Report

Customer Identity Trends Report 2025

Stärkung des Kundenvertrauens im Zeitalter von KI

Inhalt

Customer Identity im Fadenkreuz

Stärkung des Kundenvertrauens im Zeitalter von KI

Willkommen beim Customer Identity Trends Report 2025.

Die meisten Unternehmen – ob groß oder klein, Business-to-Consumer (B2C) oder Business-to-Business (B2B) – konkurrieren heute wirklich weltweit miteinander. Deshalb war es nie so wichtig, dass sie ihre Kunden verstehen und ansprechen.

Genau deshalb spielt die Kundenidentitäts- und Zugriffsverwaltung (Customer Identity and Access Management, CIAM) heute eine zentrale Rolle.

CIAM ermöglicht es Ihren Kunden, sich für Ihre digitalen Angebote *zu registrieren* und *anzumelden*. Es handelt sich also um einen sehr exponierten und häufig genutzten Berührungspunkt, der bei der Vertrauensbildung, beim Einholen des Benutzereinverständnisses und beim Erfassen der für Ihre Wachstums- und Umsatzziele so wichtigen First- und Zero-Party-Daten eine wichtige Rolle spielt. Deshalb hat die Modernisierung im Bereich CIAM – und Customer Identity allgemein – für viele Unternehmen höchste Priorität.

CIAM ist aber auch Ziel vieler Angreifer, die Ihre Login-Box als Zugang zu Informationen, Berechtigungen sowie Vorteilen betrachten, die eigentlich Account-Inhabern vorbehalten sind. Mit seinen wichtigen Authentifizierungs- und Autorisierungsfunktionen stärkt CIAM das Vertrauen, weil es die Daten der Kunden und die Unternehmen vor den Folgen von Sicherheitsverletzungen schützt. Dieser wichtige Beitrag zu einer starken Gesamtsicherheit rückt CIAM in den Mittelpunkt der Aufmerksamkeit von CISOs, CIOs und Compliance-Beauftragten.

Dank der rasanten Entwicklung und Bereitstellung GenAI-gestützter Agenten kann CIAM für Unternehmen zudem einen einzigartigen Mehrwert bereitstellen – als Anwendung für die Steuerung und Sicherung des Zugriffsumfangs von KI-Agenten. Kunden müssen wissen, dass sie KI-Agenten ihre personenbezogenen Daten anvertrauen können, da andernfalls das transformative Potenzial dieser Agenten nicht ausgeschöpft wird. Selbst wenn CIAM für CTOs und andere Technologieverantwortliche bislang noch keine große Bedeutung hatte, erfordern die neuen KI-bezogenen Anwendungen spätestens jetzt ein Umdenken.

Dieser Bericht basiert auf einer weltweiten Umfrage unter 6.750 Verbrauchern und auf Telemetriedaten der Auth0 Platform. Er untersucht zahlreiche Themen, die mit Vertrauen zu tun haben – einschließlich der Fragen, wie es in einer sich rasant verändernden digitalen Landschaft aufgebaut und gepflegt werden kann.

- Im ersten Teil werden die **Customer Experiences und Einstellungen der Kunden** untersucht, vor allem in Bezug auf Identity-Management, Authentifizierungsmethoden und Customer Journeys.
- Thema des zweiten Teils sind **Customer Identity-Bedrohungen**. Er demonstriert auf ernüchternde Weise, warum starke Sicherheitsmaßnahmen wichtig sind.
- Der dritten Teil dreht sich um das Thema **KI trifft auf Customer Identity** und liefert wichtige Erkenntnisse in Bezug auf Faktoren, die die Einführung von KI-Agenten in Unternehmen beeinflussen können.

Doch bevor wir ins Detail gehen, stellen wir einige wichtige Erkenntnisse vor.

Wichtige Erkenntnisse

Customer Experiences und Einstellungen der Kunden

Vertrauen und Betrug sind für Kunden die wichtigsten Themen

Sicherheit und Vertrauenswürdigkeit sind wichtiger als Qualität und Mehrwert
Die Reputation und Vertrauenswürdigkeit des Unternehmens (74 % der Befragten) und die Sicherheitsmaßnahmen des Unternehmens (72 %) spielen bei der Entscheidung für oder gegen einen Account bei einem Service Provider eine wichtigere Rolle als die allgemeine Qualität und der Mehrwert der Produkte oder Dienstleistungen des Unternehmens.

Identity-Betrug ist ein wichtiges Thema
Insgesamt gaben 64 % aller Befragten an, dass sie sich Sorgen wegen Identity-Betrug machen, während nur 10 % wenig oder gar keine Bedenken äußerten. Obwohl die konkreten Zahlen je nach Befragtenkohorte variierten, war die Grundstimmung an sich gleich.

Lange Registrierungs- oder Login-Formulare frustrieren Benutzer
Das Ausfüllen langer Registrierungs- oder Login-Formulare wurde am häufigsten als Ursache für Registrierungs- oder Login-Frust bei den Benutzern genannt (62 %) – weit vor der Eingabe privater oder vertraulicher Informationen (52 %).

Reibungspunkte bei Registrierungs- und Login-Experiences kosten Konversionen
Fast ein Viertel der Befragten gab an, dass sie einen Online-Kauf bei Problemen mit dem Registrierungs- oder Login-Prozess *immer* (6 %) oder *häufig* (17 %) abbrechen, während weitere 40 % den Prozess *manchmal* abbrechen. Das deutet auf ein weitverbreitetes Problem hin.

Passwörter bleiben allgegenwärtig, ihre Mehrfachverwendung erhöht aber das Risiko
Während die Befragten Passwörter als einfachste Authentifizierungsmethode ansehen, geben 68 % der Benutzer an, sie für mehrere Accounts zu verwenden – hauptsächlich weil es schwierig ist, sich individuelle Passwörter zu merken. Diese schlechte Passworthygiene erhöht das Risiko der Kunden und Unternehmen für Identity-basierte Brute-Force-Angriffe.

Wichtige Erkenntnisse

Customer Identity-Bedrohungen

Die wachsenden Risiken in einer zunehmend digitalen Welt

Betrügerische Registrierungsversuche sind an der Tagesordnung
2024 lag der Median der Registrierungsversuche, die die Kriterien eines Angriffs erfüllt haben, auf der gesamten Auth0 Platform bei 46,1 %. Dabei ist das Ausmaß dieser Brute-Force-Angriffe wirklich erschreckend: Während eines mehrmonatigen Angriffs im Einzelhandels- und E-Commerce-Sektor (der den höchsten Anteil an Angriffsereignissen unter den Top-10-Branchen auf der Auth0 Platform aufwies) überstieg die Anzahl der Registrierungsangriffe die der legitimen Registrierungen um das 120-fache.

Account-Hacking stellt eine ständige Bedrohung dar
Einige Account-Hacking-Versuche richten sich zwar auch gegen Einzelpersonen, doch in den meisten Fällen nehmen Brute-Force-Angriffstechniken die passwortbasierte Authentifizierung ins Visier, um so viele Konten wie möglich zu kompromittieren. 2024 lag der Median der Login-Versuche mit eindeutig schädlichen Verhaltensweisen auf der gesamten Auth0 Platform bei 16,9 %. Auch hier führte der Einzelhandels- und E-Commerce-Sektor die Rangliste mit 22,2 % aller Login-Versuche an.

MFA-Missbrauch ist nach wie vor verbreitet, aber möglicherweise rückläufig
2024 lag der Median der als schädlich erkannten MFA-Ereignisse auf der gesamten Auth0 Platform bei 7,3 %. Mit diesem einstelligen Wert setzt sich der Abwärtstrend fort, der erstmals im Okta The State of Secure Identity Report 2023 festgestellt wurde. Während ein winziger Teil dieser MFA-Ereignisse auf legitime MFA-Fehler (z. B. ein echter Benutzer beantwortet eine MFA-Sicherheitsabfrage mehrfach falsch) und ein wahrscheinlich etwas größerer Teil auf Angreifer zurückgeht, die mit MFA abgewehrt wurden, lässt sich die Mehrheit dieser Ereignisse mit ziemlicher Sicherheit mit MFA Fatigue-Angriffen und SMS-Pumping (Toll Fraud) in Verbindung bringen.

Wichtige Erkenntnisse

KI trifft auf Customer Identity

Menschen bevorzugen Menschen – zumindest bisher

Benutzer bevorzugen generell die Interaktion mit Menschen statt KI-Agenten

Unter allen Umfrageteilnehmern möchten 70 % am liebsten mit Menschen kommunizieren, während 16 % lieber mit einem KI-Agenten interagieren. Tatsächlich äußerte jede in dieser Studie untersuchte Kohorte (Befragte der gleichen demografischen Generation, Aufgeschlossenheit gegenüber neuen Technologien und Land des Wohnsitzes) diese Präferenz. Benutzer, die menschliche Kontakte bevorzugen, sagen vor allem, dass Menschen ihre Bedürfnisse verstehen, während Benutzer, die KI-Agenten bevorzugen, auf schnellere Lösungen, den Wegfall der menschlichen Interaktion und den Glauben an den Fortschritt verweisen.

Benutzer verwenden KI-Agenten eher für regelbasierte Aufgaben und solche, die als lästig empfunden werden

Benutzer verwenden KI-Agenten am ehesten für objektivere Aufgaben (im Gegensatz zu Aufgaben, die subjektive Überlegungen erfordern) und solche, die als lästig empfunden werden. Am anderen Ende des Spektrums zeigten die Benutzer vergleichsweise wenig Interesse daran, dass KI-Agenten Aufgaben aus dem persönlichen Verantwortungsbereich übernehmen.

Widerstand der Benutzer beruht größtenteils auf mangelndem Vertrauen

Kunden, die keine KI-Agenten nutzen, begründen dies meist mit *„Ich vertraue meine persönlichen Daten keinem KI-Agenten an“*. Generell gaben 60 % der Befragten an, dass sie über die Auswirkungen von KI auf den Datenschutz und die Sicherheit ihrer digitalen Identitäten sehr besorgt oder besorgt sind. Diese Bedenken wurden von allen in dieser Studie untersuchten Kohorten geäußert.

Menschliche Kontrolle, Transparenz und ethische Richtlinien würden das Vertrauen stärken

Die Kunden wünschen sich, dass der Mensch weiterhin eine Rolle spielt: 38 % der Befragten gaben an, dass eine menschliche Kontrolle zur Prüfung oder Bestätigung von Entscheidungen des KI-Agenten das Vertrauen erhöhen würde. Dies ist jedoch nicht immer praktikabel. Erfreulicherweise gaben die Benutzer an, dass auch Transparenz, ethisches Verhalten und Rechenschaftspflicht vertrauensbildend wirken könnten.

Customer Experiences und Einstellungen der Kunden

Umfragebasierte demografische Einblicke in Vertrauen, digitale Identitäten und Customer Journeys

Was ist den Kunden heute *wirklich* wichtig?

Für viele Unternehmen ist die Rate der erstellten Benutzer-Accounts ein wichtiger Leistungsindikator (KPI) – als Maß für den Erfolg laufender Bemühungen, aber auch als wichtige Metrik.

Produktverantwortliche und Marketingexperten können jede erfolgreiche Account-Erstellung als relativ einfache Aktivität betrachten, die ihnen signalisiert, dass ein Benutzer einen ausreichenden Mehrwert in Ihrem Angebot sieht und bereit ist, seine Beziehung zu Ihrem Unternehmen zu erweitern.

Sie müssen lediglich einige grundlegende Informationen zur Verfügung stellen *und fertig*.

Aber ist die Entscheidung, einen Account einzurichten, aus Sicht des Benutzers wirklich so einfach?

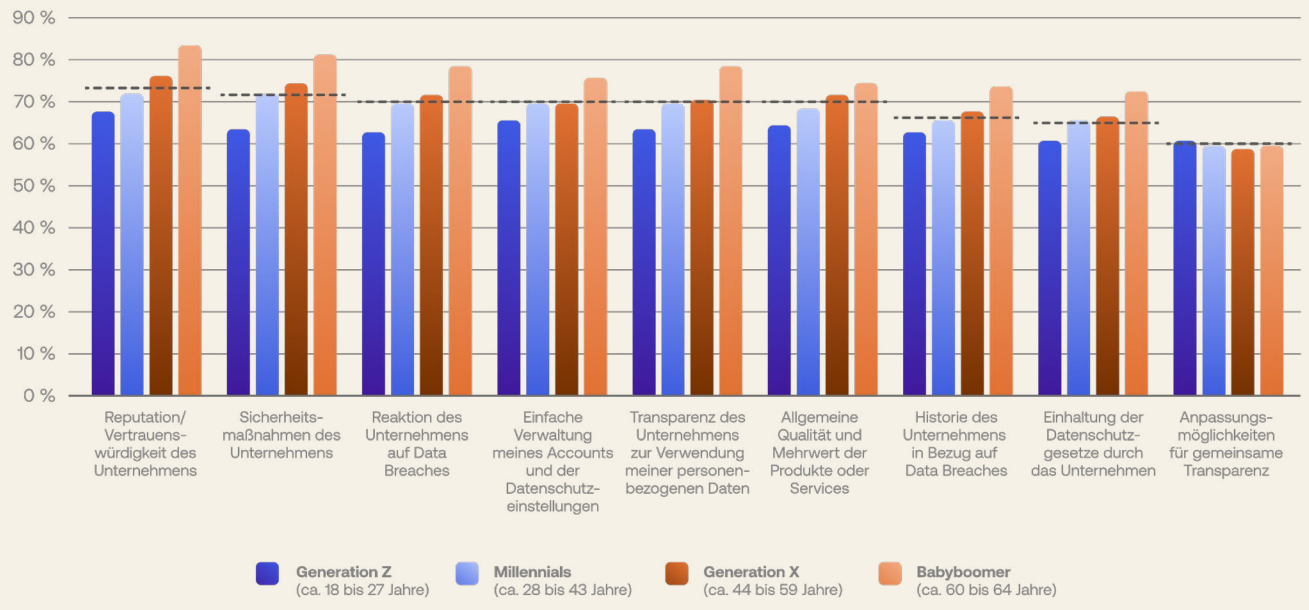
Registrierungs-entscheidungen beginnen mit Vertrauen und Sicherheit

Wenn sich Benutzer über die Website oder Anwendung eines Unternehmens registrieren,

- signalisieren sie ihre Absicht, eine Beziehung einzugehen oder fortzuführen,
- lösen sie die Erstellung einer maßgebenden Customer Identity (Kundenidentität) aus und
- stellen sie potenziell Zero- und First-Party-Daten bereit – beide werden wichtige Alternativen zu Third-Party-Cookies.

Aus diesem Grund orchestrieren Marketingexperten, Produktverantwortliche und User Experience-Designer ganze Kampagnen und optimieren die Benutzeroberflächen, um die Benutzer zur Erstellung eines Accounts zu bewegen.

Sicherheit und Vertrauen erleichtern Registrierungsentscheidungen



Einfluss von Faktoren auf die Registrierungsentscheidung, nach Generation der Befragten (Summe aus „Sehr wichtig“ und „Wichtig“)

„Wie wichtig sind die folgenden Faktoren für die Entscheidung, einen privaten Online-Account bei einem Unternehmen einzurichten?“

Der gebotene Mehrwert spielt bei der Entscheidung der Benutzer für die Erstellung eines privaten Accounts nicht die wichtigste Rolle

Insgesamt bezeichneten die Befragten häufiger die Reputation und Vertrauenswürdigkeit sowie die Sicherheitsmaßnahmen des Unternehmens als *sehr wichtig* oder *wichtig* als die allgemeine Qualität und den Mehrwert der Produkte oder Dienstleistungen des Unternehmens.

Bei ähnlichen Angeboten gewinnt die Marke mit den stärkeren Sicherheitsmaßnahmen und Datenschutzkontrollen

Kunden machen sich heute Sorgen wegen Identity-Betrug, d. h. sie legen Wert auf Sicherheit, achten auf Schlagzeilen zu Sicherheitsverletzungen und möchten die Kontrolle über ihre eigenen Daten behalten.

Ältere oder technikaffinere Benutzer legen sogar noch mehr Wert auf diese Faktoren

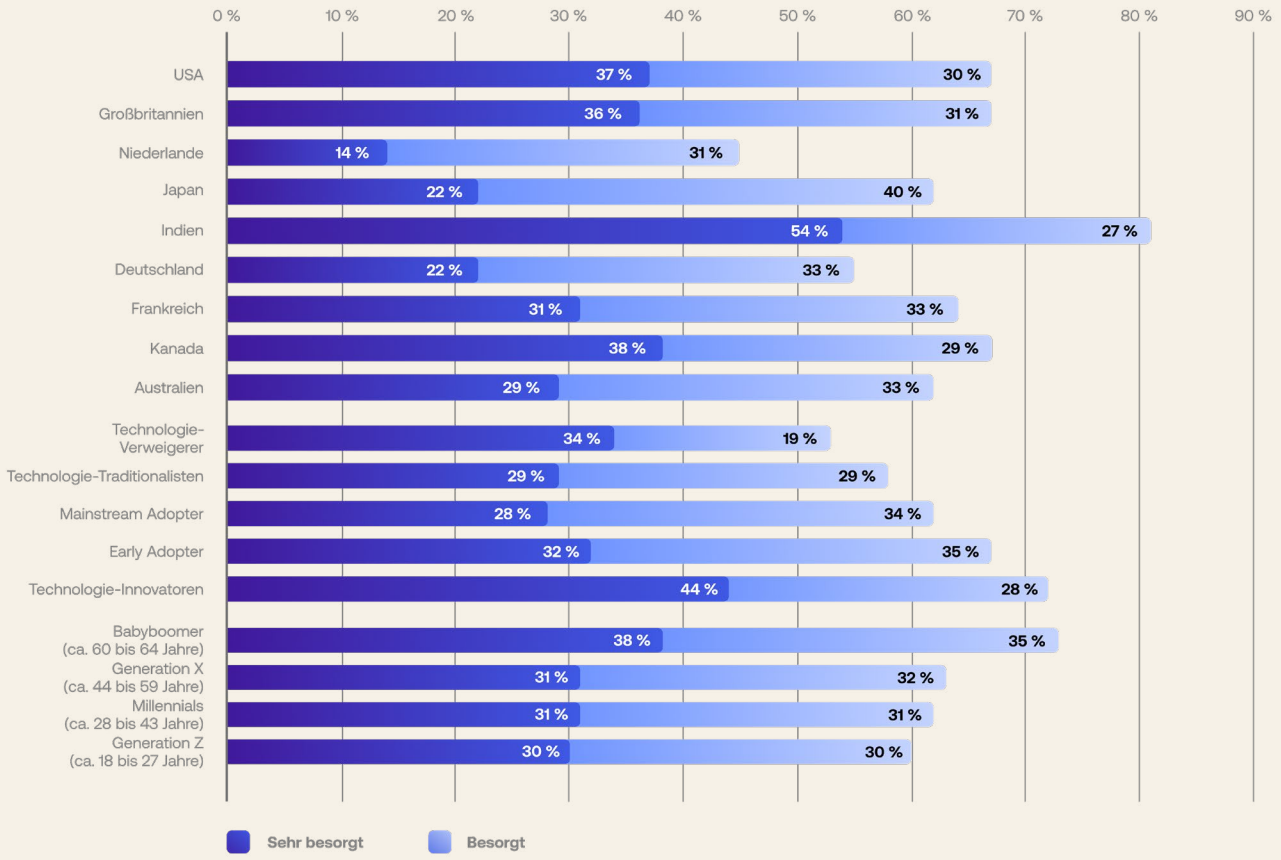
Je höher das Alter der Befragten oder ihre Affinität zu neuen Technologien, desto wichtiger sind ihnen diese Faktoren – von der Vertrauenswürdigkeit bis zur Transparenz – bei der Einrichtung eines privaten Accounts.

Kunden machen sich aus gutem Grund Sorgen wegen Identity-Betrug

Durch die digitale Transformation steht heute der Komfort im Fokus. Leider werden dieselben Technologien, die Effizienz, Skalierbarkeit und Interkonnektivität ermöglichen, regelmäßig von böswilligen Akteuren missbraucht.

Heutzutage sind Identity-Betrug (die nicht autorisierte Verwendung der Daten einer anderen Person) und sein typischer Vorläufer, der Identity-Diebstahl (die nicht autorisierte Aneignung personenbezogener Daten) leider an der Tagesordnung. Beides wird zum Teil durch laxe Sicherheits- und Datenschutzkontrollen begünstigt, die zu Data Breaches führen können und es Kriminellen leicht machen, sich als andere Benutzer auszugeben.

Alle Benutzer machen sich Sorgen wegen Identity-Betrug



Sorgen wegen Identity-Betrug, alle Kohorten

„Wie besorgt sind Sie wegen Identity-Betrug?“

Die große Mehrheit der Benutzer macht sich Sorgen wegen Identity-Betrug

32 % aller befragten Benutzer gaben an, dass sie in Bezug auf Identity-Betrug *sehr besorgt* sind, weitere 32 % sind *besorgt*. Unter Berücksichtigung der 27 %, die eher besorgt sind, bleiben nur 10 % der Befragten, die wenig oder gar nicht besorgt sind.

Sorgen wegen Identity-Betrug sind allgegenwärtig

Wie die Abbildung zeigt, macht sich jede demografische Gruppe Sorgen wegen Identity-Betrug. Die Befragten aus den Niederlanden äußerten sich am wenigsten besorgt – doch selbst hier sind 45 % *besorgt* oder *sehr besorgt*. Die größten Sorgen machen sich die Benutzer in Indien. Dort sind 54 % *sehr besorgt* und weitere 27 % *besorgt*.

Technologie-Innovatoren und Babyboomer machen sich ebenfalls viele Sorgen

Unter den Generationen äußern die Babyboomer deutlich mehr Bedenken als die anderen Kohorten. Die Unterschiede sind nicht so groß, wenn wir nach Aufgeschlossenheit gegenüber neuen Technologien gruppieren, aber die Technologie-Innovatoren stechen immer noch hervor – vor allem aufgrund der 44 % (zweithöchster Anteil aller Kohorten), die *sehr besorgt* sind.

