor dienen werden.[6]

Wenn also die Abschaffung von Passwörtern nicht der Treiber hinter der Umstellung auf passwortlose Authentifizierung ist, was ist es dann?

Wie Sie vielleicht schon erraten haben, geht es darum, den Reibungsverlust zu reduzieren.

6. Vielleicht wäre „Passwordlast“ zutreffender, aber wir glauben nicht, dass sich dieser Begriff durchsetzen wird.

Trugschluss 4: Sie haben noch keinen Passwordless Flow

Würden Sie uns glauben, wenn wir Ihnen sagen würden, dass heutzutage fast jedes Online-Unternehmen bereits über einen Passwordless Flow verfügt? Nun, es ist wahr!

Aber dieses Missverständnis entsteht, weil der bestehende Flow nicht „Passwordless“ heißt, sondern „Reset Password“.

Stellen Sie sich vor: Bei der typischen Accountwiederherstellung klickt der User auf den Button „Passwort zurücksetzen“, was eine E-Mail mit einem Link zum Zurücksetzen des Passworts triggert. Der User klickt auf diesen Link und gelangt auf eine Seite, die ihn auffordert, ein neues Passwort zu vergeben. Danach wird er in seinen Account eingeloggt – ohne das ursprüngliche Passwort einzugeben.

Die passwortlose Authentifizierung kann Reibungsverluste minimieren und gleichzeitig die Sicherheit erhöhen

Obwohl verschiedene Unternehmen Identity and Access Management (IAM) für ähnliche Zwecke nutzen, unterscheiden sich ihre genauen Anforderungen. **Technologien, die sich in Verbraucheranwendungen bewähren, müssen ein Gleichgewicht zwischen Sicherheit und User Experience herstellen.** Eine Möglichkeit, die Qualität der User Experience zu bewerten, besteht darin, zwei Messgrößen zu untersuchen:

- **Erfolgsquote** bei einer Authentifizierungsanfrage:
  Je höher die Erfolgsquote, desto besser die User Experience.
- **Zeit bis zum Abschluss** einer Authentifizierungsanfrage: Je kürzer die Zeit bis zum Abschluss, desto besser die User Experience.

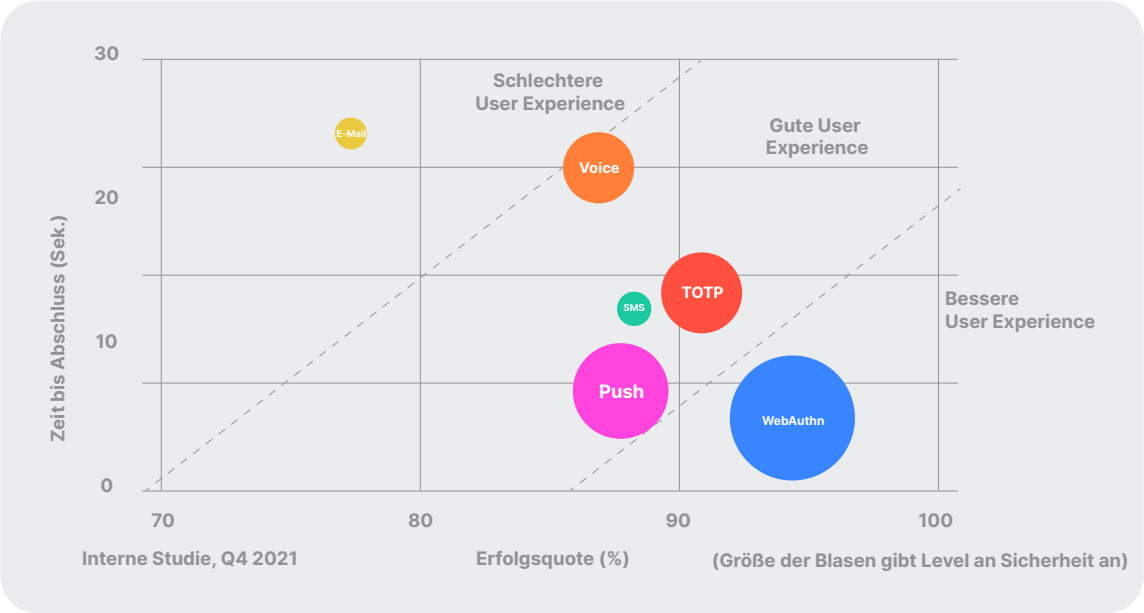
Die Kombination dieser beiden Messgrößen und der Vergleich der passwortlosen Authentifizierungsmethoden zeigt, dass die User Experience erheblich variiert. Bei näherer Betrachtung von Abbildung 3 zeigt sich Folgendes:

- Sprach- und E-Mail-Authentifizierung bieten eine schlechte User Experience: Die Erfolgsquoten sind niedrig (82 Prozent beziehungsweise 84 Prozent) und die Zeit bis zum Abschluss ist hoch, im Durchschnitt etwa 25 Sekunden für beide.
- Push-Benachrichtigungen über eine proprietäre Anwendung (Push), die Übermittlung eines Einmalpassworts (OTP) und die Verwendung von SMS als MFA-Kanal bieten eine mittelmäßige User Experience mit Erfolgsquoten von 87 bis 90 Prozent und einer durchschnittlichen Zeit von etwa 10 Sekunden.
- Die Verwendung einer proprietären Anwendung zur Übermittlung eines OTP (MFA-OTP) und die Nutzung von Device Biometrics (WebAuthn) bieten die beste User Experience – beide weisen hohe Erfolgsquoten und niedrige Zeiten bis zum Abschluss auf.

