2023

Bedrohungen für Ihre Kunden-Login-Box – und alles dahinter

The State of Secure Identity Report

okta

Inhalt

Vorwort

Sichere Kunden-authentifizierung

Kurze Innovationszyklen und ein breiterer Zugang zu Informationen haben die Nachfrage nach Identity-Lösungen in den vergangenen zehn Jahren maßgeblich verändert. Identity ist heute der Schlüssel zur Absicherung von Kunden- und Workforce-Anwendungen gleichermaßen. Gleichzeitig steigt aber sowohl die Zahl als auch die Komplexität Identity-basierter Angriffe. Identity-basierte Attacken zu erkennen und zu stoppen, ist In dieser dynamischen Landschaft von entscheidender Bedeutung. Als einer der Marktführer in diesem Bereich hat es sich Okta auf die Fahne geschrieben, Kunden zuverlässig vor Identity-basierten Angriffen zu schützen. Dabei setzen wir nicht nur auf unsere marktführenden Identity-Produkte. Wir treiben auch die Weiterentwicklung relevanter Branchenstandards voran und geben unseren Kunden robuste Best Practices an die Hand.

Den Login zu schützen, ist dabei einer der wichtigsten Schritte. Im Zuge der **Authentifizierung**, eine der wichtigsten Funktionen des **Customer Identity & Access Managements (CIAM)**, bestätigt die Login-Box die **digitale Identität** Ihrer Kunden — ein Set spezifischer Attribute, die Ihre Anwender (oder nicht-menschliche **Entitäten** wie Devices oder Systeme) im Kontext der Anwendung definieren.

Aber nicht nur legitime Nutzer haben ein Interesse daran, hinter das Login-Gateway zu gelangen. Wem auch immer es gelingt, in Ihr System einzudringen, kann viel Geld verdienen. Die monetären Anreize haben zu einem riesigen Ökosystem von Technologien, Services und anderen Ressourcen geführt, die ausschließlich dazu dienen, solche **Einbrüche** zu ermöglichen.

Die Zahl der Angriffe gegen kleine und große Unternehmen nimmt über alle Branchen hinweg kontinuierlich zu. Cyberkriminelle investieren also immer mehr Mühe und Knowhow darauf, die Login-Box zu umgehen. Dabei machen sie sich auch die enormen Potenziale der künstlichen Intelligenz (KI) zunutze – die Abwehr der Attacken erfordert also immer neue Security-Schichten und immer raffiniertere Schutzmaßnahmen.

Dies gilt umso mehr, als moderne Kunden-Portale – ganz egal, ob im B2C- (Business-to-Consumer-) oder im B2B- (Business-to-Business-)Umfeld – in aller Regel über das öffentliche Internet zugänglich sein müssen. Außerdem muss die Authentifizierung transparent genug erfolgen, um das Vertrauen der Kunden zu gewinnen, aber auch komfortabel genug, um keinen unnötigen Mehraufwand zu verursachen.

Viele Jahre lang basierte die Authentifizierung von Kunden im Prinzip auf dem Faktor Wissen – in der Regel einem Passwort –, bei dem man annehmen konnte, dass er nur dem rechtmäßigen Anwender und dem Anwendungsprovider bekannt ist. Diese Annahme hat sich aber immer wieder als falsch erwiesen: Jedes Wissen kann entwendet oder angeeignet werden (z. B. über **Open Source Intelligence**). Gerade Passwörter sind ein echtes Problem, und sowohl die Anwendungsprovider als auch die CIAM-Anbieter, auf die sie sich verlassen, sollten versuchen, ihre Kunden auf sicherere Authentifizierungsfaktoren umzustellen. Im Idealfall sollten sie auch versuchen, Ihre Kunden zur Nutzung von **Multi-Faktor-Authentifizierung (MFA)** zu bewegen.

Noch vor einigen Jahren konnte man überzeugend argumentieren, dass es unmöglich (oder zumindest nicht praktikabel) ist, die Authentifizierung sowohl angemessen sicher als auch angemessen komfortabel umzusetzen – dass also stets ein Kompromiss gemacht werden müsse, und dass MFA zu aufwändig ist, um flächendeckend eingesetzt zu werden, gerade im B2C-Umfeld.

Aber mit der deutlich besseren Verfügbarkeit von **Passkeys** und **synchronisierten Passkeys** sind wir jetzt an einem Punkt angelangt, an dem diese Argumente nicht mehr greifen. Tatsächlich sind wir sogar davon überzeugt, dass die Einführung synchronisierter Passkeys ein zentraler Meilenstein beim Schutz der **Kundenidentitäten** sein wird. Immerhin haben Passkeys längst bewiesen, dass sie nicht nur hohen Sicherheitsstandards entsprechen, sondern auch eine komfortable und hochwertige User-Experience bieten, die in vielerlei Hinsicht die Usability anderer Ansätze übertrumpft.

Und die Passkeys kommen keinen Moment zu früh. Digitale Identitäten regeln heute den Zugang zu immer mehr Anwendungen und Diensten – und beeinflussen und steuern damit viele Aspekte des modernen Lebens. In Zukunft wird die Tragweite noch wesentlich größer sein. Authentifizierung, **Autorisierung** und CIAM werden unverzichtbar sein, um Vertrauen, Sicherheit und Datenschutz zu gewährleisten. CIAM kommt also eine Schlüsselrolle zu, wenn es gilt, den freien Zugang zu Informationen sicherzustellen. Die Identity-Experten der Unternehmen werden maßgeblich darüber entscheiden, ob sich die digitale Kluft schließen wird – oder ob sie immer weiter klaffen wird.

Mit dem vorliegenden Report – dem dritten jährlichen Report zum Status der Identity-Sicherheit – wollen wir das Bewusstsein für die Gefahren schärfen, die der Customer Identity drohen – aber auch geeignete Abwehrmaßnahmen aufzeigen, um diesen Bedrohungen zu begegnen. In diesem Jahr gehen wir das Thema etwas anders an und haben unseren Report in drei Teile gegliedert:

- Vor der Login-Box – weil die Login-Box zwar zugänglich sein, aber nicht jedem präsentiert werden sollte
- An der Login-Box – wo das tägliche Ringen um Identities stattfindet
- Hinter der Login-Box – weil Secure Access nicht aufhört, nur weil ein User die Pforte passiert hat.

Vielen Dank, dass Sie mich – und das gesamte Okta-Team – auf dieser Reise begleiten.

Shiven Ramji
President, Customer Identity Cloud, Okta

Executive Summary

CIAM ist ein Teilbereich des weiter gefassten Identity- & Access-Managements (IAM), bei dem für Kunden bereitgestellte Anwendungen im Fokus stehen. In diesem Umfeld ist es besonders wichtig, den Anwendern eine hochwertige, sichere und Datenschutz-konforme Experience zu bieten, die einer zunehmend dynamischen Bedrohungslandschaft Rechnung trägt.

Der vorliegende Report dokumentiert, dass betrügerische Anmeldungen, Credential Stuffing und die Umgehung von MFA allgegenwärtige Bedrohungen sind, denen jede Login-Box gewachsen sein muss.

Executive Summary

Die Login-Box ist für Angreifer eine Goldmine

Der Report belegt, dass zwischen dem 1. Januar 2023 und dem 30. Juni 2023:

13,9 % der versuchten Account-Anmeldungen gemäß der Okta Customer Identity Cloud von Auth0 allen Kriterien eines Signup-Angriffs entsprachen:

- Betrachtet man die 10 Branchen, die in der Customer Identity Cloud am stärksten vertreten sind, war der Anteil betrügerischer Anmeldeversuche in vier davon besonders hoch: Finanzdienstleistungen (28,8 %), Medien (28,4 %) (25,1 %) und Software/SaaS/Tech (24,0 %)
- An dem mit Blick auf Anmeldebetrug „geschäftigsten" Tag dokumentierte unsere Technologie fast 10 Millionen betrügerische Anmeldeversuche
- Am 15. April wurden mehr als 64 % der Versuche, sich an einem Account anzumelden, als betrügerisch eingestuft

Insgesamt 24,3 % der Anmeldeversuche erfüllten die Kriterien der Customer Identity Cloud für Credential Stuffing:

- Von den 10 Branchen, die in unserer Technologie am stärksten vertreten sind, wiesen Einzelhandel/E-Commerce (51,3 %), Medien (42,3 %), Software/SaaS/Tech (32,1 %) und Finanzdienstleistungen (30,3 %) einen überdurchschnittlich hohen Anteil an Credential-Stuffing-Attacken auf.
- An dem mit Blick auf Credential Stuffing „geschäftigsten" Tag beobachtete die Technologie fast 27 Millionen entsprechender Vorgänge
- Am 1. Januar wurden mehr als 46 % der Versuche, sich an einem Account anzumelden, als Credential Stuffing eingestuft

Insgesamt 12,7 % der Anmeldeversuche mit MFA erfüllten die Kriterien der Customer Identity Cloud für einen MFA-Angriff (sprich: für ein bewusstes Umgehen der MFA-Vorgaben):

- Von den 10 Branchen, die in der Technologie am stärksten vertreten sind, verzeichneten Medien (12,8 %), Finanzdienstleistungen (10,9 %), produzierende Industrie (7,8 %) und Software/SaaS/Tech (6,4 %) den höchsten Anteil an Versuchen, die MFA zu umgehen.
- An dem mit Blick auf MFA-Verstöße „geschäftigsten" Tag beobachtete die Technologie fast 750.000 entsprechende Vorfälle
- Am 11. Juni wurden mehr als 30 % der MFA-Anmeldungen als Versuch, die MFA zu umgehen, eingestuft

Zu welcher Branche ein Unternehmen gehört, ist aber nicht der einzige Faktor, der die individuelle Bedrohungslage prägt. So scheint es beispielsweise, dass kleine Betriebe und große Konzerne deutlich öfter zum Ziel von Anmeldebetrug, Credential Stuffing und MFA-Umgehung werden als mittelständische Unternehmen. Eine mögliche Deutung ist, dass Cyberkriminelle große Konzerne als besonders wertvolle Ziele und kleine Betriebe als vergleichsweise leichte Ziele betrachten.

Und auch die Region, in der ein Unternehmen seinen Hauptsitz hat, wirkt sich auf die Bedrohungslage aus; Unternehmen im asiatisch-pazifischen Raum (APAC) verzeichneten bei weitem die höchsten Raten von Anmeldebetrug, während Unternehmen in Nord- und Südamerika (AMER) deutlich häufiger mit Credential-Stuffing-Attacken konfrontiert waren.

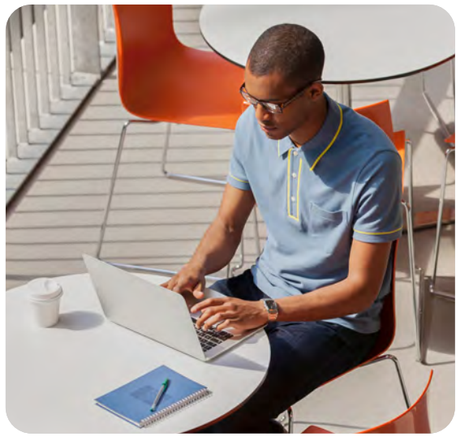
		Betrügerische Anmeldeversuche[1]		Credential-Stuffing-Versuche[2]		Versuche zur Umgehung von MFA[3]	
		Rate	Rang	Rate	Rang	Rate	Rang
	Insgesamt (über alle Technologien hinweg)	13,9 %	—	24,3 %	—	12,7 %	—
In den 10 meist-repräsentierten Branchen	Werbung/Marketing	1,0 %	10	16,7 %	6	3,4 %	9
	Finanzdienstleistungen	28,8 %	1	30,3 %	4	10,9 %	2
	Nahrung/Getränke/Gastronomie	9,0 %	8	11,4 %	8	5,5 %	5
	Gesundheitswesen	6,3 %	9	16,1 %	7	4,6 %	7
	Produzierende Industrie	25,1 %	3	17,7 %	5	7,8 %	3
	Medien	28,4 %	2	42,3 %	2	12,8 %	1
	Professional Services	13,4 %	5	7,2 %	10	4,5 %	8
	Handel	9,3 %	7	51,3 %	1	5,0 %	6
	Software/SaaS/Technologie	24,0 %	4	32,1 %	3	6,4 %	4
	Reise/Transport	9,7 %	6	7,2 %	9	2,9 %	10
Unternehmens-größe	Enterprise	19,9 %	1	39,4 %	1	9,5 %	2
	Mittelstand	12,6 %	3	20,1 %	3	9,0 %	3
	Kleinunternehmen	19,4 %	2	30,9 %	2	20,3 %	1
Sitz des Unternehmens	AMER	9,4 %	2	28,0 %	1	12,0 %	1[4]
	APAC	27,9 %	1	13,3 %	3	11,0 %	2
	EMEA	8,1 %	3	20,2 %	2	7,6 %	3

Tabelle 1: Zusammenfassung der Anzahl Identity-basierter Angriffe, wie mit Customer Identity Cloud-Technologie ermittelt (1. Januar 2023 bis 30. Juni 2023)

[1] Anteil an der Gesamtzahl der Registrierungsversuche
[2] Anteil an der Gesamtzahl der versuchten Passwortauthentifizierungen
[3] Anteil an der Gesamtzahl der MFA-Versuche
[4] Im Abschnitt „Methodik" wird erläutert, warum alle drei Regionen unter dem weltweiten Durchschnitt liegen

Executive Summary

Wie Sie Kunden mit CIAM schützen und begeistern



Anders als beim Management der Workforce Identities, bei dem von den Anwendern ein relativ hoher **Aufwand** akzeptiert wird und die User-Basis oft eine Sicherheitsschulung durchlaufen hat, müssen sich Unternehmen beim CIAM, wo diese Voraussetzungen fehlen, auf weniger aufdringliche Security-Technologien verlassen. Nur so erreichen sie ein robustes Security-Standing, ohne Abstriche bei der Benutzerfreundlichkeit in Kauf nehmen zu müssen.

Mit Blick auf steigende Kundenerwartungen und die hochgradig dynamische Bedrohungslandschaft müssen diese Technologien zudem kontinuierlich angepasst werden. Nur so lässt sich durchgehend das richtige Gleichgewicht zwischen User Experience, Security und Datenschutz gewährleisten – ein Gleichgewicht, das ganz vom Risikoprofil und von der Risikobereitschaft des Unternehmens abhängt.

Implementieren Sie mehrstufige Abwehrmaßnahmen

Grundlegende Kontrollen – etwa die Begrenzung der Übertragungsraten, die Sperrung verdächtiger IP-Adressen und die Erkennung kompromittierter Passwörter – sind wichtig, reichen für sich genommen aber nicht aus.

Und auch wirksame Passwort-Policies (z. B. Vorgaben für sichere Passwörter, ein sicheres Rücksetzungsverfahren etc.) sowie eine gute Session-Hygiene (z. B. das Entfernen von Session-Token aus URLs, die Generierung neuer, unvorhersehbarer Token nach der Anmeldung etc.) sind zwar wichtige Voraussetzungen, aber nur ein Teil der Lösung.

Immerhin investieren Cyberkriminelle viel Zeit und Ressourcen in die Umgehung von Security-Maßnahmen. Folglich werden auch die Anbieter von CIAM-Diensten und CIAM-Lösungen ihre Investitionen in zeitgemäße Schutzmaßnahmen steigern müssen.

So ist Bot Detection mit Okta AI heute in der Lage, fast 80 % der Bots zu filtern, die Authentisierungssysteme ins Visier nehmen. Ein zentraler Aspekt ist dabei, dass der zusätzliche Schutz keinen unnötigen Mehraufwand für die Nutzer bedeutet; durch sorgfältiges Training und kontinuierliche Optimierung der KI, die im Mittelpunkt der Bot-Detection steht, können wir sicherstellen, dass Anwender nur selten ein CAPTCHA beantworten müssen. So bleibt durchgehend eine hochwertige Experience garantiert.

Außerdem spricht vieles dafür, dass die hohe Wirksamkeit an sich eine sehr starke Abschreckung darstellt; bei einigen unserer größten Kunden hat der Bot-Traffic im 90-Tage-Durchschnitt um fast 90 % abgenommen, nachdem sie die Funktion Attack Protection aktiviert hatten. Das ist ein gutes Indiz dafür, dass Cyberkriminelle lieber auf einfachere Ziele geschwenkt haben.

Stärken Sie die Authentifizierung

Wir können nicht genug betonen, wie viel Potenzial Passkeys haben, wenn es gilt, die Kundenauthentifizierung im Vergleich zu passwortbasierten Anmeldungen zu verbessern. Passwörter sind die Ursache vieler Identity-basierter Threats, und Passkeys sind ein wichtiger Meilenstein, um Passwörter nachhaltig abzulösen:

- Gerade synchronisierte Passkeys unterstützen eine starke Authentifizierung, die so zuverlässig wie komfortabel ist – und eignen sich hervorragend für Mainstream-Verbraucher, denen eine hochwertige Experience besonders wichtig ist (ab dem 10. Oktober 2023 bietet Google Passkeys als Standardoption für persönliche Google-Konten an)
- **Device-gebundene Passkeys** sind eine hervorragende Option für B2B-Märkte und andere Kundenanwendungen, die eine noch stärkere Authentifizierung mit **FIDO**-zertifizierten Authentifikatoren und Sicherheitsschlüsseln erfordern

Auch die MFA spielt bei der zuverlässigen Kundenauthentifizierung eine wichtige Rolle. In der Vergangenheit taten sich gerade Organisationen mit engem Kundenkontakt oft schwer damit, MFA einzuführen und zu empfehlen – geschweige denn vorzuschreiben –, weil sie befürchteten, dass der Mehraufwand zu Lasten der Konversionsrate ginge. Das gilt aber schon seit einigen Jahren nicht mehr:

- **Adaptive MFA** ermöglicht es Anwendungsprovidern, MFA-Challenges nur bei potenziell gefährlichen Anmeldungen einzusetzen, wobei die Risikobewertung von den jeweiligen Bedrohungssignalen abhängt
- **Step-up-Authentifizierung** ermöglicht es Anwendungsprovidern, den Zugang zu Ressourcen mit geringem Risikopotenzial über einen vergleichsweise schwächeren Authentifizierungsmechanismus (z. B. ein Passwort) zu ermöglichen. Stärkere Authentifizierungsverfahren (z. B. MFA) kommen nur zum Einsatz, wenn ein Benutzer auf eine sensiblere Ressource zugreifen möchte.

Wie wir aber gesehen haben, investieren Angreifer immer mehr Ressourcen in die Umgehung vergleichsweise schwacher MFA-Faktoren. Daher ist es von entscheidender Bedeutung, dass Anwendungsprovider ihre Kunden auf Authentifikatoren migrieren, die über das Wissen hinaus auch Besitz oder biometrische Merkmale erfordern.

Build or Buy?

Eine solche mehrschichtige CIAM-Lösung im eigenen Haus zu entwickeln, ist ein anspruchsvolles Projekt, das die Kapazitäten der meisten Unternehmen bei weitem übersteigt. Denn es bedarf vieler Schichten und Technologien, um eine komfortable und hochwertige Customer Experience zu gewährleisten, ohne Abstriche beim Datenschutz in Kauf zu nehmen.

Für die meisten Unternehmen ist eine agile, sichere CIAM-Lösung der effektivste und effizienteste Ansatz, um die Weichen für ein maßgeschneidertes Customer Identity & Access Management zu stellen – und dieses bei Bedarf kontinuierlich zu optimieren, ohne Ressourcen zu binden, die eigentlich für den Ausbau der eigenen Kernkompetenzen benötigt werden.

Third-Party-Authentifizierung macht einen echten Unterschied

Eine kürzlich durchgeführte weltweite Umfrage unter Mitgliedern von App-Development-Teams unterstreicht, wie wichtig die Integration von Third-Party-Authentifizierung in SaaS-Anwendungen ist.

Die Umfrage, die auf den 675 Antworten von Experten aus 56 Ländern basiert, ergab Folgendes:

- **Authentisierung ist die drittaufwändigste Funktion, die man intern entwickeln und pflegen kann,** nach Data Management und Storage sowie DevOps-Tools & Automation
- **Third-Party-Authentifizierung verkürzt die Time-to-Market deutlicher als jede andere SaaS-Komponente:** 88 % der Unternehmen, die eine SaaS-Plattform eines Drittanbieters für die Authentifizierung nutzen, geben an, dass sie ihre Time-to-Market im vergangenen Jahr verkürzt haben

Mehr dazu im Report Wie Development-Teams ihre SaaS-Dienste beziehen ■

Einführung: Schutz von Kunden-identitäten

Der Schutz der Kundenidentitäten sollte für jeden Anwendungs- oder Serviceprovider oberste Priorität haben, und zwar aus dem einfachen Grund, dass nicht nur legitime User auf das zugreifen wollen, was sich hinter der Login-Box verbirgt – und diese böswilligen Akteure sind bereit, erhebliche Anstrengungen zu unternehmen, um zu bekommen, was sie wollen.

Mit unserem dritten jährlichen State of Secure Identity Report wollen wir das Bewusstsein schärfen für:

- Bedrohungen für die Kundenidentität
- Verfügbare Technologien, die für robusten und zuverlässigen Schutz miteinander kombiniert werden können

Um diese Ziele zu erreichen, werden wir die häufigsten und gefährlichsten Angriffsmuster von heute sowie allgemeine Trends untersuchen, die die Bedrohungslandschaft von morgen prägen werden.

Wo immer möglich, werden wir Daten aus der Okta Customer Identity Cloud von Auth0 – die Tausenden von großen und kleinen Unternehmen CIAM-Funktionalitäten bietet –, verwenden, um die Verbreitung und die Auswirkungen von Identity Threats zu veranschaulichen.

Bevor wir jedoch ins Detail gehen, lohnt es sich, einen Moment über den einzigartigen Kontext der Customer Identity nachzudenken:

- Die Notwendigkeit, eine komfortable und gleichzeitig sichere Erfahrung zu bieten
- Die zentrale Rolle von Customer Identity & Access Management (CIAM)
- Die ständige Weiterentwicklung von Authentisierungsmechanismen
- Das zweischneidige Schwert der Künstlichen Intelligenz (KI)

Einführung: Schutz von Kundenidentitäten

Kunden erwarten heute eine sichere und hochwertige Experience

Für jedes Unternehmen, das Kunden über einen digitalen Kanal bedient, ist die Minimierung von Reibungsverlusten bei jeder einzelnen Interaktion von entscheidender Bedeutung. In der Praxis bedeutet das, die Anzahl der Klicks zu minimieren, intuitive User Interfaces (UIs) zu entwickeln, Latenzzeiten zu reduzieren und eine nahtlose und komfortable User Experience (UX) über alle Kanäle (z. B. Websites und Apps) hinweg zu bieten.

Um ihre Services und legitimen Kunden zu schützen, müssen Unternehmen auch Sicherheitsmaßnahmen implementieren, die einem breiten Spektrum von identitätsbezogenen Angriffen standhalten können. Eine ideale Identity-Implementierung stellt Angreifer vor unüberwindbare Hürden und echte User vor nahezu keine – kleine Hürden zur richtigen Zeit am richtigen Ort allerdings können dazu beitragen, Vertrauen aufzubauen.

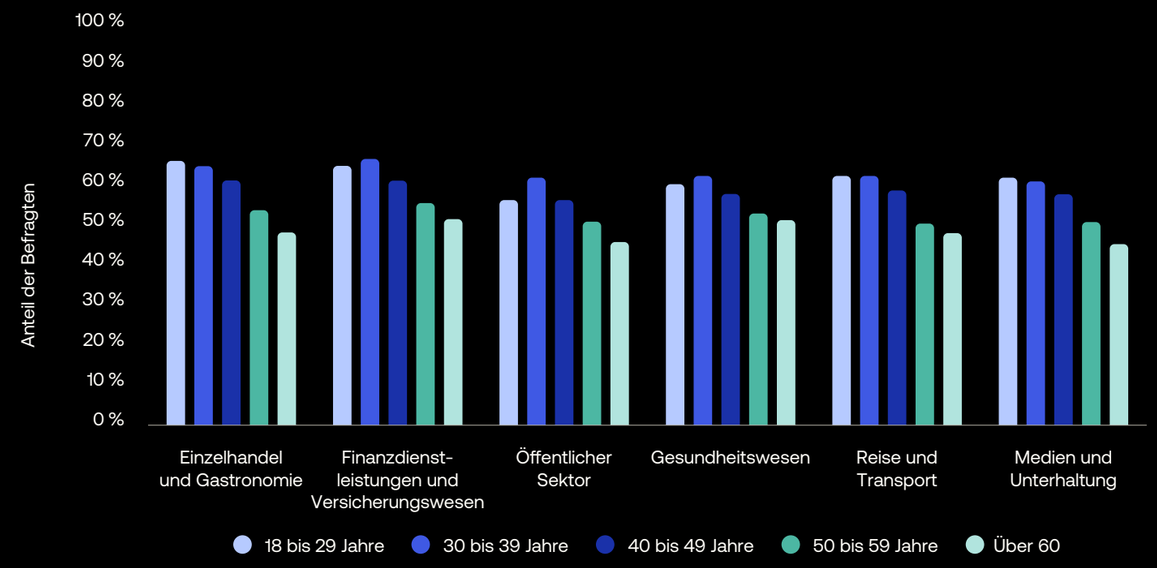
Obwohl eine solche Lösung erstrebenswert ist, gilt es in der Realität häufig Kompromisse einzugehen. Beispielsweise kann die Bereitstellung eines Mechanismus zur Erkennung und Verhinderung von groß angelegten, skriptbasierten Bot-Angriffen die Gesamtwiderstandsfähigkeit einer Anwendung erhöhen – allerdings auf Kosten einer gewissen Anzahl an Usern, die mit einer Security Challenge konfrontiert werden.

Sobald der Mechanismus implementiert ist, kann er auf der Grundlage von Erfahrungswerten feingetunt werden, um die richtige Balance zwischen Sicherheit und Komfort zu finden. In der Praxis wird diese Balance von Anwendung zu Anwendung, von Unternehmen zu Unternehmen und von Branche zu Branche variieren, da jede Kombination aus Kundenstamm, Bedrohungslandschaft und Sicherheitspräferenzen einzigartig ist. Erschwerend kommt hinzu, dass sich die Balance im Laufe der Zeit verschieben kann, wenn Bedrohungsakteure ihre Taktiken, Techniken und Verfahren (TTPs) anpassen und neue Ziele auswählen und wenn sich die Kundenpräferenzen ändern.

Doch Unternehmen, die sich die Mühe machen, eine Balance zu finden, können davon entscheidend profitieren. Der Customer Identity Trends Report 2023 von Okta, der auf einer weltweiten Umfrage unter 21.512 Verbrauchern in 14 Ländern basiert, zeigt beispielsweise, dass fast 60 % der Befragten eher bereit sind, Geld auszugeben, wenn Services einen einfachen, sicheren und reibungslosen Login-Prozess bieten (Abbildung 1) – wobei die umworbenen jüngeren Bevölkerungsgruppen solche komfortablen Erfahrungen besonders bevorzugen.