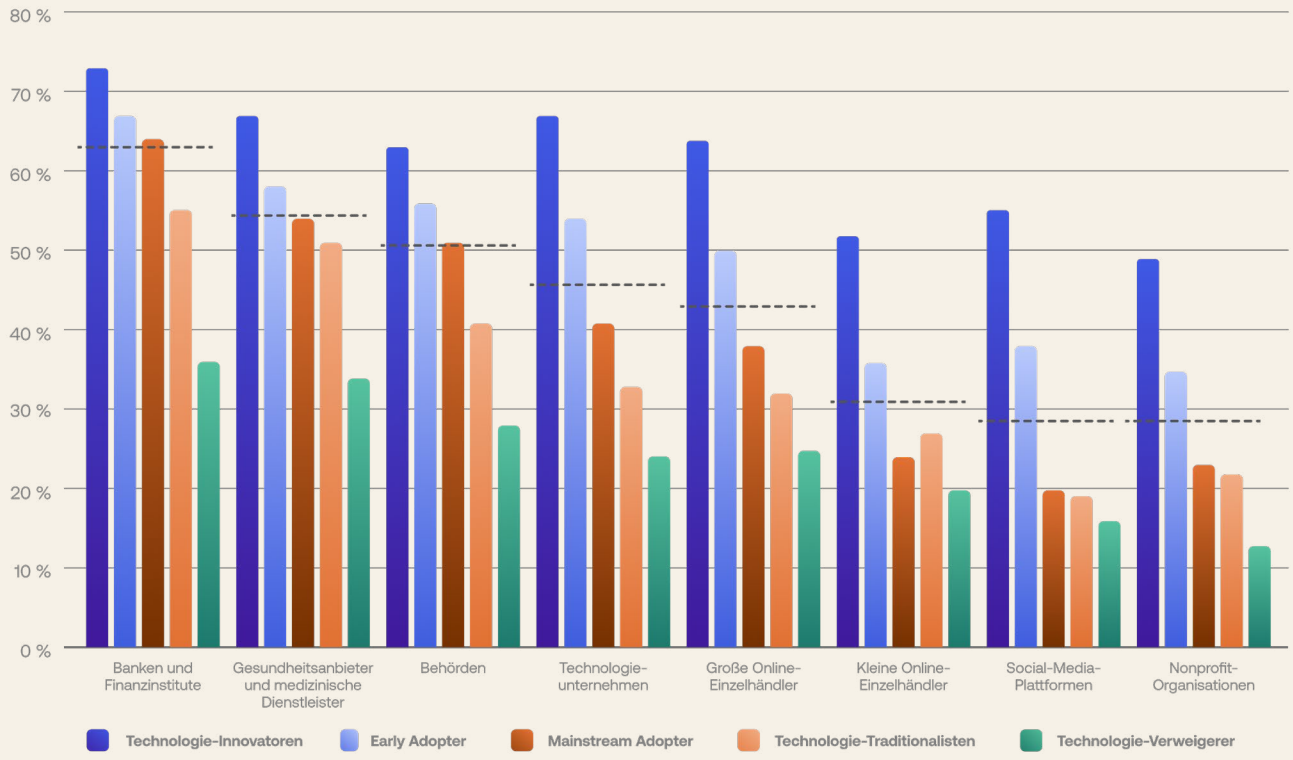
Das Vertrauen in die Daten-sicherheit hängt vom Anbieter ab

Ergebnissen der Forrester Consumer Trust Imperative Survey 2023 zufolge ist das Vertrauen der Verbraucher in ein Unternehmen ausschlaggebend für umsatzgenerierende Verhaltensweisen – einschließlich der Wahrscheinlichkeit eines erneuten Kaufs, der Bevorzugung einer Marke gegenüber Mitbewerbern und der Bereitschaft zur Weitergabe personenbezogener Daten.

Laut der PWC Trust Survey 2024 glaubt die überwiegende Mehrheit (90 %) der Führungskräfte, dass die Kunden ihrem Unternehmen vertrauen. In Wirklichkeit sind es aber nur 30 % der Verbraucher – eine krasse Fehleinschätzung.

Da Identity-Betrug mittlerweile eines der größten Probleme ist, achten die Kunden genau darauf, wie die Unternehmen und Organisationen ihre personenbezogenen Daten schützen.

Welchen Unternehmen und Organisationen vertrauen Benutzer ihre Daten an



Vertrauen in verschiedene Unternehmen und Organisationen, nach Aufgeschlossenheit der Befragten gegenüber neuen Technologien (Summe aus „Stark“ und „Eher stark“)

„Wie sehr vertrauen Sie den folgenden Unternehmen und Organisationen beim Schutz Ihrer personenbezogenen Daten?“

Hinweis: Die gestrichelten Linien zeigen den Mittelwert aller Befragten.

Das Vertrauen der Kunden variiert stark nach Art der Institution

Am oberen Ende der Skala vertrauen 63 % der Befragten den Banken und Finanzinstituten bei der Sicherung ihrer personenbezogenen Daten. Am unteren Ende sagen nur 29 % der Befragten dasselbe über Social-Media-Plattformen und Nonprofit-Organisationen.

Technikaffine Benutzer vertrauen Unternehmen und Organisationen mehr

Technologie-Innovatoren haben besonders viel Vertrauen – über alle Unternehmen und Organisationen hinweg im Durchschnitt 18 Prozentpunkte mehr als die Gesamtheit der Befragten. Technologie-Verweigerer sind ziemlich genau das Gegenteil und äußern im Durchschnitt 19 Prozentpunkte weniger Vertrauen als die Gesamtheit aller Befragten.

Banken und Finanzinstitute befinden sich in einer beneidenswerten Lage

Jede Generationenkohorte vertraut Banken und Finanzinstituten am meisten. Bei allen anderen Arten von Unternehmen und Organisationen haben jüngere Generationen mehr Vertrauen. Besonders auffällig ist diese Diskrepanz bei kleinen Online-Einzelhändlern und Social-Media-Plattformen.

Langwierige Registrierungen können Sie Kunden kosten

Die Customer Experience steht oft in einem gewissen Spannungsverhältnis mit Sicherheitskontrollen und dem Wunsch des Unternehmens, mehr über seine Benutzer zu erfahren.

So sind zum Beispiel strikte Kontrollen erforderlich, um mit Sicherheit behaupten zu können, dass jeder neue Account einem echten Benutzer (und nicht einem Bot) gehört und dass jeder Login vom tatsächlichen Besitzer des Accounts (und nicht von einem Bot) durchgeführt wird.

Ebenso sind Unternehmen bestrebt, Informationen zu sammeln, die sie für die Bereitstellung eines besseren Gesamtservices benötigen – einschließlich der starken Personalisierung, die viele Benutzer heute einfach erwarten.

Dabei müssen sie jedoch darauf achten, dass Schutzmaßnahmen und Informationsabfragen die User Experience nicht zu sehr beeinträchtigen. Besser noch: Unternehmen können Lösungen implementieren, die die Customer Experience verbessern und den geschäftlichen Anforderungen gerecht werden. Dazu gehören zum Beispiel die progressive Profilerstellung und Passkeys.

Lange Formulare sind die frustrierendste Hürde bei Registrierungen oder Logins
Lange Registrierungs- oder Login-Formulare werden von 62 % der Befragten als häufigstes Ärgernis bei Registrierungen oder Logins genannt.

Die Ursachen für Verärgerung variieren je nach Herkunftsland
Die Befragten aus Japan empfinden die meisten dieser Probleme als besonders frustrierend – und ärgern sich besonders über komplizierte Passwortanforderungen und Account-Verifizierungen.

Die Gefühlslage ist generationenübergreifend recht einheitlich
Im Vergleich zu den anderen Kohorten sind Babyboomer häufiger von langen Formularen und weniger von Verifizierungen frustriert – aber abgesehen von diesen Unterschieden herrscht zwischen den Generationen Einigkeit.

Die größten Ursachen für Verärgerung bei Registrierungen und Logins

Faktoren für Benutzerfrust bei Registrierungen oder Logins, nach Land des Wohnsitzes der Befragten (Summe der Antworten „Sehr frustrierend“ und „Frustrierend“)

„Wie beurteilen Sie die folgenden Probleme bei Registrierungen oder Logins für einen privaten Account?“

Hinweis: Die gestrichelten Linien zeigen den Mittelwert aller Befragten.

Customer Identity und Customer Journeys

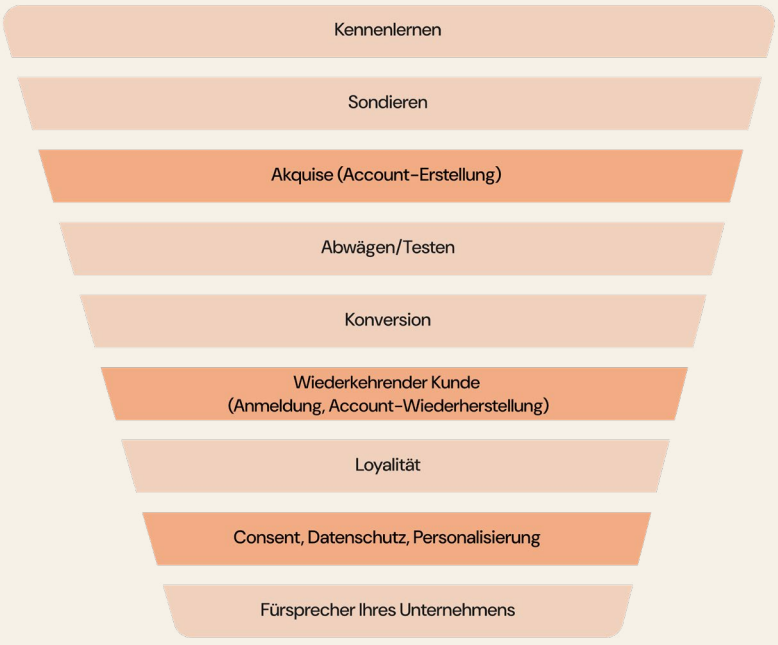
Unternehmen müssen ihren Kunden heute die Möglichkeit bieten, von jedem Endgerät aus jederzeit auf gewünschte Anwendungen und Services zuzugreifen.

Im Customer-Identity-Kontext umfassen diese Interaktionen beispielsweise (aber nicht ausschließlich):

- Registrierung bei Ihrem Service bzw. Registrierung eines Accounts bei Ihrem Unternehmen
- Anmeldung bei einem bestehenden Account
- Gewährung der Zustimmung zum Erfassen und Nutzen ihrer Daten
- Aktualisierung von Informationen und Einstellungen
- Abschluss einer Transaktion
- Zurücksetzen des Passworts

Die Optimierung dieser Abläufe und User Experiences – durch einfachere und schnellere Authentifizierungen, voraub ausgefüllte Formulare, MFA-Sicherheitsabfragen nur bei privilegiertem Zugriff, Transparenz zu Datenerfassung, Datenschutz und Datenverwendung, usw. – kann sich direkt auf Ihre Gesamtkonversionsraten auswirken.

Identity-Flows sind grundlegende Elemente der Customer Journey und haben dadurch starken Einfluss auf die Konversionsraten.

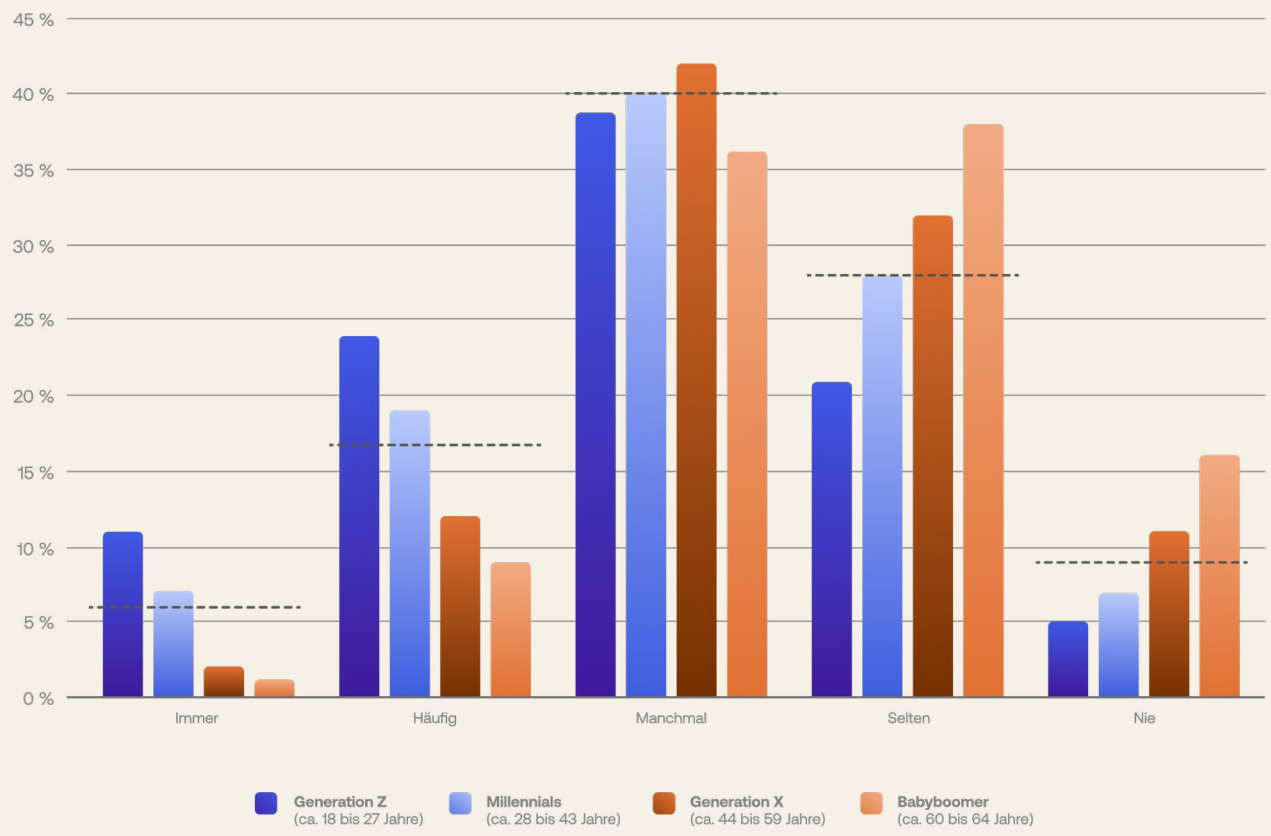


Kaufabbruch: Reibungspunkte bei der Registrierung sind für Kunden ein K.O.-Kriterium

In der digitalen Welt bezeichnet *Reibung* alles, was die Interaktionen einer Person mit Ihrem Service ausbremst oder beeinträchtigt.

Eine gewisse Zahl an Reibungspunkten ist notwendig, um Vertrauen aufzubauen und Sicherheitskontrollen zu implementieren, die Kunden und Unternehmen schützen. Unnötige Reibungspunkte führen aber zu schlechten Customer Experiences, senken die Konversionsraten und können Ihre Bemühungen untergraben, die erforderlichen Daten für 360-Grad-Profile zusammenzutragen.

Registrierungs- und Login-Probleme vertreiben Kunden



Häufigkeit der Kaufabbrüche aufgrund von Problemen bei Registrierung und Login, nach Generation der Umfrageteilnehmer

„Wie oft brechen Sie einen Online-Kauf wegen Problemen beim Registrierungs- oder Login-Prozess ab?“

Hinweis: Die gestrichelten Linien zeigen den Mittelwert aller Befragten.

Reibungspunkte bei Registrierung und Login sind die Feinde des Erfolgs

Fast ein Viertel der Befragten gab an, dass sie einen Online-Kauf bei Problemen mit dem Registrierungs- oder Login-Prozess *immer* (6 %) oder *häufig* (17 %) abbrechen, während weitere 40 % den Prozess *manchmal* abbrechen. Das deutet auf ein weitverbreitetes Problem hin.

Generation Z und Millennials reagieren besonders empfindlich auf Reibungspunkte bei Registrierung und Login

Jüngere Kohorten – die von Unternehmen in der Regel sehr geschätzt werden – berichten überdurchschnittlich oft von Kaufabbrüchen. Von den Generation Z-Befragten brechen 11 % einen Online-Kauf *immer* ab, wenn sie bei Registrierung oder Login mit Reibungspunkten konfrontiert werden, 26 % brechen *häufig* ab.

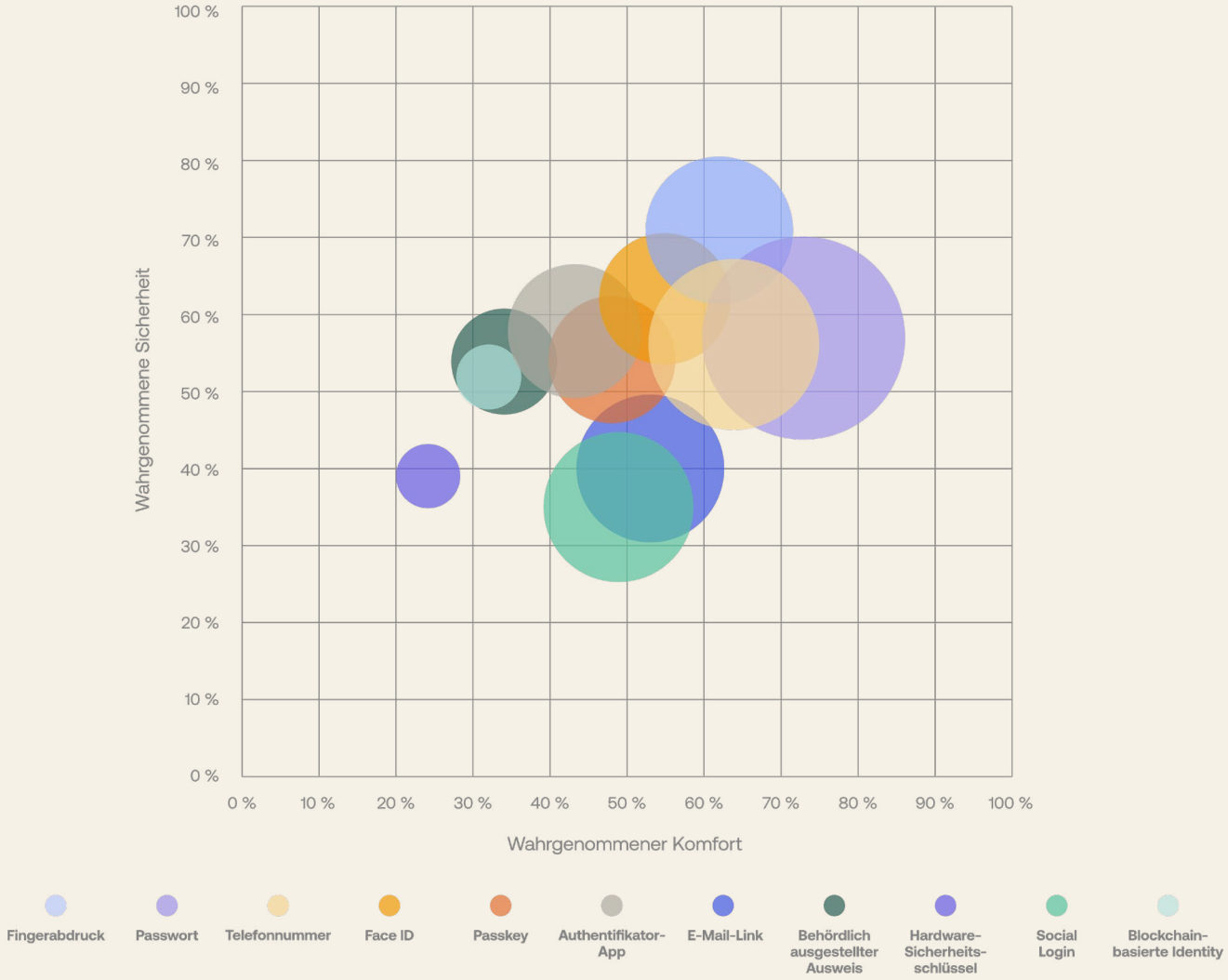
Technologie-Innovatoren zeigen von allen die geringste Toleranz

Satte 43 % der Technologie-Innovatoren brechen Online-Käufe *immer* (17 %) oder *häufig* (26 %) ab, wenn sie bei Registrierung oder Login mit Reibungspunkten konfrontiert werden – das ist der höchste Wert aller untersuchten Gruppen. Die Mitglieder dieser Gruppe wissen ganz genau, wie eine gute User Experience aussieht und erwarten genau diese von einer Marke.

Wie Komfort und Vertrautheit die Login-Gewohnheiten prägen

Für Login-Gewohnheiten gilt das Sprichwort „Schuster, bleib bei deinem Leisten“. Es besteht ein eindeutiger und starker Zusammenhang zwischen der Häufigkeit, mit der Benutzer eine Authentifizierungsmethode verwenden, und dem Komfort, den diese Methode ihrer Meinung nach bietet.
Der Korrelationskoeffizient[1] zwischen der gemeldeten Nutzung und dem wahrgenommenen Komfort beträgt 0,92 (von 1). Dies deutet auf eine enge Beziehung zwischen beiden Werten hin.

Komfort und Vertrautheit bestimmen Login-Gewohnheiten



Wahrnehmung und Nutzung von Authentifizierungsmethoden, alle Befragten

Hinweis: Dieses Diagramm kombiniert die Antworten auf drei Fragen zur Nutzung (Kreisgröße), zum wahrgenommenen Komfort (horizontale Achse, Summe der Antworten „Sehr komfortabel“ und „Komfortabel“) und zur wahrgenommenen Sicherheit (vertikale Achse, Summe der Antworten „Sehr sicher“ und „Sicher“) verschiedener Authentifizierungsmethoden.

[1] Ein numerisches Maß für die statistische Beziehung zwischen zwei Variablen, das von -1 (starke negative Korrelation) bis +1 (starke positive Korrelation) reicht. 0 bedeutet keine Korrelation.

Wir glauben, dass die starke Korrelation wahrscheinlich in beiden Richtungen besteht:

- Wenn man eine Methode häufiger nutzt, fühlt sie sich vertrauter an – und eine größere Vertrautheit beeinflusst die Meinung hinsichtlich des Komforts.
- Methoden, die als komfortabler empfunden werden, werden häufiger genutzt.

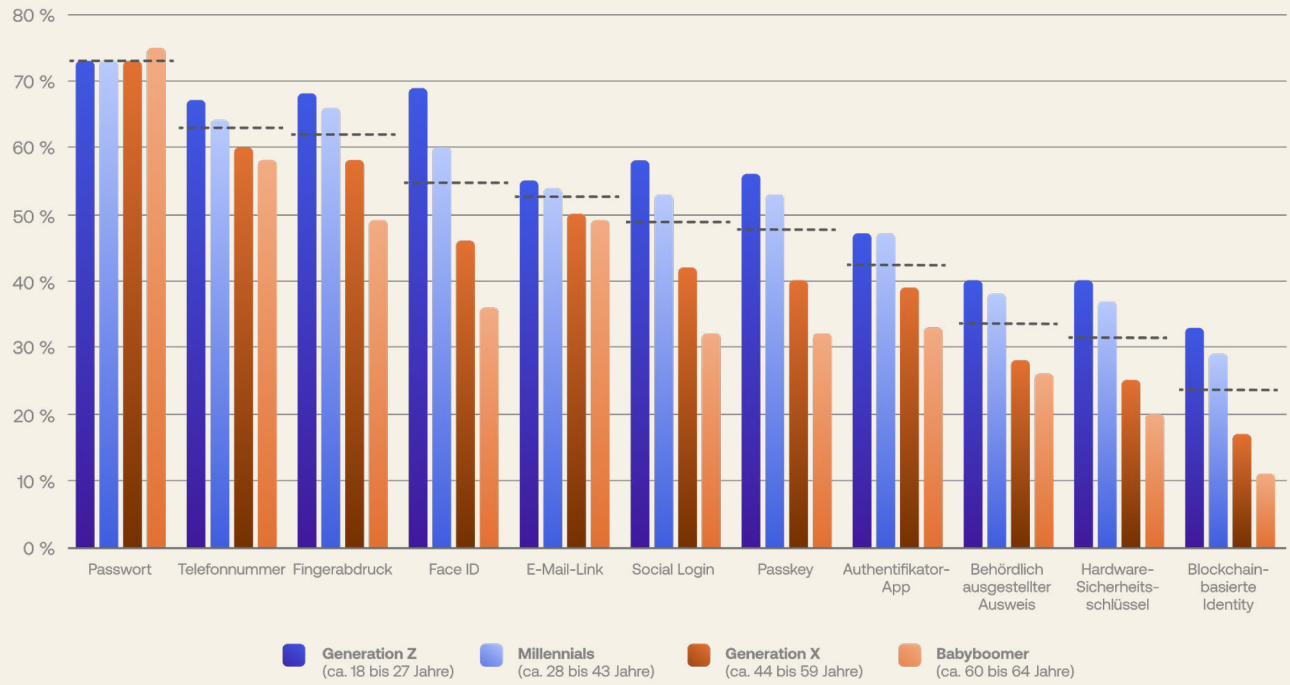
Im Gegensatz dazu beträgt der Korrelationskoeffizient zwischen wahrgenommener Sicherheit und Komfort nur 0,45 und der Koeffizient zwischen Nutzung und wahrgenommener Sicherheit sehr schwache 0,19.