Interessanterweise – und das ist wichtig – können wir auch einen hohen Grad an Korrelation zwischen den Authentifizierungsmethoden, die eine angenehme User Experience aufweisen, und denen, die die höchste Sicherheit bieten, feststellen.

Biometrische Verfahren wie WebAuthn sind ein großartiges Beispiel dafür, wie IAM-Systeme gleichzeitig eine komfortable, datenschutzkonforme und sichere Experience bieten können.

Abbildung 3: Interne Auth0-Daten zeigen, dass passwortlose Authentifizierungsmethoden Reibungsverluste minimieren und die Sicherheit erhöhen



Die Loginless Roadmap

Es mag wie ein gewaltiges Unterfangen erscheinen, vom heutigen passwortzentrierten Paradigma zum Zwischenschritt des passwortlosen Paradigmas zu gelangen, aber die Reise wird viel überschaubarer, wenn man sie in kleinere Initiativen unterteilt.

Außerdem gibt es viele Gründe, warum Sie sofort damit beginnen sollten – von der unmittelbaren Verbesserung der Conversion Rate über die relative Einfachheit einer schrittweisen Veränderung in der Gegenwart (im Vergleich zu massiven Umwälzungen in der Zukunft) bis hin zu der Tatsache, dass das Vertrauen, das für den Übergang so wichtig ist, im Laufe der Zeit aufgebaut werden muss, und, dass die verschiedenen User in ihrem eigenen Tempo vorgehen werden.

Trugschluss 5: Wir können aktuell keine nennenswerten Fortschritte machen (also warten wir ab)

Sogar unter denjenigen, die die Unvermeidbarkeit einer Zukunft ohne Login anerkennen, ist die Auffassung weit verbreitet, dass man heute nicht viel tun kann, um sich in diese Richtung zu bewegen. Dieser Trugschluss führt zu verpassten Chancen und magischem Denken, da Unternehmen auf eine perfekte Lösung warten, bevor sie die notwendigen Zwischenschritte unternehmen.

Die Wahrheit ist jedoch, dass Sie schon heute mit Ihrer Reise Richtung Loginless beginnen können, indem Sie die passwortlose Authentifizierung einführen.

Ändern Sie Ihre Einstellung in Bezug auf Identity Flows und Authentifizierung

Der erste und wichtigste Schritt besteht darin, Ihre Einstellung zu Identity Flows zu ändern. Hören Sie auf, sie als eine technische Komponente hinter den Kulissen zu betrachten, und fangen Sie an, sie als das zu sehen, was sie sind: grundlegende Elemente Ihrer Customer Journey.

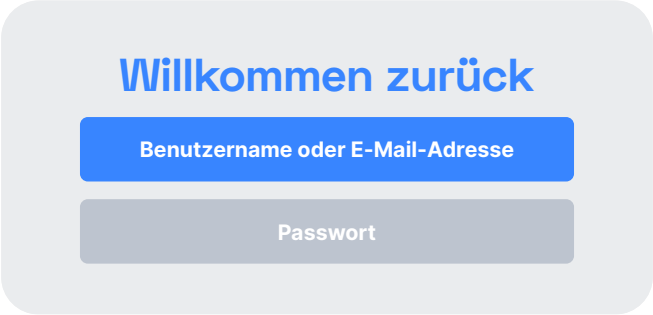
Dieses Umdenken sollte dazu führen, dass in jeder Diskussion über Identity Flows zahlreiche Stakeholder berücksichtigt werden: nicht nur Developer und Security Engineers, sondern auch Product Management, Customer Success, Marketing, Customer Experience (einschließlich Accessibility) und Revenue Owners. Mit vereinten Kräften sollte die Gruppe in der Lage sein, Komfort, Sicherheit und Datenschutz im Zusammenhang mit der Authentifizierung zu diskutieren.

Begnügen Sie sich nicht mit Passwörtern

Während die Login-Box erst mit dem Aufkommen der GUIs zu einem vertrauten Anblick wurde, war der Login mit User-ID und Passwort bereits mit den Time-Sharing-Systemen der 1960er-Jahre und später mit den Bulletin Board Systems (BBS) in den 1970er-Jahren salonfähig geworden.

Seitdem ist die Kombination aus User-ID und Passwort ein Synonym für Authentifizierung, und Passwörter sind die in Login Screens eingebettete Standardhürde.