Abbildung 1: Kunden sind online eher bereit, bei einem Unternehmen einzukaufen, wenn es ihnen eine einfache, sichere und hochwertige Experience bietet

Die Grafiken zeigen die Summe der Antworten „sehr wahrscheinlich“ und „eher wahrscheinlich“.



Einführung: Schutz von Kundenidentitäten

Die Rolle von CIAM beim Schutz von Identitäten und Anwendungen

Ein Bot-Detection-Mechanismus wie der oben beschriebene ist nur ein Element innerhalb eines Identity-Security-Stacks und Identity Security ist nur ein Aspekt des Customer Identity and Access Management.

Moderne CIAM-Lösungen ermöglichen es Unternehmen, Komfort, Datenschutz und Sicherheit für alle Arten von Usern, die Zugriff auf ihre Anwendungen und Services benötigen, miteinander in Einklang zu bringen. CIAM ermöglicht es Unternehmen auch, die User Experience kontinuierlich weiterzuentwickeln, die Anforderungen an das Engineering-Team im Zusammenhang mit identitätsbezogenen Funktionen zu minimieren – sodass es sich auf die Kernkompetenzen konzentrieren kann – sowie gesetzliche, Zertifizierungs- und vertragliche Anforderungen effizient und effektiv zu erfüllen.

In puncto Identity sind die drei Hauptmerkmale einer effektiven CIAM-Lösung Authentisierung, Autorisierung und Identity Management:

- **Robuste Authentisierung** stellt sicher, dass die User, die sich in Accounts einloggen, auch die sind, für die sie sich ausgeben.
- **Effektive Autorisierung** hilft Unternehmen, einem User die richtigen Zugriffsrechte für eine Anwendung und/oder Ressourcen zuzuweisen.
- Ein lückenloses **Identity Management** ermöglicht es Administratoren, die Berechtigungen ihrer Anwender regelmäßig zu aktualisieren und verbindliche Security-Policies durchzusetzen. Dies erlaubt es Kunden auch, ihre eigenen Identitäten, Daten und Einstellungen selbst zu verwalten – und zwar genau in dem vom Use Case und von den regulatorischen Vorgaben vorgesehenen Umfang.

Während die wörtliche Definition von CIAM gleichgeblieben ist, hat sich seine Bedeutung in der Praxis – in Bezug darauf, welche Use Cases es mit welchen funktionalen Komponenten für welche Arten von Unternehmen ermöglicht – vor allem in den letzten Jahren weiterentwickelt. Heute ist CIAM unverzichtbar für:

- **Verbraucher:** In der Business-to-Consumer-Welt (B2C) ermöglicht eine effektive CIAM-Implementierung hochgradig personalisierte Angebote und Empfehlungen, die zusätzliche Umsätze generieren und Mehrwert für Ihre Kunden schaffen – während sie gleichzeitig eine komfortable User Experience über alle Ihre digitalen Kanäle hinweg gewährleistet.
- **Geschäftskunden:** Unzählige Unternehmen setzen heute auf B2B-SaaS-Anwendungen, um effizienter und produktiver zu arbeiten. Doch in jedem Unternehmen gibt es unterschiedliche Anwender, die auch unterschiedliche Zugriffsrechte auf unterschiedliche Ressourcen benötigen. Wenn Sie ihnen eine hochwertige und sichere User Experience bieten möchten, müssen Sie die Identities und die Zugriffsrechte sorgfältig managen. CIAM bietet die Lösung, indem es B2B-SaaS-Kunden ermöglicht, Identitäten selbst zu verwalten.
- **Mehr Optionen für Partner, Lieferanten und andere Dritte:** Bei Consumer- und SaaS-Anwendungen verwalten in der Regel die Kunden ihre eigenen Identitäten. Dennoch gibt es eine Reihe von Use Cases, in denen die Identity von der Organisation verwaltet werden muss, die den jeweiligen Dienst anbietet. Für Use Cases, in denen die Kundenidentitäten dem Serviceprovider bekannt sind und von diesem bereitgestellt werden, bietet CIAM alle Tools, die Unternehmen benötigen, um Kundenaccounts zu erstellen, zu pflegen und zu schließen.

Im Workforce-Identity-Kontext können Administratoren Kontrollen mit vergleichsweise wenig Rücksicht auf die User Experience durchsetzen. Im Customer-Identity-Bereich stellt die Notwendigkeit, Reibungsverluste zu minimieren (oder zumindest sorgfältig zu managen), eine Herausforderung dar – insbesondere in Bezug auf die Authentisierung.

Einführung: Schutz von Kundenidentitäten

Wie Sie Millionen von Anwendern eine sichere und einfache Authentisierung ermöglichen

Während das Zero-Trust-Paradigma eine große Veränderung im Bereich Workforce Identity darstellt, hat CIAM schon immer in einer Zero-Trust-Welt funktioniert. In fast jedem reinen CIAM Use Case haben weder der Anwendungs- noch der Identity-Provider Kontrolle über die Endpunkte, von denen aus auf den Service zugegriffen wird.

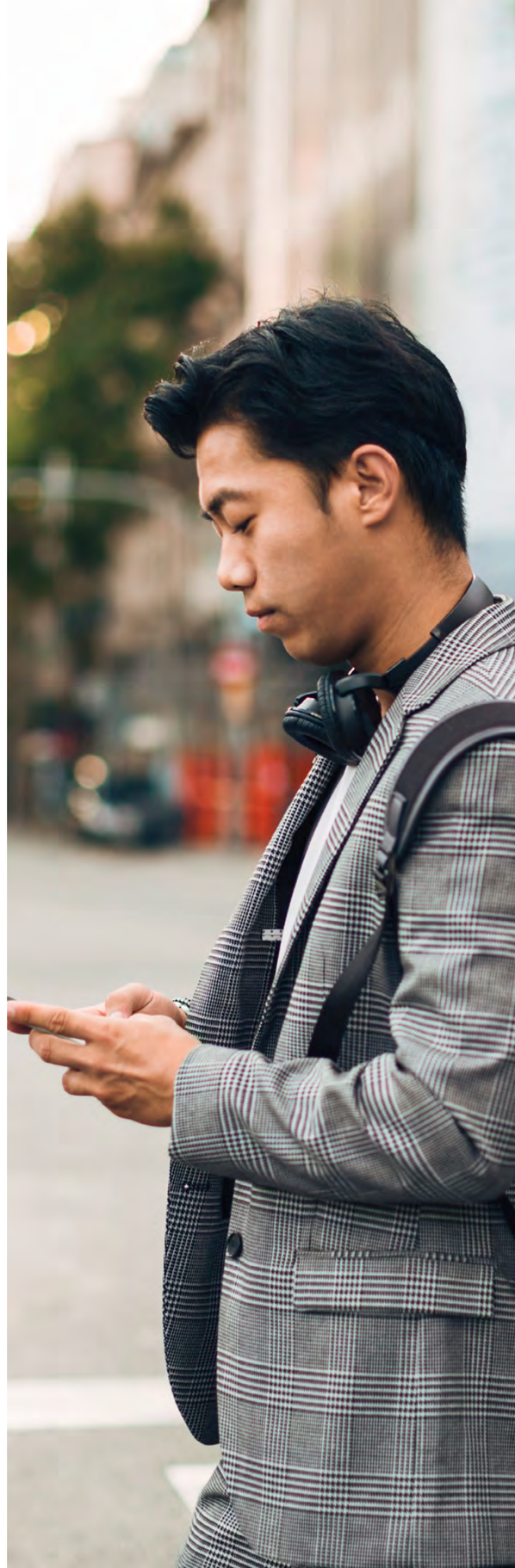
Um das notwendige Vertrauen für eine Interaktion oder Transaktion zu schaffen – sprich einen gewissen Grad an Zugriff zu erhalten –, muss jeder User einen oder mehrere Authentisierungsfaktoren vorweisen:

- **Wissen:** Etwas, das der User weiß, z. B. ein Passwort oder die Antwort auf eine Sicherheitsfrage
- **Besitz:** Etwas, das der User besitzt, z. B. ein Smartphone oder Zugriff auf einen E-Mail-Account.
- **Inhärenz:** Etwas, das dem User eigen ist – ein biometrisches Attribut, wie ein Fingerabdruck, Gesichtsscan oder Stimmprofil; in den meisten Implementierungen bestätigt das Gerät, dass die sich authentisierende Person dieselbe ist, die diesen Authentisierungstyp ursprünglich eingerichtet hat

Was jedoch als simple, von Menschen ausgefüllte Login-Box begann, hat sich im Laufe der Jahre dramatisch verändert:

- **Passwörter sind komplexer geworden:** Da Angreifer immer geschickter darin wurden, schwache Passwörter zu erraten und die weit verbreitete Wiederverwendung von Passwörtern auszunutzen, stiegen die Anforderungen an die Komplexität, was zu immer längeren Passwörtern mit Sonderzeichen, Kombinationen aus Groß- und Kleinbuchstaben und Zahlen führte
- **Passwortmanagement trat auf den Plan:** User mussten sich mit mehr – und komplexeren – Passwörtern herumschlagen, was zur zunehmenden Verbreitung von Passwortmanagern (ob im Browser oder in einer separaten Anwendung implementiert) führte
- **MFA gewann an Bedeutung:** Als **Phishing** zu einer weit verbreiteten Bedrohung wurde und online riesige Passwort-Dumps auftauchten, erwies sich MFA als effektive Schutzmaßnahme gegen **Account Takeovers** (ATOs).

Leider haben die mit traditionellen MFA-Techniken einhergehenden Reibungsverluste zu einer geringen Akzeptanz bei den Usern geführt. Zudem sind viele ältere MFA-Techniken mittlerweile gefährdet, da Angreifer skalierbare und kostengünstige Wege gefunden haben, diese wichtige Barriere zu umgehen.



Mit der Weiterentwicklung der Authentisierungstechniken und der TTPs der Angreifer haben CIAM-Lösungen neue Identity-Security-Ebenen eingeführt, um eine breite Palette automatisierter Cyberangriffe abzuwehren, die Unternehmen Geld kosten und Kundendaten bedrohen.

Moderne Schutzmaßnahmen kommen der Ideallösung immer näher und umfassen Ansätze wie adaptive MFA und Step-up-Authentisierung – die beide darauf abzielen, nur dann Hürden einzubauen, wenn das Risikolevel entsprechend hoch ist. Der Schlüssel zur Entscheidung, wann genau eine Sicherheitsabfrage erforderlich ist – d. h. zur Aufrechterhaltung eines optimalen Gleichgewichts zwischen Sicherheit und Komfort – sind intelligente Systeme, die Risikosignale und anderen Kontext (z. B. die angeforderte Zugriffsebene) erfassen, um das Risiko zu bewerten, eine geeignete Authentisierungsabfrage auszuwählen usw.

Künstliche Intelligenz (KI) ist schon lange in Identity-Systeme integriert, und ihre Bedeutung wird zweifellos zunehmen (über die Sicherheit hinaus kann KI auch zur Verbesserung der Customer Experience eingesetzt werden).

Trotz all ihres Potenzials ist KI doch auch nur ein weiteres Tool, das zum Guten wie zum Schlechten eingesetzt werden kann.

Einführung: Schutz von Kundenidentitäten

AI macht es Angreifern leicht, ihre Identity-basierten Attacken zu skalieren

Auf einer grundlegenden Ebene kann Künstliche Intelligenz als eine von einem Computer getroffene Entscheidung verstanden werden, deren „Intelligenz“ sich nicht von einer von einem Menschen getroffenen Entscheidung unterscheidet – unabhängig davon, wie die Entscheidung zustande kommt.

Die ursprüngliche Prämisse geht auf das Jahr 1943 zurück, lange vor der Erfindung des Computers mit digitalem Speicher, als der Logiker Walter Pitts und der Neurowissenschaftler Warren McCulloch versuchten, eine mathematische Darstellung der Neuronen im menschlichen Gehirn zu erstellen.

Seit den 1960er Jahren hat sich die KI zu einer sehr umfangreichen Sammlung von Algorithmen entwickelt, die verschiedene Aufgaben ausführen können. Eine dieser Aufgaben ist die Entdeckung und Erkennung von Mustern und wird allgemein als Machine Learning (ML) bezeichnet. Der Bereich Machine Learning hat sich in den letzten 15 Jahren aufgrund von Fortschritten bei der Konstruktion und Manipulation von neuronalen Netzen dramatisch entwickelt – und mit immer leistungsstärkeren Computern können neuronale Netze „vertieft“ (oder vergrößert) werden, was zur Entstehung des praktischen und wirtschaftlichen Deep Learning geführt hat.

Aber die KI-Entwicklung, die die Welt im Sturm erobert hat, ist der unglaubliche – und viele würden sagen schockierende – Aufstieg und die rasante Entwicklung der generativen KI, die vor allem durch bemerkenswerte Fortschritte bei den Large Language Models (LLMs) vorangetrieben wird.

Plötzlich sind das Schreiben von Prosa und das Entwerfen komplexer (und lebendiger, sofern das denn die Intention ist) Bilder nicht mehr die alleinige Domäne des Menschen. Weil LLMs so gut schreiben – und auch programmieren – und so vieles heute von Software gesteuert wird, sind LLMs für unerwartete Durchbrüche und Fortschritte in einer Vielzahl von Bereichen verantwortlich.

Im Identity-Security-Kontext machen Fortschritte im Bereich KI die Bedrohungslandschaft in vielerlei Hinsicht gefährlicher. KI kann zum Beispiel:

- **identitätsbasierte Angriffe geringer Qualität und hoher Intensität gefährlicher machen:** Credential Stuffing, Anmeldebetrug, SMS-Pumping-Kampagnen und andere Angriffe können schwieriger zu erkennen und effektiver/zerstörerischer werden
- **völlig neue Arten von identitätsbasierten Angriffen ermöglichen:** Einige neue Angriffe werden von Security-Teams antizipiert oder von Forschern im Voraus entdeckt, während andere erst auffallen, wenn sie in freier Wildbahn auftauchen (das Problem der „unbekannten Unbekannten“)
- **einige bestehende Schutzmaßnahmen aushebeln:** KI-basierte Tools haben bereits gezeigt, dass sie in der Lage sind, CAPTCHAs zu lösen und Sprachbiometrie mit Hilfe von Deepfakes zu überlisten

Darüber hinaus machen es die Programmier- und Skripting-Fähigkeiten der generativen KI für Bedrohungsakteure aller Qualifikationsstufen (d. h. mit oder ohne Programmierfähigkeiten) einfacher, Angriffe zu lancieren, was potenziell mehr Teilnehmer in das Cybercrime-Ökosystem lockt und ihre Effizienz verbessert.

Skalierbare und kostengünstige personalisierte Angriffe ermöglichen

Der vielleicht gefährlichste neue Identity Threat besteht jedoch darin, dass KI **Spear Phishing** in großem Maßstab ermöglicht. Stellen Sie sich die folgende Angriffspipeline vor:

1. Ein Bedrohungsakteur wählt ein Unternehmen als Ziel aus
2. Der Bedrohungsakteur verwendet **Open-Source-Intelligence (OSINT)**, um eine Mitarbeiterliste zu generieren
3. Der Bedrohungsakteur speist diese Liste in eine Social Search API ein (es stehen viele Optionen zur Verfügung), die eine Liste der Social-Media-Accounts ausgibt, die mit jedem Mitarbeiter verknüpft sind
4. Der Bedrohungsakteur filtert die Liste, um Mitarbeiter mit offenen und aktiven Social-Media-Accounts zu identifizieren, und beginnt dann, die einzelnen Accounts zu untersuchen, um festzustellen, wem der User folgt, welche Beiträge er likt, was er postet, wann er aktiv ist usw. Der Bedrohungsakteur kann sogar eine themenbezogene Sentimentanalyse durchführen, um hoch personalisierte psychologische Profile zu erstellen, und kann diese Profile im Laufe der Zeit aktualisieren
5. Der Bedrohungsakteur folgt jedem Mitarbeiter in den verfügbaren sozialen Anwendungen und beginnt auf völlig harmlose Weise zu interagieren (z. B., indem er Beiträge likt und teilt, Kommentare hinterlässt usw.), um eine Beziehung aufzubauen
6. Der Bedrohungsakteur beobachtet aktuelle Ereignisse, Nachrichten und Trends, um eine Gelegenheit zu finden, mit jedem Mitarbeiter auf einer persönlichen Ebene Kontakt aufzunehmen
7. Der Bedrohungsakteur verfasst eine E-Mail (oder eine DM über ein beliebiges Medium) und wendet sich an jede der Zielpersonen
8. Wenn die Zielperson antwortet, kann die Konversation so lange fortgesetzt werden, bis genügend Vertrauen aufgebaut ist, dass der Bedrohungsakteur mit hoher Erfolgswahrscheinlichkeit um einen Gefallen bitten kann

Bis vor kurzem war die Durchführung einer solchen Angriffskette ein mühsames, manuelles und teures Unterfangen; heute kann sie nahezu vollständig automatisiert und skaliert durchgeführt werden – personalisiert für Tausende von Mitarbeitern über unterschiedlichste Unternehmen hinweg – und das zu sehr geringen Kosten.

Schutzmaßnahmen verstärken

Zwar wird KI Angreifern zweifellos unter die Arme greifen. Glücklicherweise dient sie aber auch Security-Teams als „Power-up“. KI kann beispielsweise eingesetzt werden, um:

- **Anwendungen von Grund auf noch sicherer zu machen:** So wie Bedrohungsakteure KI nutzen können, um nach Schwachstellen und Sicherheitslücken zu suchen, können dies auch Anwendungsprovider tun – mit dem Vorteil, dass sie Software und Systeme bereits vor Release härten können.
- **die automatisierte Threat Detection zu verbessern:** Kontext- und Verhaltensanalysen sind bereits in der Lage, intelligente Risikobewertungen durchzuführen und mehrstufige Identity Threats zu erkennen, und Fortschritte in der KI werden diese Features weiter verbessern und neue hervorbringen.
- **Risiken zu minimieren:** Egal, ob es um die Automatisierung von Schutzmaßnahmen (z. B. Eindämmung, Blockieren bösartiger Aktivitäten) oder um die Kombination eines Alerts mit einem empfohlenen Playbook geht – KI wird bei der proaktiven Risikominimierung und der Reaktion auf Angriffe von unschätzbarem Wert sein.

Nun, da die Bühne bereitet ist, können wir mit unserer Reise zur Login-Box – und darüber hinaus – beginnen. ■

Teil 1: Vor der Login-Box

Ziel dieser ersten Schutzmaßnahmen ist es, zu verhindern, dass eine unbefugte Entität – Mensch oder Maschine/System – auf die Login-Schnittstelle zugreifen kann.

Je früher eine böswillige Entität herausgefiltert werden kann, desto besser, da dies die Rechenkosten reduziert und die Erkundungsmöglichkeiten des Angreifers einschränkt (z. B. durch Empfang und Analyse von Fehlermeldungen).

Zu diesem Zweck gibt es eine Reihe von Schutzmaßnahmen auf verschiedenen Ebenen der Identity-Infrastruktur:

- **Hosting-Schutz**, der vom Hosting-Provider (z. B. Microsoft Azure, Amazon Web Services) oder auf dem Hosting Layer (z. B. Cloudflare) angewendet wird
- **Plattform-Schutz**, der für eine CIAM-Plattform als Ganzes greift (z. B. Okta Customer Identity Cloud)
- **Anwendungsschutz**, der für eine einzelne CIAM-Anwendung greift (z. B. eine inhouse entwickelte Einzellösung)

Teil 1: Vor der Login-Box

Die erste Abwehrlinie sind Host-basierte Lösungen

Hosting-Provider bieten eine Reihe von Security-Features an, um den Missbrauch der von ihnen gehosteten Services zu verhindern, darunter:

- **DDoS-Abwehr (Distributed Denial of Service):** Schutzmaßnahmen sorgen dafür, dass Ihre CIAM-Anwendung auch bei groß angelegten Angriffen (insbesondere auf TCP-/UDP-Ebene) für legitime User verfügbar bleibt
- **Bot-Management:** Eine erste Ebene des Bot Filtering basiert in der Regel auf einer Kombination aus Verhaltensanalyse, Threat Intelligence und Feedbackschleifen
- **Rate Limiting:** 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

Teil 1: Vor der Login-Box

Schutzmaßnahmen auf Plattform- und Anwendungsebene profitieren vom Netzwerkeffekt

Diese Schutzmaßnahmen reichen von taktischen bis hin zu strategischen und sind am effektivsten, wenn sie in Kombination eingesetzt und an die jeweiligen Bedürfnisse angepasst werden.

Zudem profitieren sie in hohem Maße von Netzwerkeffekten. Eine CIAM-Plattform, die Customer-Identity-Services für hunderte oder tausende von Unternehmen bereitstellt, kann im Vergleich zu einer isolierten CIAM-Anwendung ein Vielfaches an Threat Intelligence sammeln, was jedem Unternehmen auf der Plattform zugutekommt. Beispielsweise können IPs, die einen Tenant angreifen, für alle Tenants gesperrt werden.

Rate Limiting

Rate Limiting (Drosselung) ist ein nützliches Tool zur Abwehr von Brute-Force-Angriffen mit hohem Volumen durch Begrenzung der Rate, mit der eine bestimmte Entität mit der CIAM-Plattform als Ganzes oder mit der CIAM-Anwendung einzelner Unternehmen interagieren kann.

In beiden Szenarien kann eine Entität, die einen vordefinierten Schwellenwert (z. B. eine maximale Anzahl von Versuchen pro Stunde) überschreitet,

- dazu aufgefordert werden, eine Challenge (z. B. CAPTCHA) zu absolvieren
- bis zum Ablauf einer gewissen Zeitspanne für den Zugriff auf die Login-Schnittstelle gesperrt werden

Darüber hinaus ist Rate Limiting ein wirksames Mittel, um die Auswirkungen von DDoS-Angriffen auf den Identity-Service einzudämmen. Bei Websites und Services, deren Funktionalitäten hinter einem Login geschützt sind, hat eine Überlastung des Authentisierungs-Service das gleiche Ergebnis zur Folge wie jede andere Art von DoS-Angriff: legitime Kunden können den Service nicht mehr nutzen.

Suspicious IP Blocking

Das Blockieren verdächtiger IPs für den Zugriff auf Internet-Services wird seit Jahrzehnten eingesetzt und ist auch heute noch nützlich – vorausgesetzt, man ist sich der Grenzen bewusst.

Das Prinzip ist einfach:

- Anhand eines bestimmten Faktors wird ermittelt, ob eine IP-Adresse vertrauenswürdig ist
- Adressen, die unter eine bestimmte Vertrauensschwelle fallen, wird der Zugriff auf die Anwendung verweigert

Dieselbe allgemeine Technik lässt sich auch auf Telefonnummern, E-Mail-Adressen (einige Anwendungen erlauben beispielsweise nur Usern kostenpflichtiger E-Mail-Services die Registrierung) und andere Variablen anwenden.

Um diese Filterung zu erleichtern, abonnieren viele Unternehmen Cybersecurity Threat Intelligence (CTI), andere führen eine proprietäre Reputations-Datenbank, die auf ihren eigenen unmittelbaren Beobachtungen beruht, und wieder andere kombinieren diese Ansätze.

Bot Detection

Bot-Traffic beeinträchtigt den Identity-Flow an allen Punkten der User Journey. Er ist nicht nur lästig (um es vorsichtig auszudrücken), sondern verursacht auch versteckte Kosten. Man bedenke, dass die Customer Identity Cloud jeden Monat Milliarden von Bot-induzierten Login-Requests verzeichnet, was für Anwendungsprovider potenziell Millionen von Dollar an Rechenkosten bedeutet, nur um diesen fingierten Traffic zu bewältigen.

Durch die Analyse einer Vielzahl von Datenquellen und Beobachtungen ist es möglich, mit hoher Sicherheit festzustellen, wann ein Verbindungsversuch von einem Bot stammt.

In einem solchen Fall kann der Request blockiert oder ignoriert, oder die Entität mit einer Challenge wie einem CAPTCHA konfrontiert werden.

Einsatz von Bots zur Bekämpfung von Bots

Als wesentlicher Bestandteil des Attack Protection-Add-ons der Customer Identity Cloud, minimiert das Bot Detection Feature das Schadenspotenzial geskripteter Angriffe z. B. Credential Stuffing, Password Guessing, Passwort Spraying) gegen native Anwendungen, **passwortlose** Flows und benutzerdefinierte Login-Pages.

Durch die Analyse von mehr als 60 Datenquellen – wie frühere Ereignisse im Zusammenhang mit einer IP-Adresse, die jüngste Login-Historie, IP-Reputationsdaten und eine Reihe anderer Faktoren – prognostiziert Bot Detection, wann ein Identity Request wahrscheinlich von einem Bot stammt. Ab einem bestimmten Schwellenwert wird eine Gegenmaßnahme, z. B. ein CAPTCHA, ausgelöst.

Bot Detection ist ein hervorragendes Beispiel dafür, wie KI ältere Techniken verbessern kann:

- Die erste Version, die im Februar 2021 gelauncht wurde, war regelbasiert und erkannte 18 % der Bots
- Die zweite Version, die im August 2021 gelauncht wurde, nutzte Machine Learning zur Verhaltensanalyse. Dieser KI-gestützte Ansatz verdoppelte die Effizienz und erkannte 45 % der Bots
- Die jüngste Version, die im Juni 2022 auf den Markt kam, erkannte 79 % der Bots — die bisher beste Performance, und das, obwohl die Bedrohungsakteure ihre eigenen Techniken ständig verfeinern

Ein zentraler Aspekt ist dabei, dass der zusätzliche Schutz keinen unnötigen Mehraufwand für die Nutzer bedeutet— Durch sorgfältiges Training und kontinuierliche Optimierung der KI, die im Mittelpunkt der Bot-Detection steht, können wir sicherstellen, dass Anwender nur selten ein CAPTCHA beantworten müssen.