Benutzer halten Passwörter für komfortabel, trotz bekannter Schwächen

Bei der Authentifizierung können drei verschiedene Arten von Faktoren zur Bestätigung der Identität eines Benutzers eingesetzt werden:

- *Wissensfaktoren*, bei denen davon ausgegangen wird, dass nur der tatsächliche Benutzer sie kennt (z. B. ein Passwort)
- *Besitzfaktoren* wie Authentifikator-Apps, behördlich ausgestellte Ausweise, Hardware-Sicherheitsschlüssel sowie Verifizierungs-Links und Passcodes, die an ein verifiziertes Ziel gesendet werden
- *Inhärenzfaktoren*, z. B. biometrische Identifikatoren

Die andauernde Attraktivität von Passwörtern basiert auf ihrem wahrgenommenen Komfort



Wahrnehmung des Komforts von Authentifizierungsmethoden, nach Generation der Befragten (Summe der Antworten „Sehr komfortabel“ und „Komfortabel“)

„Wie würden Sie jede der folgenden Methoden zur Bestätigung Ihrer Identität bei Registrierungen oder Logins für private Accounts bewerten?“

Hinweis: Die gestrichelten Linien zeigen den Mittelwert aller Befragten.

Die Authentifizierungssicherheit kann durch eine Kombination aus zwei oder mehr Faktoren erhöht werden, z. B. mit der Multi-Faktor-Authentifizierung (MFA). Unter Umständen bevorzugen Benutzer aufgrund der Einfachheit und Vertrautheit jedoch einen Ein-Faktor-Ansatz (z. B. Passwörter).

Passkeys schließen diese Lücke in der Benutzerfreundlichkeit, indem sie einen Besitzfaktor mit einem Wissens- oder Inhärenzfaktor in einer einzigen komfortablen Methode kombinieren.

Benutzer halten Passwörter für die komfortabelste Registrierungs- oder Login-Methode

73 % der Befragten stuften Passwörter als *sehr komfortabel* (40 %) oder *komfortabel* (33 %) ein – ganze 10 Prozentpunkte mehr als die zweitkomfortabelste Methode (Telefonnummer).

Biometrische Authentifikatoren spalten die Generationen

Bei der Wahrnehmung der Fingerabdruck- und Face ID-basierten Authentifizierung gibt es eine deutliche Generationenkluft. Das gleiche Muster zeigt sich, wenn man die Befragten nach ihrer Aufgeschlossenheit gegenüber neuen Technologien gruppiert.

Passkeys werden an Bedeutung gewinnen

Passkeys sind so neu, dass viele Benutzer noch nie von ihnen gehört haben. Aber mehr als die Hälfte der Generation Z- und Millennials-Befragten halten sie schon für komfortabel – ein Hinweis darauf, dass diese sicherere Authentifizierungsmethode vor einer großen Zukunft steht.

Trotz aller Warnungen werden Passwörter immer noch mehrfach verwendet

Angreifer werden immer geschickter darin, schwache Passwörter durch Brute-Force-Angriffe zu knacken und die weitverbreitete Mehrfachverwendung von Passwörtern auszunutzen. Daher haben sich die Sicherheitsanforderungen weiterentwickelt und verlangen immer komplexere Passwörter (z. B. hinsichtlich Länge, Sonderzeichen, Zahlen, Kombination von Groß- und Kleinbuchstaben usw.).

Die Benutzer ihrerseits haben diese Anforderungen – und die Sicherheitshygiene im Allgemeinen – sehr positiv angenommen, sodass passwortbasierte Angriffe inzwischen der Vergangenheit angehören. Doch halt: Stimmt das überhaupt? (Natürlich nicht.)

Mehr als zwei Drittel der Befragten verwenden Passwörter mehrfach

Fast jeder Benutzer weiß, dass er seine Passwörter nicht mehrfach verwenden soll – und doch geben 68 % zu, dass sie ein Passwort für alle Accounts (17 %) oder nur einige wenige Passwörter (51 %) verwenden.

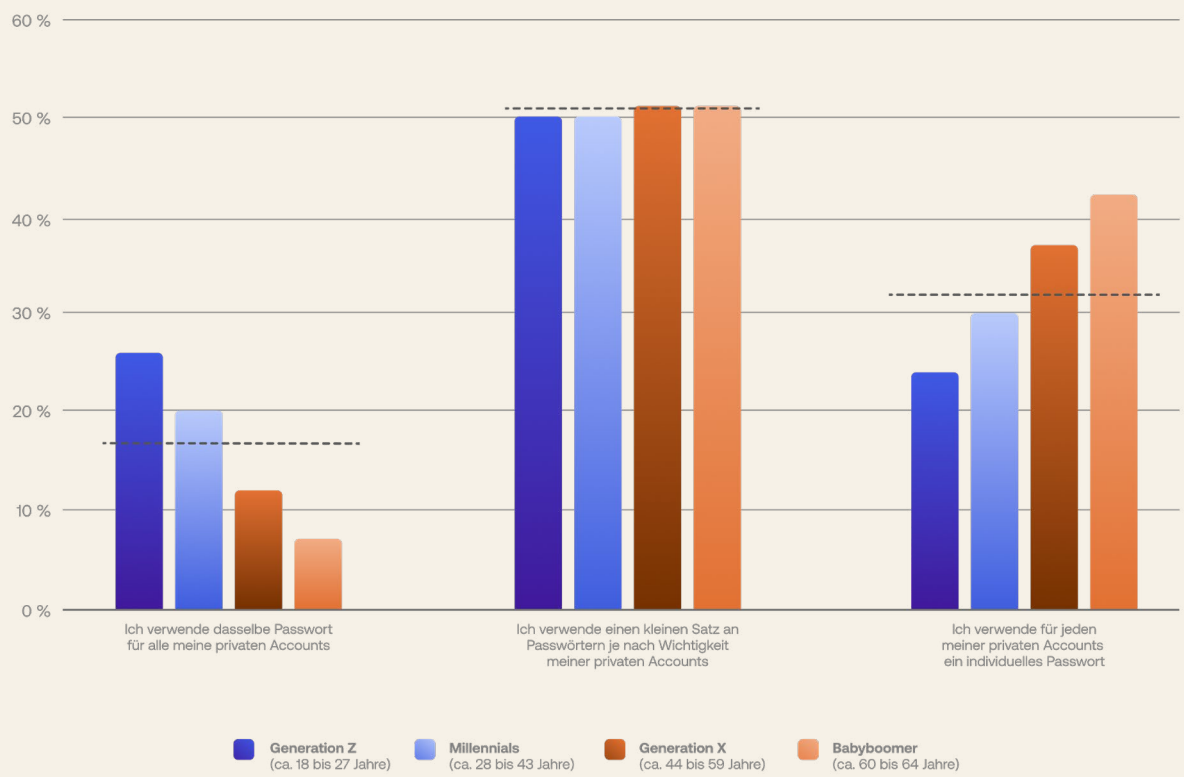
Technologie-Verweigerer und Babyboomer verwenden Passwörter am seltensten mehrfach

Diese Gruppen tragen ihren Teil dazu bei, passwortbasierte Angriffe zu bekämpfen: 42 % der Befragten in jeder Kohorte verwenden ein individuelles Passwort für jeden privaten Account.

Passwörter lassen sich so schwer merken

Auf die Frage nach dem Grund für die Mehrfachverwendung von Passwörtern gab mehr als die Hälfte der Befragten (53 %) an, dass individuelle Passwörter „*zu schwer zu merken*“ sind – 22 Prozentpunkte mehr als beim zweithäufigsten Grund, dass die Verwendung individueller Passwörter „*zu viel Zeit kostet*“.

Mehrfachverwendung von Passwörtern hält sich hartnäckig



Passworthygiene, nach Generation der Befragten

„Welche Aussage über Ihr Passwortverhalten trifft am ehesten auf Sie zu?“

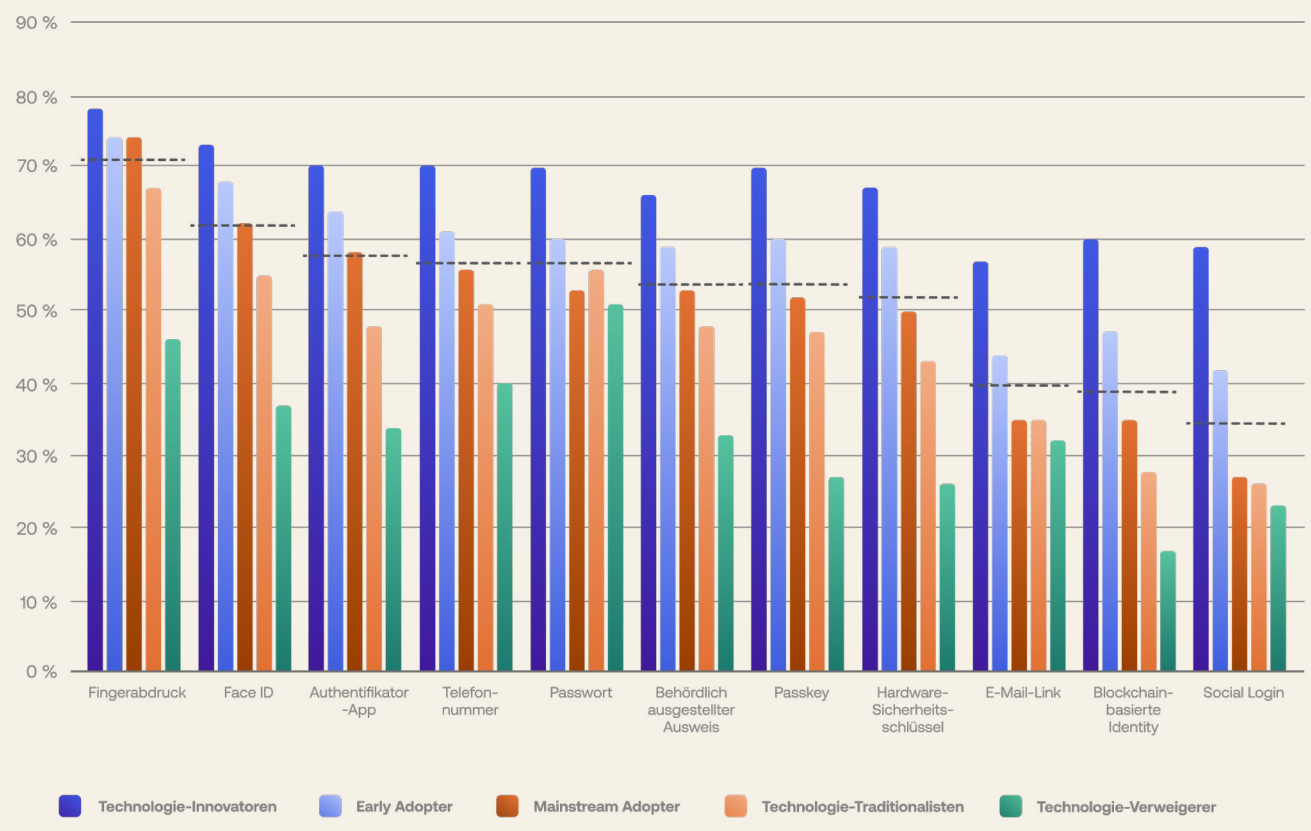
Hinweis: Die gestrichelten Linien zeigen den Mittelwert aller Befragten.

Für Kunden sind Fingerabdrücke die sicherste Login-Methode

Damit Authentifizierungstechniken in Kundenanwendungen – und insbesondere bei normalen Verbrauchern – effektiv funktionieren, müssen sie ein Gleichgewicht zwischen Sicherheit und Komfort finden.

Während Legacy-Authentifizierungsverfahren oft einen Kompromiss erforderten, kombinieren moderne Ansätze Phishing-resistente Sicherheit mit dem Komfort eines Fingerabdruck- oder Gesichtsscans oder dem Tippen auf eine Schaltfläche in einer Authentifikator-App.

Biometrie gilt als die sicherste Wahl für Logins



Wahrnehmung der Sicherheit von Authentifizierungsmethoden, nach Aufgeschlossenheit der Befragten gegenüber neuen Technologien (Summe der Antworten „Sehr sicher“ und „Sicher“)

„Als wie sicher schätzen Sie die folgenden Methoden für die Registrierung oder Anmeldung bei einem privaten Account ein?“

Hinweis: Die gestrichelten Linien zeigen den Mittelwert aller Befragten.

Biometrie führt die Hitliste an

Über alle Generationen hinweg landeten der Fingerabdruck (von 71 % aller Benutzer gewählt) und Face ID (62 %) auf den ersten beiden Plätzen. Fast das gleiche Bild zeigt sich bei der Segmentierung nach Aufgeschlossenheit gegenüber neuen Technologien – die einzigen Ausnahmen sind das größere Vertrauen der Technologie-Verweigerer in Passwörter und die Verifizierung über Telefonnummern.

Social Login wird als vergleichsweise unsicher wahrgenommen

Nur 35 % der Befragten halten Social Login für *sehr sicher* (13 %) oder *sicher* (22 %) – ein schlechtes Zeichen für Marketingspezialisten, die Benutzer für diese Methode begeistern wollen, weil sie im selben Zuge oft demografische Daten erhalten.

Wahrnehmungen variieren je nach Aufgeschlossenheit der Benutzer gegenüber neuen Technologien

Wie die Abbildung deutlich zeigt, betrachten Technologie-Innovatoren und Early Adopter eine bestimmte Authentifizierungsmethode viel eher als *sehr sicher* oder *sicher* als Mainstream Adopter, Technologie-Traditionalisten und Technologie-Verweigerer.

Personalisiert, privat und geschützt: Vertrauen in digitale Beziehungen aufbauen

Insgesamt machen die Ergebnisse der Umfrage ein Paradoxon hinter den Online-Interaktionen und digitalen Identitäten, die sie ermöglichen, sichtbar:

- Kunden wollen reibungslose, personalisierte und sofortige Customer Experiences, wenn sie sich bei Anwendungen anmelden und Einkäufe tätigen.
- Gleichzeitig wollen sie kontrollieren, welche Daten sie weitergeben, und wünschen sich angemessene Sicherheitskontrollen zum Schutz dieser Daten.

Für die Marken kommt erschwerend hinzu, dass eine Reihe von Faktoren (z. B. Land des Wohnsitzes, Alter/Generation und Aufgeschlossenheit gegenüber neuen Technologien) die Präferenzen beeinflussen und spezifische Anforderungen stellen. Statt einen einzigen Customer Identity-Ansatz zu implementieren, sollten Unternehmen verschiedene Techniken kombinieren, um die Anforderungen der digitalen Verbraucher an Personalisierung, Datenschutz und Sicherheit zu erfüllen.

Marken müssen unbedingt berücksichtigen, dass digitale Beziehungen genauso entstehen und sich entwickeln wie Beziehungen im realen Leben: *mit der Zeit*. Die Verantwortung für die Vertrauensbildung in einer digitalen Beziehung liegt beim Service Provider. Gleichzeitig muss dieses Vertrauen jederzeit neu verdient, respektiert und geschützt werden.

Bereitstellung sicherer Authentifizierungsoptionen für die Benutzer

Die Ergebnisse der Umfrage haben mehrfach gezeigt, dass verschiedene Benutzer unterschiedliche Wahrnehmungen und Präferenzen haben. Dies deutet darauf hin, dass Marken den Benutzern die Wahl zwischen verschiedenen sicheren Authentifizierungsoptionen lassen sollten.

Durch die Abkehr von der traditionellen Benutzername/Passwort-Kombination können Marken gleichzeitig für mehr Sicherheit und komfortablere User Experiences sorgen. Dabei stehen verschiedene Techniken zur Verfügung, um ein optimales Gleichgewicht für verschiedene Szenarien zu erreichen.

Zum Beispiel sind Passkeys wesentlich sicherer als Passwörter und bieten eine komfortablere Authentifizierungs-Experience, obwohl sie den Benutzern nicht so vertraut sind wie Passwörter.

Weitere Möglichkeiten zur Verringerung der Reibungspunkte bei gleichzeitiger Erhöhung der Sicherheit sind:

- **Social Logins:** Im Wesentlichen handelt es sich um Single Sign-On (SSO) für Consumer-Apps. Social Logins vereinfachen die Account-Authentifizierung und verringern das Risiko, dass Benutzer bei der Anmeldung bei Ihren Services auf Probleme stoßen. Bedenken der Benutzer hinsichtlich der Sicherheit dieses Ansatzes, die wegen der fehlenden Reibungspunkte durchaus geäußert werden, können mit einer kurzen Erläuterung der Funktionsweise ausgeräumt werden. (Gehen Sie dabei nicht so sehr auf die technischen Details, sondern vor allem darauf ein, dass die Methode genauso sicher wie die Authentifizierung des Social-Media-Anbieters ist.)
- **Biometrische Authentifizierung:** Biometrie wird von immer mehr Verbrauchergeräten unterstützt und von den Kunden bereits als äußerst sicher angesehen. Sie ersetzt die mühsame Eingabe von Passwörtern durch den Komfort eines Fingerabdrucks oder Gesichtsscans.
- **Adaptive MFA:** Dieses Tool greift nur dann auf sekundäre Faktoren zurück, wenn eine Benutzerinteraktion aufgrund von Verhaltensdaten als riskant eingestuft wird (z. B. weil eine nicht plausible Ortsveränderung festgestellt wird oder das Login von einem neuen Endgerät erfolgt).
- **Step-up-Authentifizierung:** Bei diesem Ansatz wird die Authentifizierung an die Bedeutung der Ressourcen geknüpft, auf die zugegriffen wird (z. B. kann ein Benutzer zu einer zusätzlichen Authentifizierung aufgefordert werden, wenn er versucht, Account-Informationen zu ändern oder ein vertrauliches Dokument abzurufen).

Erfassung personenbezogener Daten im Zeitalter des Datenschutzes

Unzählige Umfragen (darunter auch diese) haben ergeben, dass Benutzer durch lange Formulare genervt sind und sich fragen, was Marken mit ihren personenbezogenen Daten machen.

Um die erforderlichen Zero-Party- und First-Party-Daten für stark personalisierte User Experiences zu erfassen, die viele Abonnenten erwarten, müssen Marken kundenfreundliche Lösungen wie die **progressive Profilerstellung** nutzen. Bei dieser Technik wird der Benutzer nach und nach um Informationen gebeten, je mehr Nutzen er aus dem Service zieht. So können Reibungspunkte bei der Registrierung reduziert werden und Bedenken der Benutzer, einer unbekannten Marke zu viele Informationen zur Verfügung zu stellen, kommen gar nicht erst auf.

Zudem sollten Unternehmen die Benutzer **transparent informieren, wie ihre digitalen Identitäten verwaltet werden**, warum die Daten benötigt werden, wie sie verwendet werden und welche Sicherheitsmaßnahmen zum Schutz der Benutzer-Accounts und darin enthaltenen privaten Daten getroffen werden.

Customer Identity-Bedrohungen

Ein kurzer Überblick über die aktuell häufigsten und gefährlichsten Identity-basierten Angriffe – und wie Sie Anwendungen vor ihnen schützen können

Sichere Kundenauthentifizierung

Digitale Identitäten regeln heute bereits den Zugang zu immer mehr Anwendungen und Diensten – und beeinflussen und steuern damit viele Aspekte des modernen Lebens. Ihre Bedeutung wird noch weiter zunehmen.

Leider haben nicht nur legitime Benutzer ein Interesse daran, hinter das Login-Gateway zu gelangen. Wenn es Angreifern gelingt, in Ihr System einzudringen, können sie viel Geld verdienen. Die monetären Anreize haben zu einem riesigen Ökosystem von Technologien, Services und anderen Ressourcen geführt, die ausschließlich dazu dienen, solche Aktivitäten zu ermöglichen.

Die Angriffe gegen kleine und große Unternehmen setzen sich in allen Branchen kontinuierlich fort. Cyberkriminelle investieren immer mehr Arbeit und Knowhow, um die Login-Box zu umgehen. Daher sind zur Abwehr von Attacken immer mehr und immer raffiniertere Schutzmaßnahmen erforderlich – und deshalb besitzen Authentifizierung, Autorisierung und CIAM für den Schutz von Vertrauen, Sicherheit und Daten eine so große Bedeutung.

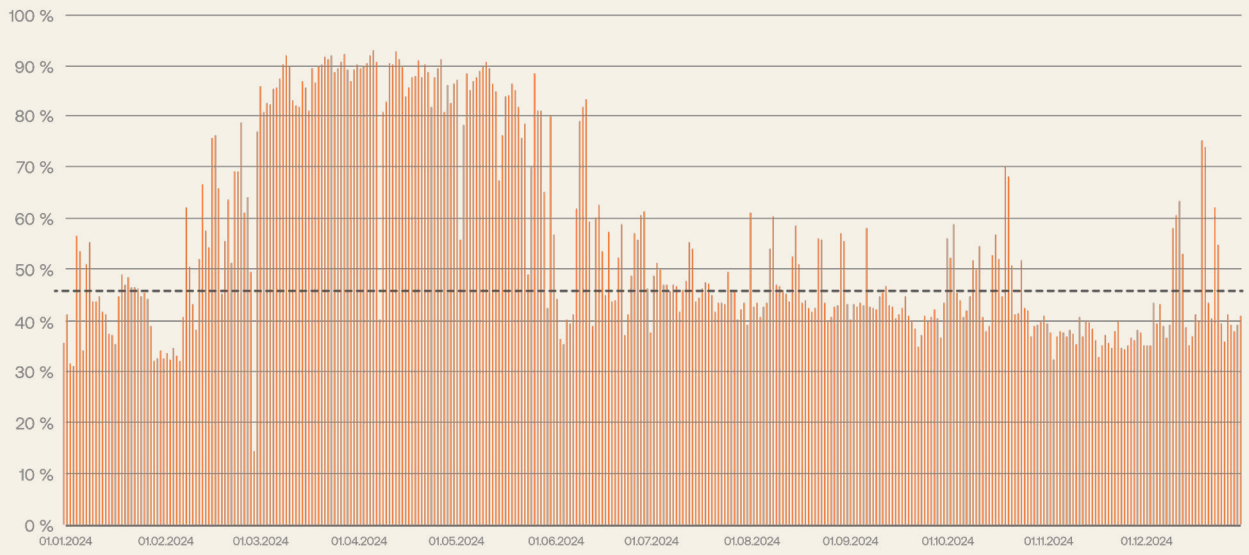
Das Böse ist immer und überall: Gefälschte Registrierungen nehmen keine Auszeit

Der einfachste Weg für böswillige Akteure, die es auf Privilegien, Services und Informationen hinter der Login-Box abgesehen haben, führt über Puppet-Accounts, die eigens zu diesem Zweck von ihnen erstellt wurden.