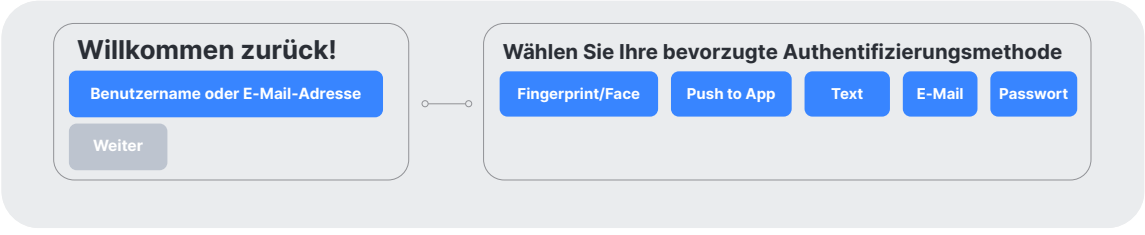
Abbildung 4: Beim passwortzentrierten Login werden in der Regel standardmäßig User-ID und Passwort abgefragt



Zugegeben: Eine Zeit lang gab es keine besseren Alternativen, aber das ist nicht mehr der Fall: Ein Passwort ist nur eine Möglichkeit, eine Identität zu verifizieren – und nicht annähernd die beste.

Der erste Schritt in Richtung passwortloser Authentifizierung besteht darin, die Verwendung des Passworts als Identitätsnachweis zu vermeiden. In diesem neuen Paradigma beginnt der Login Flow damit, dass der User nach einem Identifier (zum Beispiel User-ID, E-Mail-Adresse und so weiter) gefragt wird. Wenn es dann an der Zeit ist, die Identität zu verifizieren, werden Passwörter nur als eine von vielen verfügbaren Optionen behandelt – einschließlich biometrischer Daten, OTPs, Magic Links und so weiter –, von denen die meisten eine höhere Sicherheit und mehr Komfort bieten.

Abbildung 5: Das passwortlose Paradigma entkoppelt den Login Flow und erlaubt dem User, eine bevorzugte Authentifizierungsmethode zu wählen



Sieht man einmal von der künstlichen Komplikation ab, dass Passwörter in vielen Authentifizierungsprozessen fest verankert sind, steht der Implementierung dieses Identifier-first-Paradigmas nichts im Wege. Tatsächlich haben viele bekannte Internet-Giganten bereits mit der Umsetzung dieses Ansatzes begonnen, da sie schon vor langer Zeit den Wert der passwortlosen Authentifizierung erkannt haben.[7]

Schaffen Sie Vertrauen

Unternehmen erkennen bereits, dass ihr Erfolg vom Vertrauen der Verbraucher abhängt und dass dieses Vertrauen verdient werden muss.

Wie bei Beziehungen im realen Leben wird Vertrauen auch in der digitalen Welt im Laufe der Zeit durch sichere, komfortable, respektvolle und angenehme Interaktionen gewonnen – und die Verbraucher können selbst entscheiden, welche Informationen sie mit welchen Unternehmen teilen.

Die Last, sich dieses Vertrauen zu verdienen, liegt nun bei den Unternehmen. Diejenigen, die erfolgreich sind, werden beträchtliche Gewinne erzielen, während diejenigen, die kein Vertrauen aufbauen – oder schlimmer noch, es verletzen –, die Konsequenzen zu spüren bekommen werden.

Wert zu bieten, bevor man den User um etwas bittet, und nur die minimal erforderlichen Informationen abzufragen, sind zwei bewährte Methoden, um Vertrauen zu gewinnen. Diese Ansätze finden in unterschiedlichen Formen Ausdruck, darunter:

- **Anonymous Checkout** (auch als Guest Checkout bezeichnet), bei dem ein User einen Service nutzen kann, ohne einen Account anzulegen; Rechnungs- und Lieferinformationen werden zur Erleichterung der Transaktion erfasst, aber nicht innerhalb eines Accounts gespeichert.

7. Die WSO2 Open Banking Documentation Website enthält Ressourcen zu **Identifier-first Authentication.**

- **Progressive Profiling,** bei dem der User schrittweise nach Informationen gefragt wird (und ihm neue Authentifizierungsoptionen vorgestellt werden), je mehr Nutzen er aus dem Service zieht, während er gleichzeitig sehr schnell einsteigen kann.[8]

Trugschluss 6: Personenbezogene Daten sind mehr wert als Vertrauen

Vor allem Marketing-Teams sind süchtig nach Userdaten, schließlich helfen sie beim Retargeting und der Personalisierung, die für viele Services so wichtig sind. Folglich ist es eine beängstigende Vorstellung, dem User mehr Kontrolle darüber zu geben, welche Informationen er preisgibt!