Darüber hinaus hat eine detaillierte interne Studie, in der die Vorher-Nachher-Effekte der Bot Detection untersucht wurden, einen starken Abschreckungseffekt gezeigt:

- Im Durchschnitt stellten die Kunden, die Bot Detection aktiviert hatten, einen Rückgang des bösartigen Traffic um mehr als 40 % fest
- Bei einigen größeren Kunden in der Studie ging der Bot-Traffic um fast 90 % zurück

Diese Ergebnisse deuten darauf hin, dass Angreifer Unternehmen mit modernsten Schutzmaßnahmen lieber meiden.■

Teil 2: An der Login-Box

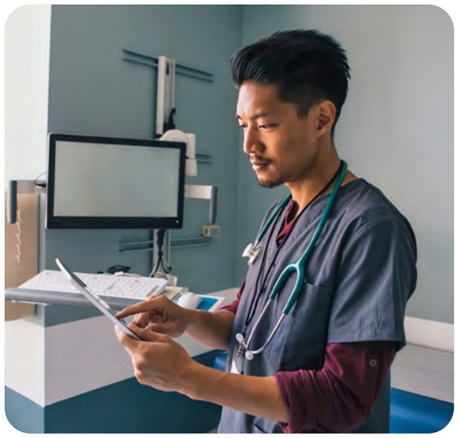
Böswillige Akteure, die es bis zur Login-Box geschafft haben, haben bereits eine Reihe von Hürden genommen. An dieser Stelle kann ein legitimer User zwei Aktionen durchführen:

- sich für einen Account registrieren
- sich in einen bestehenden Account einloggen

Wie wir sehen werden, zielen Bedrohungsakteure routinemäßig auf beide Services ab.

Teil 2: An der Login-Box

Signup-Promotions ziehen Angreifer magisch an

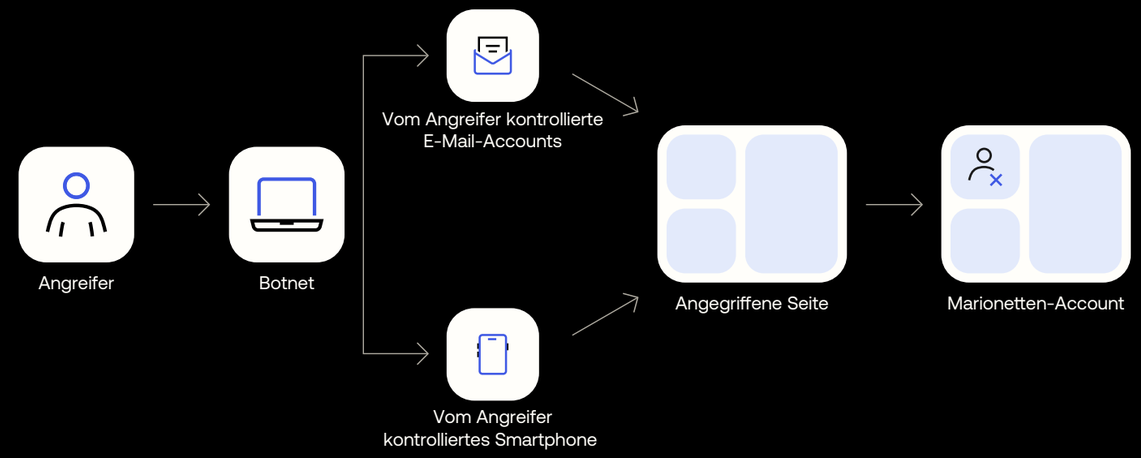


Der einfachste Weg für einen böswilligen Akteur, Zugriff auf Privilegien, Services und Informationen hinter der Login-Box zu erhalten, ist, von Anfang an Puppet-Accounts unter seiner Kontrolle zu erstellen.

Es gibt eine Reihe möglicher Motive für ein solches Vorgehen, darunter:

- **Bevorzugter Zugang zu etwas Wertvollem**, wie z. B. limitierten Sneakers, Konzertkarten, stark nachgefragten neuen Videospielkonsolen etc.
- **Awards oder Incentives in Verbindung mit der Accounterstellung**, wie etwa Geschenkkarten, Krypto-Tokens etc.
- **Spamming-, Desinformations- oder Hacktivismus-Kampagnen**, bei denen Accounts zur Teilnahme an Threads oder zur Verstärkung von Nachrichten verwendet werden
- **Synthetischer Identitätsdiebstahl**, bei dem häufig Accounts von Finanzdienstleistern und Versorgungsunternehmen verwendet werden
- **Weiterverkauf von Accounts** an interessierte Dritte
- **Beeinträchtigung der Fähigkeit des Anwendungsproviders, Services bereitzustellen**, indem der Namespace potenzieller User ausgeschöpft wird und dadurch legitime User an der Registrierung gehindert werden
- **Optimierung von ATO-Angriffen** durch Verwendung von Puppet-Accounts zur gezielten Manipulation der Login-Erfolgs- und Misserfolgsraten, um automatische Schutzmaßnahmen auszuhebeln

Abbildung 2: Anatomie einer betrügerischen Anmeldung



Anmeldebetrug richtet sich vor allem gegen Unternehmen, die im B2C-Bereich tätig sind, insbesondere gegen solche, bei denen ein User kostenlos und ohne Vorbedingungen (z. B. Kaufnachweis) ein Konto erstellen kann.

Vor allem in großem Umfang kann Anmeldebetrug erhebliche Probleme und unnötige Kosten verursachen.

Erstens können Fake-User die Erfahrung legitimer User negativ beeinflussen (z. B., indem sie ihnen begehrte Produkte wegschnappen), was zu Kundenunzufriedenheit und Reputationsschäden für das Unternehmen führt; außerdem verbrauchen sie Ressourcen und können ihren Zugriff missbrauchen, um das Unternehmen direkt anzugreifen oder zu schädigen.

Zweitens: Da eines der Hauptziele von B2C-Unternehmen darin besteht, potenzielle Kunden in Erstkunden umzuwandeln, werden die gesamten Konversionsprozesse häufig auf der Grundlage von Analysedaten optimiert, die zeigen, wie die User mit dem Service interagieren. Anmeldebetrug verfälscht diese Daten, was Geschäftsanalysen erheblich erschwert und zu kostspieligen Bereinigungsprojekten führen kann.

Da insbesondere B2C-Unternehmen so sehr auf die Maximierung der Konversionsraten angewiesen sind, besteht leider ein großer Anreiz, die Reibungsverluste während des Registrierungsprozesses zu minimieren –weniger Hürden für legitime User bedeuten allerdings auch weniger Hürden für Cyberkriminelle.

Ein Angreifer kann versuchen, nur eine relativ geringe Anzahl an Puppet-Accounts zu erstellen, oder er kann ein Botnet verwenden, um die Erstellung einer großen Anzahl an Accounts – Tausende oder gar Millionen – zu automatisieren. Letztgenanntes Szenario kann durch Listen mit häufig verwendeten Usernamen unterstützt werden.

Ein plötzlicher Anstieg der fehlgeschlagenen Signups (oder der Rate fehlgeschlagener Signups) ist ein deutlicher Indikator dafür, dass Ihre Anwendung angegriffen wird. In diesem Fall sollten Sie sich den Registrierungs-Traffic genauer ansehen und prüfen, ob Schwellenwerte oder Regeln modifiziert werden sollten.

Aggregierte Betrachtung

Abbildung 3 zeigt eine aggregierte (d. h. technologieübergreifende) Betrachtung der Anmeldebetrugsversuche über einen Zeitraum von 30 Monaten. Bereits auf den ersten Blick stechen zwei Dinge ins Auge:

1. Anmeldebetrug ist bei Customer-Signup-Services allgegenwärtig
2. Das Volumen der Anmeldebetrugsversuche (und damit ihr „Beitrag“ zur Gesamtzahl der Anmeldeversuche) schwankt stark von Tag zu Tag

Etwas weniger offensichtlich sind zwei wichtige Trends.

Erstens ist der tägliche Anteil betrügerischer Anmeldeversuche in der Spitze im selben Zeitraum zurückgegangen:

- Im Jahr 2021 machten betrügerische Anmeldeversuche nicht selten (93 Fälle) noch die Mehrheit der gesamten Anmeldeversuche an einem bestimmten Tag aus, und es gab 19 Fälle, in denen mehr als 70 % der Anmeldeversuche betrügerisch waren
- Im Jahr 2022 machten betrügerische Anmeldeversuche nur in fünf Fällen mehr als 60 % der Anmeldeversuche aus
- Im ersten Halbjahr 2023 wurden nur an einem Tag (dem 15. April) mehr als 50 % der Anmeldeversuche als betrügerisch eingestuft

Zweitens ist der Anteil betrügerischer Anmeldeversuche an der Gesamtzahl der Anmeldeversuche in diesem 30-monatigen Zeitraum deutlich zurückgegangen:

- Im Jahr 2021 wurden 31,8 % der Anmeldeversuche als betrügerisch eingestuft
- Im Jahr 2022 sank dieser Anteil auf 18,6 %
- Im ersten Halbjahr 2023 war der Anteil auf 13,9 % gesunken

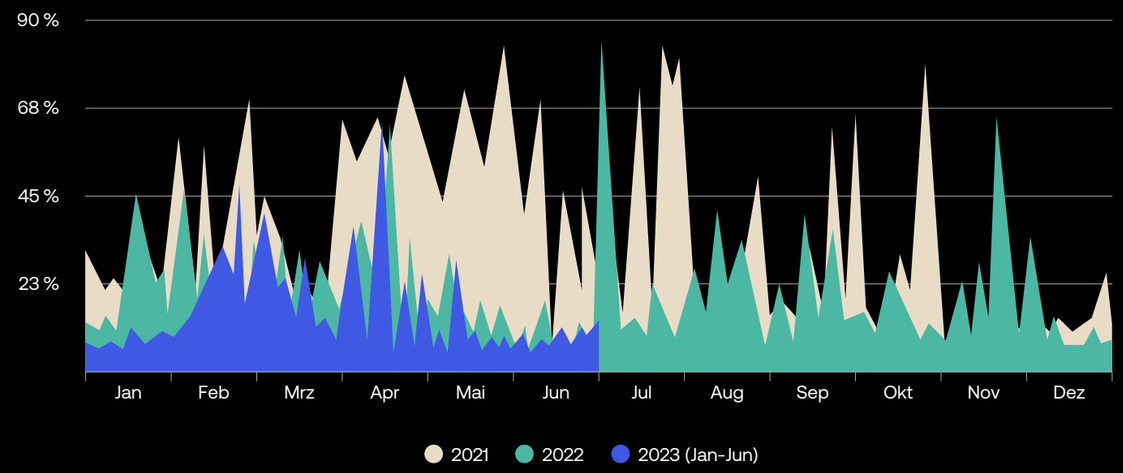
Wir gehen davon aus, dass der Hauptgrund für diese positiven Trends in der kontinuierlichen Verbesserung der mehrstufigen Schutzmechanismen der Technologie liegt und nicht in einem starken Rückgang der Versuche böswilliger Akteure, betrügerische Accounts zu erstellen (wir werden auf diese Hypothese in Kürze zurückkommen).

Es ist auch wichtig zu erkennen, dass nur die hartnäckigsten Angreifer die erforderlichen Schwellenwerte erreichen, um als betrügerisch eingestuft zu werden; außerdem implementieren viele Tenants Kontrollen, die böswillige Anmeldeversuche verhindern, sobald eine Entität als Teil eines Anmeldebetrugsversuchs identifiziert wurde – wenn das der Fall ist, werden diese Versuche nicht einmal als betrügerische Anmeldeereignisse gezählt/geloggt.

Darüber hinaus – und bitte verzeihen Sie die Wiederholung, aber das ist wirklich ein wichtiger Punkt – haben böswillige Akteure bereits einen Spießrutenlauf durch Host-, Plattform- und Anwendungs-Schutz absolviert, bevor sie den Login-Screen überhaupt zu Gesicht bekommen.

Aus diesen Gründen sollten die oben genannten und in den folgenden Abbildungen dargestellten Prozentsätze als absolutes Minimum betrachtet werden. Realistisch betrachtet besteht für einen Signup-Service ohne mehrere Schichten robuster Schutzmaßnahmen die große Gefahr, von geskripteten Accountregistrierungen überflutet – wenn nicht gar völlig erdrückt – zu werden.

Abbildung 3: Betrügerische Registrierungen sind eine allgegenwärtige Bedrohung. Ihr Anteil an der Gesamtzahl der Registrierungsversuche in der Customer Identity Cloud nimmt dank innovativer neuer Funktionalitäten unserer Produkte ab.



Segmentanalyse

Eine genauere Betrachtung der zugrundeliegenden Daten zeigt, dass betrügerische Anmeldeversuche ungleichmäßig verteilt sind.

Von den zehn in der Customer Identity Cloud am stärksten vertretenen Branchen weisen Finanzdienstleistungen (28,8 %), Medien (28,4 %), produzierende Industrie (25,1 %) und Software/SaaS/Technologie (24,0 %) alle einen überdurchschnittlich hohen Anteil an betrügerischen Anmeldeversuchen auf (Abbildung 4).

Warum sind Accounts aus diesen Branchen bei Angreifern so beliebt? Das lässt sich nicht mit Sicherheit sagen, und die Antworten können sehr vielfältig sein, aber hier sind einige mögliche Erklärungen:

- Finanzdienstleister und -institute bieten häufig Willkommensboni und andere Vergünstigungen (z. B. Travel Points, niedrigere Zinssätze) für neue Accounts an, und alles, was einen Geldwert hat, ist für Cyberkriminelle attraktiv. Accounts können auch für Geldwäsche und als Sprungbrett für synthetischen Identitätsdiebstahl missbraucht werden.
- Medien bieten häufig Kommentarforen, sodass die Kontrolle über Accounts die Möglichkeit bietet, Desinformationen, Hassbotschaften, Propaganda, Spam-Links und andere schädliche Inhalte an ein breites Publikum zu verteilen.
- Unternehmen der produzierenden Industrie sind bei Cyberkriminellen sehr beliebt, da jede Produktionsunterbrechung den Druck erhöht, Lösegeldforderungen zu erfüllen – daher ist es möglich, dass zumindest einige betrügerische Accounts als Teil längerer Angriffsketten erstellt werden. Darüber hinaus bieten Hersteller, die direkt an Verbraucher verkaufen, möglicherweise besonderen Zugang zu Produktionsläufen oder Artikeln mit begrenztem Lagerbestand, was es für potenzielle Wiederverkäufer attraktiv macht, eine große Anzahl an Accounts zu erstellen.
- Viele Software-/SaaS-/Technologie-Services verwenden ein Freemium-Modell, bei dem ein oder mehrere Faktoren (z. B. Nutzungsstunden, Speichervolumen, verfügbare Rechenressourcen usw.) begrenzt sind; betrügerische Accounts können ein Versuch sein, diese Beschränkungen zu umgehen.

Bitte beachten Sie: Weitere Hintergründe zur Analyse nach Branche finden Sie in Anhang C.

Interessanterweise scheint der Anteil betrügerischer Anmeldeversuche bei Groß- und Kleinunternehmen deutlich höher zu sein als bei mittelständischen Unternehmen (Abbildung 5).

Cyberkriminelle haben die gleichen wirtschaftlichen Anreize wie legitime Unternehmen und versuchen, ihren Gewinn zu maximieren, sodass die Beobachtungen darauf hindeuten, dass der erwartete Wert eines Anmeldebetrugs bei Groß- und Kleinunternehmen höher ist als bei mittelständischen Unternehmen.

Wir dürfen annehmen, dass Cyberkriminelle davon ausgehen, dass Unternehmen gut geschützt sind (d. h., dass die Erfolgschancen relativ gering sind), dass aber der Return on Investment (ROI) eines erfolgreichen Angriffs hoch genug ist, um den Aufwand zu rechtfertigen.

Bei Kleinunternehmen kann genau das Gegenteil der Fall sein: Der Gewinn pro Angriff ist geringer, aber die Erfolgsaussichten sind so hoch, dass sich ein Angriff lohnt.

Bitte beachten Sie: Weitere Hintergründe zur Analyse nach Unternehmensgröße finden Sie in Anhang D.

Weitere Unterschiede ergeben sich, wenn man nach den Regionen aggregiert, in denen Unternehmen ihren Hauptsitz haben (Abbildung 6). Unternehmen mit Sitz in Nord- und Südamerika (9,4 %) und in der EMEA-Region (8,1 %) weisen einen vergleichsweise deutlich geringeren Anteil an betrügerischen Anmeldeversuchen auf als Unternehmen mit Sitz in der APAC-Region (27,9 %).

Eine solch starke Diskrepanz zwischen APAC und den anderen Regionen kann ein Symptom für einen weniger ausgereiften Identity-Security-Ansatz sein, der sich in einer geringeren Anzahl von Security-Produkten und -Features in der Accountregistrierungspipeline manifestiert.

Bitte beachten Sie: Weitere Hintergründe zur Analyse nach Region finden Sie in Anhang E.

Abbildung 4: Finanzdienstleister und Medienunternehmen weisen einen überdurchschnittlich hohen Anteil an betrügerischen Registrierungsversuchen auf

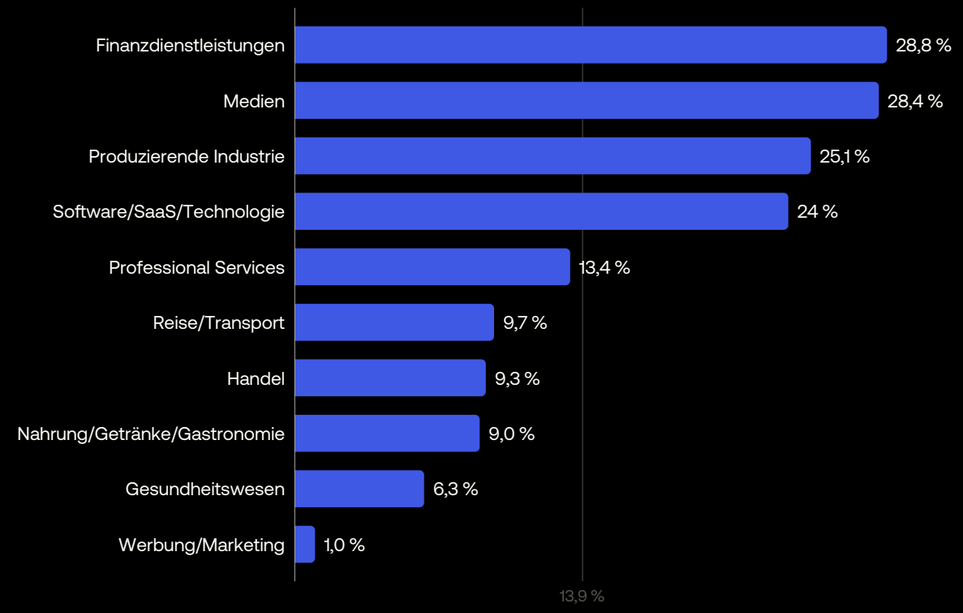


Abbildung 5: Betrügerische Registrierungen scheinen in Großunternehmen und Kleinbetrieben besonders häufig zu sein

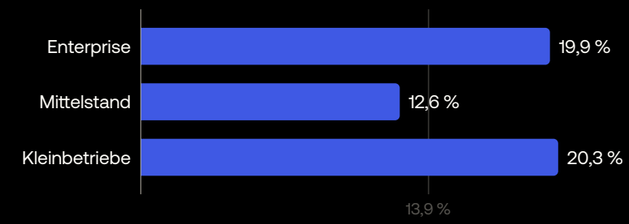
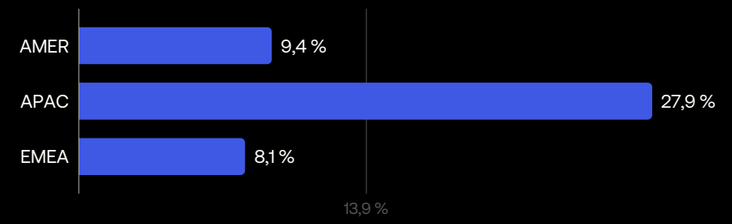


Abbildung 6: Unternehmen in der APAC-Region verzeichnen einen wesentlich höheren Anteil an betrügerischen Anmeldeversuchen als Unternehmen in Nord-, Mittel- und Südamerika oder EMEA



Schutzmaßnahmen

Zusätzlich zu den Schutzmaßnahmen vor dem Zugriff auf die Login-Box gibt es eine Reihe weiterer Ansätze, die zur Reduzierung betrügerischer Anmeldeversuche eingesetzt werden können, darunter:

- **Regeln und Aktionen vor dem Signup** (z. B. eine Challenge erzwingen, mehr Informationen anfordern), um die Wahrscheinlichkeit eines Fake-Users weiter zu verringern
- **Social Login**, um den Schutz vor betrügerischen Anmeldeversuchen „outzusourcen“
- **Identitätsprüfung**, wenn das Risiko als besonders hoch eingeschätzt wird
- **Validierung von Kontaktinformationen** (z. B. E-Mail-Adresse, Telefonnummer) durch einen One-Time Passcode oder einen **Magic Link**

Entscheidend ist, dass die Erkenntnisse aus Anmeldeversuchen, die – aus unterschiedlichsten Gründen – fehlschlagen, in die Gesamtbewertung der Threat Intelligence einfließen sollten. Beispielsweise sollte eine IP, die innerhalb eines bestimmten Zeitfensters (z. B. einer Stunde) versucht, eine bestimmte Anzahl von Accounts (z. B. 10) zu registrieren und dabei scheitert, als riskant eingestuft werden – wobei die Einstufung „riskant“ dazu führt, dass Verbindungsversuche von dieser IP auf Plattform- oder Anwendungsebene (d. h., vor der Login-Box) gefiltert werden.

Abgesehen von Social Login geht jedoch jeder der oben genannten Ansätze mit zusätzlichen Reibungsverlusten im Anmeldeprozess einher – es muss also darauf geachtet werden, die richtige Balance zu finden.

Darüber hinaus müssen sich Unternehmen darüber im Klaren sein, dass Bedrohungsakteure damit begonnen haben, SMS- und Anruf-basierte Validierungsmethoden zu missbrauchen (siehe unten).

Threat Spotlight: SMS Pumping und Mautbetrug

Die flächendeckende Verfügbarkeit der SMS macht sie zu einem attraktiven Kanal für Identity-Prozesse. So bieten oder erlauben die Signup-Prozesse vieler Sites beispielsweise nur SMS-basierte Registrierung (z. B. Toast, Uber), und SMS ist ein beliebter Mechanismus zur Übermittlung von Registrierungs- und MFA-Challenges (z. B. **OTPs** und Magic Links).

Leider missbrauchen Angreifer Formularfelder, um Anwendungsprovider dazu zu bringen, SMS-Nachrichten oder Telefonanrufe an Premium-Rate-Nummern zu senden – und sich so einen Teil der Einnahmen zu sichern.

In beiden Fällen trägt das Unternehmen, deren Anwendung missbraucht wird, die Kosten, die beträchtlich sein können – im Februar 2023 behauptete Elon Musk, dass Twitter 60 Millionen US-Dollar pro Jahr aufgrund „gefälschter 2FA-SMS-Nachrichten“ verliert.

Wie bei den anderen in diesem Report untersuchten Angriffen haben Bedrohungsakteure Taktiken entwickelt, um das Risiko, entdeckt zu werden, zu verringern. Zum Beispiel:

- wechseln sie die Telefonnummern, um zu vermeiden, dass die Schwellenwerte pro Nummer überschritten werden
- gehen sie unauffällig und langsam vor und dehnen den Angriff über viele Tage, Wochen oder Monate hin aus (im Grunde so lange wie nur irgend möglich, bevor sie erwischt werden)

Viele Unternehmen verlassen sich bei der User-Registrierung und -Authentisierung auf SMS, sodass ein einfaches Abschalten dieses Kanals keine praktikable Option ist. Stattdessen braucht die Identity-Infrastruktur ein hochintelligentes Verfahren, um Telefonbetrug zu verhindern oder einzudämmen.

Social Login

Social Login bietet **Single Sign-on (SSO)** für Endanwender. Unter Verwendung bestehender Login-Informationen von einem Social-Networking-Provider wie Facebook, Twitter oder Google, kann sich der User einfach bei einem Third-Party-Service registrieren (und anschließend einloggen), anstatt einen neuen Account zu erstellen.

Neben einer nahtlosen User Experience kann Social Login auch zur Bekämpfung von Anmeldebetrug beitragen – *wenn der Provider starke Schutzmaßnahmen implementiert hat.*

Die Herausforderung besteht darin, dass sich die Services in dieser Hinsicht unterscheiden, sodass die Anwendungsprovider entscheiden müssen, welche Drittanbieter vertrauenswürdig sind.

Social Login bietet auch andere potenzielle Vorteile für Anwendungsprovider, darunter:

- **Mehr Registrierungen:** Viele User ziehen es vor, einen bestehenden Account wiederzuverwenden, anstatt einen neuen zu erstellen
- **Verifizierte E-Mail:** Der Social-Network-Provider ist für die Verifizierung der E-Mail-Adresse des Users verantwortlich. Wenn der Provider diese Informationen weitergibt, erhalten Sie eine echte E-Mail-Adresse anstatt der gefälschten, die häufig für die Registrierung bei Webanwendungen verwendet werden. Social-Provider kümmern sich auch um den Password-Recovery-Prozess
- **Bessere Personalisierungs- und Anpassungsmöglichkeiten:** Social-Networking-Provider können Ihnen zusätzliche Informationen zur Verfügung stellen, denen die User zugestimmt haben, z. B. Standort, Interessen, Geburtstag usw., die Sie nutzen können, um Ihre Services zu verbessern
- **One-Click-Return-Erfahrung:** Nachdem sich User mit Social Login bei Ihrer Anwendung registriert haben, können sie einfach zurückkehren, da sie wahrscheinlich in ihrem sozialen Netzwerk eingeloggt sind und ein Klick genügt, um sich in Ihrer Anwendung einzuloggen

Identitätsprüfung

Eines der häufigsten Missverständnisse im Zusammenhang mit CIAM ist, dass Authentisierung und Identitätsprüfung gleichbedeutend sind. Während die Authentisierung (z. B. der Login mit Username und Passwort) zeigt, dass ein User über die Credentials für einen bestimmten Account verfügt, beweist sie nicht, dass der User derjenige ist, der er vorgibt zu sein. Hier kommt die Identitätsprüfung ins Spiel.

Die Identitätsprüfung verwendet zusätzliche Verifizierungen, um ein hohes Maß an Vertrauen darin zu schaffen, dass Ihre potenziellen Kunden die sind, die sie vorgeben zu sein.

Im Zusammenhang mit CIAM ist es wichtig, dass Lösungen zur Identitätsprüfung skalierbar sind, da CIAM in der Regel Echtzeit-Workflows erfordert, um die mit saisonalen Schwankungen und erfolgreichen Werbeprogrammen verbundenen Spitzen zu bewältigen. Glücklicherweise wurde in den letzten Jahren eine Reihe von automatisierten Identitätsprüfungsverfahren entwickelt, um den realen Anforderungen der Kundenregistrierung gerecht zu werden:

- **Wissensbasierte Authentisierung (KBA)**, die sich etwas zunutze macht, was ein User – und im Idealfall nur er – weiß
- **Dokumentenscan und Kreuzvalidierung**, bei der anhand eines vertrauenswürdigen Lichtbildausweises – z. B. Reisepass oder Führerschein – überprüft wird, ob die behauptete Identität eines Users mit seiner tatsächlichen Identität übereinstimmt
- **Telefonproviderverifizierung**, bei der ausgenutzt wird, dass die Identität des Users bereits bei der Registrierung für einen Telefonservice nachgewiesen wurde

Teil 2: An der Login-Box

Die Mehrfach-verwendung von Passwörtern öffnet Account-Übernahmen Tür und Tor

Während betrügerische Anmeldungen (mindestens) ein kostspieliges Ärgernis sind, stellen Account Takeovers eine größere Bedrohung für Sicherheit und Datenschutz dar.