Dies kann vor allem dann erhebliche Probleme und unnötige Kosten verursachen, wenn solche Fälle im großen Maßstab vorkommen. Gefälschte Benutzer haben zum Beispiel diese Möglichkeiten:

- Als Ausgangspunkt dienen, um später als etablierte Accounts für die Umgehung von Kontrollen missbraucht zu werden
- Vorhandene Benutzer-Accounts auflisten/erkennen
- Prämien kassieren, z. B. Registrierungsboni
- Für Denial-of-Service-Angriffe genutzt werden, indem sie Ressourcen belegen und Anzahlbegrenzungen überschreiten

Gefälschte Registrierungen sind eine ständige Bedrohung



Angriffe mit verdächtiger Registrierung, nach Tag (1. Januar bis 31. Dezember 2024)

Hinweis: Jede Spalte zeigt den Anteil der Registrierungsversuche auf der Auth0 Platform an einem bestimmten Tag, die die Kriterien für einen Registrierungsangriff erfüllten. Die gestrichelte Linie zeigt den Median (46,1 %) dieser täglichen Registrierungsversuche auf der gesamten Plattform. (Definition eines Registrierungsangriffs siehe Methodik.)

Darüber hinaus werden oft ganze Konversionsabläufe auf der Grundlage der Interaktion der Benutzer mit dem betreffenden Service optimiert. Betrügerische Registrierungen verfälschen diese Daten und erschweren Analysen, was unter Umständen kostspielige Behebungen notwendig macht.

Betrügerische Registrierungen bleiben ein alltägliches Problem

- Schon ein kurzer Blick auf die Grafik genügt, um zu erkennen, dass gefälschte Registrierungen eine ständige Bedrohung darstellen.
- 2024 lag der Median der Registrierungsversuche, die die Kriterien eines Angriffs erfüllt haben, auf der gesamten Auth0 Platform bei 46,1 %. Dies bedeutet die Umkehr eines Abwärtstrends und geht einher mit einer Zunahme der Registrierungsangriffe, die von anderen großen Technologieunternehmen gemeldet wurden. Einige Marktteilnehmer führen den Anstieg auf KI-gestützte Angriffs-Workflows zurück.

Bedrohungen im Alltag variieren stark

- Am 6. April erfüllten 92,5 % der Registrierungsversuche die Kriterien für einen Registrierungsangriff.
- Im Gegensatz dazu waren es am 29. Februar nur 14,4 % – ein großer Ausreißer, denn an keinem anderen Tag lag der Anteil der Registrierungsangriffe unter 30 %.
- Für den gesamten Jahresverlauf sehen wir eine Mischung aus kurzfristigen Ausschlägen.
- Am deutlichsten vielleicht ist der anhaltende Anstieg von schädlichem Verhalten von Mitte Februar bis Ende Mai.

Betrüger konzentrieren sich auf große Einzelhändler und Finanz-dienstleister

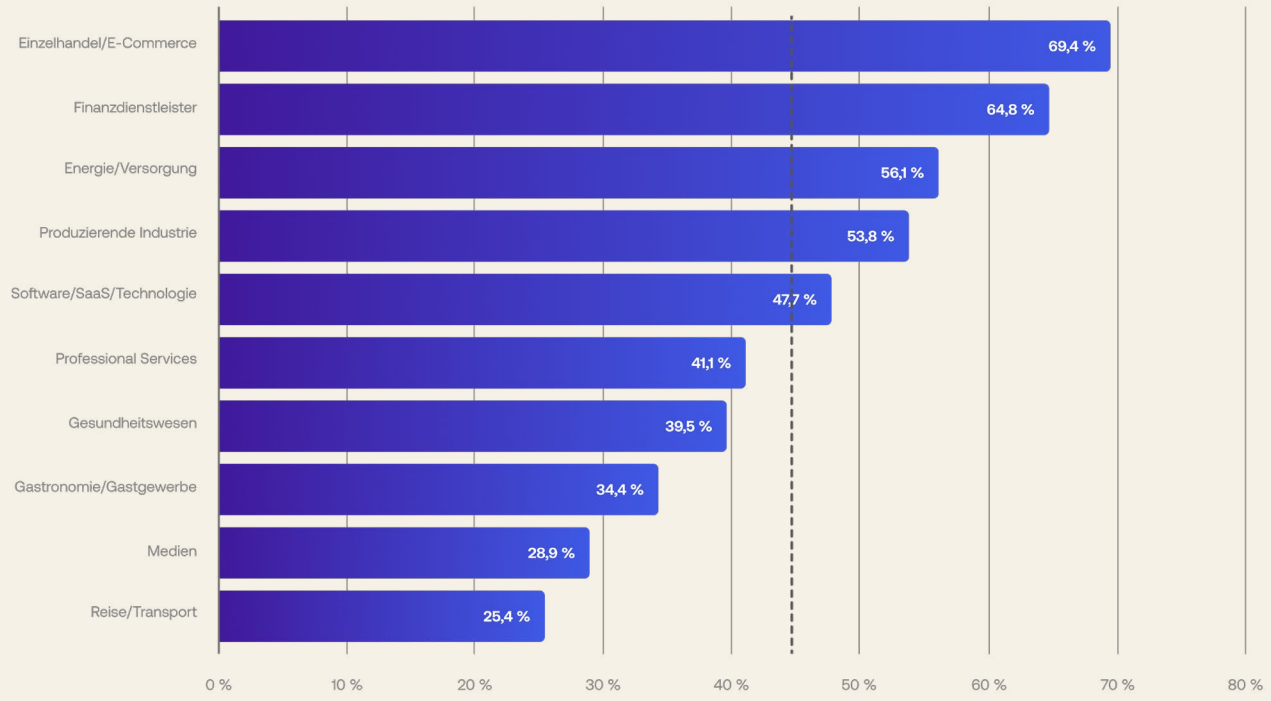
Bei genauerer Betrachtung der zugrunde liegenden Daten wird deutlich, dass die betrügerischen Registrierungsversuche ungleichmäßig verteilt sind.

Unternehmen verschiedener Branchen und Größen sind unterschiedlich stark von Angriffen betroffen.

Einzelhandels- und E-Commerce-Unternehmen sind die Top-Ziele von gefälschten Registrierungen

- 2024 entfielen fast 70 % der Registrierungsversuche bei Einzelhandels- und E-Commerce-Unternehmen auf Registrierungsangriffe – der höchste Anteil unter den 10 Branchen, die auf unserer Plattform am stärksten vertreten sind.
- Viele Online-Einzelhändler bieten Anreize für die Registrierung und exklusive Features für Mitglieder. Diese Programme könnten das Interesse von Angreifern wecken.

Betrüger konzentrieren sich auf Einzelhandel und Finanzsektor



Angriffe mit verdächtiger Registrierung, nach Branche (1. Januar bis 31. Dezember 2024)

Hinweis: Jeder Balken zeigt den Median der täglichen Registrierungsversuche für eine bestimmte Branche, die die Kriterien für einen Registrierungsangriff im Jahr 2024 erfüllten. Die gestrichelte Linie zeigt den Mittelwert (44,5 %) der täglichen Mediane pro Branche über alle Branchen auf der Auth0 Platform (d. h. nicht nur die Top 10).

Auch Finanzdienstleister stehen im Fadenkreuz

- Fast 65 % der versuchten Registrierungen bei Finanzdienstleistern waren mit Registrierungsangriffen verbunden.
- Zu dieser Kategorie gehören insbesondere viele Kryptowährungs-Startups, die oft Coins/Token als Willkommensgeschenke anbieten.
- Aber auch Accounts bei traditionelleren Finanzdienstleistern können attraktiv sein, weil sie Geldwäsche und Synthetic Identity Fraud erleichtern.

Große Unternehmen ziehen die meiste unerwünschte Aufmerksamkeit auf sich

- Große Unternehmen waren mit 64,3 % der Registrierungsversuche am stärksten von Registrierungsangriffen betroffen.
- Mittelständische Unternehmen schnitten deutlich besser ab: Nur 18,2 % der Registrierungsversuche erfüllten die Kriterien für einen Registrierungsangriff.
- Kleine Unternehmen lagen mit 43,3 % der Registrierungsversuche, die eindeutig schädliches Verhalten zeigten, genau im Mittelfeld.

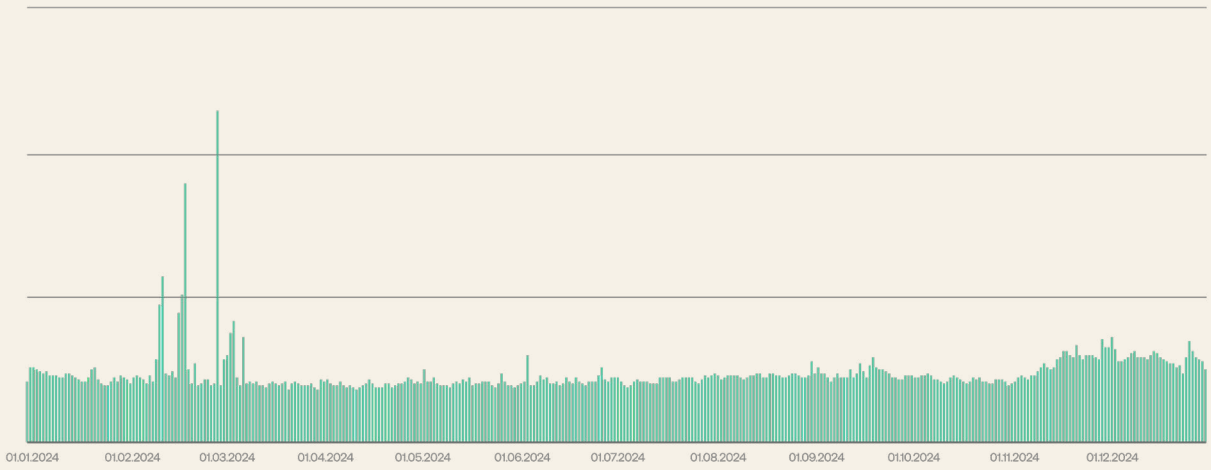
Werfen wir zur Veranschaulichung einen kurzen Blick auf den Einzelhandels- und E-Commerce-Sektor, da er in der Grafik auf der vorherigen Seite an erster Stelle steht.

Aus dem Diagramm der legitimen Registrierungsereignisse geht hervor, dass die Anzahl der echten Registrierungen, die über die Auth0 Platform abgewickelt werden, ziemlich konstant ist.

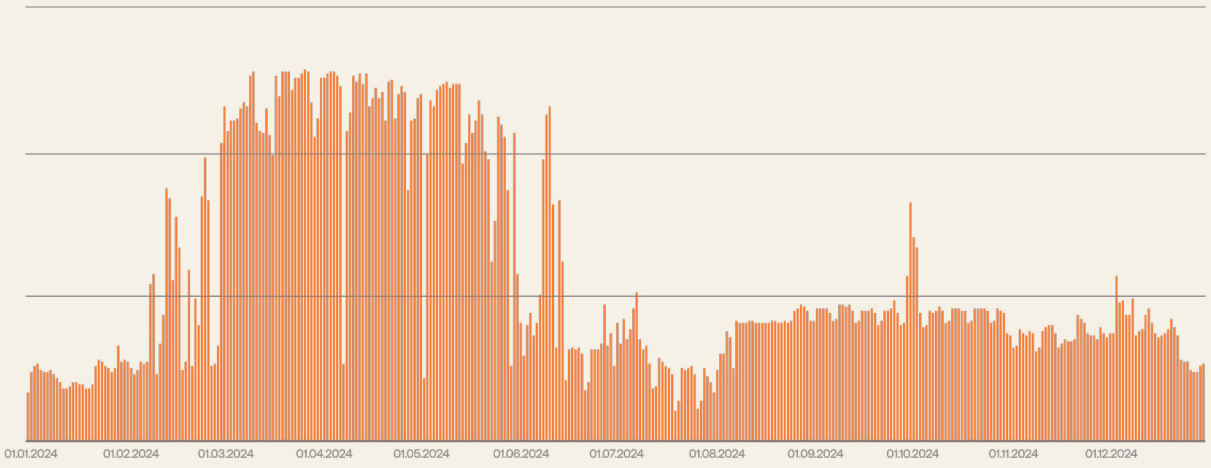
Im offensichtlichen Gegensatz dazu zeigt das Diagramm der Registrierungsangriffsereignisse eine viel größere Schwankungsbreite. Darüber hinaus sehen wir oben, dass der Einzelhandels- und E-Commerce-Sektor von einem mehrmonatigen Anstieg betroffen war.

In diesem Angriffszeitraum **überstieg die Zahl der Registrierungsangriffe die Zahl der legitimen Registrierungen um das 120-fache**.

Das massive Ausmaß der Registrierungsangriffe



Legitime Registrierungen im Einzelhandels- und E-Commerce-Sektor, nach Tag (1. Januar bis 31. Dezember 2024)



Verdächtige betrügerische Registrierungen im Einzelhandels- und E-Commerce-Sektor, nach Tag (1. Januar bis 31. Dezember 2024)

Hinweis: Im Gegensatz zu den meisten anderen Diagrammen in diesem Bericht präsentieren diese beiden Diagramme die absoluten Zahlen (nicht die relativen Anteile). Um den visuellen Vergleich zu erleichtern, nutzen sie denselben logarithmischen vertikalen Zugang, gekürzt um viele Größenordnungen.

Wie Sie sich vor Login-Angriffen schützen

Wenn Sie Angreifer so früh wie möglich erkennen und aus der Registrierungspipeline werfen, können Sie die Systemlast reduzieren und die Aufklärungsaktivitäten der Angreifer einschränken (z. B. durch den Empfang und die Analyse von Fehlermeldungen).

Hierfür gibt es auf den verschiedenen Ebenen der Identity-Infrastruktur eine Reihe möglicher Abwehrmaßnahmen:

Maßnahmen auf Host-Ebene zum Schutz vor Brute-Force-Angriffen

Hinweis: *Diese Schutzmaßnahmen gelten für alle im Bericht untersuchten Brute-Force-Angriffe (d. h. nicht nur für Registrierungsangriffe).*

Um den Missbrauch der von ihnen gehosteten Services zu verhindern, wenden Hosting-Anbieter (z. B. Cloudflare, Microsoft Azure, Amazon Web Services) eine Reihe von Schutzmaßnahmen an. Im Customer Identity-Kontext werden diese Schutzmaßnahmen vor der CIAM-Funktionalität implementiert und umfassen in der Regel:

- **Abwehr von Distributed-Denial-of-Service-(DDoS-)Angriffen:** Schutzmaßnahmen gewährleisten die Funktion Ihrer CIAM-Anwendung für legitime Benutzer auch bei groß angelegten Angriffen (insbesondere auf TCP/UDP-Ebene).
- **Bot-Management:** Eine erste Ebene der Bot-Filterung basiert in der Regel auf einer Kombination aus Verhaltensanalyse, Threat Intelligence und Feedback Loops.
- **Anzahlbegrenzung:** Kontrollen schützen vor DoS-Angriffen, Brute-Force-Strategien und API-Missbrauch, indem sie die Rate begrenzen, mit der eine bestimmte Entität auf die CIAM-Plattform/Anwendung zugreifen kann.

Maßnahmen auf Plattformebene zum Schutz vor Brute-Force-Angriffen

Hinweis: *Diese Schutzmaßnahmen gelten für alle im Bericht untersuchten Brute-Force-Angriffe (d. h. nicht nur für Registrierungsangriffe).*

Ihre CIAM-Plattform sollte eine Reihe von Schutzfunktionen für die Abwehr von Registrierungsangriffen bieten. Bei der Wahl der richtigen Reaktion auf schädliches Verhalten müssen jedoch die damit verbundenen Kompromisse berücksichtigt werden – insbesondere die Frage, wie viele Reibungspunkte Ihre Benutzer während des Registrierungsprozesses tolerieren würden.

Wie so oft im Bereich der Sicherheit sind mehrstufige Lösungen am effektivsten. Je mehr dieser Techniken Sie implementieren können, desto sicherer sind Ihre Kunden und Ihr Unternehmen.

1. **Funktionen zur Bot-Erkennung:** Funktionen zur Bot-Erkennung (Bot Detection) auf Plattformebene analysieren in der Regel Telemetriedaten (stehen hier in größerer Zahl als auf der Host-Ebene zur Verfügung) und können vorhersagen, wann ein Registrierungsversuch wahrscheinlich von einem Bot kommt. Ab einem bestimmten Vorhersage-/Konfidenzschwellenwert schlägt der Account-Registrierungsprozess eine Gegenmaßnahme vor, die ein legitimer Benutzer leicht ausführen kann, für einen Bot aber schwierig – und kostspielig – umzusetzen ist.
2. **Aktivierte bzw. erweiterte CAPTCHA-Sicherheitsabfragen:** Wenn Ihre Anwendungen heute noch kein CAPTCHA verwenden, sollten Sie diese Funktion unbedingt aktivieren. CAPTCHAs bedeuten zwar mehr Reibungspunkte, viele Benutzer kennen sie aber schon und verstehen, warum sie eingesetzt werden. Ein ausgewogener Ansatz wäre es, CAPTCHAs nur anzuzeigen, sobald ein Risikogrenzwert erreicht wird. In diesem Fall sollten Sie CAPTCHAs immer einblenden, sobald es Anzeichen für eine groß angelegte Registrierungsangriffskampagne gibt. Kein CAPTCHA ist allerdings perfekt, sodass ein hartnäckiger Angreifer am Ende immer einen Weg finden wird, es zu umgehen. Das Ziel ist nicht, den Registrierungsprozess hundertprozentig sicher zu machen, sondern einen Missbrauch so weit zu erschweren, dass ein Angreifer ablässt und sich ein leichteres Ziel sucht.
3. **Verschärfte Schwellenwerte für Brute-Force-Angriffe und verdächtige IP-Adressen:** Beide Ansätze begrenzen die Anzahl der zulässigen Verbindungen und sollten für echte Kunden kein Problem sein.
4. **Blockierung von IP-Adressen, von denen Missbrauch ausgeht:** Sie sollten auf Ihrer CIAM-Plattform Regeln für Zugriffskontrolllisten (ACLs) implementieren können, um IP-Adressen, von denen Missbrauch ausgeht, vollständig zu blockieren.
5. **Blockierung schädlicher Aktivitäten mithilfe von WAF-Regeln (Web Application Firewall) am Edge:** Wenn Sie einen Edge Provider oder eine ausreichend ausgestattete CIAM-Plattform nutzen, sollten Sie IP-Adressen, ASNs (Autonomous System Numbers), geografische Standorte, TLS-Clients oder andere HTTP-Header-Elemente (z. B. User-Agent-Strings), von denen Missbrauch ausgeht, blockieren.

Spezielle Maßnahmen zum Schutz vor Registrierungsangriffen

Neben den bereits genannten Ebenen für den Schutz vor Brute-Force-Angriffen gibt es verschiedene Spezialtechniken für Registrierungsangriffe, mit denen sich betrügerische Registrierungen eindämmen lassen:

Die effektivste Technik besteht vielleicht darin, die **Benutzer** zu **ermutigen, sich mit einem Passkey zu registrieren**, da die Kryptografie dahinter es außerordentlich schwierig macht, Passkeys im Rahmen eines Registrierungsangriffs zu missbrauchen. Auch wenn es den Rahmen dieses Berichts sprengt: **Die Analyse der Auth0 Platform-Telemetrie zeigt, dass Angreifer noch keine massenhaften Angriffe auf Registrierungs- oder Anmeldungsvorgänge mit Passkeys durchführen.**

Weitere Schutzmaßnahmen sind:

- **Regeln und Aktionen, die bereits vor der Registrierung greifen** (z. B. eine CAPTCHA-Abfrage oder die Abfrage weiterer Informationen), um die Wahrscheinlichkeit eines Fake-Users weiter zu verringern
- **Social Login**, um den Schutz vor betrügerischen Registrierungsversuchen „auszulagern“
- **Identity Proofing**, wenn das Risiko als besonders hoch eingestuft wird
- **Validieren der Kontaktinformationen** (z. B. E-Mail-Adresse, Telefonnummer) durch einen einmaligen Passcode oder einen Magic Link

Entscheidend ist, dass die aus der Untersuchung von Angriffen gewonnenen Erkenntnisse für weitere Optimierungen genutzt werden.

Um diesen Punkt zu veranschaulichen, kehren wir zu den oben präsentierten Diagrammen zurück, die legitime und betrügerische Registrierungen im Einzelhandels- und E-Commerce-Sektor gegenüberstellen. Es fällt auf, dass einige Spitzen bei den zugelassenen Registrierungen mit dem Beginn eines längeren Angriffszeitraums mit hohem Volumen zusammenfallen.

Diese kurzzeitigen Spitzen stellen Angriffe dar, bei denen ein Teil des schädlichen Datenverkehrs der Erkennung entgangen ist. Dies zeigt nicht nur, wie wichtig präventive Kontrollmechanismen wie Bot-Erkennung und CAPTCHA sind, sondern dass auch Protokolle und Sicherheits-Dashboards geprüft werden müssen, um Einblicke in die sich weiterentwickelnden Taktiken der Angreifer zu erhalten.

In diesem Fall konnte das Auth0-Security-Team die Schutzmaßnahmen der Plattform aufgrund der Analyse schnell anpassen, sodass sich die Quote der legitimen Registrierungen trotz des monatelangen Bombardements mit gefälschten Registrierungsversuchen wieder normalisierte.

Der anhaltende Kampf gegen Account-Hacking

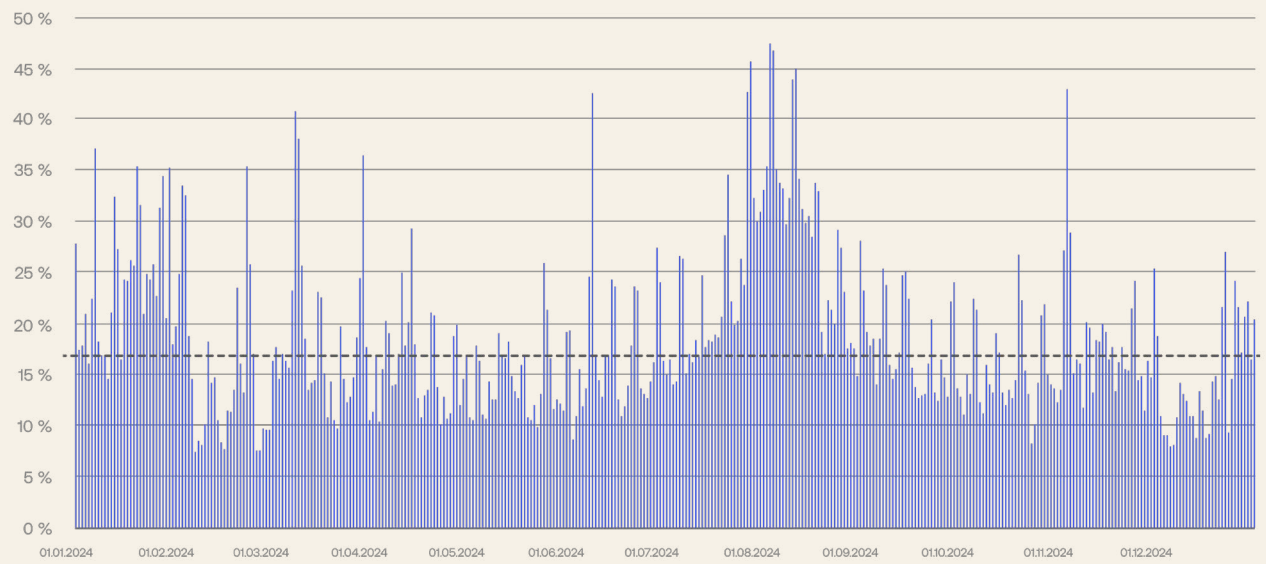
Während betrügerische Registrierungen (mindestens) ein kostspieliges Ärgernis sind, stellt Account-Hacking eine deutlich größere Bedrohung für Sicherheit und Datenschutz dar.