Dieser Denkansatz greift jedoch zu kurz. Auf lange Sicht ist Vertrauen für loyale – und ja, hochprofitable – Beziehungen unerlässlich. Außerdem hat es handfeste kurzfristige Vorteile, wenn Sie Ihren Kunden vertrauen: Wenn Sie beispielsweise die Anzahl der bei der Registrierung erforderlichen Felder reduzieren, können Sie die Conversion Rate drastisch erhöhen.[9]

Und es gibt noch einen weiteren Grund, über seinen Schatten zu springen und den Verbrauchern mehr Kontrolle zu geben: Die Big Player tun es bereits. Unternehmen wie Apple und Facebook[10] sowie Finanzinstitute wie Fidelity Investments[11] haben die wachsende Bedeutung von Vertrauen erkannt – sei es, um sich einen Wettbewerbsvorteil zu verschaffen oder ein wahrgenommenes Defizit auszugleichen – und sie sehen nicht nur die vertrauensorientierte Zukunft, sondern arbeiten auch daran, sie so schnell wie möglich zu verwirklichen.

8. Erfahren Sie mehr über Progressive Profiling in **Progressive Profiling: Vital Info from Happy Customers.**
9. In einem von Unbounce vorgestellten Beispiel führte die Reduzierung der Anzahl der erforderlichen Felder von 11 auf 4 direkt zu einem Anstieg der Conversion Rate um 120 Prozent; siehe **How To Optimize Contact Forms For Conversions**.
10. Siehe das von Facebook gesponserte Video **Consumers Want Control. To Compete, Your Brand Needs to Give It to Them** [Harvard Business Review].
11. Siehe **Financial industry to give consumers more control over their data** [Akoya].

Fangen Sie an zu vertrauen

Auch wenn es Ihnen vielleicht unangenehm ist, mehr Vertrauen in Ihre Kundeninteraktionen einfließen zu lassen, ist es wichtig zu wissen, dass sich Vertrauen in einem Spektrum bewegt und in Beziehung zum Risiko steht – es ist nicht binär, sodass man einem Nutzer entweder absolut vertraut oder nicht vertraut. Es ist bereits möglich, viele Faktoren zu berücksichtigen und einen „Trust Score“ oder ein „Risk Profile“ zu ermitteln, das die Authentifizierungsprozesse und die User Experience beeinflusst. Zum Beispiel:

- **Adaptive MFA** ist eine Technik, die MFA nur dann einsetzt, wenn eine User-Interaktion aufgrund von Verhaltensdaten als riskant eingestuft wird.[12]
- **Step-up-Authentisierung** ist eine Technik, die Identity Requests an den Stellenwert der Ressource und den Risikograd anpasst, wenn diese kompromittiert werden sollte.[13]

12. Erfahren Sie mehr in **Auth0 Launches Adaptive MFA to Increase Security and Reduce Friction for End Users.**

13. Weitere Informationen finden Sie unter **What Is Step-Up Authentication, and When Should You Use It?.**

Trugschluss 7: Passwörter sind sicher; andere Authentifizierungsmethoden sind es nicht

Die traditionelle Login-Box mit ihrer Kombination aus User-ID und Passwort hat das kollektive Bewusstsein im Hinblick auf Vertrauen unterwandert, indem sie:

1. ein falsches Gefühl von Sicherheit vermittelt hat, das auf dem Trugschluss basiert, dass Passwörter sicher sind.
2. die Wahrnehmung geprägt hat, dass alles, was kein Passwort hat, per se nicht sicher ist.

Infolgedessen sind Unternehmen verständlicherweise vorsichtig, wenn es darum geht, ohne Passwörter zu arbeiten. Außerdem ist die Gefahr von Markenschäden und Bußgeldern aufgrund von Breaches groß genug, um jeden vernünftigen Sicherheits- oder Produktverantwortlichen davon abzuhalten, den Usern zu viel Vertrauen entgegenzubringen.

In Wahrheit macht die Kombination aus Anfälligkeit für eine Reihe von Angriffen (z. B. Brute Force, Password Spraying) und schlechten Angewohnheiten der User Passwörter zu einem Sicherheitsrisiko. Darüber hinaus bieten viele andere Optionen (z. B. MFA, OTP, Magic Link, Push-Benachrichtigungen und so weiter) höhere Sicherheit.

Es ist wichtig, die vielen Missverständnisse im Zusammenhang mit Passwörtern zu erkennen, denn dadurch ändert sich Ihre Wahrnehmung der Risiken und Vorteile in puncto Vertrauen – und das wiederum bringt Sie voran.

Nutzen und fördern Sie biometrische Authentifizierung

Usern die Möglichkeit zu geben, sich mit den biometrischen Funktionen ihres Endgeräts zu authentifizieren, hat zwei Vorteile:

- Es reduziert die Reibungsverluste bei der Authentifizierung erheblich, was die Kundenbindung und den Umsatz erhöht.
- Es erhöht die Sicherheit, da der Flow nicht von böswilligen Akteuren angezapft werden kann.

In den letzten Jahren hat die FIDO Alliance unermüdlich darauf hingearbeitet, Usern zu helfen, sich mit maximaler Sicherheit und minimalen Reibungsverlusten zu authentifizieren. Der daraus resultierende WebAuthn-Standard bietet die Grundlage dafür.