In einem B2C-Kontext können Angreifer 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 (PII) erlangen.

In einem B2B-Kontext kann ein Angreifer, dem es gelingt, einen User-Account zu kompromittieren, über diesen Account Zugang zu hochsensiblen Daten erlangen – ein Breach, der für das betroffene Unternehmen schwerwiegende rechtliche und vertragliche Sanktionen nach sich zieht.

Obwohl einige ATO-Versuche auf Einzelpersonen abzielen (wir werden einige Ansätze in Teil 3 untersuchen), sind die meisten Brute-Force-Angriffe (z. B. T1110), die eine oder mehrere der folgenden Techniken anwenden:

- **Credential Stuffing** (z. B. T1110.004): Ein Bedrohungsakteur versucht, bekannte Credentials (z. B. aus einem Breach/Dump) bei anderen Websites und Services zu verwenden
- **Password Spraying** (z. B. T1110.003): Ein Bedrohungsakteur probiert eine relativ kurze Liste der am häufigsten verwendeten Passwörter über viele verschiedene Accounts hinweg aus
- **Password Guessing** (z.B. T1110.001): Ein etwas gröberer Ansatz, bei dem ein Bedrohungsakteur viele Passwörter über eine beliebige Anzahl an Accounts hinweg ausprobiert

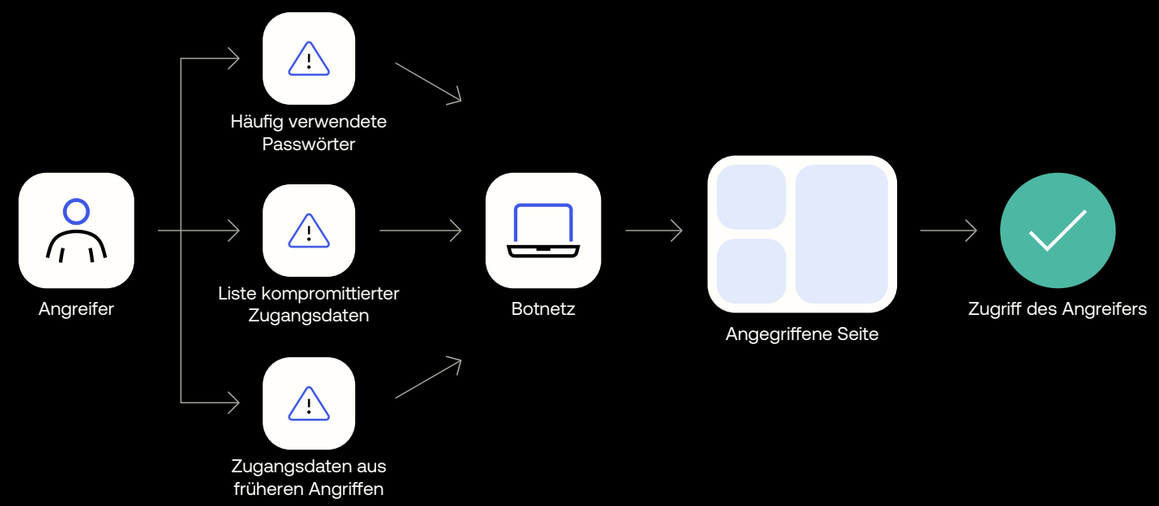
Es ist zu beachten, dass jeder dieser Angriffe, wenn er in ausreichendem Umfang durchgeführt wird, zu einer Verlangsamung der Authentisierung für legitime User oder sogar zu einem vollständigen Ausfall des Authentisierungsservices führen kann – ob beabsichtigt oder nicht.

Alle drei Ansätze basieren auf schlechten Passwortgewohnheiten der User (z. B. einfache Passwörter, Wiederverwendung von Passwörtern) – ein weit verbreitetes Problem, das die Kosten und den Aufwand für die Durchführung dieser Angriffe drastisch reduziert. Kleine Optimierungen – einschließlich der Verwendung von Listen geleakter Passwörter und Wörterbüchern mit häufig darin verwendeten Wörtern – kann die Wahrscheinlichkeit drastisch erhöhen, das richtige Passwort zu versuchen (oder, genauer gesagt, ein Passwort, das den gleichen Hashwert wie das richtige Passwort hat).

Von den drei oben beschriebenen Angriffen ist Credential Stuffing der effektivste (aus Sicht des Bedrohungsakteurs) und der gefährlichste (aus Sicht des Anwendungsproviders und seiner Kunden), da er präziser ist. Durch das Ausprobieren bekannter Paare von Usernamen und Passwörtern ist die Wahrscheinlichkeit, dass automatisierte Erkennungsmechanismen ausgelöst werden, etwas geringer.

Leider ist die Hürde für solche Angriffe sehr niedrig, und Bedrohungsakteure versuchen, die Schutzmaßnahmen mit einer Reihe von Taktiken auszuhebeln. Beispielsweise kann ein Angreifer bekannte gültige Credentials – vielleicht von betrügerischen Accounts, die bereits unter seiner Kontrolle stehen – in den Login-Stream einstreuen, um die Fehlerrate sorgfältig zu steuern:

Abbildung 7: Anatomie einer Credential-Stuffing-Attacke



Für raffiniertere Bedrohungsakteure sind Credential-Stuffing-Angriffe attraktiv, da die Grenzkosten nahe Null liegen. Betrachten wir eine über Abbildung 7 hinaus erweiterte Kill Chain, in der der Bedrohungsakteur einen Cybercrime-Service nutzt, um eine Phishing-Kampagne zu starten – mit dem Ziel, an Credentials zu gelangen. Es ist bekannt, dass die erbeuteten Credentials zum Zeitpunkt der Erbeutung aktiv sind, was es dem Bedrohungsakteur ermöglicht, einen Credential-Stuffing-Angriff mit einer hohen Erfolgsquote zu starten. In diesem Szenario reicht es aus, einige wenige Parameter in einem Skript zu ändern, um verschiedene Unternehmen und Services anzugreifen.

Neben Account Takeovers wird Credential Stuffing häufig auch für den Zwischenschritt der Accountidentifizierung/-validierung verwendet. Ein Bedrohungsakteur kann beispielsweise einen umfangreichen Credential Dump durch einen dedizierten Service laufen lassen und dann die validierte Liste zu einem hohen Preis verkaufen.

Aggregierte Betrachtung

Abbildung 8 zeigt einen 30-monatigen Überblick über Credential-Stuffing-Versuche in der Customer Identity Cloud. Ähnlich wie bei den betrügerischen Anmeldeversuchen lässt ein erster Blick vermuten, dass der Anteil der Anmeldeversuche, die auf Credential Stuffing zurückzuführen sind, in diesem Zeitraum deutlich zurückgegangen ist – was auch tatsächlich der Fall ist:

- Im Jahr 2021 waren 42,8 % der Anmeldeversuche auf Credential Stuffing zurückzuführen (wie bei den betrügerischen Anmeldeversuchen sind die für diese Bezeichnung zu erfüllenden Kriterien sehr streng, und wenn sie einmal als solche gekennzeichnet sind, werden weitere Versuche gar nicht erst protokolliert)
- Im Jahr 2022 betrug der Anteil 33,4 %
- Im ersten Halbjahr 2023 sank der Anteil auf 24,3 %

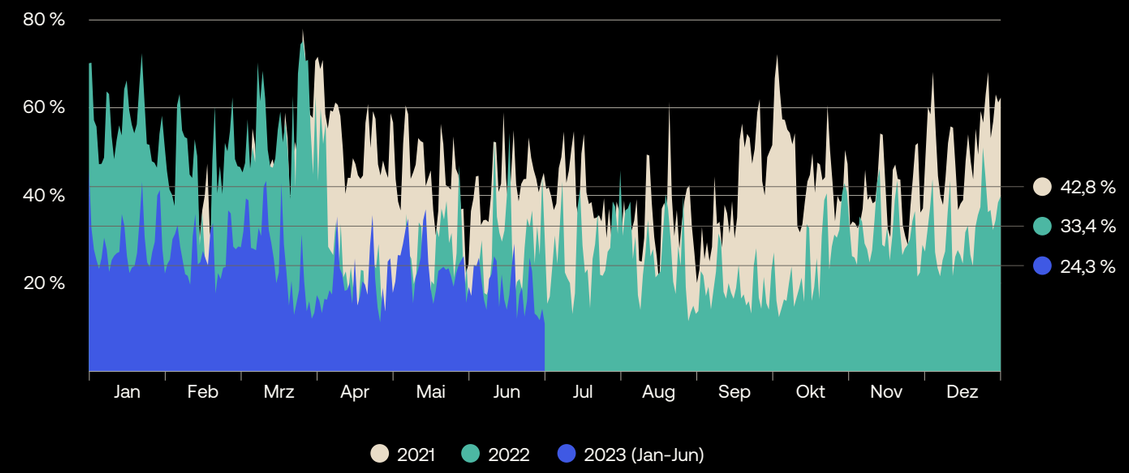
Eine genauere Betrachtung zeigt, dass es im April 2022 eine große Veränderung gab:

- Vom 1. Januar 2021 bis zum 31. März 2022 waren 47,3 % der Anmeldeversuche auf Credential Stuffing zurückzuführen
- Vom 1. Mai 2022 bis zum 30. Juni 2023 waren nur noch 24,6 % der Anmeldeversuche auf Credential Stuffing zurückzuführen

Was geschah im April 2022? Kurz gesagt wurde in den ersten beiden Wochen des Monats die Reihenfolge geändert, in der die Schutzebenen der Consumer Identity Cloud böswilligen Traffic filtern – Bot-Detection wurde „hochgestuft“, sodass sie früher in der Pipeline greift.

Wir glauben, dass diese eine Anpassung nicht nur für den drastischen und nachhaltigen Rückgang von Credential Stuffing und anderen Brute-Force-Angriffen auf die Login-Box verantwortlich ist, sondern auch für einen Großteil der Verbesserungen, die in der (auf betrügerische Anmeldeversuche bezogenen) Analyse in Abbildung 3 festgestellt wurden – was nicht nur die Bedeutung mehrerer Schutzebenen, sondern auch ihrer optimalen Organisation unterstreicht.

Abbildung 8: Der Anteil von Credential-Stuffing-Angriffen an der Gesamtzahl der Login-Versuche hat 2023 deutlich abgenommen. Ein Grund für diese Abnahme könnten die verbesserten Bot-Detection-Funktionalitäten der Customer Identity Cloud sein.



Segmentanalyse

Eine Segmentierung der technologieübergreifenden Beobachtungen nach Branchen (Abbildung 9) unterstreicht, wie problematisch Credential Stuffing für bestimmte Branchen ist.

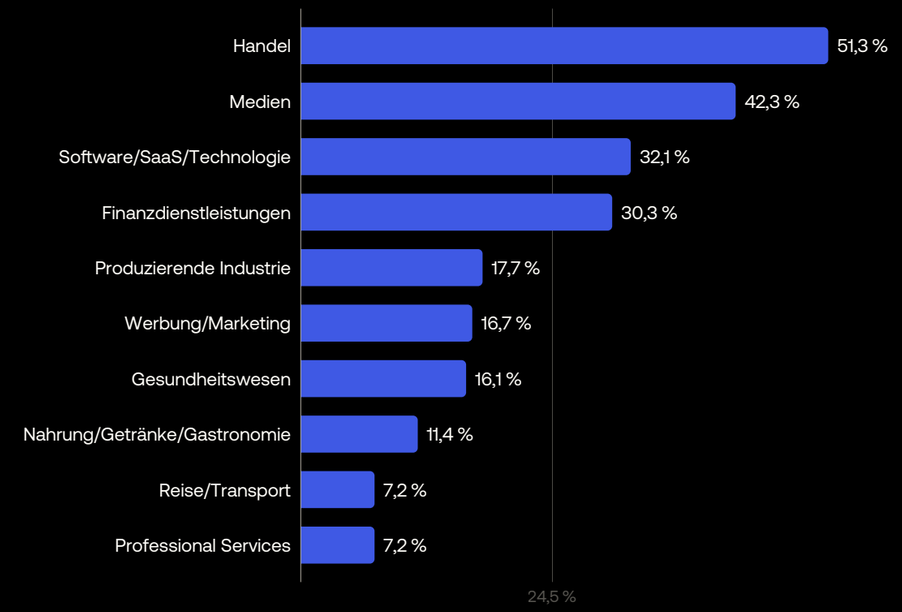
Im Bereich Einzelhandel/eCommerce sind mehr als die Hälfte (51,3 %) aller Anmeldeversuche auf Credential Stuffing zurückzuführen. Es liegt auf der Hand, dass Cyberkriminelle es auf solche Accounts abgesehen haben – sei es, um Treuepunkte zu stehlen, sich unrechtmäßig Zugriff auf begrenzte Ressourcen zu verschaffen, mit dem Geld anderer Leute einzukaufen, an Zahlungsinformationen zu gelangen oder aus anderen Gründen.

Medien sind ebenfalls mit einem sehr hohen Anteil von Credential-Stuffing-Versuchen (42,3 %) konfrontiert, wahrscheinlich aus den gleichen Gründen, die bereits untersucht wurden.

Den dritthöchsten Anteil weisen Software/SaaS/Technologie-Unternehmen auf (32,1 %). In diesem Fall ist es möglich, dass Angreifer den Account missbrauchen, um auf vertrauliche Informationen zuzugreifen und diese zu exfiltrieren – entweder, um sie direkt zu verwenden oder um sie in einen größeren Angriff zu integrieren. Ein Phishing-Versuch erscheint beispielsweise glaubwürdiger, wenn er sich auf Projektinformationen bezieht, die nur innerhalb eines vertrauenswürdigen Services verfügbar sind.

Abschließend sind auch Finanzdienstleister überdurchschnittlich häufig von Credential-Stuffing-Angriffen betroffen. Hier könnte ein Angreifer aus verschiedenen Motiven handeln, z. B., um personenbezogene Daten zu stehlen, zu verkaufen oder zu verwenden, um synthetischen Identitätsbetrug oder Finanzbetrug zu begehen (z. B., um Transaktionen und Überweisungen zu veranlassen).

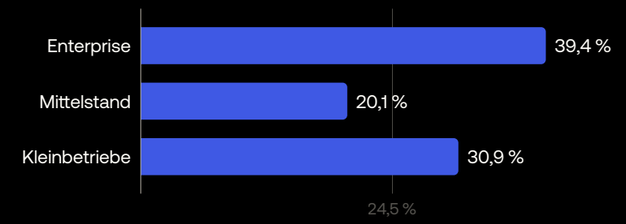
Abbildung 9: Einzelhandels- und E-Commerce-Unternehmen sehen sich einer außerordentlich hohen Zahl von Credential-Stuffing-Versuchen ausgesetzt, die fast doppelt so hoch ist wie der Durchschnitt



Wie bei den betrügerischen Anmeldeversuchen zeigt sich auch hier, dass der Anteil an Credential-Stuffing-Versuchen bei Klein- und Großunternehmen höher ist als bei mittelständischen (Abbildung 10).

Diese Beobachtung stützt die zuvor aufgestellte These, dass Klein- und Großunternehmen den höchsten ROI für Cyberkriminelle bieten, während mittelständische als nicht lukrativ angesehen werden können.

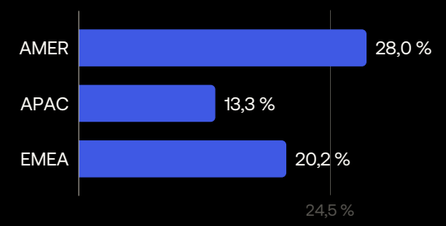
Abbildung 10: Große und kleine Unternehmen scheinen als Ziel attraktiver zu sein als mittelständische Anbieter, möglicherweise, weil der ROI für die Angreifer schwerer zu erreichen ist



Wie Abbildung 11 zeigt, sind Unternehmen mit Hauptsitz in Nord-, Mittel- und Südamerika häufiger von Credential-Stuffing-Versuchen betroffen (28,0 %) als Unternehmen in APAC (13,3 %) oder EMEA (20,2 %).

In Nord- und Südamerika sind überproportional viele Unternehmen aus den Branchen Einzelhandel/eCommerce, Medien, Software/SaaS/Technologie und Finanzdienstleistungen ansässig. Es ist möglich, dass diese Konzentration, sowohl aufgrund der Größe der Unternehmen als auch aufgrund von deren Bekanntheit bei Cyberkriminellen, zu dem im Datensatz beobachteten höheren Anteil an Credential-Stuffing-Versuchen beiträgt.

Abbildung 11: Unternehmen mit Sitz in Nord-, Mittel- und Südamerika sind häufiger Credential Stuffing-Versuchen ausgesetzt als Unternehmen mit Sitz in APAC oder EMEA



Passwörter verursachen Probleme

Wenn ein Accountinhaber dasselbe (oder ein ähnliches) Passwort auf mehreren Websites verwendet, führt dies zu einem Dominoeffekt, bei dem ein einziges Credential-Paar verwendet werden kann, um mehrere Anwendungen zu kompromittieren.

Realistischerweise ist nicht davon auszugehen, dass User ihre Passwortgewohnheiten kollektiv und spontan ändern werden. Der Customer Identity Trends Report 2023 von Okta hat beispielsweise Folgendes festgestellt:

- 33 % der Umfrageteilnehmer geben an, dass es sie frustriert, ein Passwort wählen zu müssen, das bestimmten Vorgaben genügt
- 25 % fanden es frustrierend, für jeden Online-Service ein neues Passwort erstellen zu müssen

Erschwerend kommt hinzu, dass aktive Accounts in der Regel nur einen Bruchteil der Accounts eines User ausmachen; viele andere werden vergessen oder aus anderen Gründen nicht gepflegt. Ein Breach bei einem dieser vernachlässigten Services kann einen Bedrohungsakteur mit einer großen Menge an User-Credentials und damit verbundenen personenbezogenen Daten versorgen.

Und Cyberkriminelle sind geschickt darin, diese Informationen in großem Umfang zu nutzen, um die Accounts von Verbrauchern bei anderen Marken zu kompromittieren. Der Data Breach Investigation Report (DBIR) 2023 von Verizon hat beispielsweise ergeben, dass 86 % der Webanwendungs-Breaches auf gestohlene Credentials zurückzuführen sind. Darüber hinaus sind Credentials und personenbezogene Daten (die verkauft, aber auch zur Wiederherstellung von Passwörtern missbraucht werden können) die am häufigsten exfiltrierten Daten – und befeuern kontinuierlich den Angriffszyklus.

Die Zukunft muss – und wird – anders aussehen.

Aus User-Sicht wird die traditionelle Login-Erfahrung zur seltenen Ausnahme, Passwörter werden zur letzten Authentisierungsoption – und mit der Abhängigkeit von Passwörtern verschwindet auch eine ganze Klasse von Identity-Angriffen.

Erfahren Sie mehr über diese vielversprechende Zukunft und darüber, was Sie heute tun können, in passwortlose Authentisierung: Maximierung der Conversions (und Verbesserung der Sicherheit) im Convenience-Zeitalter

Schutzmaßnahmen

Aufbauend auf den bereits ergriffenen Schutzmaßnahmen gibt es eine Reihe zusätzlicher Techniken, die dazu beitragen können, ATOs zu verhindern.

Zwei einfache Ansätze sind:

- **Impossible Travel:** Erkennen, wenn ein „User“ versucht, sich von einem Ort einzuloggen, den er innerhalb der Zeit, die seit seinem letzten erfolgreichen Login vergangen ist, nicht erreichen kann.
- **Social Login:** Social Login vereinfacht nicht nur den Login, sondern erhöht auch die Sicherheit, da ein User eher bereit ist, sich um den Schutz seiner wichtigen Social-Accounts zu kümmern.

Zu den fortgeschritteneren Techniken gehören Breached Password Detection, die Implementierung effektiver Passwortmanagement-Policies (einschließlich Zurücksetzen) und – für die höchste Stufe der Authentisierungssicherheit – starke MFA.

Aber der vielleicht effektivste und „einfachste“ Schutz gegen passwortbasierte ATOs ist der Verzicht auf Passwörter – eine Vision, die viel realistischer geworden ist, seit Apple, Google und Microsoft sich verpflichtet haben, einen gemeinsamen passwortlosen Login-Standard zu unterstützen.

Passkeys

Passkeys sind FIDO-Zugangsdaten, die von Browsern erkannt werden können oder in nativen Anwendungen oder Security Keys zur passwortlosen Authentisierung enthalten sind. Basierend auf den Standards der FIDO Alliance und des World Wide Web Consortium (W3C) ersetzen Passkeys Passwörter durch kryptographische Key-Paare und können auf die gleiche Weise abgerufen (d. h. verwendet) werden, auf die User ihre mobilen Endgeräte entsperren – in der Regel via Biometrie oder durch Eingabe eines Zugangscodes.

Passkeys gibt es in zwei Formen: gerätegebundene Passkeys und **synchronisierte Passkeys.**

Jeder gerätegebundene Passkey ist an ein bestimmtes Gerät gebunden, das als Besitzfaktor dient. Gerätegebundene Passkeys können mit FIDO-zertifizierten Authentifikatoren und Security Keys verwendet werden, einschließlich solcher, die eine Sicherheitszertifizierung erhalten haben.

Gerätegebundene Passkeys gibt es seit mehreren Jahren, aber einige der Aspekte, die zu starker Authentisierung beitragen (z. B. die Bindung an ein bestimmtes Gerät), standen ihrer breiten Akzeptanz bisher im Weg.

Synchronisierte Passkeys hingegen werden über einen Cloud-Service (z. B. ein OS-Ökosystem oder einen Passwortmanager) zwischen den Geräten eines Users synchronisiert, wodurch eine für den User sehr vertraute User Experience entsteht – eine notwendige Voraussetzung für breite Akzeptanz, insbesondere bei Verbrauchern.

Wenn sich ein User einloggen möchte, fragt ihn die Website oder der Service, ob er seinen Passkey verwenden möchte. Dazu authentisiert sich der User einfach auf seinem Endgerät (z. B. via Biometrie, PIN oder Muster).

Aus Sicht der Website oder des Service validiert der Passkey sowohl einen Besitzfaktor (d. h. ein Endgerät, das zur Verwendung des synchronisierten Passkeys berechtigt ist) als auch entweder einen Inhärenzfaktor (wenn Biometrie verwendet wird) oder einen Wissensfaktor (wenn ein Zugangscode verwendet wird). Auf diese Weise erhöhen synchronisierte Passkeys die Accountsicherheit für die Mehrheit der User erheblich – und tragen dazu bei, passwortbasierte ATOs einzudämmen.

Passkeys-Handbuch

Die breite Akzeptanz von Passkeys (in jeder Form) aufseiten der Benutzer wäre ein wichtiger Schritt im Kampf gegen Phishing, Kontoübernahmen und andere Identity Threats.

Mehr dazu in unserem Passkey Primer: Wie Sie mit Phishing-resistenter FIDO-Authentisierung die User-Experience verbessern und Account-Übernahmen verhindern

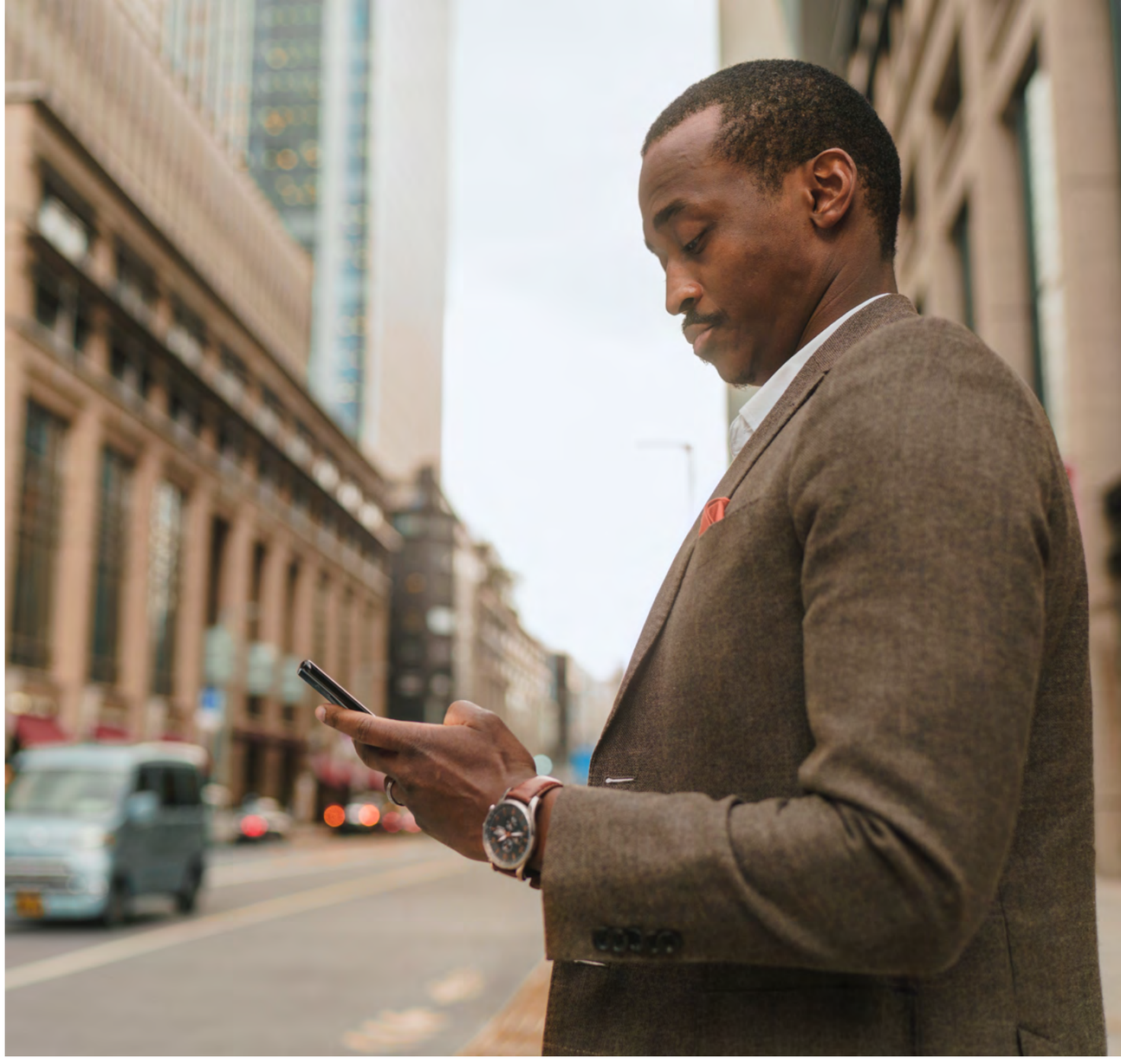
Breached Password Detection

Ein bedauerlicher, aber sehr realer Aspekt der heutigen Bedrohungslandschaft ist, dass es ganze Marktplätze gibt, die Angreifern bei ihren Unterfangen unter die Arme greifen. Beispielsweise können Bedrohungsakteure leicht umfangreiche Listen mit kompromittierten Credentials erwerben.