Im B2C-Umfeld können Angreifer etwa Zugang zu Ressourcen (z. B. Treuepunkte), Privilegien (z. B. die Möglichkeit, Käufe zu tätigen, insbesondere bei Produkten mit begrenztem Angebot) und wertvollen demografischen und personenbezogenen Daten erlangen.

Im B2B-Umfeld können Angreifer durch die Kompromittierung eines User Accounts auf äußerst sensible Daten zugreifen. Diese Sicherheitsverletzung kann zu erheblichen gesetzlichen und Vertragsstrafen für das betroffene Unternehmen führen.

Einige Account-Hacking-Versuche richten sich zwar auch gegen Einzelpersonen, doch in den meisten Fällen nehmen Brute-Force-Angriffstechniken die passwortbasierte Authentifizierung ins Visier, um so viele Konten wie möglich zu kompromittieren.

Account-Hacking: eine dauerhafte Bedrohung



Angriffe mit verdächtigen Logins, nach Tag (1. Januar bis 31. Dezember 2024)

Hinweis: Jede Spalte zeigt den Anteil der passwortbasierten Authentifizierungsereignisse an einem bestimmten Tag, die die Kriterien eines Login-Angriffs erfüllten. Die gestrichelte Linie zeigt den Median (16,9 %) dieser täglichen Login-Versuche auf der gesamten Plattform. (Definition eines Login-Angriffs siehe Methodik.)

Login-Angriffe machen Account-Hacking zu einer ständigen Bedrohung

- 2024 lag der Median der Login-Versuche mit eindeutig schädlichen Verhaltensweisen auf der gesamten Auth0 Platform bei 16,9 %.
- Mit diesem Wert setzt sich ein Abwärtstrend fort, der erstmals im Okta The State of Secure Identity Report 2023 festgestellt wurde.

Wie bei den gefälschten Registrierungen verbergen sich hinter dem Durchschnittswert enorme tägliche Schwankungen

- Im gesamten Jahr lag die höchste tägliche Quote von Login-Angriffen bei 47,4 % – die niedrigste bei 7,6 %.
- Darüber hinaus sehen wir denselben Mix aus kurzfristigen Spitzen (wenn auch viel mehr als bei den gefälschten Registrierungen) und anhaltenden mehrwöchigen Zeiträumen mit hohen Login-Angriffsquoten.

Häufigste Ziele für Account-Hacking: Online-Händler und E-Commerce

Bei genauerer Betrachtung der Daten zeigt sich, dass es Angreifer beim Account-Hacking besonders auf hochwertige Branchen abgesehen haben.

Einzelhandels- und E-Commerce-Unternehmen sind die Hauptziele von Login-Angriffen

- Ein Blick auf das Diagramm (unten) zeigt, dass der Einzelhandels- und E-Commerce-Sektor ein statistischer Ausreißer ist: Bei Unternehmen dieser Gruppe weisen 22,2 % der Login-Versuche ein eindeutig schädliches Verhalten auf – mehr als doppelt so viele wie im Durchschnitt aller Branchen.

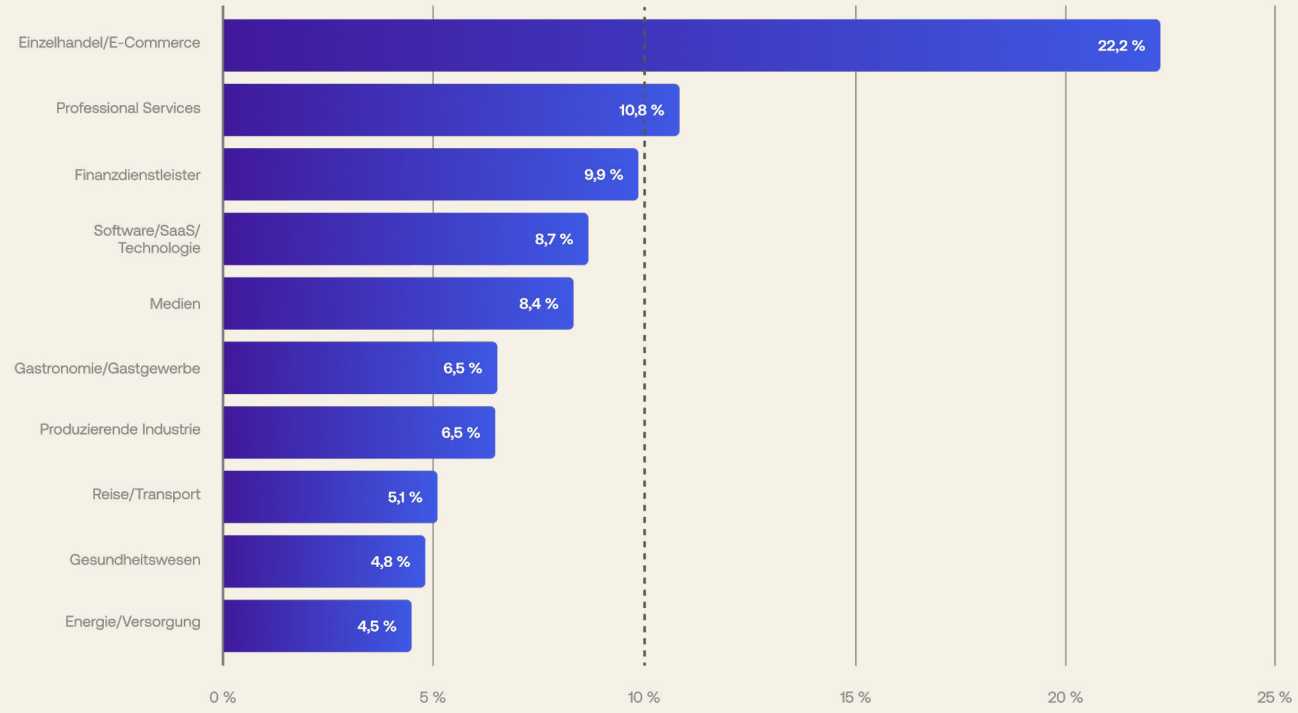
Professional Services-Anbieter und Finanzdienstleister stehen ebenfalls unter Beschuss

- In beiden Branchen liegen die Login-Angriffsquoten in etwa auf dem Niveau des mittleren Medianwerts aller Branchen.
- Noch etwas haben sie gemeinsam: Unternehmen in diesen Gruppen speichern wahrscheinlich streng vertrauliche personenbezogene Daten, einschließlich finanzieller Details, die für Angreifer attraktiv sind.

Wie bei den gefälschten Registrierungen ziehen große Unternehmen die meiste unerwünschte Aufmerksamkeit für Login-Angriffe auf sich

- Die höchste Quote schädlicher Logins gab es im Enterprise-Segment: 24,9 % der versuchten Logins erfüllten die Kriterien für einen Login-Angriff.
- Nichtsdestotrotz gehören Login-Angriffe auch für mittelständische Unternehmen (7,6 %) und kleine Unternehmen (9,4 %) nach wie vor zum Alltag, wenn auch in deutlich geringerem Umfang.

Konzentrationen verdächtiger Account-Hacking-Angriffe



Angriffe mit verdächtigen Logins, nach Branche (1. Januar bis 31. Dezember 2024)

Hinweis: Jeder Balken zeigt den Median der täglichen Login-Versuche für eine bestimmte Branche, die die Kriterien eines Login-Angriffs im Jahr 2024 erfüllten. Die gestrichelte Linie zeigt den Mittelwert (10,0 %) der täglichen Mediane pro Branche über alle Branchen auf der Auth0 Platform (d. h. nicht nur die Top 10).

Maßnahmen zum Schutz vor Account-Hacking: Zwei Diagramme erzählen eine Geschichte

Da Einzelhandels- und E-Commerce-Unternehmen im Jahr 2024 die höchste Login-Angriffsquote verzeichneten, sollten wir uns dieses Segment noch einmal genauer ansehen.

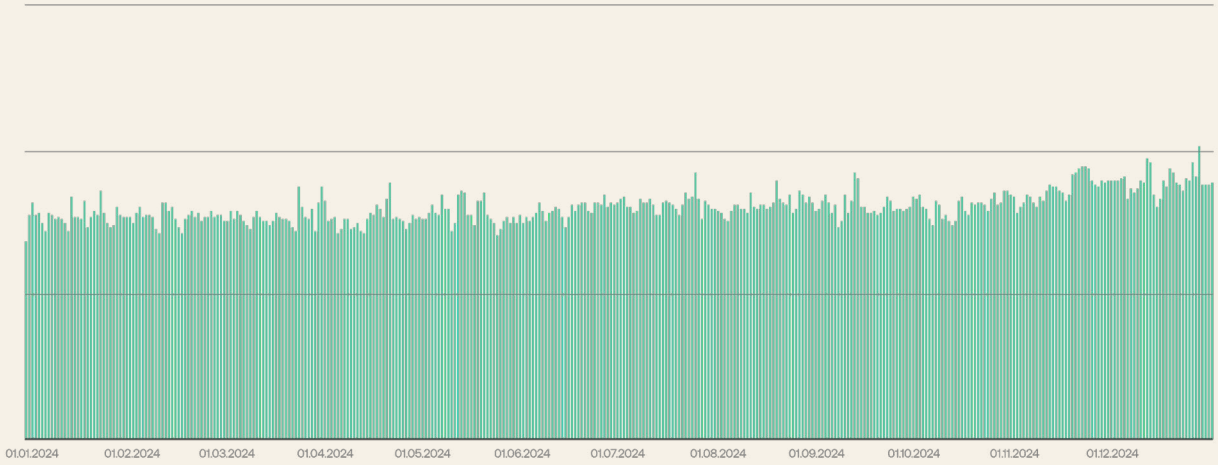
Das Diagramm für die legitimen Passwort-Authentifizierungsereignisse zeigt das stetige Niveau der legitimen Login-Aktivitäten.

Das Diagramm für die Login-Angriffsereignisse ist dagegen nicht annähernd so konsistent. Die Zahlen schwanken stark im Jahresverlauf und zeigen eine anhaltende Angriffskampagne von Mitte Juni bis Mitte September.

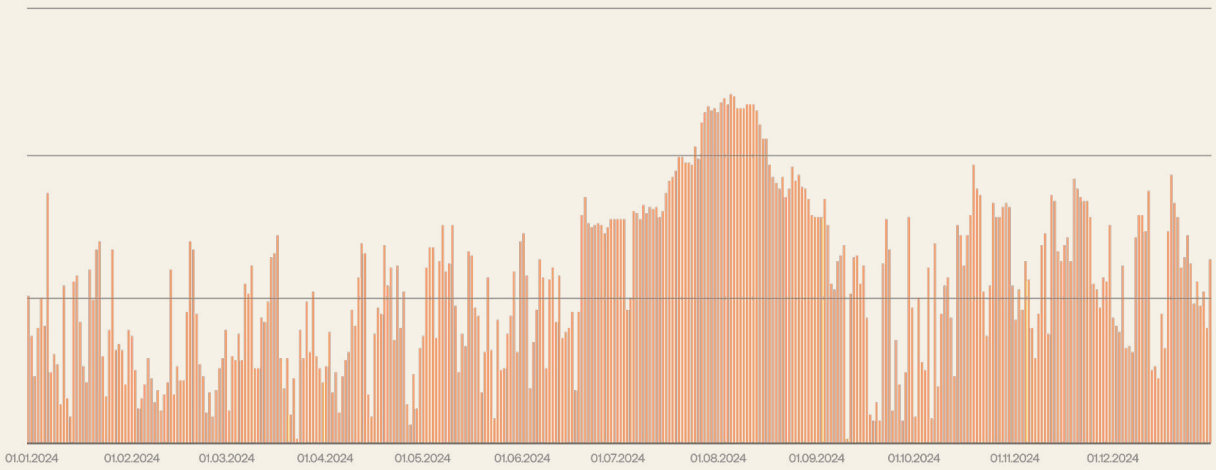
An einem normalen Tag ohne großes schädliches Verhalten überwiegen die echten Ereignisse zur Passwort-Authentifizierung die Login-Angriffsereignisse um etwa 10 zu 1.

Während der längeren Angriffskampagne übertrafen die Login-Angriffe die legitimen Passwort-Authentifizierungen jedoch um mehr als das 62-fache.

Ein genauerer Blick auf die Authentifizierungen im Einzelhandel und E-Commerce



Legitime Passwort-Authentifizierungen, Einzelhandels- und E-Commerce-Sektor, nach Tagen (1. Januar bis 31. Dezember 2024)



Verdächtige schädliche Passwort-Authentifizierungsversuche, Einzelhandels- und E-Commerce-Sektor, nach Tag (1. Januar bis 31. Dezember 2024)

Hinweis: Im Gegensatz zu den meisten anderen Diagrammen in diesem Bericht präsentieren diese beiden Diagramme die absoluten Zahlen (nicht die relativen Anteile). Um den visuellen Vergleich zu erleichtern, nutzen sie denselben logarithmischen vertikalen Zugang, gekürzt um viele Größenordnungen.

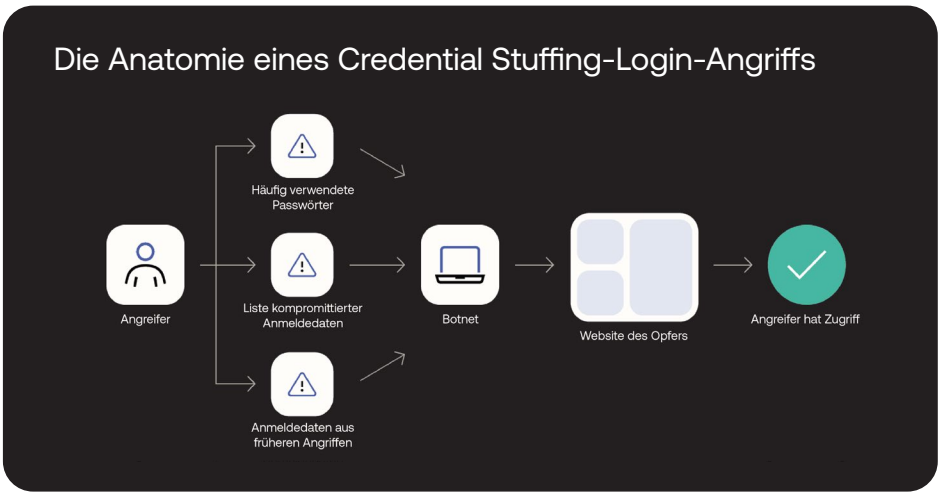
Wie Sie sich vor Login-Angriffen schützen

Login-Angriffe mit Brute-Force – vor allem Credential Stuffing, Password Spraying und Password Guessing – nutzen schlechte Passwortgewohnheiten und -richtlinien aus. Dazu gehören:

- **Mehrfachverwendung von Passwörtern:** Wie bereits erwähnt, geben 68 % der Benutzer zu, dieselben Passwörter für mehrere Konten zu verwenden.
- **Geringfügig abgeänderte Passwörter:** Viele Benutzer, die für jeden Account ein individuelles Passwort erstellen, ändern dabei einen kleinen Satz von Passwörtern jeweils nur leicht ab (z. B. dasselbe Passwort mit einer anderen Zahl am Ende).
- **Kurze Passwörter:** Generell gilt: Je länger ein Passwort ist, desto mehr Aufwand muss ein Angreifer betreiben, um es zu knacken.
- **Lange verwendete Passwörter:** Benutzer, die Passwörter mehrfach verwenden und diese darüber hinaus nie ändern, machen ihren Account anfälliger für Kompromittierungen.

Solche Gewohnheiten reduzieren die Kosten und den Aufwand für die Angreifer ungemein. Schon wenige Optimierungen (z. B. Listen mit bereits gehackten Passwörtern oder Wörterbücher mit Wörtern, die häufig in Passwörtern (oder Passphrasen) verwendet werden) können die Wahrscheinlichkeit, das richtige Passwort auszuprobieren (oder, genauer gesagt, ein Passwort auszuprobieren, das den gleichen Hash-Wert wie das richtige Passwort hat), drastisch erhöhen.

Leider ist die Hürde für Login-Angriffe sehr niedrig und Angreifer wenden verschiedene Taktiken an, um Schutzmaßnahmen zu umgehen. Ein Angreifer kann z. B. bekannte gültige Anmeldedaten – vielleicht von betrügerischen Accounts, die bereits unter seiner Kontrolle stehen – in den Login-Stream einbauen, um die Fehlerquote gezielt zu steuern.



Maßnahmen auf Plattformebene zum Schutz vor Login-Angriffen mit Brute-Force

Hinweis: *Diese Schutzmaßnahmen sollten zusätzlich zu den bereits genannten Maßnahmen gegen Brute-Force-Angriffe angewendet werden.*

Ihre CIAM-Plattform sollte eine Reihe von Schutzfunktionen für die Abwehr von Login-Angriffen bieten. Wie bei Registrierungsangriffen müssen bei der Wahl der richtigen Reaktion auf schädliches Verhalten die Auswirkungen auf legitime Benutzer berücksichtigt werden.

Auch hier sind mehrstufige Lösungen am effektivsten. Und je mehr dieser Techniken Sie implementieren, desto sicherer sind Ihre Kunden und Ihr Unternehmen.

- **Legen Sie fest, dass Benutzer kompromittierte Passwörter ändern müssen.** Sofern eine Funktion zur Erkennung kompromittierter Passwörter (Breached Password Detection) verfügbar ist, sollten Kunden, deren Anmeldedaten online veröffentlicht wurden, zur Passwortrücksetzung gezwungen werden. Dieser Ansatz schützt nicht vor Wörterbuchangriffen, aber diese können gut mit strengeren Brute-Force-Schwellenwerten bekämpft werden.
- **Deaktivieren Sie nicht benötigte und nicht genutzte Funktionen.** Nicht genutzte Endpunkte oder Funktionen können Ihre Angriffsfläche unnötig erweitern und Angreifern die Umgehung von Kontrollen (z. B. Bot-Schutz) ermöglichen. Wenn Sie eine Funktion für Ihre Anwendungsfälle nicht unbedingt benötigen, empfehlen wir ihre Deaktivierung, um Missbrauch durch Angreifer zu vermeiden.
- **Blockieren Sie Logins in Szenarien mit nicht plausiblen Ortsveränderungen.** Blockieren Sie Login-Versuche von Standorten, die in der Zeit seit dem letzten erlaubten Login realistischerweise nicht erreicht werden können.
- **Setzen Sie MFA für kompromittierte Accounts durch.** Dieser Ansatz vermeidet unnötige Reibungspunkte, weil er MFA nur bei Benutzern anwendet, deren Accounts nachweislich kompromittiert wurden.
- **Implementieren Sie adaptive MFA.** Dieser Ansatz vermeidet unnötige Reibungspunkte, weil er MFA-Sicherheitsabfragen nur bei Login-Versuchen anwendet, die eine vordefinierte Risikoschwelle überschreiten.

- **Setzen Sie starke, Phishing-resistente MFA durch.** Favorisieren Sie bei der Einführung von MFA vor allem Authentifikator-Apps und WebAuthn-basierte Methoden. Wenn Sie MFA länger im Einsatz haben, sollten Sie versuchen, bestehende Benutzer zu diesen stärkeren sekundären Faktoren zu migrieren.

Der vielleicht wirksamste Schutz vor passwortbasiertem Account-Hacking ist jedoch die **komplette Abkehr von Passwörtern** – eine Möglichkeit, die durch die neuen Passkeys inzwischen viel realistischer erscheint (insbesondere im Endverbrauchermarkt).

MFA-Missbrauch ist häufig, es gibt aber Anzeichen für einen Rückgang

Bei MFA-Sicherheitsabfragen muss ein Benutzer seine Identität anhand von zwei oder mehr Faktoren nachweisen.

Starke MFA bietet durchaus einen wirksamen Schutz vor Account-Hacking. Dennoch werden MFA-Implementierungen leider routinemäßig von Angreifern missbraucht.

Wie in der Methodik erläutert, gehören zu den in diesem Bericht dargestellten schädlichen MFA-Ereignissen folgende Aktivitäten:

- Versuche, MFA durch Bombing/Fatigue-Angriffe zu umgehen
- Toll Fraud-Versuche, bei denen MFA missbraucht wird, um Telefon- oder SMS-Nachrichten auszulösen
- Fälle, in denen ein Angreifer wiederholt eine MFA-Sicherheitsabfrage nicht beantworten kann
- Fälle, in denen ein legitimer Benutzer wiederholt eine MFA-Sicherheitsabfrage nicht beantworten kann (stellen nur einen winzigen Bruchteil der Ereignisse dar und verfälschen die Analyse nicht)

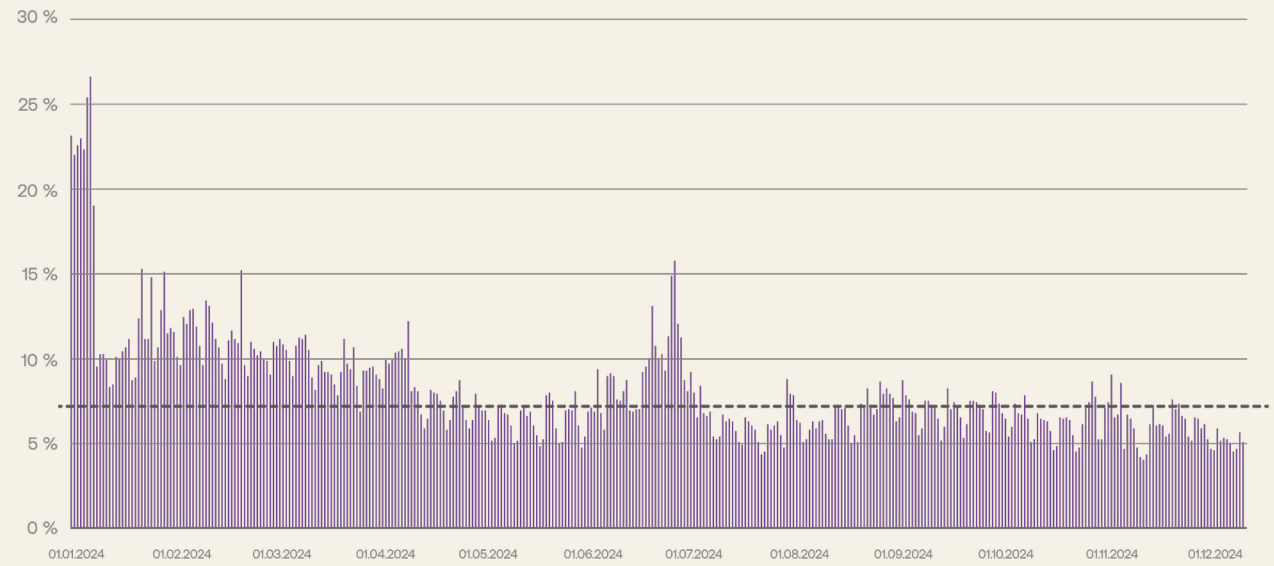
MFA-Missbrauch findet häufig statt...

- 2024 lag der Median der als schädlich erkannten MFA-Ereignisse auf der gesamten Auth0 Platform bei 7,3 %, wobei die Mehrheit wahrscheinlich auf MFA Fatigue-Angriffe und SMS-Pumping (Toll Fraud) zurückgeführt werden kann.