WebAuthn ist die einzige standardbasierte Authentifizierungsmethode, die Phishing unmöglich macht, da sie den Public/Private Key an eine bestimmte Web Domain bindet – was es einem User unmöglich macht, sich versehentlich auf einer Phishing-Website zu authentifizieren.[14]

Durch die Verwendung von Device Biometrics für MFA macht WebAuthn die Sicherheit und den Komfort von WebAuthn-gestützten Flows für jeden verfügbar, dessen Endgerät und Browser die biometrische Authentifizierung unterstützten.[15]

Es reicht jedoch nicht aus, den Usern einfach nur WebAuthn-fähige Identity Flows anzubieten. Während technisch versierte User diese Option vielleicht schon sehnsüchtig erwartet haben, schenkt die Mehrheit Ihrer User den jüngsten Fortschritten bei der Authentifizierung wahrscheinlich keine besondere Beachtung. Um die Akzeptanz zu fördern, sollten Sie die WebAuthn Device Biometrics als das promoten, was sie sind – der einfachste und sicherste Authentifizierungsmechanismus – und Ressourcen bereitstellen, die den Usern zeigen, wie sie sich anmelden können (Die Mühe lohnt sich – vesprochen!).

14. Siehe WebAuthn: **Beyond the Password** [W3].
15. Keys sind eine weitere großartige WebAuthn-fähige Möglichkeit, den Zugriff zu sichern, aber ihr Einsatz ist meist auf technisch versierte User oder Unternehmensumgebungen mit relativ hohen Sicherheitsanforderungen beschränkt.

Trugschluss 8: Biometrische Authentifizierung ist datenschutzrechtlich bedenklich

Es gibt zwei große Missverständnisse in Bezug auf biometrische Verfahren und Datenschutz:

1. Bedenken der User, dass ihre persönlichen biometrischen Daten an ein Unternehmen weitergegeben werden.
2. Bedenken der Unternehmen hinsichtlich des Handlings (z. B. Speicherung, Sicherung) biometrischer Daten.

In Wahrheit sieht der WebAuthn-Standard vor, dass alle biometrischen Daten auf dem Enderät gespeichert werden (und dort verbleiben). Einige Gerätehersteller gehen sogar noch einen Schritt weiter und setzen spezielle Subsysteme ein, die die sensiblen Daten noch weiter isolieren.[16]

Das Ergebnis dieser Maßnahmen ist, dass sich im Hinblick auf biometrische Verfahren weder User noch Unternehmen Sorgen um den Datenschutz machen müssen.

Priorisieren Sie Accessibility

Wie bereits erwähnt, reduzieren barrierefreie Authentifizierungsprozesse Reibungsverluste und maximieren Ihre Marktreichweite. In der Vergangenheit war Accessibility bei Design-Prozessen oft mehr Randnotiz als grundlegende Anforderung. Eine nachhaltige Auswirkung der COVID-19-Pandemie ist jedoch das gestiegene Bewusstsein für die Bedeutung barrierefreier digitaler Experiences und deren Abhängigkeit von inklusiven Design-Prozessen. Ein Auszug aus dem State of Digital Accessibility Report 2021 von Level Access:

> *Wenn es um das Menschsein geht, haben wir drei einfache Bedürfnisse: Wir wollen verdienen, lernen und dazugehören. Können wir unseren eigenen Lebensunterhalt bestreiten, uns entwickeln, unsere Talente entfalten und Teil von etwas Größerem sein, haben wir eine gute Basis, um ein erfülltes Leben zu führen.*

16. Die Secure Enclave von Apple beispielsweise ist vom Hauptprozessor isoliert, um eine zusätzliche Sicherheitsebene zu schaffen, und so konzipiert, dass sensible Userdaten auch dann sicher sind, wenn der Kernel des Anwendungsprozessors kompromittiert wird.

> *Letztes Jahr verloren wir während der Pandemie den physischen Zugang zu vielen unserer Erwerbs-, Bildungs- und Teilhabemöglichkeiten. Technologie musste die Lücke schließen – und zwar sofort –, egal ob Unternehmen darauf vorbereitet waren oder nicht. Normalerweise dauern Paradigmenwechsel einige Generationen, aber die Umstellung auf Virtual Work geschah an einem Wochenende.*
>
> *Unternehmen befassen sich intensiv mit Digital Access für ihre Mitarbeiter und User.*

Glücklicherweise sind Sie nicht auf sich allein gestellt, wenn es um die Entwicklung barrierefreier Experiences geht. Das World Wide Web Consortium (W3) hat beispielsweise eine Website eingerichtet, die sich mit barrierefreier Authentifizierung befasst.[17] Auf der Grundlage der Web Content Accessibility Guidelines (WCAG)[18] bietet die Website Erklärungen, Links zu Ressourcen und Beispiele für barrierefreies Design, darunter:

- Unterstützung von WebAuthn, damit sich der User mit seinem Endgerät statt mit User-ID/Passwort authentifizieren kann
- Möglichkeit des Login mit einem Third-Party Provider unter Verwendung von OAuth
- mehrere Optionen für den zweiten Faktor bei der Zwei-Faktor-Authentifizierung, einschließlich einer USB-basierten Methode, bei der der User einfach einen Button betätigt, um einen Time-Based Token einzugeben