Die Risiken, die durch kompromittierte Credentials entstehen, lassen sich bis zu einem gewissen Grad managen, indem man dieselben Listen verwendet, um zu erkennen, wenn User ein Passwort verwenden, das in einem Breach aufgetaucht ist. Nach der Erkennung kann ein Anwendungsprovider den User warnen und ihn dazu ermuntern oder auffordern, bestimmte Maßnahmen zu ergreifen (z. B. Änderung des Passworts, Nutzung starker MFA).

Glücklicherweise machen es dedizierte Passwortmanager und in Webbrowser und Betriebssysteme integrierte Features Usern leichter, längere und komplexere Passwörter zu erstellen, sicher zu speichern und einfach zu verwenden – und adressieren damit einige der Hauptgründe, warum User schwache Passwörter wählen und wiederverwenden. Darüber hinaus warnen diese Lösungen die User häufig, wenn ihre Credentials in Leaks auftauchen, was das Risikobewusstsein erhöht.

Es bleibt zu hoffen, dass der Nutzen kompromittierter Passwörter und die Bedrohung, die von ihnen ausgeht, durch diese Bemühungen zurückgehen werden.



Mit Credential Guard die Lücke schließen

Es ist wichtig, sich bewusst zu machen, dass zwischen dem Zeitpunkt, an dem kompromittierte Credentials auf Cybercrime-Marktplätzen verfügbar werden, und dem Zeitpunkt, an dem sie in Threat-Intelligence-Feeds auftauchen, oft eine lange Zeitspanne liegt, in der Angreifer genügend Zeit haben, sie auszunutzen.

Credential Guard schließt diese Lücke mit einem Experten-Team, das sich in kriminelle Communities einschleust und Zugriff auf exponierte Daten erhält, sobald Breaches auftreten. Dieser Vorteil ermöglicht es Ihnen, Ihre User und Anwendungen durch schnelleres Zurücksetzen gestohlener Passwörter besser zu schützen.

Mehr dazu unter Kompromittierte Passwörter schneller entdecken mit Auth0 Credential Guard

Wirksame Passwort-Policies

Zusätzlich zu Breached Password Detection gibt es einige simple – aber wirksame – Möglichkeiten, um die Identity Security zu erhöhen:

- Verlangen Sie starke Passwörter von Ihren Usern
- Verhindern Sie, dass User zu einem Passwort zurückkehren, das sie bereits in dieser Anwendung verwendet haben (d. h., verhindern Sie Passwortrotation)
- Implementieren Sie einen robusten Passwortrücksetzungsprozess

Das Zurücksetzen von Passwörtern ist eine Notwendigkeit für jede Anwendung – aber wenn Ihr Passwortrücksetzungsprozess Ihren Kunden das Leben schwer macht, geben Sie ihnen einen Grund, Ihren Service nicht mehr zu nutzen.

Für etwas mehr Kontext: Der Customer Identity Trends Report 2023 von Okta kam zu folgenden Ergebnissen:

- 63 Prozent der Befragten gaben an, sich mindestens einmal im Monat nicht in einen Account einloggen können, weil sie ihren Usernamen oder ihr Passwort vergessen haben.
- 24 % haben diese Herausforderung mindestens einmal pro Woche
- 6 % täglich damit zu kämpfen haben

Und obwohl es in der Regel möglich ist, ein Passwort zurückzusetzen, kann es vorkommen, dass Kunden – vor allem im B2C-Bereich – entscheiden, dass sich der Aufwand einfach nicht lohnt, was nicht nur zu Umsatzeinbußen führt, sondern auch zum Verlust von Usern, denn nur 52 % der Befragten gaben an, dass sie noch Zugriff auf all ihre Accounts haben.

Gute Passwortrücksetzungsprozesse erfüllen zwei Aufgaben:

1. **Sie minimieren den Aufwand für den Kunden:** Es sollte nicht länger als eine Minute dauern, bis Ihr Kunde sein Passwort zurückgesetzt hat, und der Prozess sollte nur Informationen erfordern, die der Kunde bereitwillig eingibt, z. B. E-Mail-Adressen
2. **Stellen Sie sicher, dass die Kundendaten sicher sind:** Zum Beispiel durch Schutzmaßnahmen gegen mehrfach fehlgeschlagene Logins und durch das Versenden von Informationen ausschließlich über sichere Kanäle

E-Mail wird am häufigsten für das Zurücksetzen von Passwörtern verwendet, da es beide Kriterien erfüllt: Sie minimiert Reibungsverluste, da die Eingabe einer E-Mail-Adresse für den Kunden schnell und einfach ist, und sie schützt die Daten des Kunden (unter der Voraussetzung, dass nur der Kunde Zugriff auf sein Postfach hat).

Ein einziger Fehler beim Zurücksetzen des Passworts kann die gesamte Customer Experience im Zusammenhang mit Ihrem Produkt ruinieren. Solche Fehler treten häufig auf in Form von:

- **Sicherheitsfragen:** Statische Informationen – wo Sie zur Schule gegangen sind, der Mädchenname Ihrer Mutter, sogar der Name Ihres Haustiers – sind über OSINT leicht zugänglich
- **Passwörtern in Plain-Text:** Anstatt das Passwort zurückzusetzen, senden einige Websites das ursprüngliche Passwort an den Kunden zurück, was eine massive Schwachstelle darstellt – damit ein Passwort im Plain Text gesendet werden kann, muss es im Plain Text gespeichert werden, was die Chancen eines Angriffs erhöht
- **Fehlermeldungen:** Wenn eine Anwendung anzeigt, ob eine E-Mail-Adresse registriert ist oder nicht, kann ein Angreifer möglicherweise herausfinden, ob ein Kunde einen Account hat –eine weitere Information, die er gegen Ihren Kunden verwenden kann
- **Informationen, die unnötigerweise abgefragt werden:** Sicherheit und Usability müssen in einem ausgewogenen Verhältnis stehen – einen Lichtbildausweis anzufordern ist zwar eine sichere Praxis, wirkt sich aber insgesamt negativ auf die Customer Experience aus

(Starke) Multi-Faktor-Authentifizierung (MFA)

Der Schutz von Accounts durch den Einsatz von MFA erhöht den Zeit- und Arbeitsaufwand und letztlich auch die Kosten von Account Takeovers drastisch.

In der Praxis wird die Wirksamkeit von MFA als Maßnahme gegen ATOs jedoch durch zwei Faktoren eingeschränkt:

1. Geringe Akzeptanz aufseiten von Anwendungsprovidern und Kunden
2. Verwendung von Zweitfaktoren, die von Bedrohungsakteuren umgangen werden können

Obwohl eine detaillierte Untersuchung von MFA-Akzeptanz, -Anmeldung und -Nutzung den Rahmen dieses Reports sprengen würde, können wir die verfügbaren Daten nutzen, um das Thema ein Stück weit zu beleuchten.

Im gesamten Datensatz beträgt das Verhältnis zwischen den passwortbasierten Authentisierungen insgesamt und den gültigen MFA-Versuchen etwa 41, d. h., auf einen gültigen MFA-Versuch kommen etwa 41 passwortbasierte Authentisierungen.

Anhand dieses Verhältnisses können wir die relativen Raten der MFA-Nutzung nach Branche ermitteln und vergleichen (Abbildung 12).

Es zeigt sich, dass nur drei der zehn am stärksten vertretenen Branchen eine überdurchschnittliche MFA-Nutzung aufweisen, d. h., ein geringeres Verhältnis von passwortbasierten Authentisierungen zu gültigen MFA-Versuchen.

In der Finanzdienstleistungsbranche beobachten wir 12 passwortbasierte Authentisierungen für jedes gültige MFA-Event. Das Verhältnis in der produzierenden Industrie ist mit 24 doppelt so hoch wie bei den Finanzdienstleistungen, aber immer noch deutlich niedriger als die 37 im Bereich Professional Services.

Es fällt auch auf, dass drei der am stärksten vertretenen Branchen – Nahrung/Getränke/Gastronomie (137), Medien (155) und Werbung/Marketing (400) – extrem hohe Quoten aufweisen, was auf eine relativ geringe MFA-Nutzung hindeutet.

Um unsere Neugier zu befriedigen, haben wir einen Blick über die 10 am stärksten vertretenen Branchen hinaus gewagt und fünf mit unterdurchschnittlichen Quoten entdeckt (Abbildung 13). Drei Branchen – Rechtsdienstleistungen (4), Telekommunikation (6) und die öffentliche Hand (6) – sind eine Klasse für sich. In Anbetracht dessen, dass alle drei mit sensiblen Daten oder wichtigen Infrastrukturen arbeiten, ist eine höhere MFA-Nutzung beruhigend.

Auch wenn das oben dargestellte Verhältnis nur ein Näherungswert ist, deutet es doch stark darauf hin, dass bestimmte Branchen stärker auf MFA setzen als andere – insbesondere Branchen, die mit sensiblen Daten oder Systemen arbeiten, scheinen eine höhere MFA-Nutzung zu haben.

Da sich der Identitätsschutz allgemein jedoch verbessert hat und die Akzeptanz von MFA langsam zunimmt, haben sich die Angreifer darauf konzentriert (Abbildung 14), diese Schutzmaßnahmen auszuhebeln.

Abbildung 12: In streng regulierten Branchen ist der Einsatz von MFA tendenziell besonders hoch. Finanzdienstleister und Healthcare-Anbieter liegen beide nahe am oder knapp unter dem Durchschnitt (unter den zehn im Datensatz am häufigsten vertretenen Branchen).

Verhältnis der Passwort-Authentifizierungen insgesamt zu validen MFA-Versuchen (Zehn am stärksten vertretene Branchen, 2023)

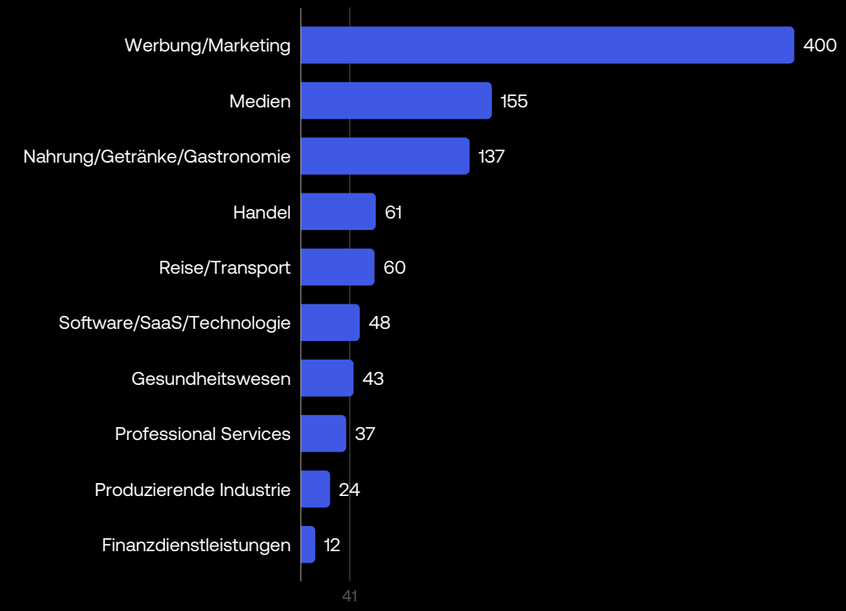
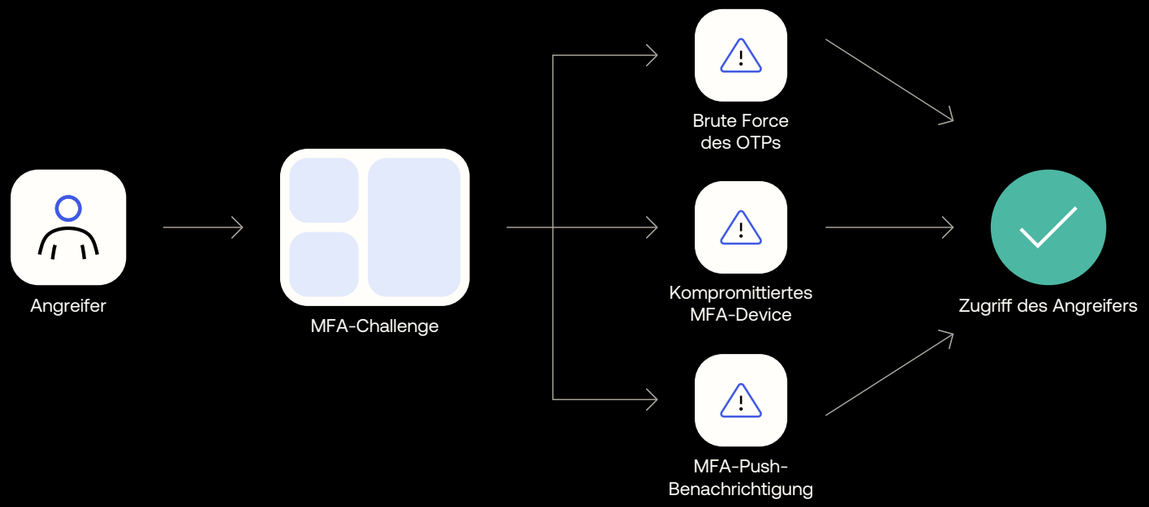


Abbildung 13: Sieht man von den zehn am stärksten vertretenen Branchen ab, weisen fünf weitere ein überdurchschnittlich hohes Verhältnis von gültigen MFA-Versuchen zur Gesamtzahl der Passwort-Authentifizierungen auf

Verhältnis der Passwort-Authentifizierungen insgesamt zu validen MFA-Versuchen (andere relevante Branchen, 2023)

Abbildung 14: Anatomie typischer MFA-Umgehungen



Zum Beispiel sind mehrere Tools verfügbar, die es leicht machen, einige der vergleichsweise schwächeren sekundären Faktoren anzugreifen – insbesondere per SMS übermittelte Einmalpasswörter (OTPs). Der häufigste Angriffsvektor ist die Anwendung von Brute Force, um **MFA-Müdigkeit** zu erzeugen. Dabei wird versucht, den User zu täuschen oder dazu zu drängen, die MFA-Challenge zu vervollständigen, obwohl er den Request nicht initiiert hat; durch das Vervollständigen der Challenge würde der User dem Angreifer unbeabsichtigt erlauben, sich einzuloggen.

Darüber hinaus setzen Bedrohungsakteure **SIM Swapping** und/oder **Social Engineering** ein, um MFA-Schutzmaßnahmen auszuhebeln.

Beim SIM Swapping überzeugt der Bedrohungsakteur den Mobilfunkanbieter des Users, dessen Mobilfunknummer auf eine SIM-Karte zu übertragen, die sich im Besitz des Bedrohungsakteurs befindet. Bedrohungsakteure können sich beim SIM Swapping Social Engineering (z. B. Täuschung eines Helpdesk-Mitarbeiters), einen böswilligen Insider oder einen Breach (d. h. Zugriff auf die Verwaltungsservices des Netzbetreibers) zunutze machen.

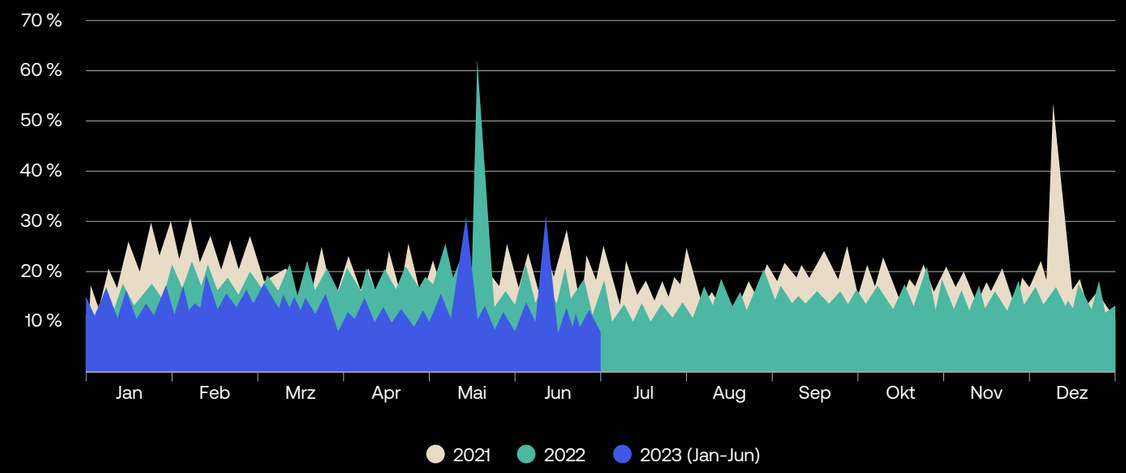
War das SIM Swapping erfolgreich, können alle MFA-Faktoren, die auf der Telefonnummer basieren (z. B. SMS-OTP, SMS-Magic-Link, Voice-OTP), vom Bedrohungsakteur abgeschlossen werden.

Bedrohungsakteure können Social-Engineering-Taktiken auch direkt gegen den Anwendungsprovider einsetzen. Beispielsweise könnte ein Angreifer, der im Besitz einiger persönlicher Daten ist (die oft ohne Weiteres käuflich erworben oder über OSINT gewonnen werden können), versuchen, einen Helpdesk-Mitarbeiter dazu zu bringen, die Bankverbindung zu ändern. Alternativ dazu könnten Bedrohungsakteure sogar direkt auf User zugehen und versuchen, sie dazu zu bringen, bestimmte Schutzmaßnahmen zu deaktivieren.

Leider sinken die Kosten für die Durchführung von Social-Engineering-Kampagnen ständig, was zum Teil auf eine höhere Effizienz (z. B. durch KI, Automatisierung), zum Teil auf massive Datenlecks und Dumps und zum Teil auf die Bereitschaft vieler User zurückzuführen ist, Informationen online (z. B. in sozialen Medien) zu teilen.

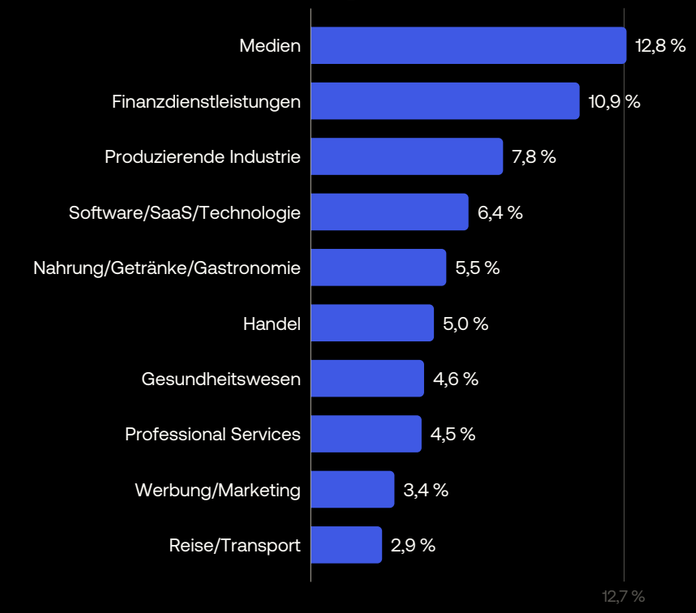
Aus all diesen Gründen ist MFA Bypass ein sehr reales Risiko für Unternehmen und ihre Kunden. In den ersten sechs Monaten des Jahres 2023 (Abbildung 15) erfüllten 12,7 % der MFA-Versuche MFA-Bypass-Kriterien. Dies ist zwar ein Rückgang im Vergleich zu 2022 (15,5 %) und 2021 (18,1 %), doch dürfte dieser Rückgang eher auf eine Änderung der Taktik als auf eine Verringerung der Bedrohung selbst zurückzuführen sein.

Abbildung 15: Die Umgehung von MFA hat zwischen 2021 und 2022 abgenommen, bleibt aber immer noch ein gefährlicher Angriffsvektor, da die Kosten von Social-Engineering-Angriffen sinken



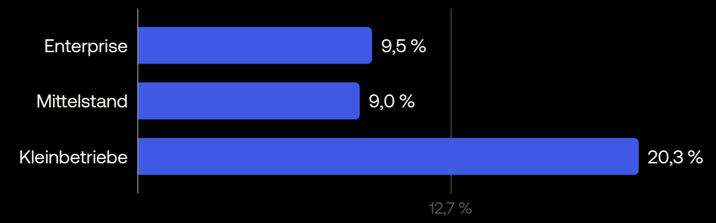
Interessanterweise verzeichnet nur eine der zehn am stärksten vertretenen Branchen einen überdurchschnittlich hohen Anteil an MFA-Bypass-Versuchen (Abbildung 16): Medien mit 12,8 % (und damit knapp über dem Durchschnitt). Der Gesamtdurchschnitt wird angeführt von der öffentlichen Hand (29,9 %) und der Entertainment-Branche (28,6 %) sowie von Kunden, die wir keiner bestimmten Branche zuordnen konnten.

Abbildung 16: Die gute Nachricht? In einigen Branchen ist der Anteil der MFA-Umgehungen durchschnittlich oder unterdurchschnittlich. Die Reise- und Transport-Branche steht an der Spitze (unter den zehn im Datensatz am häufigsten vertretenen Branchen).



Kleinunternehmen scheinen besonders bedroht zu sein (Abbildung 17), da mehr als ein Fünftel (20,3 %) der gesamten MFA-Versuche die Kriterien für einen MFA-Bypass-Versuch erfüllen.

Abbildung 17: Kleine Unternehmen scheinen von MFA-Umgehungsversuchen häufiger betroffen zu sein als große oder mittelständische Unternehmen



Angesichts der gefährlichen und sich rasant entwickelnden Bedrohungslandschaft ist es bei der Implementierung von MFA wichtig, dass die Lösung:

- **richtig implementiert wird:** Schwachstellen und Workarounds (z. B. Unterstützung von Legacy-Authentisierung oder Umgehung von MFA durch Administratoren) werden ausgenutzt werden
- **starke sekundäre Faktoren verwendet:** MFA-Bypass-Techniken zielen in der Regel auf ältere Faktoren ab (z. B. solche, die auf SMS basieren) ab, und Brute-Force-Angriffe konzentrieren sich nach wie vor hauptsächlich auf wissensbasierte Authentifikatoren – daher kann die Verwendung von Authentifikatoren, die auf Besitz oder Biometrie basieren, die Wahrscheinlichkeit eines erfolgreichen Brute-Force-Angriffs drastisch reduzieren

Wie bereits erwähnt, müssen Technologien, die sich in Verbraucheranwendungen bewähren, ein Gleichgewicht zwischen Sicherheit und Usability herstellen – und frühere Authentisierungsmethoden erzwangen oft einen Kompromiss.

Dieser Kompromiss entpuppt sich jedoch zunehmend als Fehlentscheidung:

- **Adaptive MFA** ist eine flexible, erweiterbare MFA-Policy, die dazu beitragen kann, ATOs zu verhindern, ohne die Hürden für echte User zu erhöhen. Dies wird erreicht, indem das potenzielle Risiko bei jeder Login-Transaktion bewertet wird und der User nur bei Bedarf zu einer zusätzlichen Verifizierung aufgefordert wird
- **Neue MFA-Methoden sind sicher und komfortabel:** MFA-Methoden, die auf **WebAuthn**-fähiger Gerätebiometrie (bspw. Apple Face ID, Apple Touch ID, Windows Hello) oder WebAuthn-fähigen Security Keys (bspw. YubiKey, Feitian, Titan) basieren, bieten gleichzeitig hohe Sicherheit (Bedrohungsakteure hassen WebAuthn) und hohe Usability und bringen die Authentisierung der in der Einleitung dieses Reports vorgestellten Ideallösung immer näher

Während es unwahrscheinlich ist, dass dedizierte Security Keys bei Verbrauchern breite Akzeptanz finden, kommen biometrische Funktionen immer häufiger in erschwinglichen Geräten zum Einsatz. Sich via Gerätebiometrie authentisieren zu können, hat für User zwei Vorteile:

- Reibungsverluste bei der Authentisierung werden deutlich reduziert, was die Userbindung und den Umsatz erhöht
- Sie erhöht die Sicherheit, da der Prozess nicht von böswilligen Akteuren „gephisht“ werden kann ■

Teil 3: Hinter der Login-Box

Der Schutz von Kundenidentitäten – und der damit verbundenen Rechte und Privilegien – endet nicht mit der Authentisierung, sondern sollte während der gesamten Session des Users fortbestehen.

Teil 3: Hinter der Login-Box

In einer passwortlosen Welt sind Session-Token für Angreifer noch wertvoller

Nachdem sich ein User bei einer Anwendung authentisiert hat, speichert der Browser ein Web-Cookie. Innerhalb des Web-Cookies befindet sich ein Session-Token – ein spezieller Datenblock, der von der Anwendung generiert wird –, mit dem ein eingeloggter User getrackt werden kann, um sicherzustellen, dass er sich nicht erneut einloggen muss, bis die Session abläuft oder der User sich ausloggt.

Wenn ein Angreifer ein Session-Cookie stiehlt und es in den Browser einspeist, kann er oft so lange auf dieselbe Session zugreifen wie der rechtmäßige User, und zwar so lange wie die Session aktiv ist (dieser Zeitraum variiert je nach Anwendungsprovider).

Es gibt eine Reihe von Möglichkeiten, wie ein Session-Token kompromittiert werden kann, darunter:

- **Client-seitige Angriffe** (z. B. T1539, T1185): Es gibt eine Reihe von Möglichkeiten, ein Session-Token vom Client zu extrahieren, einschließlich Cross-Site Scripting (XSS), bösartigem JavaScript und Malware; insbesondere enthalten viele der heute am weitesten verbreiteten Malware-Familien „Infostealer"-Module, die in der Lage sind, Cookies zu extrahieren.
- **Adversary-in-the-Middle-Phishing-Angriffe (AiTM)** (z. B. T1557, T1566, T1539): Mit Hilfe von Social Engineering leiten Angreifer User auf eine bösartige Website, die transparent als Reverse-HTTP-Proxy-Server konfiguriert ist, der Requests zwischen einem User und einer fingierten Webanwendung übermittelt; wenn sich ein User über eine dieser bösartigen Websites bei der legitimen Webanwendung einloggt, kann der Angreifer auf die Credentials des Users und das an den Browser zurückgegebene Session-Token zugreifen. Alternativ kann ein Angreifer den Netzwerk-Traffic mitlesen (möglicherweise mit Hilfe eines bösartigen Access Points), um das Session-Token zu verfolgen und zu stehlen.