...ist aber möglicherweise auf dem Rückzug

- Zum Kontext: Der Okta The State of Secure Identity Report 2023 zeigt einen mehrjährigen Rückgang bei MFA-Missbrauchs und stellt fest, dass in der ersten Hälfte des Jahres 2023 insgesamt 12,7 % der MFA-Versuche als schädlich eingestuft wurden.
- Im Vergleich dazu lag der Mittelwert für 2024 bei 7,8 % – und fiel in der letzten Jahreshälfte unter 7 %.

Angreifer treffen auf MFA und missbrauchen sie



Verdächtige schädliche MFA-Ereignisse, nach Tag (1. Januar bis 31. Dezember 2024)

Hinweis: Jede Spalte zeigt den Anteil der MFA-Ereignisse an einem bestimmten Tag, die die Kriterien für eine schädliche MFA-Aktivität erfüllten. Die gestrichelte Linie zeigt den Median (7,3 %) dieser täglichen MFA-Ereignisse auf der gesamten Plattform. (Definition eines schädlichen MFA-Ereignisses siehe Methodik.)

Licht, Kamera, Action: Mediensektor am häufigsten von schädlichen MFA-Ereignissen betroffen

Die Aufschlüsselung der schädlichen MFA-Ereignisse nach Branchen zeigt enorme Unterschiede.

Medienunternehmen verzeichnen weiterhin den höchsten Anteil an schädlichen MFA-Ereignissen

- 2024 wiesen mehr als 20 % der MFA-Ereignisse in der Medienbranche schädliche Verhaltensweisen auf.
- Auch im Okta The State of Secure Identity Report 2023 führt die Medienbranche mit 12,8 % die Tabelle an.

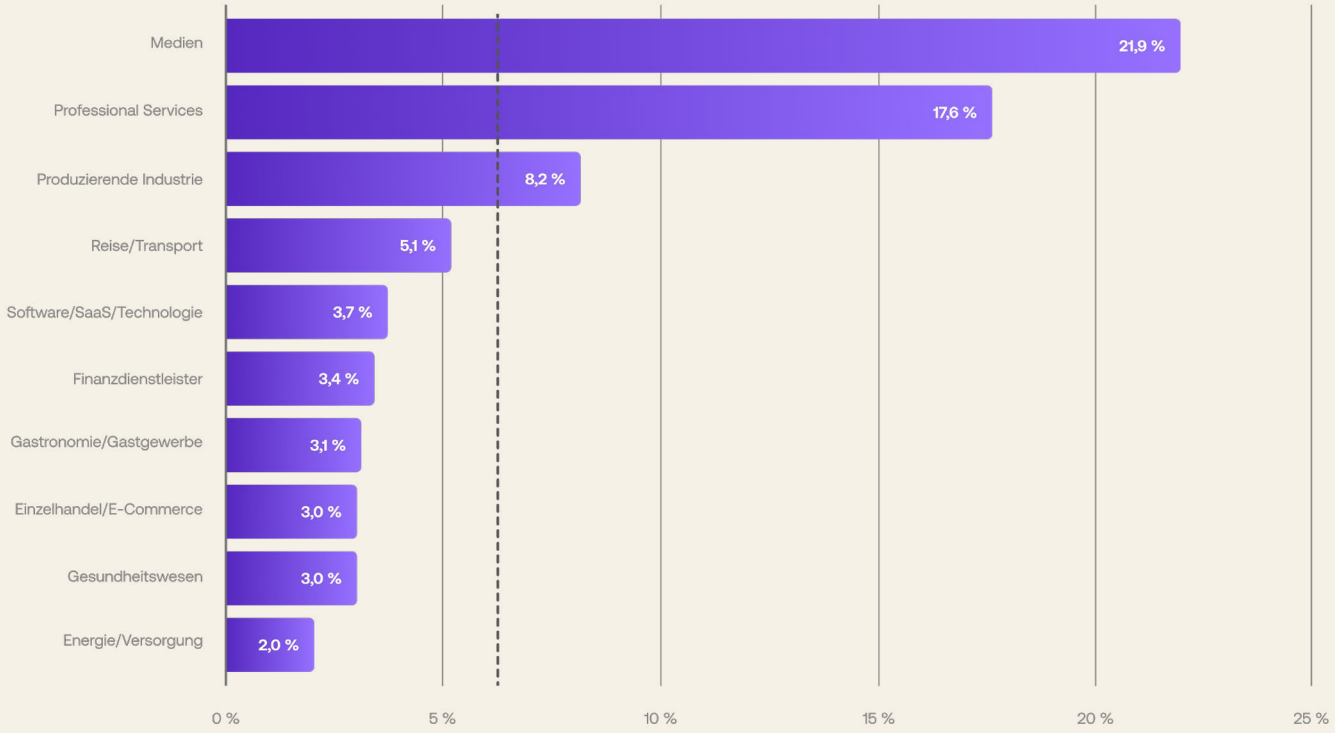
Professional Services- und Industrieunternehmen verzeichnen ebenfalls überdurchschnittlich viele schädliche MFA-Ereignisse.

- Bei Professional Services-Anbietern wurden 17,6 % der MFA-Ereignisse mit schädlichen Verhaltensweisen in Verbindung gebracht.
- Laut dem Okta The State of Secure Identity Report 2023 Okta belegten die Fertigungsunternehmen erneut den dritten Platz. Dabei ist die Quote schädlicher MFA-Ereignisse fast gleich geblieben – 8,2 % im Jahr 2024 gegenüber 7,8 %.

Große Unternehmen verzeichnen den höchsten Anteil an schädlichen MFA-Ereignissen

- 2024 zeigten 11,6 % der MFA-Ereignisse bei großen Unternehmenskunden schädliche Verhaltensweisen – fast doppelt so viel wie der Gesamtdurchschnitt.
- Mittelständische Unternehmen (3,1 %) verzeichneten erneut die niedrigste Missbrauchsquote, kleine Unternehmen (6,0 %) lagen genau im Durchschnitt.

MFA kommt in der Medienbranche auf den Prüfstand



Verdächtige schädliche MFA-Ereignisse, nach Branche (1. Januar bis 31. Dezember 2024)

Hinweis: Jeder Balken zeigt den Median der täglichen MFA-Ereignisse für eine bestimmte Branche, die die Kriterien für eine schädliche MFA-Aktivität im Jahr 2024 erfüllten. Die gestrichelte Linie zeigt den Mittelwert (6,0 %) der täglichen Mediane pro Branche über alle Branchen auf der Auth0 Platform (d. h. nicht nur die Top 10).

Angreifer betreiben ihr Geschäft rund um die Uhr

Werfen wir nun einen genaueren Blick auf die Medienbranche.

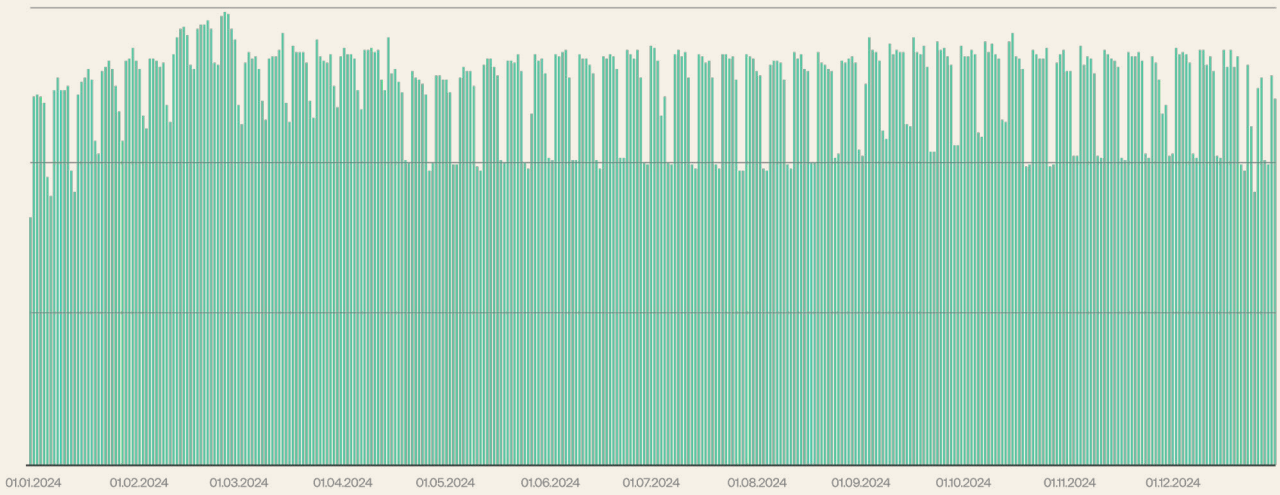
Ein Umstand, der sofort auffällt, ist die offensichtliche Abweichung zwischen Wochentagen und Wochenenden. Tatsächlich folgt auch der Anteil der MFA-Ereignisse, die eindeutig schädliche Verhaltensweisen zeigen, diesem Muster:

- An Wochentagen liegen die Werte durchgehend im Bereich um 25 %.
- An den Wochenenden fallen die Werte unter 10 %.

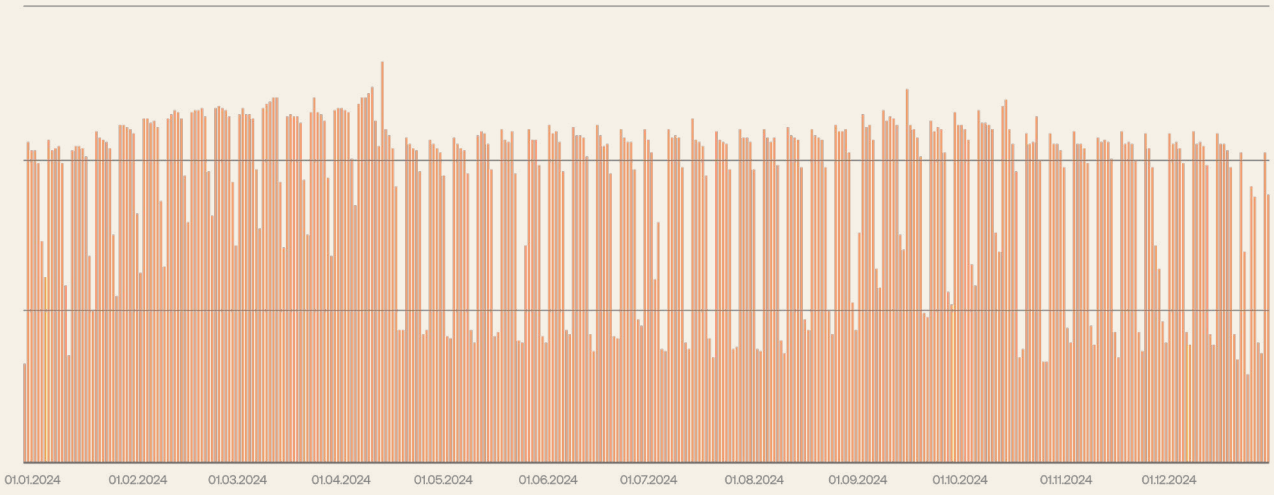
Außerdem – und im Gegensatz zu den oben gezeigten branchenspezifischen Diagrammen – können wir feststellen, dass es keine besonders groß angelegten bzw. lang anhaltenden Angriffe gab.

All dies deutet darauf hin, dass Kunden-Accounts bei Medienunternehmen einer ziemlich konstanten Rate von Login-Angriffen ausgesetzt sind – und dass die MFA-Schutzmechanismen ständig auf Herz und Nieren geprüft werden.

MFA-Ereignisse in der Medienbranche



Legitime MFA-Ereignisse, Mediensektor, nach Tag (1. Januar bis 31. Dezember 2024)



Verdächtige schädliche MFA-Ereignisse, Mediensektor, nach Tag (1. Januar bis 31. Dezember 2024)

Hinweis: Im Gegensatz zu den meisten anderen Diagrammen in diesem Bericht präsentieren diese beiden Diagramme die absoluten Zahlen (nicht die relativen Anteile). Um den visuellen Vergleich zu erleichtern, nutzen sie denselben logarithmischen vertikalen Zugang, gekürzt um viele Größenordnungen.

Wie Sie sich vor MFA-Missbrauch schützen

Angesichts der gefährlichen und sich schnell entwickelnden Bedrohungslandschaft ist es wichtig, dass Ihre MFA diese Anforderungen erfüllt:

- **Sie ist richtig implementiert:** Alle Lücken und Umgehungsmöglichkeiten (z. B. Unterstützung von Legacy-Authentifizierungen oder Umgehung von MFA durch Administratoren) werden früher oder später ausgenutzt.
- **Sie nutzt starke sekundäre Faktoren:** Techniken zur Umgehung der MFA zielen in der Regel auf ältere (z. B. SMS-basierte) Faktoren ab und Brute-Force-Angriffe konzentrieren sich nach wie vor hauptsächlich auf wissensbasierte Authentifizierungsfaktoren. Daher können Besitzfaktoren oder biometrische Faktoren die Wahrscheinlichkeit eines erfolgreichen Brute-Force-Angriffs drastisch verringern.

Wie bereits erwähnt, müssen Technologien, die sich für Consumer-Apps eignen, ein Gleichgewicht zwischen Sicherheit und Benutzerfreundlichkeit finden. Während bei Legacy-Authentifizierungsmethoden früher noch Kompromisse eingegangen werden mussten, ist das heute glücklicherweise immer seltener notwendig:

- **Adaptive MFA** ist eine flexible, erweiterbare MFA-Richtlinie, die Account-Hacking verhindern kann und für echte Benutzer nicht mit weiteren Reibungspunkten verbunden ist. Dazu wird das potenzielle Risiko jeder Login-Transaktion analysiert und der Benutzer nur bei Bedarf zu einer zusätzlichen Verifizierung aufgefordert.
- **Neue MFA-Methoden sind sicherer und komfortabler:** MFA-Methoden, die auf WebAuthn-fähiger Biometrie für Benutzergeräte (z. B. Apple Face ID, Apple Touch ID, Windows Hello) oder WebAuthn-fähigen Sicherheitsschlüsseln (z. B. YubiKey, Feitian, Titan) basieren, bieten gleichzeitig mehr Sicherheit (Angreifer hassen WebAuthn) und Komfort (Umfrageteilnehmer haben Fingerabdruck und Face ID als sehr komfortabel bewertet).

Auch wenn Verbraucher in der breiten Masse wahrscheinlich nie dedizierte Sicherheitsschlüssel nutzen werden, setzen sich biometrische Funktionen in preisgünstigen Geräten zunehmend durch.

KI trifft auf Customer Identity

Die KI-Agenten sind da. Vertrauen die Benutzer ihnen schon bei Entscheidungen und personenbezogenen Daten?

„Ja, da kann ich Ihnen helfen. Wie lautet Ihre Kreditkartennummer?“

Das Debüt von ChatGPT Ende 2022 markierte einen Wendepunkt in der Beziehung zwischen Mensch und künstlicher Intelligenz (KI). Innerhalb weniger Monate kletterte die Zahl der aktiven Benutzer pro Monat auf 100 Millionen. Einen solchen Anstieg hatte es bislang bei keinen anderen neuen Technologie gegeben.

Generative KI (GenAI) wurde zum Standard und die GenAI-Agenten folgten schnell. Diese nicht-menschlichen Identities haben diese Eigenschaften:

- Sie führen Aktionen im Namen von Benutzern und Unternehmen aus
- Sie sind autonom, zielstrebig und nicht an eine Wenn-Dann-Logik gebunden
- Sie benötigen Zugriff auf mehrere Systeme, um ihre Aufgaben zu erfüllen
- Sie werden immer häufiger – laut unserer Umfrage **treffen 37 % der Kunden auf Online-Plattformen oder Websites *sehr häufig* oder *häufig* auf KI-Agenten**

KI-Agenten bieten enorme Vorteile, benötigen für ihre Aktionen aber sensible, wertvolle und möglicherweise sogar vertrauliche Informationen von Unternehmen und Verbrauchern.

Vor allem aber sind sie auf Vertrauen angewiesen.

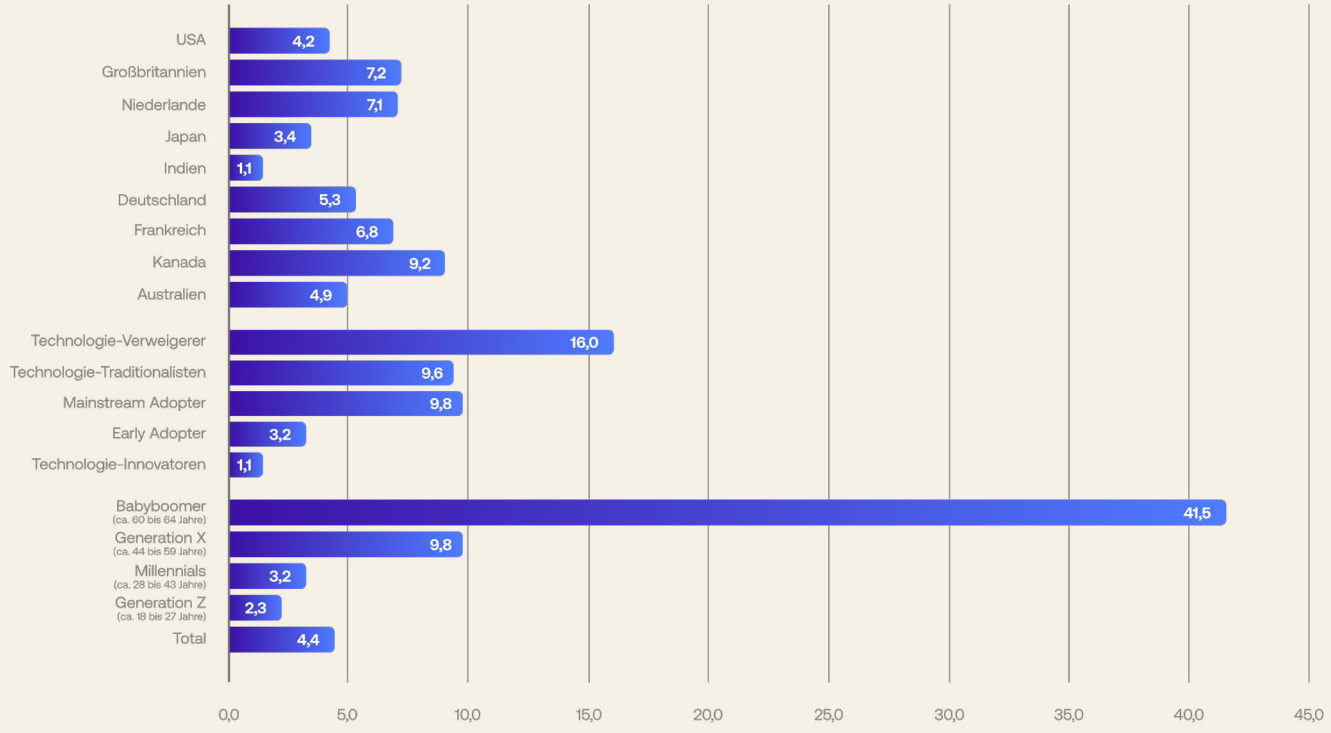
KI-Agenten haben die Menschen (noch) nicht überzeugt

Die ständige Verfügbarkeit und unendliche Skalierbarkeit von KI-Agenten macht sie sehr attraktiv für Unternehmen, die sich eine profitable Kombination aus gutem Kundenservice und weniger Kosten wünschen.

Aber: Sind die Benutzer für diese schöne neue Welt schon bereit oder ziehen sie es vor, die Dinge auf altmodische Weise zu regeln – durch Interaktion mit einem Menschen?

Eine einfache Frage, von deren Antwort viel abhängt.

Die meisten Benutzer bevorzugen Menschen



Verhältnis zwischen Benutzern, die Interaktionen mit menschlichen Agenten gegenüber KI-Agenten bevorzugen, alle Kohorten

„Welche der folgenden Antworten beschreibt Ihre Präferenz für die Interaktion mit dem KI-Agenten eines Unternehmens gegenüber einem menschlichen Vertreter am besten?“

Benutzer bevorzugen stark und generell die Interaktion mit Menschen gegenüber KI-Agenten

Über alle Befragten hinweg äußerten 86 % eine Präferenz für die eine oder andere Variante, wobei 70 % Interaktionen mit Menschen und 16 % die KI bevorzugten – ein Verhältnis von 4,4 zu 1. Tatsächlich bevorzugte jede in dieser Studie untersuchte Kohorte Interaktionen mit einem Menschen gegenüber dem KI-Agenten eines Unternehmens.

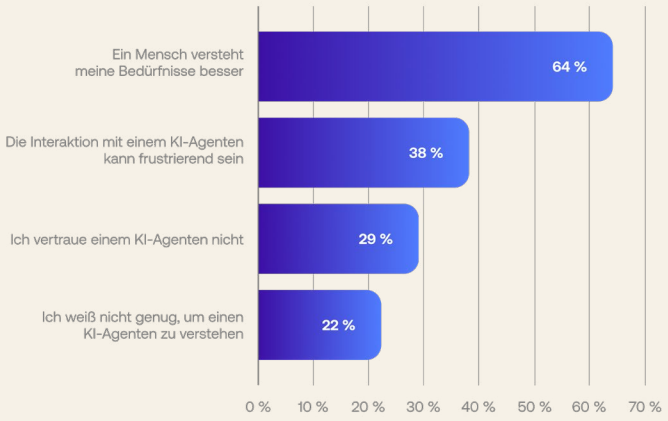
Alter der Befragten und Aufgeschlossenheit gegenüber neuen Technologien beeinflussen die Präferenzen

Technologie-Innovatoren bevorzugen Menschen in einem Verhältnis von 1,1, Technologie-Verweigerer 16 Mal häufiger. Analog bevorzugen Generation Z-Benutzer Interaktionen mit einem Menschen im Verhältnis von nur 2,3, während bei den Babyboomern 83 % Menschen und nur 2 % KI-Agenten bevorzugen. Das entspricht einem Verhältnis von 41,5!

Präferenzen in allen Ländern recht einheitlich

Befragte aus Indien (die Menschen im Verhältnis 1,1 bevorzugen) und Kanada (9,2) nehmen als Ausreißer die Positionen an beiden Enden der Ländertabelle ein – die übrigen sieben Länder liegen alle zwischen 3,4 (Japan) und 7,2 (Großbritannien).

Warum Benutzer menschliche Hilfe bevorzugen

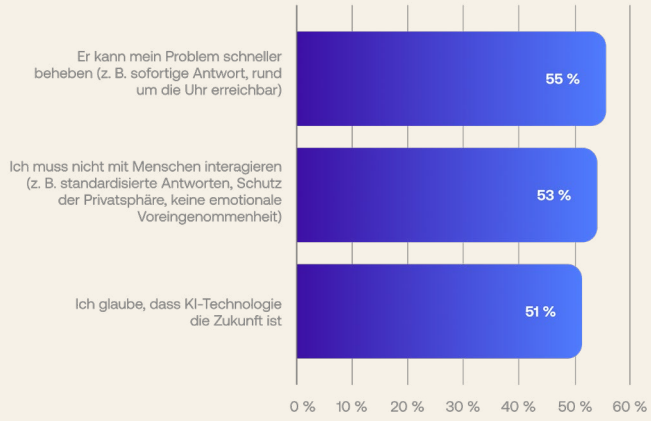


Gründe für die bevorzugte Interaktion mit Menschen, alle Befragten

„Aus welchen Gründen ziehen Sie es vor, mit einem Menschen zu kommunizieren?“

Hinweis: Die Frage wurde nur Befragten gestellt, die es vorziehen, mit menschlichen Vertretern eines Unternehmens zu interagieren.