Kehrt erst einmal eine gewisse Normalität wie zu Zeiten vor der Pandemie zurück, haben wir alle die Chance, zu einer barrierefreieren Welt beizutragen. Um es mit den Worten des CEO von Level Access zu sagen:

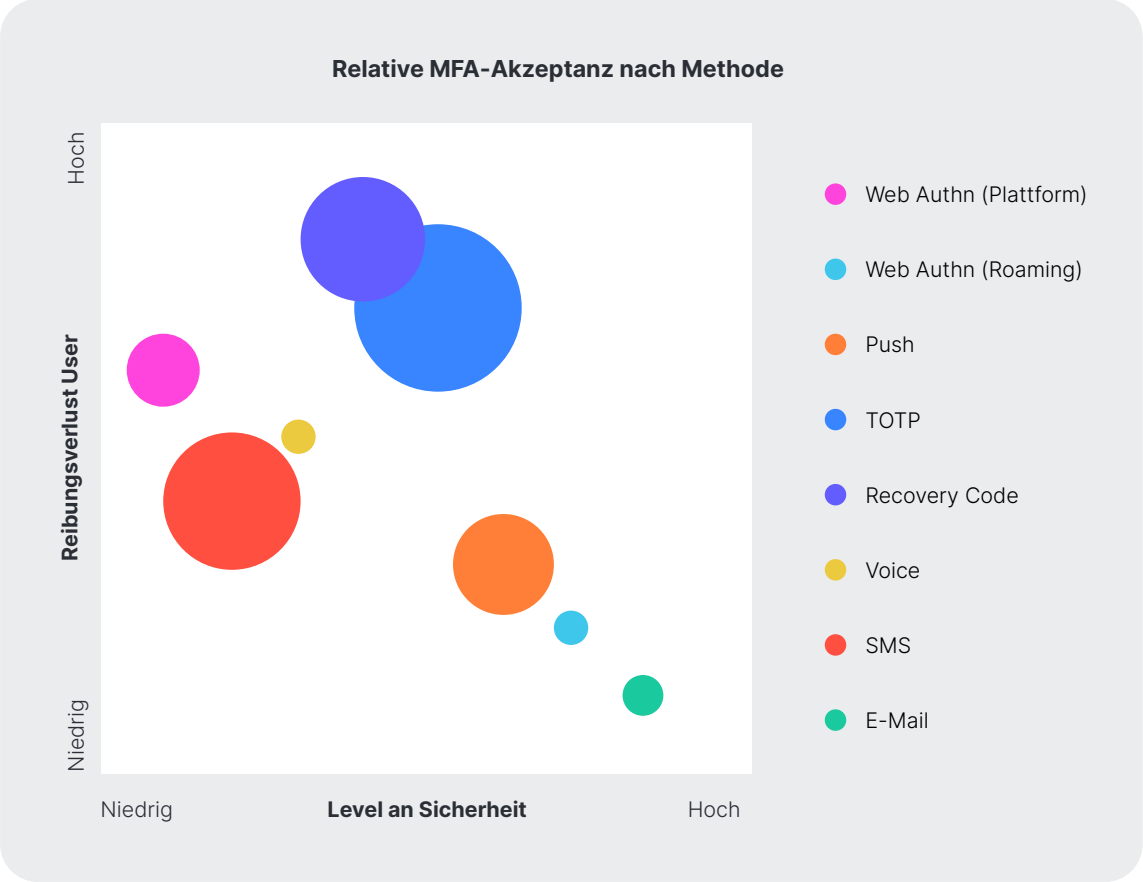
> *Hoffentlich ist es eine Mischung aus den besten Aspekten des Lebens vor 2020 und des Lebens jetzt – mit Technologie als Quelle für Einkommen, Bildung und Zugehörigkeit.*

17. Siehe **Understanding Success Criterion 3.3.7: Accessible Authentication** [W3].
18. Siehe **Web Content Accessibility Guidelines (WCAG) 2.2** [GitHub].

Nutzen Sie Progressive Enrollment

Heutzutage gibt es viele Authentifizierungsoptionen. Die Akzeptanz ist jedoch sehr unterschiedlich (Abbildung 6).

Abbildung 6: Neue MFA-Methoden, die auf WebAuthn basieren, bieten eine großartige Kombination aus hohem Level an Sicherheit und geringem Reibungsverlust für den User, aber die Akzeptanz bleibt in der Regel hinter den Möglichkeiten zurück



19

Eine Reihe von Faktoren beeinflusst die relativen Akzeptanzraten der verschiedenen Authentifizierungsmethoden, darunter:

19. Erfahren Sie mehr über MFA in **The State of Secure Identity.**

- Angebot des IAM-Providers
- Einweisung des Application Providers
- Geräteunterstützung (zum Beispiel WebAuthn)
- User Awareness
- Wahrgenommener Nutzen für den User
- Userpräferenzen

Als Application Provider müssen Sie nicht nur die modernsten Authentifizierungsmethoden unterstützen, sondern auch die weit verbreiteten, älteren Mechanismen, um der Mehrheit der User eine optimale User Experience zu bieten.