Session Hijacking ist zwar bis zu einem gewissen Grad skalierbar, wird aber eher als Teil eines gezielten Angriffs auf bestimmte User in wertvollen Unternehmen eingesetzt.

Wir gehen jedoch davon aus, dass Bedrohungsakteure mit zunehmender Akzeptanz der passwortlosen Authentisierung mehr Aufwand in Session-Hijacking-TTPs investieren werden.

Sessions zum Verkauf

Viele gestohlene Session-Tokens werden anschließend auf Cybercrime-Marktplätzen verkauft, sodass Bedrohungsakteure, die einen Account bei einem bestimmten Unternehmen kompromittieren wollen, einfach ein passendes Token kaufen können – oft für nur ein paar Dollar.

Wie weiter unten erläutert, besteht eine Möglichkeit, diesem Risiko zu begegnen, darin, die maximale Session-Dauer zu verkürzen. Das deckt die Situationen, in denen ein User direkt angegriffen wird, zwar nicht ab, kann aber bei der Bekämpfung von Infostealer-Malware sehr effektiv sein, da es zwischen dem Abgreifen des Tokens (und der Credentials) und der Veröffentlichung auf einem Schwarzmarkt in der Regel zu einer Verzögerung kommt.

Schutzmaßnahmen

Drei Möglichkeiten zur Verbesserung der Session-Sicherheit und zum Schutz vor Session Hijacking:

- Session-Token nicht in die URL einbetten
- Verwendung eines serverseitigen, sicheren Session-Managers, der nach dem Login ein neues und zufälliges Session-Token generiert
- Sicheres Speichern von Session-Tokens und Entwerten nach dem Logout
- Verkürzen der maximalen Session-Dauer

Anwendungsprovider sollten auch eine erneute Authentisierung der User in Betracht ziehen, wenn die Umstände dies rechtfertigen (siehe unten).

Best Practices für das Application Session Management

Ist ein Identity Provider (IdP) involviert, kann Application Session Management eine ziemliche Herausforderung sein – und die ersten Lösungen, die einem in den Sinn kommen, sind oft unvollständig.

Mehr dazu in Best Practices für das Application Session Management

Step-up-Authentisierung

Wie bereits mehrfach erwähnt, ist ein ausgewogenes Verhältnis zwischen Sicherheit und Usability entscheidend für eine positive User Experience.

Step-up-Authentisierung ermöglicht es Anwendungsprovidern, dieses Gleichgewicht feingranular auszubalancieren, in diesem Fall durch Anpassung der Identity Requests an die Bedeutung der Ressource und den Risikograd, sollte diese offengelegt werden.

Dieser abgestufte Ansatz stellt sicher, dass User (oder Entitäten, die sich als User ausgeben) mit einem Satz Credentials auf einige Ressourcen zugreifen können, aber nach weiteren Credentials (z. B. MFA) gefragt werden, wenn sie Zugriff auf sensible Ressourcen anfordern.

Das Risiko der Step-up-Authentisierung liegt in der Implementierung – wirksame Implementierungen erfordern sorgfältige Planung und Überlegung.

Lückenlose Authentisierung

Die Tatsache, dass ein User eine Authentisierungs-Challenge absolviert hat, ist noch lange kein Grund, ihm dauerhaften Zugriff zu gewähren.

Durch kontinuierliches Monitoring von Signalen (z. B. Standort des Users, Gerät, Apps, Nutzungsmuster, Tageszeit, Eingabeverhalten etc.) prüft das Authentisierungssystem bei Bedarf, ob das Vertrauen noch ausreichend ist, um dem User weiterhin Zugriff zu gewähren.

Diese „kontinuierliche Authentisierung“ ist außerordentlich leistungsstark, da sie sowohl die Sicherheit als auch die User Experience verbessert – und das Vertrauen, das sie vermittelt, geht weit über das hinaus, was ein Passwort allein bieten kann.

Kontinuierliche Authentisierung im Customer-Identity-Kontext würde jedoch umfangreiche – und wahrscheinlich kontinuierliche – bewusste Zustimmung der User sowie (möglicherweise) eine Form des Device Monitoring erfordern. Diese Anforderungen schränken die Einsatzmöglichkeiten solcher Lösungen drastisch auf B2B-Szenarien und hochsensible B2C-Use-Cases (z. B. Finanz- und Gesundheitswesen) ein. ■

Verbessern Sie mit CIAM die Security und den Benutzer-komfort

CIAM richtig hinzubekommen, sprich: skalierbar so zu implementieren, dass die Lösung allen Anforderungen an Usability, Security und Datenschutz gerecht wird, ist für jedes Unternehmen eine Herausforderung:

- CIAM steht im Mittelpunkt Ihrer Kunden-Anwendungen und ist damit ein wichtiges Tool, um den Markt zu analysieren und das Kaufverhalten, die Konversion und die Kundenbindung zu steuern, das Ihre Marketing- und Customer-Experience-Spezialisten gleichermaßen schätzen werden
- Gleichzeitig wirkt sich das CIAM nachhaltig auf die Security und den Datenschutz aus, und ist damit in hohem Maße für CISOs, CIOs und Compliance-Verantwortliche interessant
- Und: Als leistungsstarke Technologie-Suite fällt CIAM auch in den Verantwortungsbereich Ihrer IT-Abteilung, oder sogar Ihres CTOs (wenn die Lösung im Unternehmen zurecht als Innovations- und Digitalisierungstreiber wahrgenommen wird)

Die Verantwortlichen müssen abteilungsübergreifend zusammenarbeiten, um CIAM so zu implementieren, dass jederzeit die richtige Balance zwischen der Qualität der Customer Experience und der Sicherheit der Systeme gewährleistet ist – und das über alle Use Cases, Kundentypen, Datentypen und branchenspezifischen Risiken hinweg, und unter Berücksichtigung der jeweiligen Risikobereitschaft.

Wie Sie die Kundenidentitäten schützen

Die zunehmend raffinierten Identity-basierten Angriffe von heute zu stoppen und die Business-Modelle der Cyberkriminellen zu durchkreuzen, ohne die User Experience zu beeinträchtigen, ist alles andere als einfach. Sie benötigen dafür eine Reihe leistungsfähiger Security-Tools, die auf verschiedensten Ebenen zu einer durchgängigen Security-Strategie kombiniert werden müssen.

Diese Tools auszuwählen, zu integrieren, zu konfigurieren, kontinuierlich zu überwachen, anzupassen und zu orchestrieren erfordert hohe Kompetenz, ist aufwändig im Betrieb und bindet wertvolle Ressourcen, die lieber in die Weiterentwicklung der Kernkompetenzen des Unternehmens investiert werden sollten.

Diese und viele andere Gründe sprechen dafür, eine Best-of-Breed-CIAM-Lösung mit einer agilen, sicheren Architektur und starken Schutzmechanismen zu implementieren – mit Blick auf die Sicherheit der Identitäten ein weitaus effizienterer Ansatz als die Entwicklung eines eigenen Identity-Stacks.

Best Practices im Bereich Kundenidentität

Ganz egal, ob Sie eine eigene Lösung entwickeln oder sich auf einen Identity-as-a-Service-Anbieter verlassen, haben wir einige allgemeingültige Empfehlungen für Sie:

- **Verwenden Sie generische Fehlermeldungen:** Detaillierte Fehlermeldungen machen es Angreifern leicht, weil sie zusätzliche Informationen über die im System angelegten Benutzer liefern. Mit generischen Fehlermeldungen tappen Cyberkriminelle im Dunkeln
- **Implementieren Sie ein sicheres Session-Management:** Verwenden Sie ein Server-seitiges, sicheres Session-Management, das nach der Anmeldung eine neue Session-ID generiert. Integrieren Sie die Session-ID nicht in die URL, und stellen Sie sicher, dass diese sicher abgelegt und nach der Abmeldung ungültig gemacht wird
- **Stellen Sie Anwendungen nicht mit Default-Zugangsdaten bereit:** Standard-Admin-Credentials sind ein gefährlicher Angriffsvektor, da viele Unternehmen sie unverändert lassen. Auch wenn es attraktiv erscheint, neue Geräte und User mit Standard-Credentials auszustatten, ist es besser, Technologien wie OpenID Connect zu verwenden, passwortlose Authentisierung einzuführen oder User zu zwingen, beim ersten Login ein Passwort festzulegen
- **Speichern Sie keine Plain-Text-Passwörter:** Wenn Ihre Passwortdatenbank wirklich unlesbar ist, hat sie für Hacker keinen Wert. Verschlüsselung macht Ihr Unternehmen zu einem unattraktiven Ziel – vorausgesetzt, sie wird robust implementiert

Im nächsten Schritt gilt es einige grundlegende Verteidigungsmaßnahmen zu ergreifen:

- **Begrenzen Sie die Zahl fehlgeschlagener Anmeldeversuche:** Bei Brute-Force-Angriffen wie dem Credential Stuffing stehen jeder erfolgreichen Anmeldung unzählige Fehlversuche gegenüber. Nutzen Sie diesen Effekt, um Angriffe zu erkennen und Gegenmaßnahmen einzuleiten
- **Stellen Sie die Verwendung starker Passwörter sicher:** Viele Brute-Force-Angriffe machen sich schwache oder gängige Passwörter zunutze. Setzen Sie verbindliche Vorgaben für die Länge, Komplexität und Rotationsfrequenz von Passwörtern vor. Orientieren Sie sich dabei an den NIST-Empfehlungen oder an anderen Evidenz-basierten Richtlinien
- **Achten Sie auf Login-Versuche mit kompromittierten Passwörtern:** Viele Benutzer verwenden dieselben oder ähnliche Passwörter auf mehreren Websites. Kommt es auf einer dieser Seiten zu einem Breach, können also viele andere Seiten gefährdet sein. Stellen Sie daher sicher, dass Ihre Anwender kompromittierte Zugangsdaten zeitnah tauschen

Setzen Sie auf stärkere Authentifizierungsverfahren:

- **Implementieren Sie Passkeys:** Passkeys bieten robuste Authentifizierungssicherheit, und synchronisierte Passkeys garantieren eine hochwertige User Experience, die es braucht, um breite Akzeptanz bei den Kunden zu erreichen
- **Bieten Sie starke MFA:** Favorisieren Sie bei der Einführung von MFA vor allem Authentifizierungs-Apps und WebAuthn-basierte Methoden. Wenn Sie MFA länger im Einsatz haben, sollten Sie versuchen, bestehende Anwender auf diese stärkeren sekundären Faktoren zu migrieren – und sich sukzessive von Legacy-Ansätzen verabschieden
- **Setzen Sie auf adaptive MFA und Step-up-Authentifizierung:** In Unternehmen, die den Mehraufwand für ihre Benutzer möglichst minimieren möchten, haben sich diese Lösungen bewährt, um ein besseres Gleichgewicht zwischen Security und Usability zu erreichen

Erfahren Sie mehr über Identity Management mit Auth0 von Okta ■

Über Okta

Okta ist das weltweit führende Identity-Unternehmen. Als der führende unabhängige Identity-Partner ermöglichen wir es jedermann, jede Technologie sicher zu nutzen – überall, mit jedem Device und jeder App. Die weltweit renommiertesten Marken vertrauen beim Schutz von Zugriff, Authentisierung und Automatisierung auf Okta. Im Mittelpunkt unserer Okta Workforce Identity und Customer Identity Clouds stehen Flexibilität und Neutralität. Mit unseren individualisierbaren Lösungen und unseren über 7.000 schlüsselfertigen Integrationen können sich Business-Verantwortliche und Entwickler ganz auf neue Innovationen und eine rasche Digitalisierung konzentrieren. Wir entwickeln eine Welt, in denen Ihre Identity ganz Ihnen gehört. Mehr unter okta.com/de.

Auth0 ist die zugrundeliegende Technologie von Okta und der Flaggschiff-Produktlinie – Okta Customer Identity Cloud. Entwickler können unter Auth0.com mehr erfahren und ein kostenloses Konto erstellen.

Disclaimer:

Diese Informationen und die darin enthaltenen Empfehlungen stellen keine Rechts-, Datenschutz-, Sicherheits-, Compliance- oder Geschäftsberatung dar. Dieses Dokument dient nur zu allgemeinen Informationszwecken und gibt womöglich nicht den aktuellen Stand aller relevanten Fragen wieder. Es liegt in Ihrer Verantwortung sich mit Blick auf die Rechtslage, den Datenschutz, die Security, die Compliance und das Business beraten zu lassen. Stützen Sie sich nicht allein auf die enthaltenen Empfehlungen. Okta übernimmt keine Haftung für Verluste oder Schäden, die sich potenziell aus der Umsetzung der Empfehlungen in diesem Report ergeben haben. Okta gibt keine Zusicherungen, Garantien oder sonstigen Zusicherungen in Bezug auf den Inhalt dieser Materialien. Informationen zu den vertraglichen Zusicherungen von Okta an seine Kunden finden Sie unter okta.com/agreements.

Alle Produkte, Merkmale oder Funktionen, auf die hier verwiesen wird und die derzeit noch nicht in der Breite verfügbar sind, werden möglicherweise nicht zum angekündigten Zeitpunkt oder überhaupt nicht bereitgestellt. Produkt-Roadmaps stellen keine Zusage, keine Verpflichtung und kein Versprechen dar, ein Produkt, ein Feature oder eine Funktionalität bereitzustellen. Sie sollten sich bei Ihren Kaufentscheidungen nicht auf sie verlassen.

Nachwort

Autorisierung, der nächste Meilenstein

Digitale Identitäten werden in den kommenden Monaten, Jahren und Jahrzehnten zweifellos an Bedeutung gewinnen. Folglich wird die Fähigkeit, Kundenidentitäten zu managen und zu schützen, Grundlage für praktisch jede digitale Interaktion sein.

Wie wir gesehen haben, sind Bedrohungen für die Kundenidentität allgegenwärtig, raffiniert und entwickeln sich ständig weiter – was bedeutet, dass CIAM-Services ständig antizipieren, reagieren und sich anpassen müssen.

Wir gehen beispielsweise davon aus, dass die zunehmende Verwendung von Passkeys dazu führen wird, dass sich Cyberkriminelle verstärkt auf TTPs nach der Authentisierung konzentrieren werden, was die Bedeutung von sicherem Session-Management, Step-up-Authentisierung und kontinuierlicher Authentisierung erhöht.

Authentisierung ist jedoch nur ein Aspekt von CIAM. Autorisierung – der Prozess, durch den festgelegt wird, auf welche Ressourcen ein User zugreifen darf – ist ebenso wichtig, auch wenn ihr nicht so viel Aufmerksamkeit geschenkt wird. Da immer mehr Rechte, Informationen, Services und andere Privilegien durch digitale Identitäten geschützt werden, wird die Autorisierung im Kontext personalisierter Angebote und als entscheidender Schutz vor Eindringlingen und den häufig damit verbundenen Datenlecks in den Vordergrund rücken.

Letztlich geht es beim Schutz der Kundenidentität um den Aufbau und die Aufrechterhaltung des Vertrauens, das den unzähligen Interaktionen zwischen Menschen und Unternehmen in unserem Alltag zugrunde liegt.

Die Herausforderung – ebenso wie unser Commitment – könnte nicht größer sein.

Shiven Ramji
President, Customer Identity Cloud, Okta

Anhänge

Anhänge

Anhang A: Glossar

In diesem Report werden einige Fachbegriffe verwendet:

- **Account Takeover (ATO):** Das Ziel vieler Angriffe auf Identity-and-Access-Management-Systeme (IAM), bei denen ein Bedrohungsakteur Zugriff auf einen bestehenden Account eines legitimen Users erhält und die Kontrolle darüber übernimmt
- **Adaptive Multi-Faktor-Authentifizierung (Adaptive MFA):** Eine flexible, erweiterbare MFA-Policy, die dazu beitragen kann, Anwendungen vor böswilligen Akteuren zu schützen, ohne die Hürden für legitime User zu erhöhen; der Ansatz bewertet das potenzielle Risiko bei jeder Login-Transaktion und fordert den User gegebenenfalls zu einer zusätzlichen Verifizierung auf
- **Authentisierung:** Die Bestätigung einer digitalen Identität (d. h., wie Apps erkennen, wer ein User ist)
- **Autorisierung:** Der Prozess, bei dem festgelegt wird, auf welche Ressourcen ein User zugreifen darf (d. h., wie Apps bestimmen, was ein User tun darf)
- **Customer Identity & Access Management (CIAM):** Wie Unternehmen ihren Usern Zugriff auf ihre digitalen Assets gewähren und wie sie die Daten dieser User verwalten, sammeln, analysieren und sicher speichern
- **Digitale Identität:** Die Attribute, die einen bestimmten User im Kontext einer Anwendung definieren.
- **Eindringen:** Ein Sicherheitsvorfall (oder eine Kombination mehrerer Sicherheitsvorfälle), bei dem ein nicht autorisierter User Zugriff auf ein System oder eine Systemressource erhält
- **Entität:** Ein eindeutiges und identifizierbares Objekt, das unabhängig von Änderungen seiner Attribute existiert; im CIAM-Kontext ist eine Entität in der Regel entweder ein User, ein Gerät oder eine Computerressource (z. B. ein System oder eine Anwendung)
- **FIDO:** Steht für „Fast Identity Online“; wird oft als Abkürzung für die FIDO Alliance verwendet, ein offener Branchenverband, der es sich zur Aufgabe gemacht hat, Authentisierungsstandards zu entwickeln und zu fördern, um die Abhängigkeit von Passwörtern zu reduzieren
- **Gerätegebundener Passkey:** Ein Passkey, der an ein bestimmtes Gerät gebunden ist und somit als Besitzfaktor dient
- **Kundenidentität:** Wie Marken kontinuierlich mehr über ihre Kunden erfahren und Vertrauen aufbauen, indem sie verstehen, wer ihre Kunden sind und wie sie interagieren möchten
- **Magic Link:** Ein von der Authentisierungs-API generierter Link, der an den User gesendet wird; wenn der User auf den Link klickt, wird er direkt eingeloggt (ein Magic Link erfüllt eine ähnliche Funktion wie ein User, der eine E-Mail mit einem OTP erhält, zu einer Anwendung zurückkehrt und das OTP eingibt – ohne dass diese Schritte tatsächlich nötig sind)
- **MFA-Müdigkeit:** Eine Technik, die von Angreifern verwendet wird, um einen User mit MFA-Benachrichtigungen zu überfluten, in der Hoffnung, dass der User diese akzeptiert/genehmigt, wodurch der Angreifer Zugriff auf einen Account oder ein Gerät erhält
- **Multi-Faktor-Authentifizierung (MFA):** Eine Methode zur Userauthentisierung, die mehr als einen Faktor erfordert (z. B. Biometrie, One-Time Passcode, Authenticator-App usw.)
- **One-Time Passcode/Passwort (OTP):** Eine Abfolge von numerischen oder alphanumerischen Zeichen, die von der Authentisierungs-API generiert wird, um einen User für einen einzelnen Login oder eine einzelne Transaktion zu authentisieren
- **Open-Source Intelligence (OSINT):** Das Sammeln, Analysieren und Verbreiten von Informationen, die öffentlich verfügbar und legal zugänglich sind (gemäß SANS)
- **Passkey:** FIDO-Zugangsdaten, die von Browsern erkannt werden können oder in nativen Anwendungen oder Security Keys zur passwortlosen Authentisierung enthalten sind
- **Passwortlos:** Passwortlose Authentisierung (oft abgekürzt als „passwortlos“) bezieht sich auf jeden Mechanismus, der einen User authentisiert, ohne dass der User sein Passwort eingeben muss
- **Phishing:** Eine Social-Engineering-Technik, bei der in der Regel Täuschung, Druck oder Manipulation eingesetzt werden, um User dazu zu bringen, vertrauliche Informationen preiszugeben
- **Reibungsverlust:** In der digitalen Welt bezieht sich Reibungsverlust auf alles, was die Interaktion einer Person mit Ihrem Service beeinträchtigt. Zu diesen Interaktionen gehören (unter anderem) die Registrierung für Ihren Service, das Einloggen in einen bestehenden Account, das Wiederherstellen verlorener Accountinformationen und das Bezahlen eines Einkaufs
- **SIM Swapping:** Eine Social-Engineering-Technik, bei der in der Regel Täuschung, Druck oder Manipulation eingesetzt werden, um User dazu zu bringen, vertrauliche Informationen preiszugeben
- **Single Sign-on (SSO):** Eine Authentisierungslösung, die es einem User ermöglicht, sich einmal mit einer einzigen Identität einzuloggen und dann auf weitere unabhängige Systeme zuzugreifen, ohne die Authentisierungsfaktoren erneut eingeben zu müssen
- **Social Engineering:** Oberbegriff für alle Taktiken und Techniken, die darauf abzielen, eine Zielperson zur Preisgabe vertraulicher Informationen oder zur Durchführung einer Handlung im Namen des Bedrohungsakteurs zu bewegen
- **Social Login:** Eine Implementierung von Single Sign-On, die es Usern ermöglicht, sich von einem einzigen Account – in der Regel bei einem Social-Network-Provider – aus bei mehreren Anwendungen und Services einzuloggen
- **Spear Phishing:** Eine sehr gezielte Form des Phishing (z. B. auf eine Einzelperson oder ein Unternehmen ausgerichtet), häufig auf Basis besonders relevanter Informationen und Details, von denen die Zielperson annimmt, dass sie nicht allgemein bekannt sind
- **Step-up-Authentisierung:** Ein Authentisierungsansatz, der darauf abzielt, ein Gleichgewicht zwischen Sicherheit und Reibungsverlusten herzustellen, indem er Usern den Zugriff auf einige Ressourcen mit einem Satz Credentials ermöglicht, sie aber auffordert, weitere Credentials einzugeben, wenn sie auf sensible Ressourcen zugreifen möchten
- **Synchronisierter Passkey:** Ein Passkey, der sicher zwischen mehreren Geräten ausgetauscht werden kann (z. B. innerhalb eines OS-Ökosystems oder über einen Passwortmanager)
- **WebAuthn:** Abkürzung für den Web Authentication JavaScript API Standard, Teil der FIDO2-Spezifikation

Anhänge

Anhang B: Methodologie

Dieser Report basiert auf Daten aus der Okta Customer Identity Cloud, powered by Auth0, die CIAM-Funktionalitäten für Tausende von Groß- und Kleinunternehmen weltweit bereitstellt.

Genauer gesagt summiert der Report die täglichen Ereignisprotokolle in Zähler (z. B. betrügerische Anmeldeereignisse) und Nenner (z. B. gesamte Anmeldeereignisse), was eine aussagekräftige Normalisierung von Bedrohungstrends ermöglicht und den laufenden Veränderungen in der Kundenzusammensetzung der Customer Identity Cloud Rechnung trägt.

Wo solche Informationen verfügbar sind, werden die Ereignisdaten mit der Branche (vom Kunden ausgewählt), der Größe (z. B. Klein-, mittelständisches, Großunternehmen) und dem Hauptsitz des Kunden verknüpft, bevor sie anonym aggregiert werden.

Da dieser Report auf Implementierungen im produktiven Einsatz basiert, erfasst er die tatsächliche Aktivität in der Customer Identity Cloud und wird somit maßgeblich von den Produkten und Features beeinflusst, die jeder Kunde nutzt (und deren Konfiguration), sowie von den sich entwickelnden Möglichkeiten dieser Produkte und Features.

Um zu ermitteln, welche 10 Branchen in der Customer Identity Cloud am stärksten vertreten sind, haben wir jede Branche anhand von vier Faktoren eingestuft (in den ersten sechs Monaten des Jahres 2023):

- Anzahl der Tenants
- Gesamtzahl der Anmeldeereignisse
- Gesamtzahl der Passwortauthentisierungen
- Gesamtzahl der MFA-Versuche

Es wurde davon ausgegangen, dass die 10 Branchen mit dem höchsten durchschnittlichen Ranking am stärksten vertreten sind.

Teilmengenanalysen hängen von Attributen ab, die möglicherweise nicht für alle Kunden/Tenants verfügbar sind (z. B. Branche, Größe, Hauptsitz). Das bedeutet, dass Diagramme, die eine globale Aggregation auf der Grundlage solcher Attribute darstellen, nicht alle Tenants umfassen. Während beispielsweise Abbildung 3 auf den Daten aller Tenants basiert, enthält Abbildung 6 nur die Tenants, für die:

- wir einen zugehörigen Hauptsitz haben,
- der in den Regionen AMER, APAC oder EMEA liegt.

Das bedeutet, dass in Abbildung 6 keine Daten von Tenants enthalten sind, für die wir keinen Hauptsitz haben oder deren Hauptsitz außerhalb dieser drei Regionen liegt (z. B. Afrika).

In einem Extremfall führte dieser Teilmengeneffekt zu einem Szenario, in dem alle drei Hauptregionen einen unterdurchschnittlichen (d. h. unter dem weltweiten Durchschnitt liegenden) Anteil an MFA-Bypass-Versuchen aufwiesen. Die einfache Erklärung dafür lautet, dass Kunden, die entweder außerhalb der drei Hauptregionen ansässig sind oder für die wir keine Daten zum Hauptsitz haben, ebenfalls zum weltweiten Durchschnitt beitragen und ihn – in diesem Fall – stärker erhöhen als Kunden, die bekanntermaßen in AMER, APAC oder EMEA ansässig sind.