Warum Benutzer KI-Agenten bevorzugen



Gründe für die Bevorzugung von Interaktionen mit KI-Agenten eines Unternehmens, alle Befragten

„Aus welchen Gründen ziehen Sie es vor, mit KI-Agenten zu kommunizieren?“

Hinweis: Die Frage wurde nur Befragten gestellt, die es vorziehen, mit KI-Agenten eines Unternehmens zu interagieren.

Benutzer bevorzugen Menschen vor allem, weil sie ihre Bedürfnisse verstehen
Fast zwei Drittel der Befragten (64 %), die Interaktionen mit Menschen bevorzugen, gaben an, dass „*ein Mensch meine Bedürfnisse besser versteht*“. Für Unternehmen, die KI-Agenten einführen, stellt dies zumindest kurzfristig eine potenzielle Hürde dar.

Frustrierende User Experiences und mangelndes Vertrauen in KI-Agenten tragen ebenfalls zur Präferenz für menschliche Vertreter bei
38 % der Benutzer gaben an, dass „*die Interaktion mit einem KI-Agenten frustrierend sein kann*“ und 29 % vertrauen KI-Agenten einfach nicht. Diese Hindernisse lassen sich (zumindest theoretisch) mit einer effizienten und transparenten Implementierung überwinden.

Benutzer, die KI-Agenten bevorzugen, verweisen auf schnellere Lösungen, den Wegfall der menschlichen Interaktion und den Glauben an den Fortschritt
Interessanterweise gab es keinen einzigen Grund, der sich statistisch gesehen als häufigster Grund dafür herausstellte, dass manche Benutzer Interaktionen mit KI-Agenten bevorzugen.

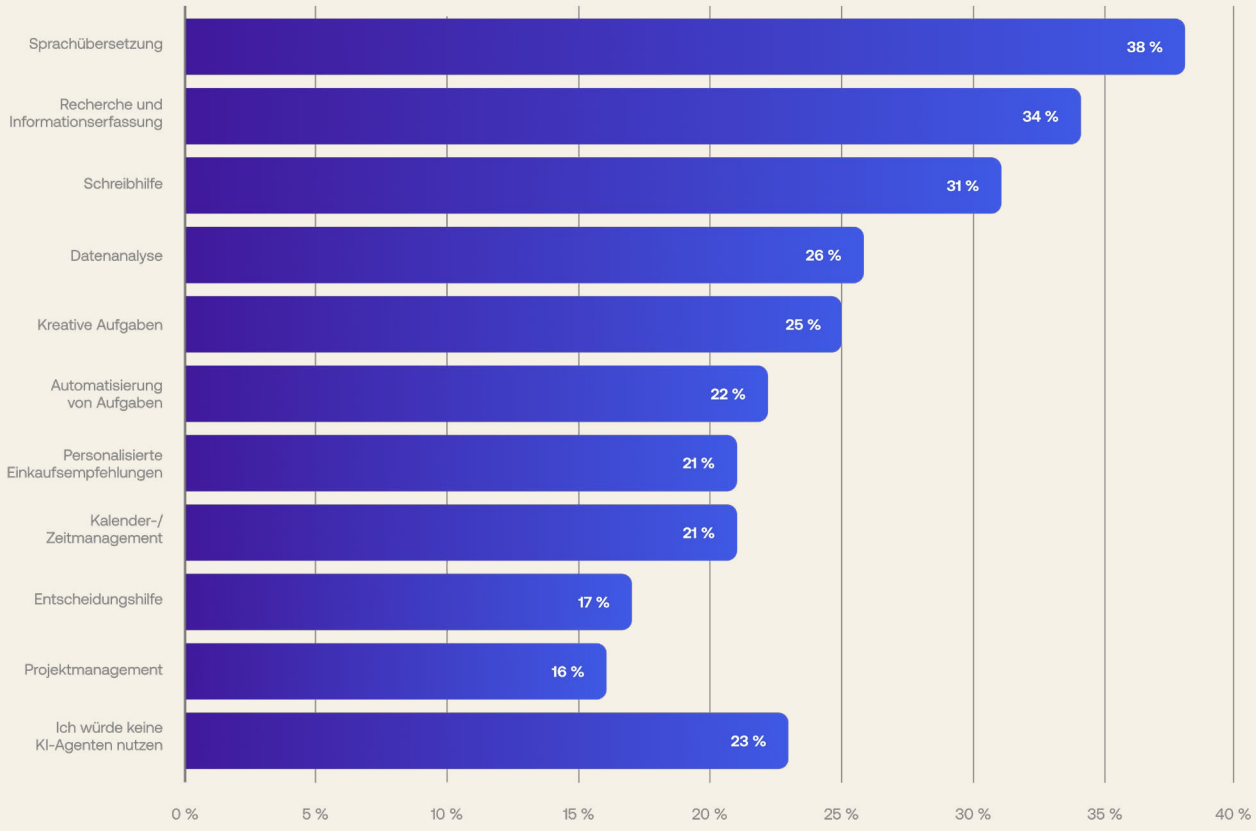
- 55 % verwiesen auf schnellere Problemlösungen – einschließlich der Rund-um-die-Uhr-Verfügbarkeit automatisierter Systeme.
- 53 % gaben an, dass sie Interaktionen mit Menschen lieber vermeiden – zumindest dann, wenn eine standardisierte Antwort bevorzugt wird oder Bedenken hinsichtlich des Schutzes der Privatsphäre oder emotionaler Voreingenommenheit bestehen.
- 51 % sind entschlossen, mit der Zeit zu gehen, und sehen in der KI-Technologie die Zukunft.

Fachkraft, aber nicht Entscheider: Die Vertrauens-kurve der KI-Agenten

Die potenziellen Anwendungen für KI-Agenten sind scheinbar grenzenlos – aber nur, wenn die Kunden auch bereit sind, sie zu nutzen.

Leider scheinen die Benutzer nicht nur zu zögern, KI-Agenten mit Aufgaben oder Aktivitäten in ihrem Namen zu betrauen, auch das Maß an Vertrauen variiert von Aufgabe zu Aufgabe.

KI-Agenten: Aufgabe für Aufgabe Vertrauen gewinnen



Vertrauen in KI-Agenten, nach Aufgabe, alle Befragten

„Bei welchen alltäglichen Aufgaben oder Tätigkeiten nutzen Sie KI-Agenten oder würden Sie sie nutzen?“

Hinweis: Die Option „Ich würde keine KI-Agenten nutzen“ hat alle anderen Optionen ausgeschlossen.

Benutzer stehen KI-Agenten nach wie vor skeptisch gegenüber

Bevor wir uns die spezifischen Aufgaben ansehen, für die Kunden KI-Agenten nutzen würden, soll erwähnt werden, dass die häufigste Antwort der Befragten (Sprachübersetzung) nur von 38 % der Benutzer gewählt wurde – was auf ein Zögern oder eine Skepsis seitens der Kunden schließen lässt.

Benutzer verwenden KI-Agenten eher für regelbasierte Aufgaben und solche, die als lästig empfunden werden

Die vier Aufgaben, für die Benutzer am ehesten KI-Agenten nutzen würden (Sprachübersetzung, Recherche, Schreibhilfe und Datenanalyse), sind alle eher mühsam und objektiv – ähnlich wie bei der traditionellen Nutzung von Computern.

Benutzer verwenden KI-Agenten weniger wahrscheinlich für subjektive und persönliche Aufgaben

Am anderen Ende des Spektrums zeigten die Benutzer vergleichsweise wenig Interesse daran, dass KI-Agenten Aufgaben aus dem persönlichen Verantwortungsbereich übernehmen, z. B. kreative Aufgaben, personalisierte Einkaufsempfehlungen, Kalender-/Zeitmanagement und Entscheidungshilfe.

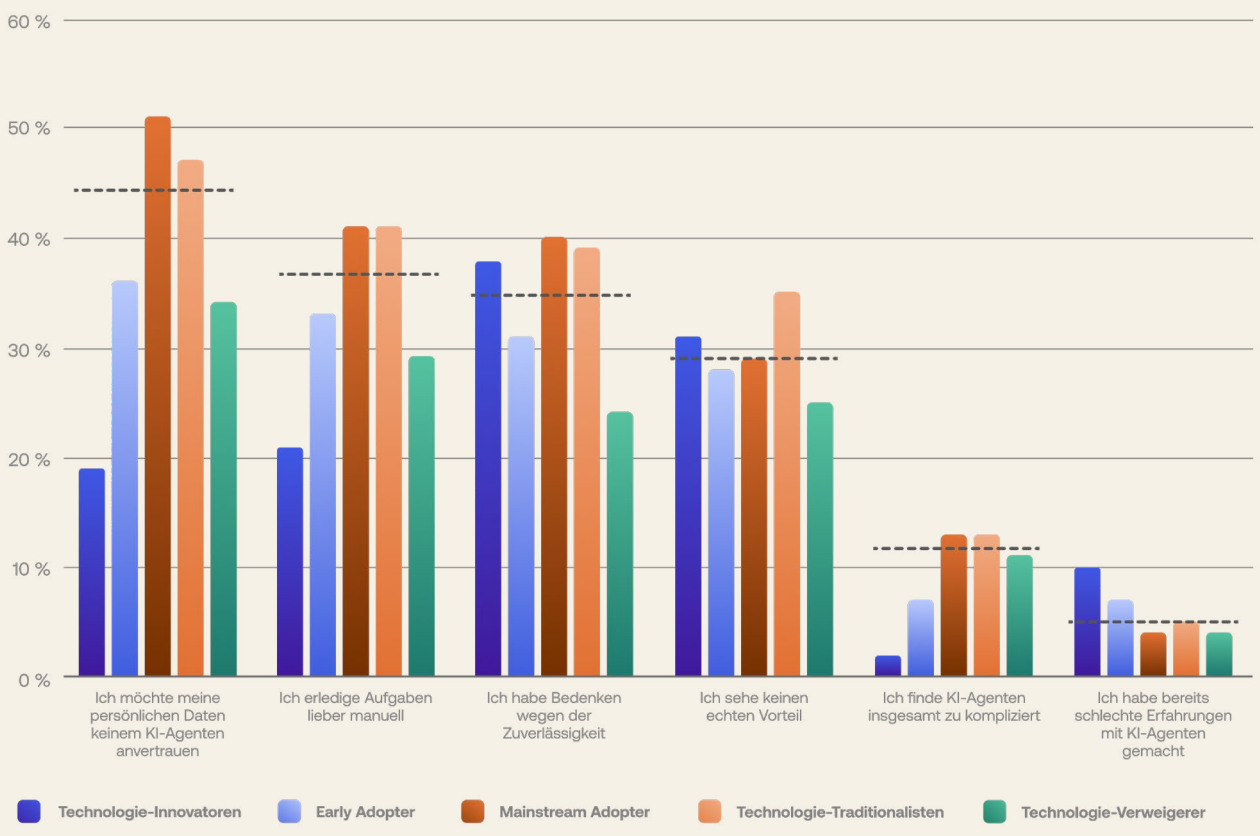
Die Vertrauens-lücke zwischen Benutzern und KI-Agenten

Im Diagramm auf der vorherigen Seite sehen wir, dass **fast ein Viertel der Benutzer nicht die Absicht hat, KI-Agenten zu nutzen**, wobei 23 % der Befragten die alle anderen Optionen ausschließende Option „*Ich würde keine KI-Agenten nutzen*“ wählten.

Für diesen Wert waren vor allem die Generation X (32 %), die Babyboomer (42 %), die Technologie-Traditionalisten (43 %), die Technologie-Verweigerer (bemerkenswerte 73 %) und die Befragten aus Japan (37 %) verantwortlich.

Die Gründe für diese Antworten können Unternehmen Aufschluss über die Strategien geben, die sie bei der Einführung von KI-Agenten und den begleitenden Schulungsmaßnahmen anwenden sollten.

Bis zur Nutzung der KI-Agenten durch die Kunden ist es noch ein weiter Weg



Gründe für die Ablehnung von KI-Agenten, nach Aufgeschlossenheit des Befragten gegenüber neuen Technologien

„Aus welchen Gründen würden Sie KI-Agenten nicht nutzen?“

Hinweis: Die Frage wurde nur Befragten gestellt, die die Antwort „Ich würde keine KI-Agenten nutzen“ gewählt haben. Die gestrichelten Linien zeigen den Mittelwert aller Befragten.

Bei Kunden, die keine KI-Agenten nutzen würden, ist mangelndes Vertrauen das größte Hindernis

Kunden, die keine KI-Agenten nutzen (44 % der Befragten), begründen dies meist mit „*Ich vertraue meine persönlichen Daten keinem KI-Agenten an*“.

Bedenken wegen der Zuverlässigkeit sind ein weiteres Hindernis

Mehr als ein Drittel (35 %) der Kunden, die keine KI-Agenten nutzen wollen, äußerten Bedenken wegen ihrer Zuverlässigkeit. Dieses Problem dürfte sich mit dem demografischen Wandel und immer ausgereifteren Implementierungen im Laufe der Zeit verringern.

Die gute Nachricht für Service Provider: Komplexität und schlechte Erfahrungen sind im Grunde kein Thema mehr

Während die von den Kunden genannten Hauptgründe für die Ablehnung von KI-Agenten eher spekulativ sind, zeigt die Umfrage ganz konkret, dass vergleichsweise wenige Benutzer KI-Agenten als zu komplex empfinden oder schlechte Erfahrungen gemacht haben.

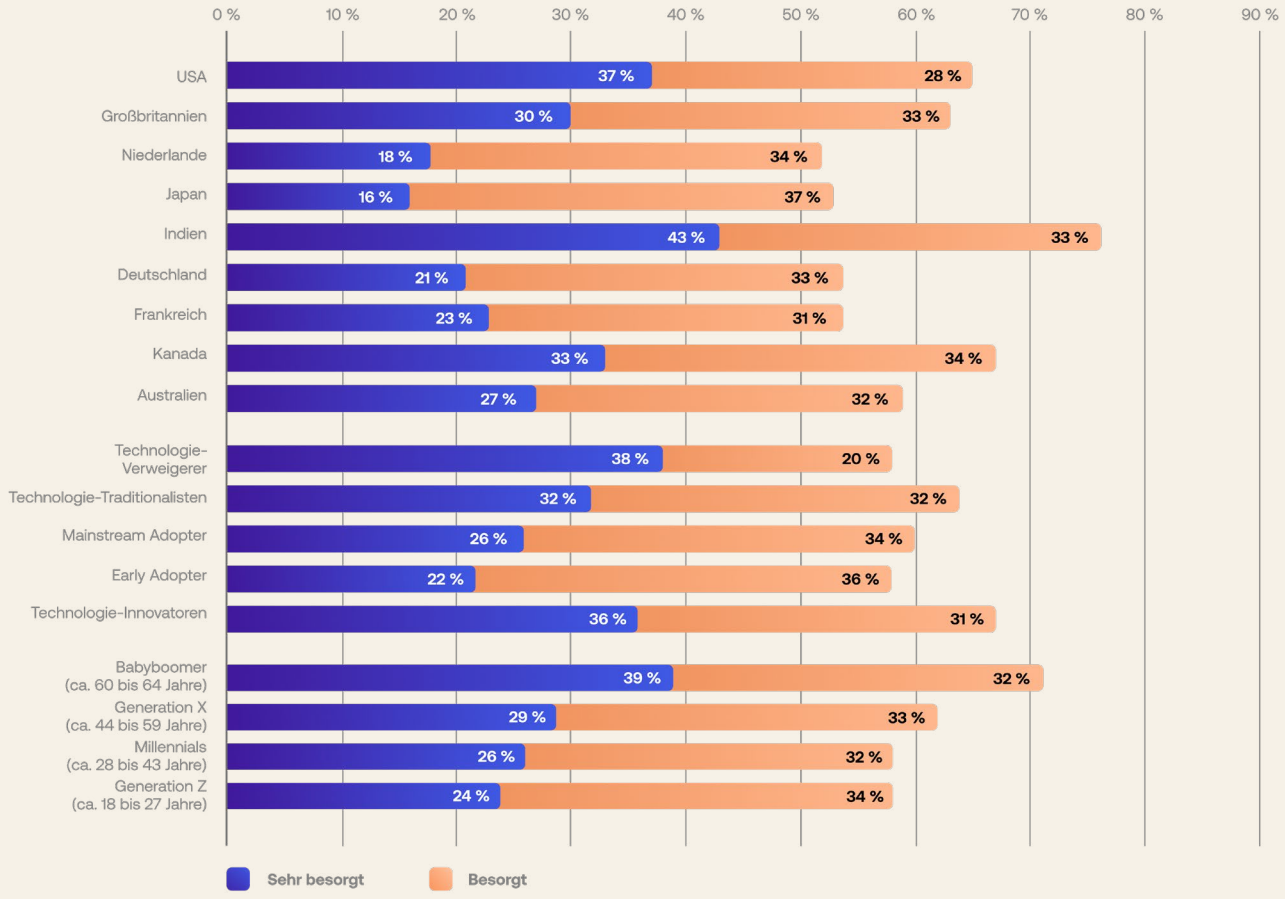
Eine universelle Sorge: Auswirkungen von KI auf Datenschutz und Sicherheit

Wie wir gesehen haben, lehnen einige Benutzer KI-Agenten wegen Datenschutzbedenken ab. An dieser Stelle muss jedoch darauf hingewiesen werden, dass solche Bedenken zwar kein K.O.-Kriterium, aber dennoch weit verbreitet sind.

Die Mehrheit der Benutzer ist besorgt: Ganze 60 % der Befragten gaben an, dass sie über die Auswirkungen von KI auf den Datenschutz und die Sicherheit ihrer digitalen Identitäten sehr besorgt oder besorgt sind. Im Gegensatz dazu gaben nur 9 % der Befragten an, wenig oder gar keine Bedenken zu haben.

Diese Bedenken sind universell: Es gibt zwar gewisse Unterschiede, aber jede in dieser Studie untersuchte Kohorte äußerte mehrheitlich Besorgnis.

Kohortenübergreifend überwiegen Bedenken wegen Datenschutz und Sicherheit bei KI



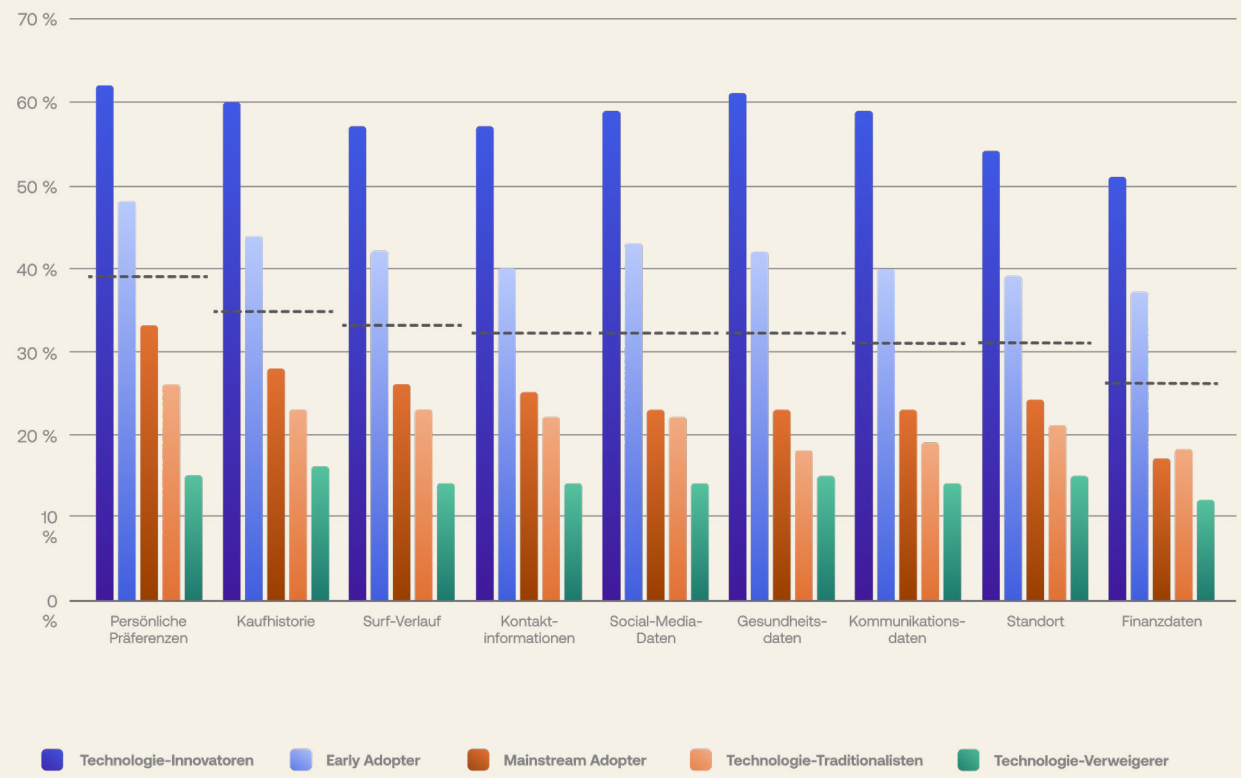
Sorgen über die Auswirkungen von KI auf Datenschutz und die Sicherheit digitaler Identities, alle Kohorten

„Wie besorgt sind Sie wegen der Auswirkungen von KI auf den Datenschutz und die Sicherheit Ihrer digitalen Identitäten?“

Die Bereitschaft der Benutzer, personenbezogene Daten gegenüber KI-Agenten preis-zugeben, ist sehr unterschiedlich ausgeprägt

Langfristig gesehen steckt der Unterstützungswert der KI noch in den Kinderschuhen. Für viele Anwendungsfälle benötigt der KI-Agent jedoch Zugang zu personenbezogenen Daten – und muss den Benutzer danach fragen oder um seine Zustimmung bitten, auf bereits im Unternehmen gespeicherte Daten des Benutzers zugreifen zu dürfen.

Die Bereitschaft, Informationen gegenüber KI-Agenten preiszugeben, schwankt



Wahrscheinlichkeit, personenbezogene Informationen gegenüber KI-Agenten preiszugeben, nach Aufgeschlossenheit der Befragten gegenüber neuen Technologien (Summe der Antworten „Sehr wahrscheinlich“ und „Wahrscheinlich“)

„Wie wahrscheinlich ist es, dass Sie dem KI-Agenten eines Unternehmens verschiedene Arten personenbezogener Informationen zur Verfügung stellen?“

Hinweis: Die gestrichelten Linien zeigen den Mittelwert aller Befragten.

Im Großen und Ganzen halten es die Benutzer für unwahrscheinlich, dass sie personenbezogene Informationen gegenüber einem KI-Agenten eines Unternehmens preisgeben

Sogar persönliche Präferenzen (wie die Lieblingsfarbe oder das Lieblingsteam im Sport) – die harmloseste der neun verfügbaren Optionen – werden nur von 39 % der Befragten *sehr wahrscheinlich* oder *wahrscheinlich* preisgegeben.

Die Wahrscheinlichkeit variiert stark nach Alter und Aufgeschlossenheit gegenüber neuen Technologien

Wie das Diagramm anschaulich zeigt, korreliert die Wahrscheinlichkeit, personenbezogene Informationen gegenüber KI-Agenten eines Unternehmens preiszugeben, stark mit der Aufgeschlossenheit gegenüber neuen Technologien. Ein ähnliches, wenn auch weniger extremes Muster lässt sich generationenübergreifend erkennen.