Natürlich liegt es in Ihrem besten Interesse – und dem Ihrer Kunden –, Ihre User auf die sichereren und reibungsärmeren Optionen upzugraden. Ein effektiver Weg, dies zu tun, ist die Kombination aus Incentives und Progressive Enrollment.

Ähnlich wie beim Progressive Profiling, bei dem Sie Ihre Informationsabfrage auf mehrere Interaktionen verteilen, um Vertrauen aufzubauen, **ist Progressive Enrollment ein intelligenter Weg, um die User dazu zu ermuntern, sich für einen stärkeren Authentifizierungsmechanismus zu entscheiden**. Beispielsweise können User, die Voice, SMS oder E-Mail nutzen, aufgefordert werden, auf eine Alternative wie Push-Benachrichtigungen oder biometrische Verfahren umzusteigen. Darüber hinaus können User Biometrics-fähige Endgeräte nach und nach registrieren, wenn sie sie verwenden, und haben so die Flexibilität, mehrere passwortlose Authentifizierungsoptionen zu nutzen.

Progressive Enrollment kann sogar mit einer Geräteerkennung kombiniert werden, sodass nur User mit WebAuthn-kompatiblen Endgeräten dazu ermuntert werden, sich für einen stärkeren Authentifizierungsmechanismus zu entscheiden, oder nur User der Mobile App dazu aufgefordert werden, Push-Benachrichtigungen zu aktivieren.

Trugschluss 9: Sobald man eine bestimmte Authentifizierungsmethode anbietet, ist die Arbeit getan

Einfach nur eine bestimmte Methode anzubieten, reicht nicht aus. Während technisch versierte User die neueste Option vielleicht schon sehnsüchtig erwartet haben, schenkt der Großteil Ihres Kundenstamms den jüngsten Fortschritten bei der Authentifizierung wahrscheinlich keine besondere Beachtung.

Um die Akzeptanz zu fördern, sollten Sie:

- die Registrierung so einfach wie möglich gestalten, indem Sie in nur wenigen Schritten ein Minimum an Informationen abfragen
- über die Vorteile der Registrierung aufklären (z. B. „WebAuthn Biometric Authentication ist der einfachste und sicherste Weg, Ihren Account zu schützen“) und Hinweise zur Registrierung geben
- die Option promoten (Nutzung von Progressive Enrollment) und Incentives bieten

In Kombination werden diese Techniken dazu beitragen, Ihre User auf die komfortabelsten und sichersten Authentifizierungsmethoden umzusatteln.

Fazit

Die traditionelle Authentifizierung stellt eine digitale Barriere dar, die viele bekannte Schwachstellen aufweist:

- Die meisten Login- und Account Creation Flows sind für den User mit zu viel Aufwand und Reibungsverlust verbunden.
- Die heute am weitesten verbreiteten Methoden sind für Angreifer viel zu leicht auszunutzen.
- Traditionelle Systeme sind nicht intelligent, sprich, sie behandeln legitime User und Angreifer auf dieselbe Weise.

Da unnötige Reibungsverluste bei Accounterstellung und Login mittlerweile als ein wesentliches Hindernis für Kundenakquise, Conversions und Markentreue angesehen werden, werden in den kommenden Jahren traditionelle Authentifizierungssysteme durch passwortlose und letztlich Loginless-Systeme ersetzt, die eine angenehme User Experience, Datenschutz und erhöhte Sicherheit gleichzeitig bieten.

In dieser Zukunft ohne Login:

- werden Identity-Systeme Continuous Authentication nutzen, um Zugriff zu gewähren, wenn Sie „Sie“ sind, und den Zugang zu verweigern, wenn „Sie“ nicht Sie sind.
- werden digitale Experiences sicher, mühelos und angenehm sein.
- werden digitale Beziehungen auf dieselbe Art und Weise entstehen und sich weiterentwickeln wie im wirklichen Leben – mit der Zeit.
- werden Verbraucher entscheiden, was sie mit anderen teilen, wie sie Zugriff erhalten und welchen Unternehmen sie ihre Daten anvertrauen.
- wird die Verantwortung, eine vertrauensvolle digitale Beziehung aufzubauen, bei den Unternehmen liegen.
- muss Vertrauen immer verdient, respektiert und geschützt werden.

Der Weg in eine Zukunft ohne Login führt über Passwordless, ein IAM-Paradigma, bei dem ein User ohne Eingabe eines Passworts authentifiziert wird.

Die biometrische Authentifizierung mit WebAuthn ist zwar das Paradebeispiel für passwortlose Authentifizierung, aber nicht das einzige: Auch andere Methoden bieten mehr Komfort und höhere Sicherheit als Passwörter und sind weniger geräteabhängig als moderne biometrische Verfahren.

Trugschluss 10: Es ist zu schwierig, auf Passwordless umzustellen

Zugegeben, an diesem Trugschluss ist etwas Wahres dran: CIAM ist komplex, Entwickler arbeiten bereits hart an der Maintenance und Erweiterung bestehender Lösungen, und Ressourcenknappheit kann Ihre Fähigkeit, große neue Initiativen in Angriff zu nehmen, beeinträchtigen.