Anhänge

Anhang C: Überblick nach Branche

Die folgenden Abschnitte bieten zusätzlichen Kontext zu den 10 Branchen, die im Datensatz 2023 am stärksten vertreten sind:

Finanzdienstleistungen

Umfasst Banking, Versicherungs-, Vermögensmanagement- und sonstige Services im Zusammenhang mit der Verwaltung und Umschichtung von Kapital

Gesundheitswesen

Umfasst Healthcare-Provider, Kostenträger (z. B. Krankenversicherungen), Pharmaunternehmen und Gesundheitstechnologie

Handel

Umfasst Unternehmen, die Produkte und Services über physische Geschäfte oder digitale Plattformen an Verbraucher verkaufen und vertreiben

Medien

Umfasst Unternehmen, die Content wie Nachrichten, Unterhaltung und Werbung erstellen, verbreiten und senden

Nahrung/Getränke/Gastronomie

Umfasst die Herstellung und den Vertrieb von – sowie Services in Verbindung mit Nahrung und Getränken sowie Freizeit- und Beherbergung, etwa Hotels und Restaurants

Produzierende Industrie

Umfasst die Produktion von Sachgütern, von Unterhaltungselektronik bis hin zu Kraftfahrzeugen

Professional Services

Umfasst eine breite Palette von Services zur Unterstützung von Unternehmen, z. B. Rechts- und Unternehmensberatung, Buchhaltung und Marketing

Reise/Transport

Umfasst Fluggesellschaften, Eisenbahnen, Hotels, Reisebüros und verwandte Services, die auf die Beförderung von Personen und Gütern spezialisiert sind

Software/SaaS/Technologie

Umfasst Entwicklung, Vertrieb und Support von Software, einschließlich Software-as-a-Service (SaaS) und Technologie

Werbung/Marketing

Spezialisiert auf Konzeption, Durchführung und Skalierung von Kampagnen zur Information und Aktivierung von Zielgruppen zur Unterstützung von Produkten und Services

Tabelle 2: Werbung/Marketing

Überblick über Identity-Threat-Trends im Bereich Werbung/Marketing

	2021	2022	1H2023
Betrügerische Anmeldeversuche	1,4 %	1,5 %	1,0 %
Credential-Stuffing-Versuche	2,7 %	4,9 %	16,9 %
Versuche zur Umgehung von MFA	17,6 %	4,1 %	3,4 %

Tabelle 3: Finanzdienstleistungen

Überblick über Identity-Threat-Trends im Bereich Finanzdienstleistungen

	2021	2022	1H2023
Betrügerische Anmeldeversuche	23,4 %	50,8 %	28,8 %
Credential-Stuffing-Versuche	46,6 %	41,8 %	30,3 %
Versuche zur Umgehung von MFA	3,7 %	4,8 %	10,9 %

Abbildung 18: 30-monatiger Überblick über die täglichen Identity-Threats in Werbe-/Marketingunternehmen

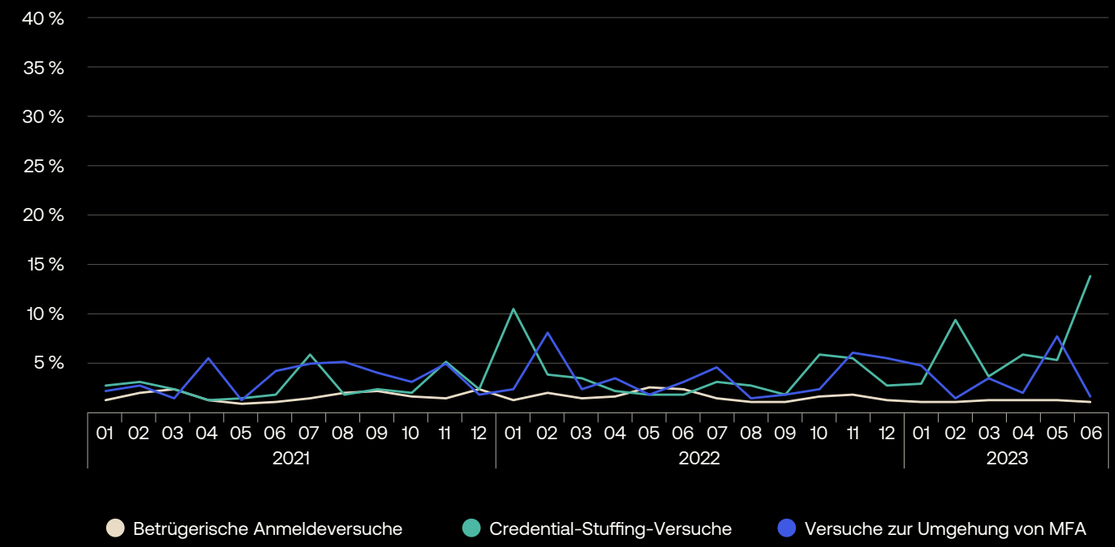


Abbildung 19: 30-monatiger Überblick über die täglichen Identity-Threats in der Branche Finanzdienstleistung

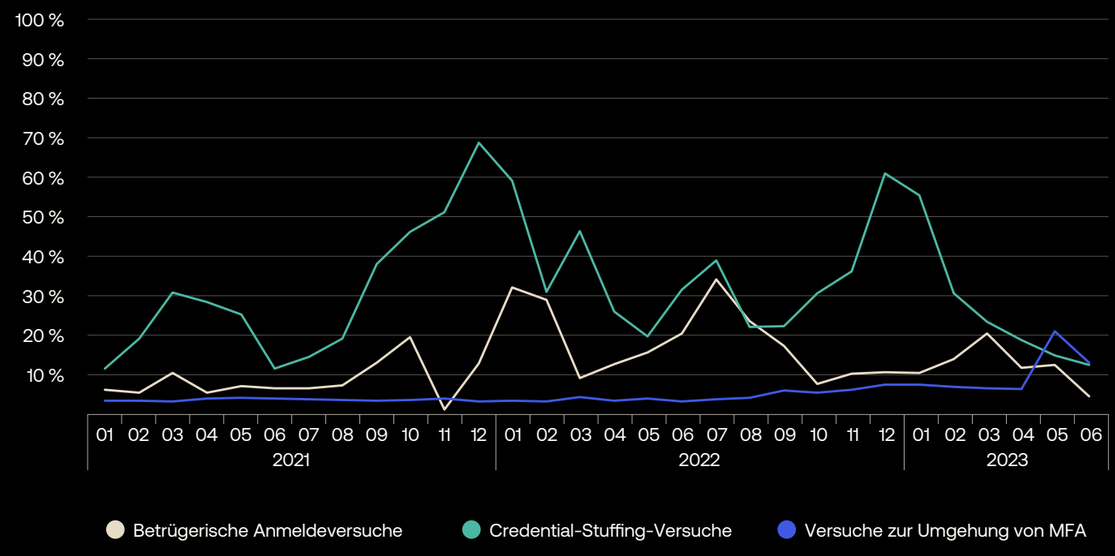


Tabelle 4: Nahrung/Getränke/Gastronomie

Überblick über Identity-Threat-Trends im Bereich Nahrung/Getränke/Gastronomie

	2021	2022	1H2023
Betrügerische Anmeldeversuche	3,3 %	17,8 %	9,0 %
Credential-Stuffing-Versuche	23,6 %	21,5 %	11,4 %
Versuche zur Umgehung von MFA	8,3 %	9,2 %	5,5 %

Tabelle 5: Gesundheitswesen

Überblick über Identity-Threat-Trends im Gesundheitswesen

	2021	2022	1H2023
Betrügerische Anmeldeversuche	1,9 %	2,8 %	6,3 %
Credential-Stuffing-Versuche	4,5 %	3,3 %	16,1 %
Versuche zur Umgehung von MFA	6,0 %	9,0 %	4,6 %

Abbildung 20: 30-monatiger Überblick über die täglichen Identity-Threats in der Branche Nahrung/Getränke/Gastronomie

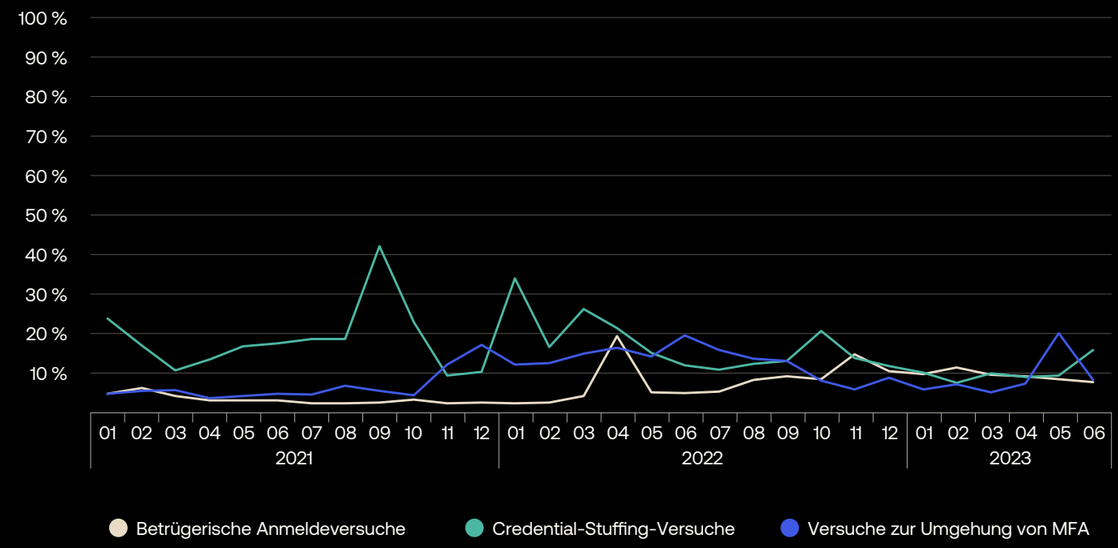


Abbildung 21: 30-monatiger Überblick über die täglichen Identity-Threats im Gesundheitswesen

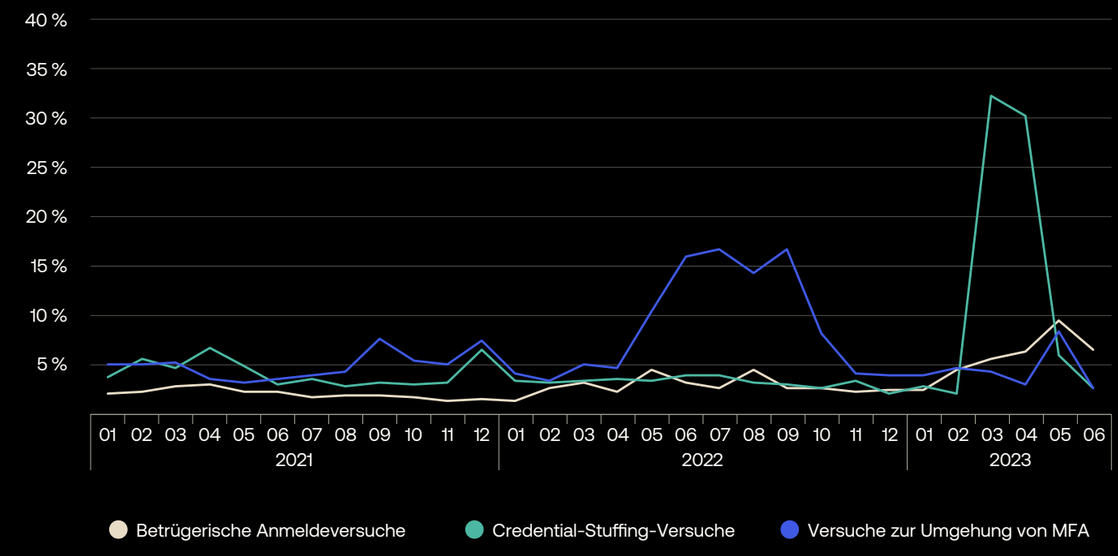


Tabelle 6: Produzierende Industrie

Überblick über Identity-Threat-Trends in der produzierenden Industrie

	2021	2022	1H2023
Betrügerische Anmeldeversuche	14,3 %	17,8 %	25,1 %
Credential-Stuffing-Versuche	45,9 %	18,4 %	17,7 %
Versuche zur Umgehung von MFA	6,5 %	10,0 %	7,8 %

Tabelle 7: Medien

Überblick über Identity-Threat-Trends im Bereich Medien

	2021	2022	1H2023
Betrügerische Anmeldeversuche	9,0 %	15,7 %	28,4 %
Credential-Stuffing-Versuche	22,7 %	17,9 %	42,3 %
Versuche zur Umgehung von MFA	27,4 %	25,1 %	12,8 %

Abbildung 22: 30-monatiger Überblick über die täglichen Identity-Threats in Finanzdienstleistungsunternehmen

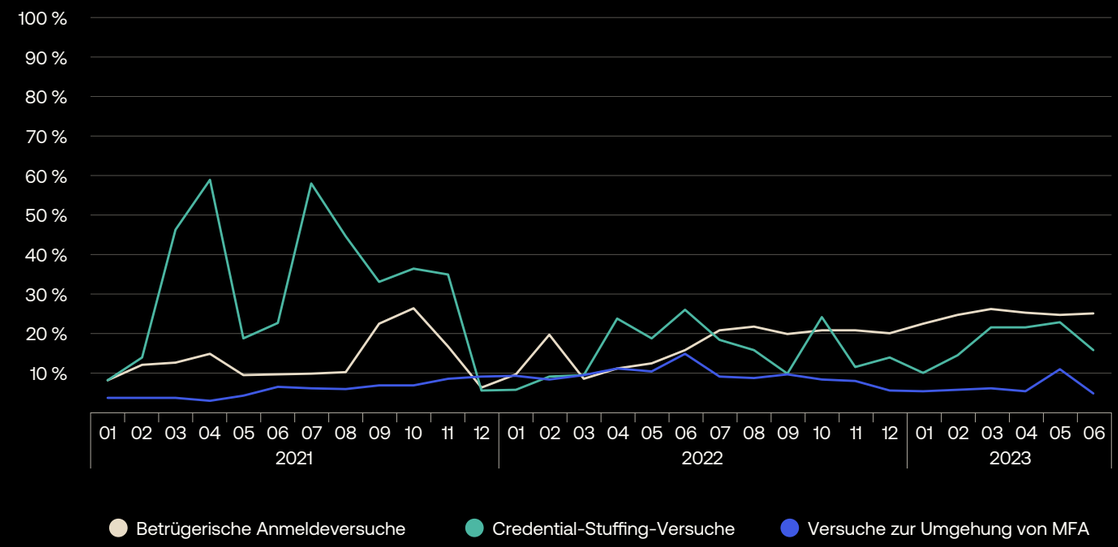


Abbildung 23: 30-monatiger Überblick über die täglichen Identity-Threats in der Branche Medien

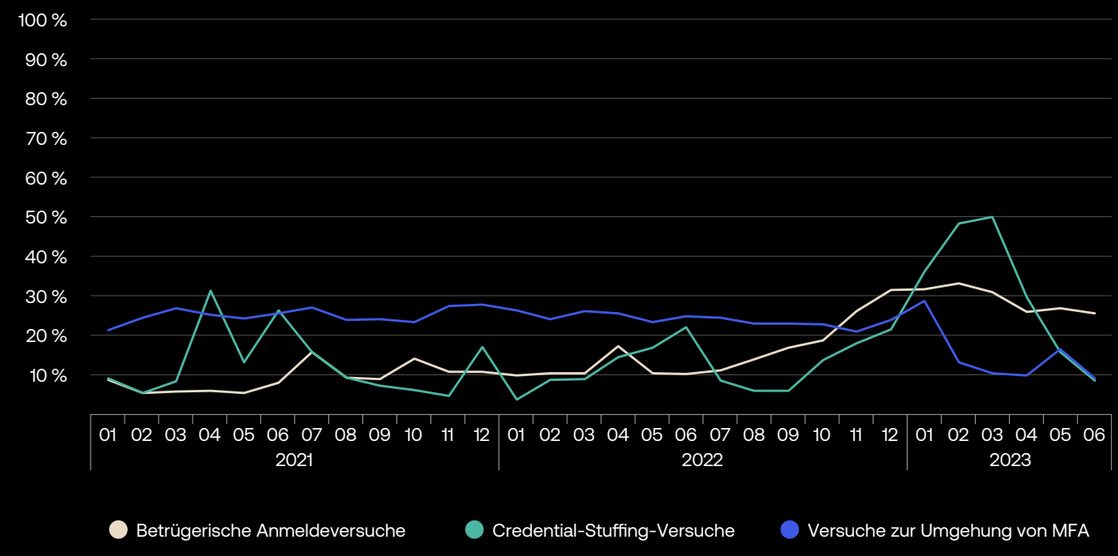


Tabelle 8: Professional Services

Überblick über Identity-Threat-Trends im Bereich Professional Services

	2021	2022	1H2023
Betrügerische Anmeldeversuche	5,9 %	6,1 %	13,4 %
Credential-Stuffing-Versuche	7,3 %	4,8 %	7,2 %
Versuche zur Umgehung von MFA	13,1 %	6,7 %	4,5 %

Tabelle 9: Handel

Überblick über Identity-Threat-Trends im Handel

	2021	2022	1H2023
Betrügerische Anmeldeversuche	2,0 %	3,6 %	9,3 %
Credential-Stuffing-Versuche	55,6 %	56,8 %	51,3 %
Versuche zur Umgehung von MFA	5,7 %	5,3 %	5,0 %

Abbildung 24: 30-monatiger Überblick über die täglichen Identity-Threats in der Branche Progfessional Services

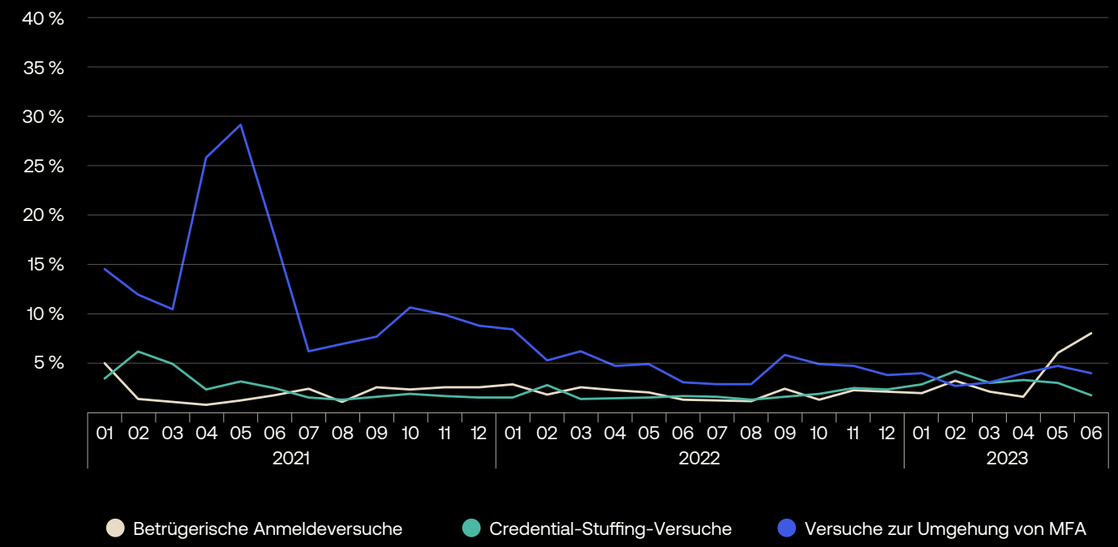


Abbildung 25: 30-monatiger Überblick über die täglichen Identity-Threats in Handel und E-Commerce

Tabelle 10: Software/SaaS/Technologie

Überblick über Identity-Threat-Trends im Bereich Software/SaaS/Technologie

	2021	2022	1H2023
Betrügerische Anmeldeversuche	54,9 %	26,1 %	24,0 %
Credential-Stuffing-Versuche	53,6 %	34,5 %	32,1 %
Versuche zur Umgehung von MFA	37,5 %	21,6 %	6,4 %

Tabelle 11: Reise/Transport

Überblick über Identity-Threat-Trends im Bereich Reise/Transport

	2021	2022	1H2023
Betrügerische Anmeldeversuche	5,1 %	13,7 %	9,7 %
Credential-Stuffing-Versuche	27,4 %	19,0 %	7,2 %
Versuche zur Umgehung von MFA	6,9 %	3,0 %	2,9 %

Abbildung 26: 30-monatiger Überblick über die täglichen Identity-Threats in der Branche Software/SaaS/Technologie

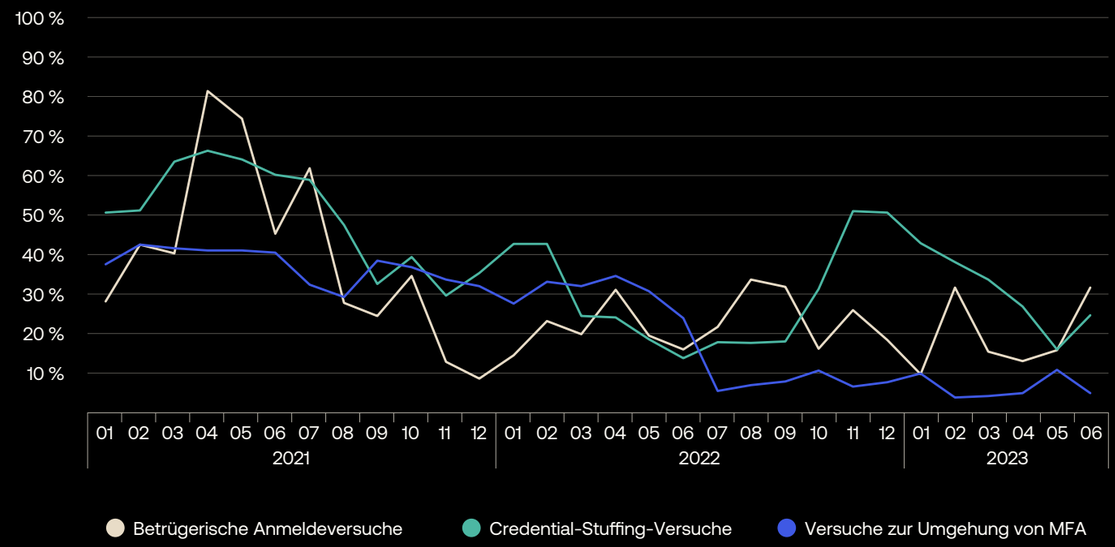
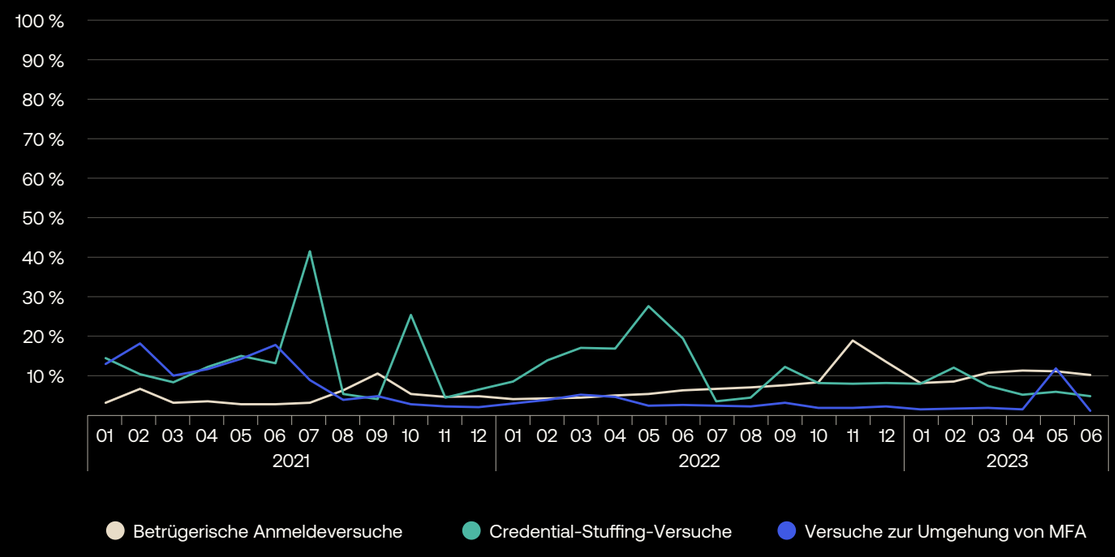


Abbildung 27: 30-monatiger Überblick über die täglichen Identity-Threats in der Branche Reise/Transport



Anhänge

Anhang D: Überblick nach Unternehmensgröße

Die folgenden Abschnitte bieten zusätzlichen Kontext zu kleinen, mittelständischen und Großunternehmen.