Befragte aus Indien sind signifikante Ausreißer

Bei allen neun Arten personenbezogener Daten ist die Wahrscheinlichkeit, dass Befragte aus Indien diese an KI-Agenten eines Unternehmens weitergeben, fast doppelt so hoch wie bei Befragten aus anderen Ländern.

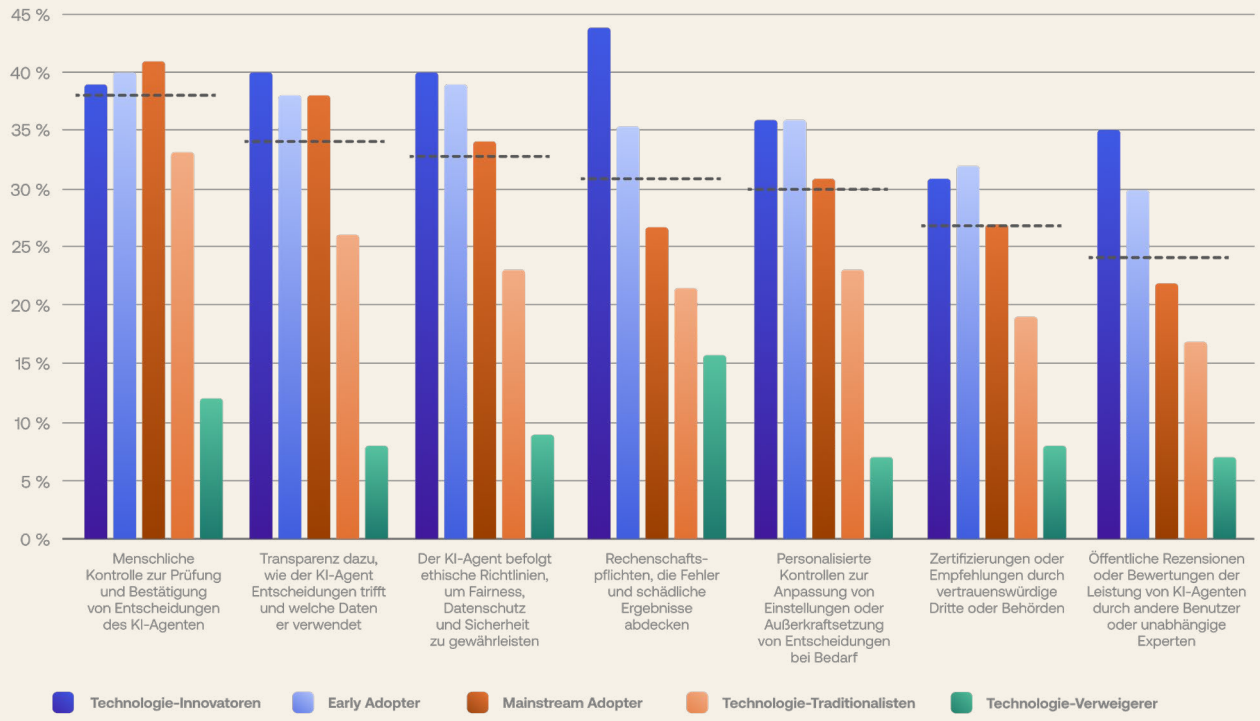
Vertrauen ist das fehlende Puzzleteil bei den heutigen KI-Agenten

Gegenseitiges Vertrauen ist bei Parteien ohne eine gemeinsame Vergangenheit nicht die Norm, sondern muss im Laufe der Zeit immer wieder verdient werden.

KI-Agenten sind aber neu – und zumindest für einige Menschen noch komplettes Neuland, sodass sich viele erst noch eine Meinung bilden müssen.

Was können Unternehmen tun, um eine Basis für Vertrauen zu schaffen?

Möglichkeiten für den Aufbau von Vertrauen in KI-Agenten



Faktoren, die das Vertrauen in KI-Agenten verbessern würden, nach Aufgeschlossenheit der Befragten gegenüber neuen Technologien

„Was würde Ihr Vertrauen in KI-Agenten verbessern, damit sie in Ihrem Namen handeln oder Entscheidungen treffen dürfen?“

Hinweis: Die gestrichelten Linien zeigen den Mittelwert aller Befragten.

Kunden wollen von Menschen auf dem Laufenden gehalten werden

38 % der Befragten gaben an, dass eine menschliche Aufsichtsperson, die die Entscheidungen der KI-Agenten prüft oder bestätigt, mehr Vertrauen schaffen würde. Tatsächlich war diese Option bei 14 der 18 untersuchten demografischen Gruppen die häufigste Wahl.

Transparenz, ethisches Verhalten und Rechenschaftspflichten sind ebenfalls beliebte Elemente, die Vertrauen schaffen

Die Beliebtheit dieser Auswahlmöglichkeiten zeigt, dass die Frage, wie KI-Agenten Entscheidungen treffen und welche Rechtsmittel ggf. zur Verfügung stehen, viele Benutzer interessiert.

Generation Z-Kunden schätzen Ethik über alles

Generation Z war die einzige Altersgruppe, bei der die menschliche Kontrolle nicht ganz oben auf der Liste stand. Stattdessen führte mit 37 % Zustimmung die Antwort „*Der KI-Agent befolgt ethische Richtlinien, um Fairness, Datenschutz und Sicherheit zu gewährleisten*“.

Absicherung von KI-Agenten von Anfang an

Wenn es um Interaktionen mit KI-Agenten geht, haben Benutzer eindeutig Vertrauensprobleme. Bei vielen lassen sich diese Probleme wahrscheinlich auf Bedenken über die Weitergabe personenbezogener Daten sowie auf das allgegenwärtige Problem des Identity-Betrugs zurückführen.

Diese Vertrauensprobleme sind nicht unbegründet, denn leider bleibt in der Eile, mit der KI-Agenten bereitgestellt werden, die Sicherheit auf der Strecke:

- Anwendungen wie Chatbots oder KI-Agenten, die GenAI nutzen, verwenden für die Benutzerinteraktion und -authentifizierung andere Muster als für Webanwendungen und Mobilgeräte-Apps.
- Da die Entwickler ihre KI-Agenten so schnell wie möglich an den Start bringen müssen, werden KI-Anwendungen ohne Identitäts- und Zugriffsmanagement (IAM) entwickelt und bereitgestellt.

Versäumnisse oder Nachlässigkeiten können aber dazu führen, dass KI-Agenten auf die falschen Daten zugreifen und sensible Prozesse einleiten, für die sie eigentlich nicht vorgesehen sind. Sollte ein Angreifer einen Weg finden, die Kontrolle zu übernehmen, ist das Missbrauchspotenzial immens.

Hinzu kommt, dass sich der Schutz dieser KI-Agenten nach ihrer Inbetriebnahme noch viel schwieriger gestaltet. Damit Entwickler ihre KI-Agenten von Anfang absichern können, haben wir vier kritische Anforderungen formuliert, bei denen das Identity-Management entscheidend ist. Diese Anforderungen sind zwar nicht neu, aber bei GenAI-Anwendungen besonders relevant.

Authentifizierung

Damit KI-Agenten sicherer arbeiten können, müssen sie wie jede andere Anwendung Benutzer authentifizieren können.

Der Agent muss prüfen, wer der Benutzer ist, bevor er Datenzugriff gewährt oder Entscheidungen trifft. Dies könnte bedeuten, dass die Identität eines Kunden überprüft wird, bevor ein Kauf bestätigt wird, oder dass die Anmeldedaten eines Patienten überprüft werden, bevor der Agent auf medizinische Akten zugreifen kann.

Wie bei jeder anderen Anwendung muss die Authentifizierung nahtlos und sicher erfolgen.

Aufruf von APIs

KI-Agenten nutzen APIs, um im Namen der Benutzer mit Anwendungen und Backend-Systemen zu interagieren.

Ohne strenge Identity-Kontrollen könnten KI-Agenten auf falsche APIs zugreifen, vertrauliche Daten an nicht autorisierte Quellen weitergeben oder gar nicht in der Lage sein, Aufgaben im Namen von Benutzern auszuführen.

Um solche Funktionen sicher zu implementieren, müssen die Access Token für die KI-Agenten verschlüsselt und geschützt werden – und sie dürfen nicht fest codiert sein.

Asynchrone Benutzerbestätigung

Im Gegensatz zu herkömmlichen Anwendungen oder menschlichen Kundendienstmitarbeitern erledigen KI-Agenten Aufgaben nicht immer sofort. Einige Aktionen (z. B. Datenverarbeitung, Transaktionsgenehmigungen oder Entscheidungen) können Minuten, Stunden oder sogar Tage dauern, sodass der KI-Agent eine Aufgabe möglicherweise noch lange nach Ende der eigentlichen Session bearbeiten muss.

Die heutigen Sicherheitssysteme sind jedoch nicht für langwierige, asynchrone Arbeitsabläufe konzipiert. Die Absicherung von KI-Agenten erfordert einen Ansatz, bei dem sie die betreffende Aufgabe just-in-time authentifizieren können, ohne Angreifern Tür und Tor zu öffnen.

Autorisierung

Nicht jeder KI-Agent sollte die gleichen Berechtigungen haben – einige sollten nur Daten abrufen, andere sollten Befehle ausführen und wieder andere sollten risikoreiche Entscheidungen treffen (z. B. einen Kredit genehmigen oder eine Erstattung bearbeiten).

Ohne die richtigen Zugriffskontrollen könnten KI-Agenten jedoch ihre Grenzen überschreiten.

Genau wie menschliche Benutzer sollten auch KI-Agenten nur die Berechtigungen erhalten, die sie tatsächlich benötigen – und nicht mehr. Diese detaillierten Berechtigungen müssen dynamisch aktualisiert werden, um veränderten Geschäftsregeln, Compliance-Anforderungen und Risikostufen Rechnung zu tragen.

Fazit

Vertrauen aufbauen und Schritt mit den Kundenbedürfnissen halten

Je mehr sich die Dinge ändern...

Die Technologie entwickelt sich rasant weiter und bietet neue Verfahren zur Bereitstellung von Anwendungen, stärkere Methoden zum Schutz dieser Dienste sowie – leider – böswilligen Akteuren mehr und kostengünstigere Möglichkeiten, Kunden und Unternehmen das Leben schwer zu machen.
Es gibt aber auch Konstanten in dieser Welt der Veränderungen: Kunden wollen komfortable und sichere User Experiences, legen Wert auf den Schutz ihrer Daten und schätzen die Flexibilität sowie das Verständnis, die nur Menschen bieten können.

Vertrauenswürdige und komfortable User Experiences

Moderne Authentifizierungsmethoden – darunter Passkeys, Social Logins, Biometrie, adaptive MFA und Step-up-Authentifizierung – ermöglichen komfortable und sichere Registrierungs- bzw. Login-Experiences. In Verbindung mit einem zurückhaltenden Ansatz bei der Erfassung von First-Party- und Zero-Party-Daten – und einer transparenten Kommunikation, warum personenbezogene Daten benötigt, wie sie verwendet und wie sie geschützt werden – können diese modernen Ansätze die Bedenken der Kunden im Zusammenhang mit Identity-Betrug zerstreuen.

Schutz vor gängigen Identity-Bedrohungen

Die häufigsten und umfangreichsten Identity-basierten Angriffe richten sich gegen ältere, anfällige Authentifizierungsformen, insbesondere Passwörter und ältere MFA-Techniken. Die einfachste und effektivste Möglichkeit, Ihre Anwendungen zu schützen, besteht ganz praktisch in der Einführung – und Durchsetzung – einer Phishing-resistenten Authentifizierung mit Passkeys und biometrischen Verfahren. Wie bereits erwähnt, besteht das Ziel nicht darin, Ihre Registrierungs- und Anmeldevorgänge zu 100 % vor Missbrauch zu schützen, sondern den Missbrauch so schwer zu machen, dass Angreifer sich leichtere Ziele suchen.

Sichere Einführung von KI-Agenten

Im besten Fall stehen die Kunden den KI-Agenten skeptisch gegenüber – eine Haltung, die vor allem durch die Sorge um den Datenschutz und einen wahrgenommenen Mangel an Optionen geprägt wird, wenn der Agent etwas Falsches oder Unerwartetes macht. Bei der Einführung solcher Funktionen muss Sicherheit von Anfang an an erster Stelle stehen. Achten Sie besonders auf die IAM-Aspekte, da KI-Agenten neuen und ungewohnten Interaktions- und Authentifizierungsmustern folgen, und informieren Sie Ihre Benutzer darüber, wie Sie Ihre KI-Agenten unter besonderer Berücksichtigung der Sicherheit entwickelt haben. Last but not least sollten Sie auch den Wert menschlicher Mitarbeiter nicht außer Acht lassen. Wenn die Umfrage eines deutlich gezeigt hat, dann dass die Benutzer immer noch Wert auf eine menschliche Beziehung legen.

Methodik

So haben wir diesen Bericht erstellt

Diese Ausgabe des Customer Identity Trends Reports stützt sich auf zwei primäre Datenquellen:

1. Eine weltweite Umfrage unter Verbrauchern
2. Operative Telemetriedaten der Auth0 Platform

Verbraucher-umfrage

Statista hat im Auftrag von Auth0 eine weltweite Umfrage unter 6.750 Verbrauchern durchgeführt, von denen jeweils 750 aus neun Ländern stammten: Australien, Deutschland, Frankreich, Großbritannien, Indien, Japan, Kanada, Niederlande und USA.

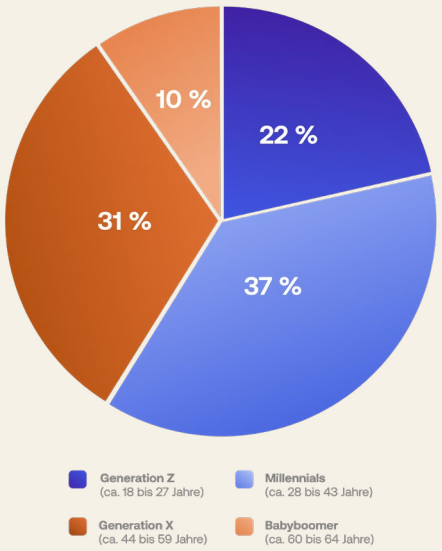
Die Daten wurden im Februar 2025 über eine E-Mail-Einladung und eine Online-Umfrage erhoben. Alle Teilnehmer waren mindestens 18 Jahre alt.

In diesem Report bezeichnen wir diese Umfrage als „unsere Umfrage“ bzw. „die Umfrage“ und die Personen, die die Umfrage abgeschlossen haben, als „Umfrageteilnehmer“ oder „Befragte“.

Mit dem Begriff „Kohorten“ beziehen wir uns auf Gruppen von Befragten mit einem gemeinsamen Merkmal:

- Land des Wohnsitzes (neun Kohorten);
- Alter/Generation (vier Kohorten) oder
- Aufgeschlossenheit gegenüber neuen Technologien (fünf Kohorten).

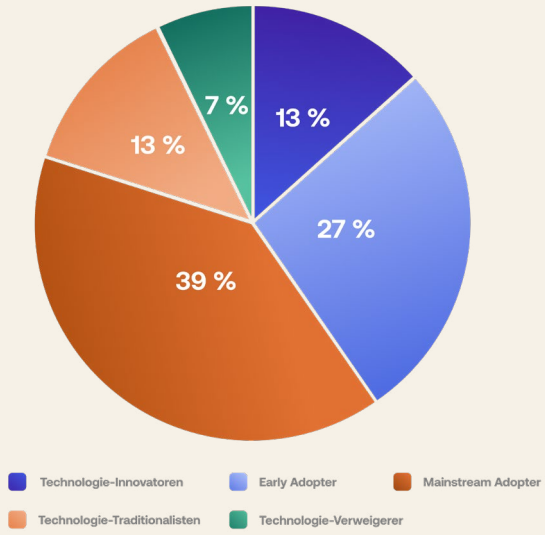
Befragte nach Generation



Die Befragten gaben ihr Alter an, das zur Bestimmung ihrer Geburtsgeneration herangezogen wurde:

- Generation Z (ca. 18 bis 27 Jahre)
- Millenials (ca. 28 bis 43 Jahre)
- Generation X (ca. 44 bis 59 Jahre)
- Babyboomer (ca. 60 bis 64 Jahre)

Befragte nach Aufgeschlossenheit gegenüber neuen Technologien



Die Umfrageteilnehmer wurden auch gefragt, welche der folgenden Aussagen ihre Aufgeschlossenheit gegenüber neuen Technologien am besten beschreibt, und daraufhin einer der angegebenen Kohorten zugeordnet:

- Ich suche aktiv nach neuen Technologien und probiere sie noch vor anderen aus (Technologie-Innovatoren)
- Ich interessiere mich für neue Technologien und probiere sie kurz nach ihrer Markteinführung aus (Early Adopter)
- Ich warte, bis neue Technologien weit verbreitet sind und sich als zuverlässig erwiesen haben (Mainstream Adopter)
- Ich bleibe lieber bei vertrauten Technologien und probiere selten neue aus (Technologie-Traditionalisten)
- Ich meide neue Technologien, solange sie nicht absolut notwendig sind (Technologie-Verweigerer)

Operative Telemetriedaten

Teile dieses Berichts verwenden operative Telemetriedaten der Auth0 Platform, die CIAM-Funktionen für Tausende von Unternehmen auf der ganzen Welt bereitstellt.

Für den Zeitraum vom 1. Januar 2024 bis zum 31. Dezember 2024 summiert der Bericht die täglichen Ereignisprotokolle im Zusammenhang mit legitimen Aktivitäten und erkannten Bedrohungen (siehe Definitionen unten). Dies ermöglicht eine aussagekräftige Normalisierung der Bedrohungstrends und die Kontrolle der laufenden Veränderungen in der Kundenzusammensetzung.

Wo solche Informationen verfügbar sind, werden die Ereignisdaten mit der Branche (selbst gewählt) und der Größe des Kunden (z. B. kleines Unternehmen, mittelständisches Unternehmen, großes Unternehmen) verknüpft und anschließend anonym aggregiert. Kunden, für die bestimmte Informationen nicht verfügbar sind, werden in den entsprechenden Aggregationen nicht berücksichtigt.

Da dieser Bericht auf realen Produktionsbereitstellungen basiert, erfasst er die tatsächliche Aktivität auf der Auth0 Platform und berücksichtigt daher sowohl die Produkte und Features, die jeder Kunde aktiviert hat (sowie deren Konfigurationen), als auch die neuen Fähigkeiten dieser Produkte und Features.

Um den wahren Stand der Identity-Sicherheit abzubilden, haben wir uns bewusst dafür entschieden, Ausreißer nicht zu berücksichtigen oder extreme Ereignisse (z. B. groß angelegte Angriffe) aus unserer Analyse herauszufiltern. Aufgrund der verzerrenden Wirkung, die solche Ereignisse auf die Durchschnittswerte haben können, haben wir, sofern nicht anders angegeben, den arithmetischen Medianwert und nicht den Mittelwert angegeben. Bei der Aggregation über mehrere Tage (z. B. für eine Jahresstatistik) oder Branchen wird der Mittelwert verwendet.

Registrierungsangriffe

Einen **Registrierungsangriff** definieren wir als Vorgang, bei dem eine einzelne IP-Adresse mindestens 10 fehlgeschlagene Registrierungen an einem einzigen Tag verzeichnet.

Eine Registrierung kann fehlschlagen, wenn:

- Die Kennung (Benutzername, E-Mail-Adresse, Telefonnummer usw.) bereits registriert wurde
- Fehler bei der Validierung der Kennung auftreten
- Die Begrenzung für die Anzahl der Registrierungen überschritten wird
- Benutzerdefinierte Datenbankskripte fehlschlagen

Fälle, in denen Benutzer das Ausfüllen des Registrierungsformulars einfach abbrechen, werden nach unserer Definition nicht als Registrierungsangriff gewertet.

Login-Angriffe

Die in diesem Bericht untersuchten **Login-Angriffe** umfassen drei Arten von Brute-Force-Angriffen.

- **Credential Stuffing:** Ein Bedrohungsakteur versucht, bekannte Anmeldedaten (z. B. aus einem Data Breach/Dump) bei anderen Websites und Services zu verwenden.
- **Password Spraying:** Ein Bedrohungsakteur probiert eine relativ kurze Liste der am häufigsten verwendeten Passwörter bei vielen verschiedenen Accounts aus.
- **Password Guessing:** Ein etwas gröberer Ansatz, bei dem ein Bedrohungsakteur viele Passwörter bei einer beliebigen Anzahl an Accounts ausprobiert.

Einen **Login-Angriff** definieren wir als Vorgang, bei dem eine einzelne IP-Adresse mehr als 10 Ereignisse im Zusammenhang mit fehlgeschlagenen Logins auslöst.

Zu diesen Ereignissen gehören Fehler wie

- Ungültiger Benutzer oder ungültiges Passwort
- Login-Versuche mit gestohlenen Anmeldedaten
- Die IP-Adresse wird durch andere Attack Protection-Features (z. B. Brute-Force-Schutz, Suspicious-IP-Throttling usw.) für Logins gesperrt

Schädliche MFA-Ereignisse

Ein **schädliches MFA-Ereignis** definieren wir als Vorgang, bei dem eine einzelne IP-Adresse innerhalb einer Stunde mindestens 10 der folgenden MFA-bezogenen Ereignisse auslöst:

- E-Mail-, SMS- oder Push-MFA-Benachrichtigung gesendet
- MFA-Authentifizierung fehlgeschlagen oder zurückgewiesen
- Benutzer überschreitet Grenzwert für OTP-Codefehler
- Benutzer gibt ungültigen Wiederherstellungscode ein oder überschreitet Grenzwert für Wiederherstellungscode-Fehler

In der Praxis werden nach dieser Definition folgende Ereignisse erfasst:

- Versuche, MFA durch Bombing/Fatigue-Angriffe zu umgehen (z. B. indem Benachrichtigungen an einen Benutzer ausgelöst werden, bis er die Sicherheitsabfrage beantwortet, um dem Terror ein Ende zu setzen)
- Toll Fraud-Versuche, bei denen MFA missbraucht wird, um das Senden von Telefon- oder SMS-Nachrichten an kostenpflichtige Nummern auszulösen. Dies treibt die Kosten für den Application Provider in die Höhe, während der Angreifer einen Teil des Erlöses erhält
- Fälle, in denen ein Angreifer wiederholt eine MFA-Sicherheitsabfrage nicht beantworten kann
- Fälle, in denen ein legitimer Benutzer wiederholt eine MFA-Sicherheitsabfrage nicht richtig beantwortet (stellen nur einen winzigen Bruchteil aller MFA-Missbrauchsfälle dar)

Zitieren aus dem Customer Identity Trends Report 2025

Wir freuen uns, wenn Customer Identity Trends Report-Informationen weitergegeben werden. So können Sie die Daten, Statistiken und anderen Informationen aus dem Customer Identity Trends Report 2025 korrekt zitieren:

- **Erwähnen Sie uns**
  Bitte zitieren Sie die Quelle als „Auth0 Customer Identity Trends Report 2025“, wenn Sie Inhalte aus diesem Bericht wiedergeben.
- **Keine Änderungen**
  Inhalte müssen genau wie im Report zitiert werden. Wenn Sie etwas umformulieren möchten, bitten wir darum, das mit uns abzuklären.
- **Bitte weitergeben**
  Wenn Sie den Report weitergeben möchten, benutzen Sie dafür bitte einen Link zu unserer Download-Seite: auth0.com/customer-identity-trends-report

Wir würden uns freuen, wenn Sie unsere Erkenntnisse unverändert und allgemein verfügbar machen.