Auth0 existiert jedoch genau deswegen, weil CIAM so komplex ist. Indem wir Identity-Lösungen entwickeln, die für Entwickler einfach zu bedienen sind, nehmen wir ihnen diese Last ab.
Außerdem ist die Umstellung auf Passwordless kein Alles-oder-Nichts-Vorhaben; vielmehr können schrittweise Anpassungen vorgenommen werden, und zwar sofort.

Mit einem disziplinierten Ansatz und dem richtigen IAM-Partner gibt es keinen Grund, warum Sie nicht führend im Bereich Passwordless werden können. Auth0 kann Ihrem Development Team helfen, loszulegen und schnell erste Erfolge zu erzielen.

Was Sie jetzt tun können

Während wir uns auf eine Zukunft ohne Login zubewegen, gibt es eine Menge, was Unternehmen in der Zwischenzeit tun können. Sie können die Vorteile der Loginless-Bausteine nutzen, um immer einen Schritt voraus zu sein. Hier sind einige Dinge, die Sie tun können:

- **Implementieren Sie Passwordless mit biometrischem WebAuthn**
  Ermöglicht es Usern, sich mit den Device Biometrics ihres Endgeräts zu authentifizieren – bei minimalen Reibungsverlusten und erhöhter Sicherheit.

- **Messen und benchmarken Sie Conversion-Metriken**
  Die Authentifizierung ist eine Schlüsselkomponente von Conversion-Metriken und kann deren Wirksamkeit stark beeinflussen. Diese Metriken vor und nach der Implementierung von Passwordless mit WebAuthn Biometrics zu tracken, hilft Ihnen, die Customer Journey Ihrer User zu verstehen und bietet klare Optimierungsansätze.

- **Etablieren Sie bewährte Security Practices**
  Es ist nicht mehr notwendig, Komfort zugunsten von Sicherheit zu opfern. Bewährte Security Practices wie Adaptive MFA, Bot Detection und Step-Up Authentication sorgen für ein hohes Maß an Sicherheit und minimieren gleichzeitig die Beeinträchtigungen für User.

- **Nutzen Sie Progressive Enrollment**
  Die beste Security ist die, die tatsächlich genutzt wird. Wenn Sie Ihre User dazu ermuntern, sich mittels Progressive Enrollment für einen stärkeren Authentifizierungsmechanismus zu entscheiden, schützen Sie sie und deren persönliche Daten und stärken gleichzeitig die Security Ihres Unternehmens als Ganzes.

- **Denken Sie an Accessibility**
  Während Reibungsverluste für viele User eine Unannehmlichkeit darstellen, können sie für andere eine große Herausforderung sein. Abgesehen davon, dass Accessibility als Schlüsselvariable bei der Entwicklung von Identity-Systemen zu berücksichtigen einfach das Richtige ist, maximiert die Entwicklung von Anwendungen, die von allen genutzt werden können, auch Ihre Marktreichweite.

Wenn Sie dieser Roadmap folgen, können Unternehmen Conversion Rates und Umsatz steigern, indem sie Reibungsverluste reduzieren, ihre Marktreichweite vergrößern und die Accessibility verbessern – und das alles bei erhöhter Sicherheit.

Erfahren Sie mehr über Identity Management mit Auth0

Identity ist für die Nutzung von Online-Anwendungen von entscheidender Bedeutung und wird mit der zunehmenden Verbreitung des Zero-Trust-Paradigmas noch wichtiger werden.

Identity ist aber auch komplex – selbst erfahrene Profis empfinden die Entwicklung effektiver und effizienter Implementierungen als Herausforderung.

Auth0 nimmt Ihnen das Identity and Access Management ab, sodass Sie sich auf Ihr Kerngeschäft fokussieren können.

Auth0 ist eine einfach zu implementierende, flexible und sichere Authentifizierungs- und Autorisierungs-Plattform. Aufbauend auf einer Reihe von kombinierbaren Bausteinen, die über APIs und Protokolle zugänglich sind, bietet die Auth0 Identity Platform mehrere Lösungen für jeden Identity Use Case ohne Kompromisse bei Komfort, Datenschutz oder Sicherheit.

Erfahren Sie mehr unter **auth0.com/identity-platform.**

Auth0 bietet eine Plattform zur Authentifizierung, Autorisierung und Sicherung des Zugriffs für Anwendungen, Endgeräte und User. Security- und Development-Teams vertrauen beim Thema Identity auf die Einfachheit, Flexibilität und das Know-how von Auth0. Bei mehr als 4,5 Milliarden Login-Vorgängen jeden Monat schützt Auth0 Identities, damit globale Unternehmen innovativ sein und ihren Kunden weltweit vertrauenswürdige, erstklassige digitale Experience bieten können.

Weitere Informationen finden Sie unter **https://auth0.com** oder folgen Sie **@auth0** auf Twitter.