Tabelle 12: Kleinbetriebe

Überblick über Identity-Threat-Trends für Kleinbetriebe

	2021	2022	1H2023
Betrügerische Anmeldeversuche	65,1 %	44,6 %	19,4 %
Credential-Stuffing-Versuche	54,0 %	35,7 %	30,9 %
Versuche zur Umgehung von MFA	9,1 %	25,0 %	20,3 %

Abbildung 28: 30-monatiger Überblick über die täglichen Identity-Threats in Kleinunternehmen

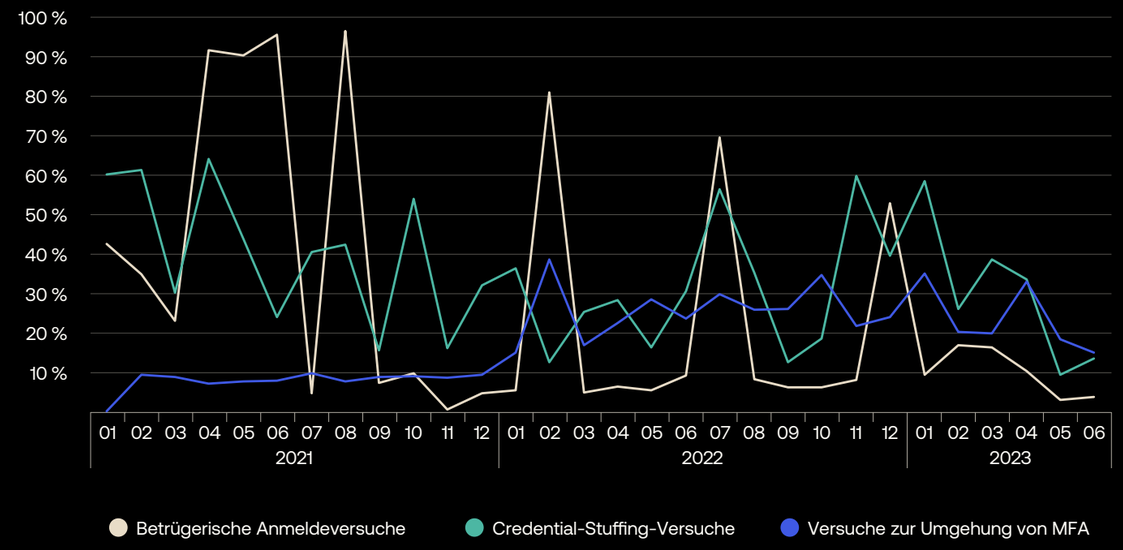


Tabelle 13: Mittelstand

Überblick über Identity-Threat-Trends für den Mittelstand

	2021	2022	1H2023
Betrügerische Anmeldeversuche	39,9 %	6,0 %	12,6 %
Credential-Stuffing-Versuche	32,1 %	30,5 %	20,1 %
Versuche zur Umgehung von MFA	4,4 %	6,2 %	9,0 %

Abbildung 29: 30-monatiger Überblick über die täglichen Identity-Threats im Mittelstand

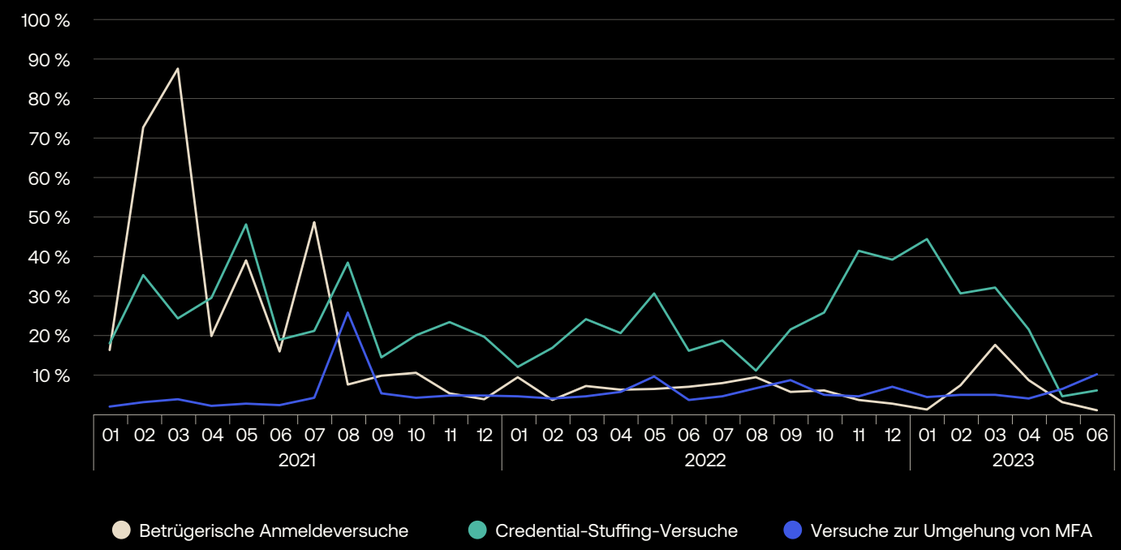
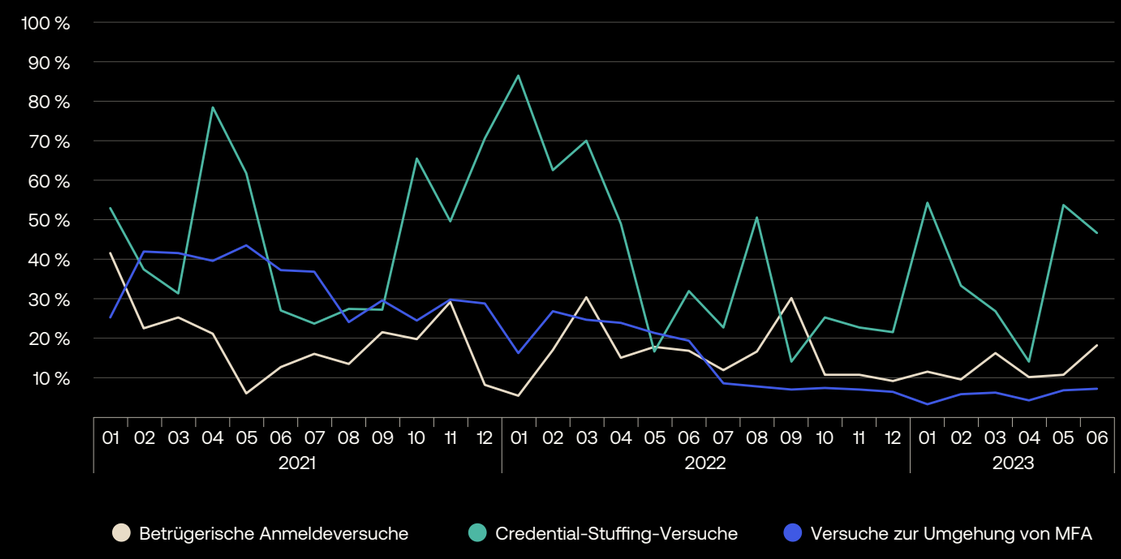


Tabelle 14: Enterprise

Überblick über Identity-Threat-Trends für das Enterprise-Segment

	2021	2022	1H2023
Betrügerische Anmeldeversuche	16,2 %	20,7 %	19,9 %
Credential-Stuffing-Versuche	50,6 %	44,0 %	39,4 %
Versuche zur Umgehung von MFA	32,3 %	16,4 %	9,5 %

Abbildung 30: 30-monatiger Überblick über die täglichen Identity-Threats in der Branche Enterprise



Anhänge

Anhang E: Überblick nach Region

Die folgenden Abschnitte bieten zusätzlichen Kontext für geografisch orientierte Analysen.

Bitte beachten Sie: Mit der Verkleinerung des Fokusbereichs verringert sich auch der Stichprobenumfang des betreffenden Datensatzes, was zu häufigeren und stärkeren kurzfristigen Schwankungen führen kann.

Tabelle 15: Nord- und Südamerika

Umfasst potenziell alle Länder, die in der Liste der United States Federal Aviation Authority für die westliche Hemisphäre aufgeführt sind.

Überblick über Identity-Threat-Trends für Unternehmen mit Hauptsitz in Nord- und Südamerika

	2021	2022	1H2023
Betrügerische Anmeldeversuche	35,8 %	14,7 %	9,4 %
Credential-Stuffing-Versuche	48,1 %	43,8 %	28,0 %
Versuche zur Umgehung von MFA	6,9 %	11,0 %	12,0 %

Tabelle 16: Lateinamerika

Umfasst potenziell folgende Länder: Argentinien, Belize, Bolivien, Brasilien, Chile, Costa Rica, Ecuador, El Salvador, Französisch-Guayana, Guatemala, Guyana, Honduras, Kolumbien, Mexiko, Nicaragua, Panama, Paraguay, Peru, Surinam, Uruguay und Venezuela.

Überblick über Identity-Threat-Trends für Unternehmen mit Hauptsitz in Lateinamerika

	2021	2022	1H2023
Betrügerische Anmeldeversuche	15,8 %	13,7 %	5,7 %
Credential-Stuffing-Versuche	59,0 %	31,3 %	17,6 %
Versuche zur Umgehung von MFA	5,0 %	4,8 %	10,7 %

Abbildung 31: 30-monatiger Überblick über die täglichen Identity-Threats in Unternehmen mit Sitz in Nord- und Südamerika

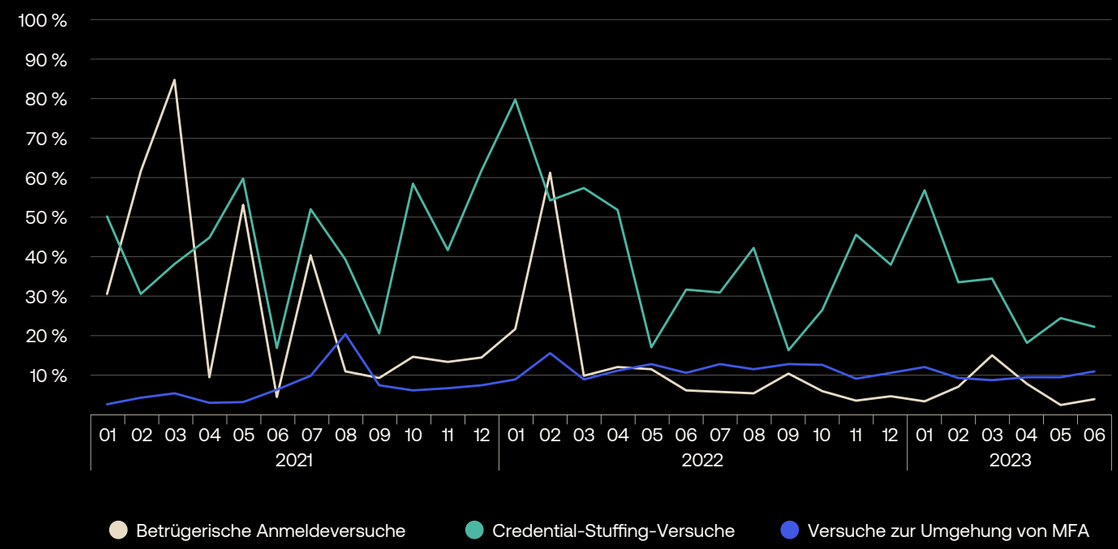


Abbildung 32: 30-monatiger Überblick über die täglichen Identity-Threats in Unternehmen mit Sitz in Lateinamerika

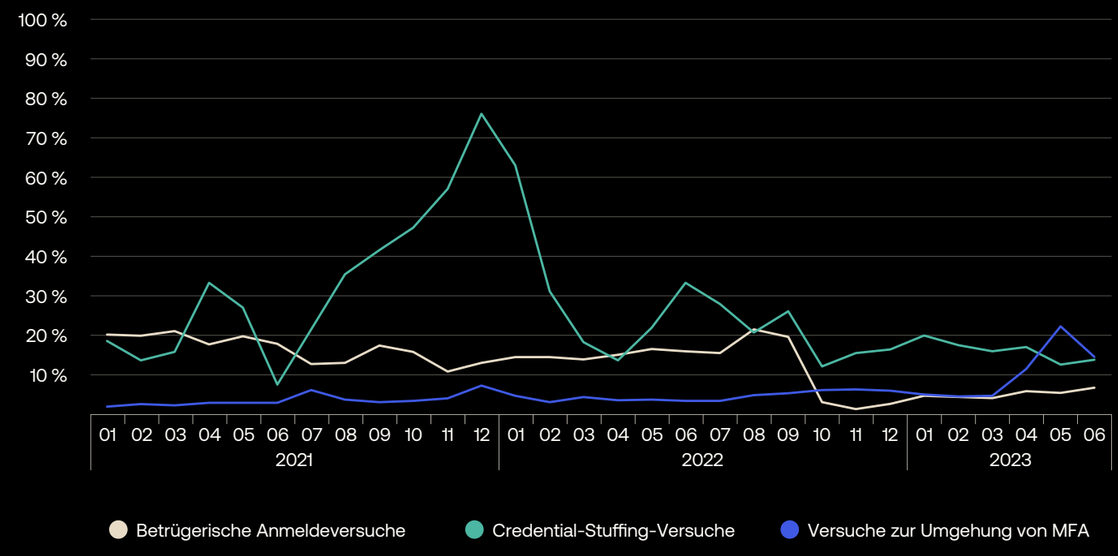


Tabelle 17: Vereinigte Staaten und Kanada

Überblick über Identity-Threat-Trends für Unternehmen mit Hauptsitz in den Vereinigten Staaten oder Kanada

	2021	2022	1H2023
Betrügerische Anmeldeversuche	37,1 %	14,8 %	9,5 %
Credential-Stuffing-Versuche	46,1 %	45,1 %	28,5 %
Versuche zur Umgehung von MFA	7,5 %	14,1 %	12,4 %

Tabelle 18: Europa, Nahost und Afrika

Umfasst potenziell alle Länder, die in der Liste der United States Federal Aviation Authority für Afrika, Europa und Nahost aufgeführt sind.

Überblick über Identity-Threat-Trends für Unternehmen mit Hauptsitz in Europa, Nahost oder Afrika

	2021	2022	1H2023
Betrügerische Anmeldeversuche	18,1 %	20,5 %	8,1 %
Credential-Stuffing-Versuche	26,4 %	14,1 %	20,2 %
Versuche zur Umgehung von MFA	34,8 %	20,3 %	7,6 %

Abbildung 33: 30-monatiger Überblick über die täglichen Identity-Threats in Unternehmen mit Sitz in Lateinamerika

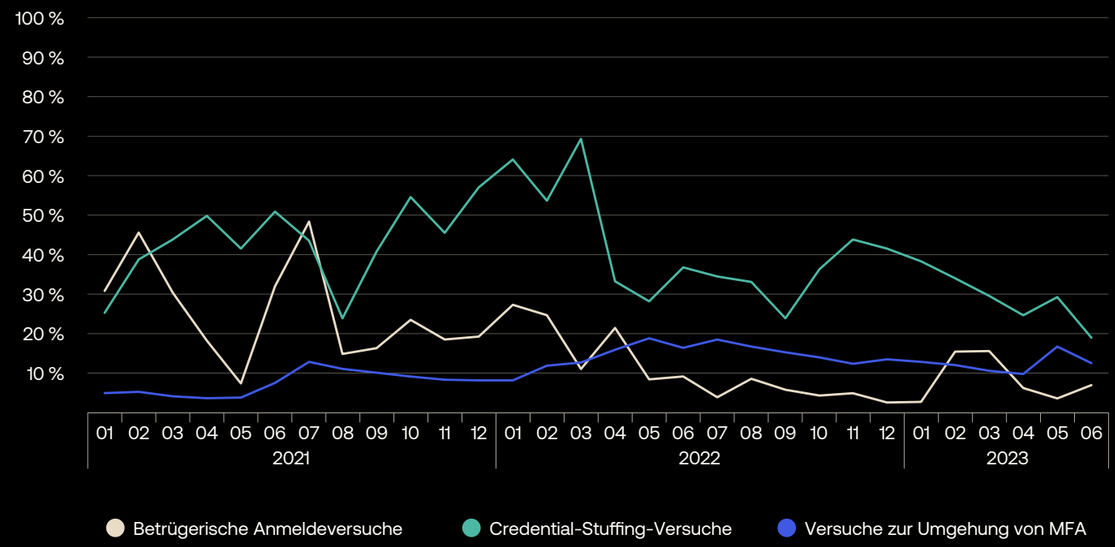


Abbildung 34: 30-monatiger Überblick über die täglichen Identity-Threats in Unternehmen mit Sitz in Europa, Nahost oder Afrika

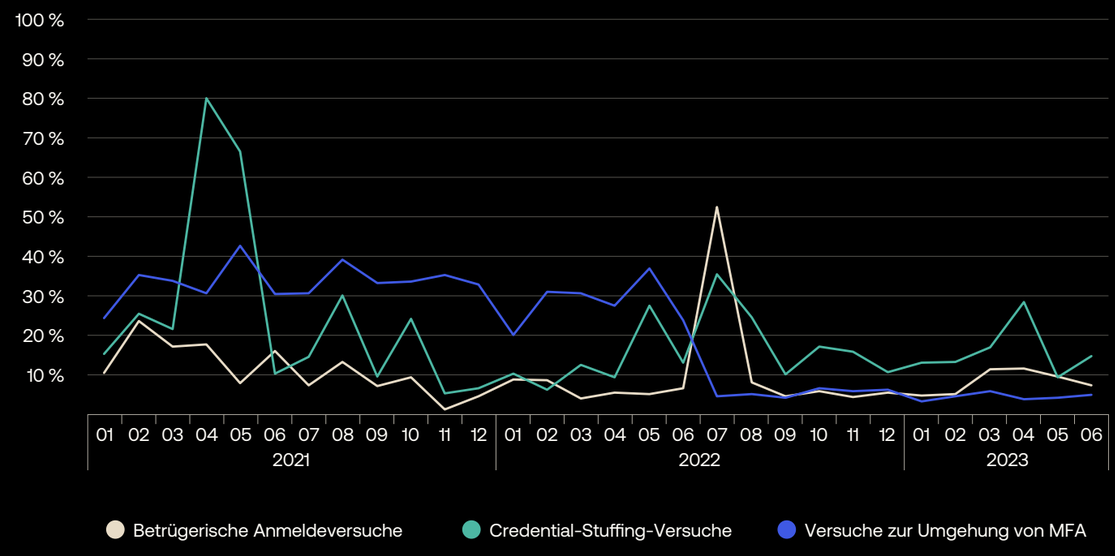


Tabelle 19: Nordische Länder

Umfasst potenziell folgende Länder: Dänemark, Finnland, Island, Norwegen, Schweden und Grönland.

Überblick über Identity-Threat-Trends für Unternehmen mit Hauptsitz in den nordischen Ländern

	2021	2022	1H2023
Betrügerische Anmeldeversuche	45,4 %	14,9 %	5,2 %
Credential-Stuffing-Versuche	15,0 %	5,2 %	12,5 %
Versuche zur Umgehung von MFA	6,0 %	2,9 %	4,1 %

Tabelle 20: Südeuropa

Umfasst potenziell folgende Länder: Andorra, Bosnien und Herzegowina, Bulgarien, Gibraltar, Griechenland, Italien, Kosovo, Kroatien, Malta, Montenegro, Nord-Mazedonien, Portugal, San Marino, Serbien, Slowenien, Spanien, Türkei, Vatikanstad und Zypernt.

Überblick über Identity-Threat-Trends für Unternehmen mit Hauptsitz in Südeuropa

	2021	2022	1H2023
Betrügerische Anmeldeversuche	11,7 %	15,2 %	24,8 %
Credential-Stuffing-Versuche	18,1 %	14,9 %	10,9 %
Versuche zur Umgehung von MFA	5,2 %	4,7 %	5,5 %

Abbildung 35: 30-monatiger Überblick über die täglichen Identity-Threats in Unternehmen mit Sitz in den nordischen Ländern

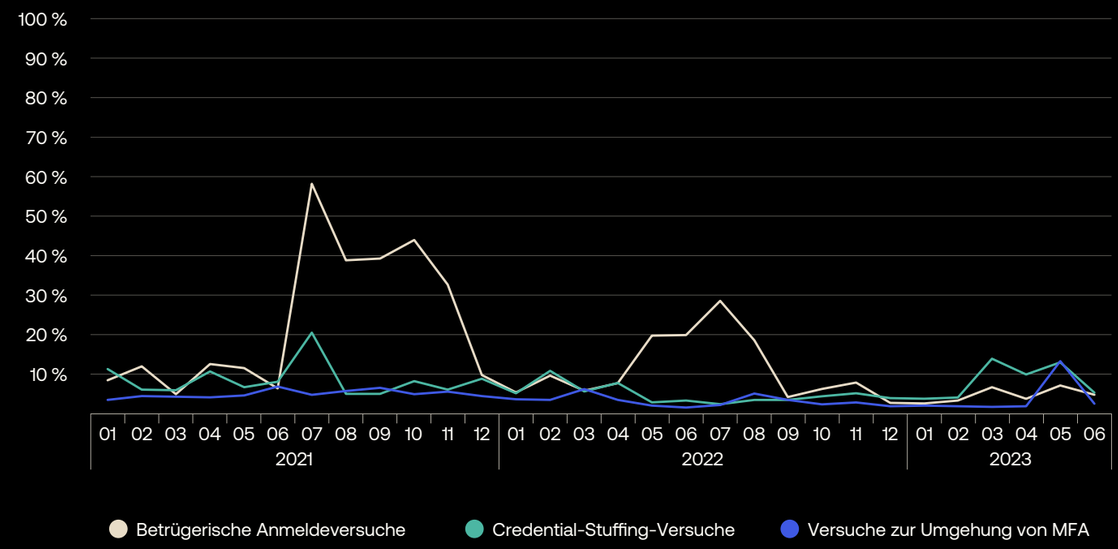


Abbildung 36: 30-monatiger Überblick über die täglichen Identity-Threats in Unternehmen mit Sitz in Südeuropa

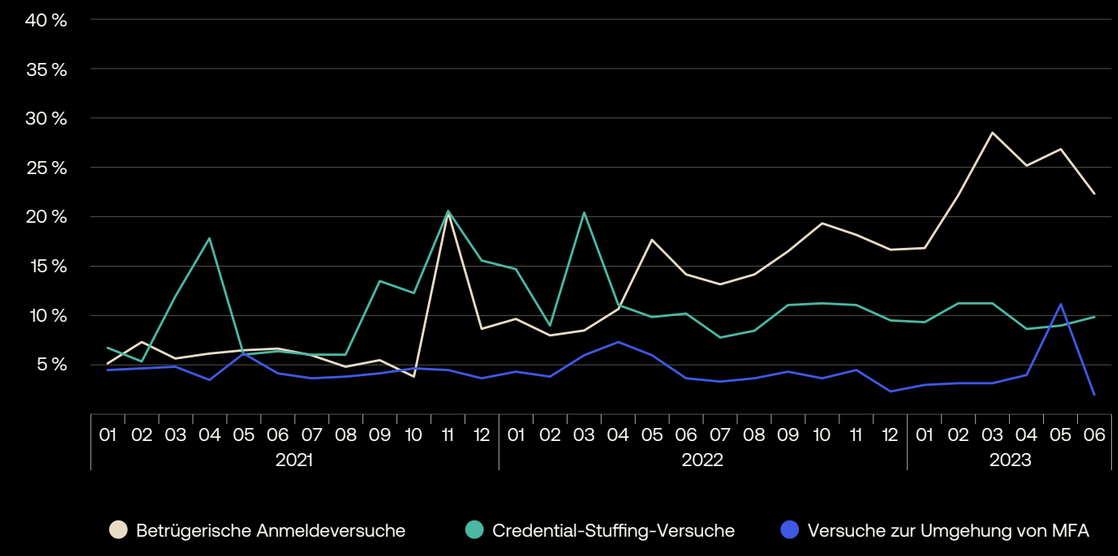


Tabelle 21: Vereinigtes Königreich

Umfasst potenziell folgende Länder: England, Nordirland, Schottland und Wales.

Überblick über Identity-Threat-Trends für Unternehmen mit Hauptsitz im Vereinigten Königreich

	2021	2022	1H2023
Betrügerische Anmeldeversuche	5,1 %	11,1 %	13,6 %
Credential-Stuffing-Versuche	14,5 %	12,9 %	13,3 %
Versuche zur Umgehung von MFA	1,6 %	2,7 %	4,6 %

Tabelle 22: Westeuropa

Umfasst potenziell folgende Länder: Belgien, Deutschland, Frankreich, Liechtenstein, Luxemburg, Monaco, Niederlande , Österreich und Schweiz.

Überblick über Identity-Threat-Trends für Unternehmen mit Hauptsitz in Westeuropa

	2021	2022	1H2023
Betrügerische Anmeldeversuche	14,6 %	28,7 %	5,1 %
Credential-Stuffing-Versuche	22,7 %	11,2 %	6,3 %
Versuche zur Umgehung von MFA	10,8 %	11,1 %	14,5 %

Abbildung 37: 30-monatiger Überblick über die täglichen Identity-Threats in Unternehmen mit Sitz in Großbritannien

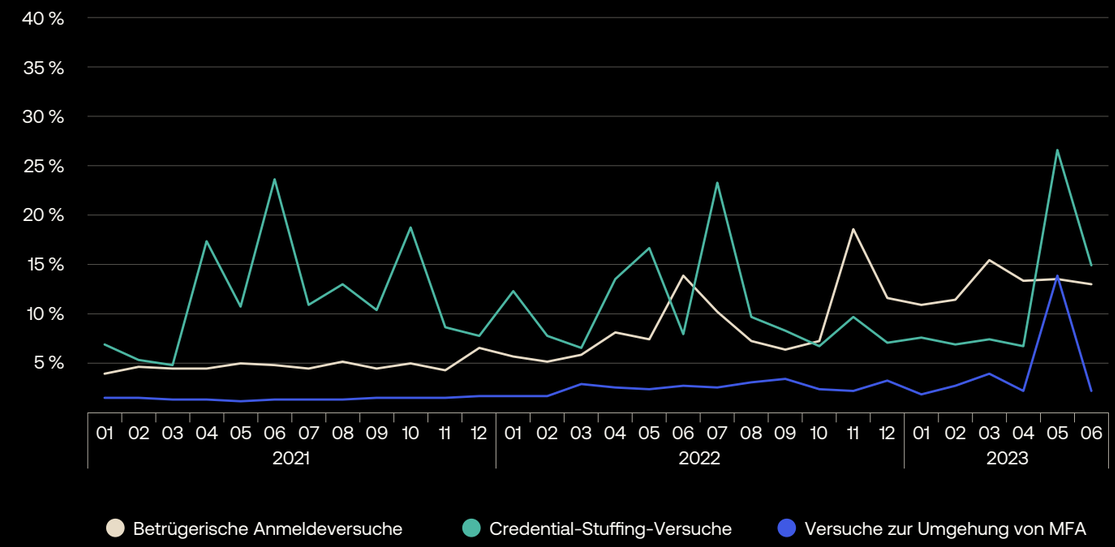


Abbildung 38: 30-monatiger Überblick über die täglichen Identity-Threats in Unternehmen mit Sitz in Westeuropa

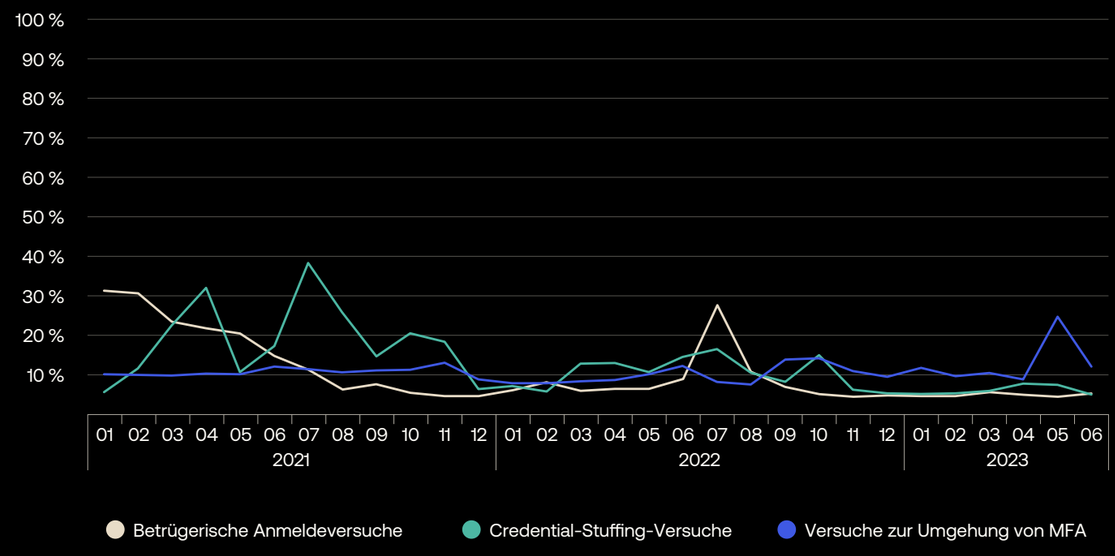


Tabelle 23: APAC

Umfasst potenziell alle Länder, die in der Liste der United States Federal Aviation Authority für APAC aufgeführt sind.

Überblick über Identity-Threat-Trends für Unternehmen mit Hauptsitz in APAC

	2021	2022	1H2023
Betrügerische Anmeldeversuche	52,4 %	28,9 %	27,9 %
Credential-Stuffing-Versuche	55,0 %	24,3 %	13,3 %
Versuche zur Umgehung von MFA	6,9 %	10,3 %	11,0 %

Abbildung 39: 30-monatiger Überblick über die täglichen Identity-Threats in Unternehmen mit Sitz in der APAC-Region

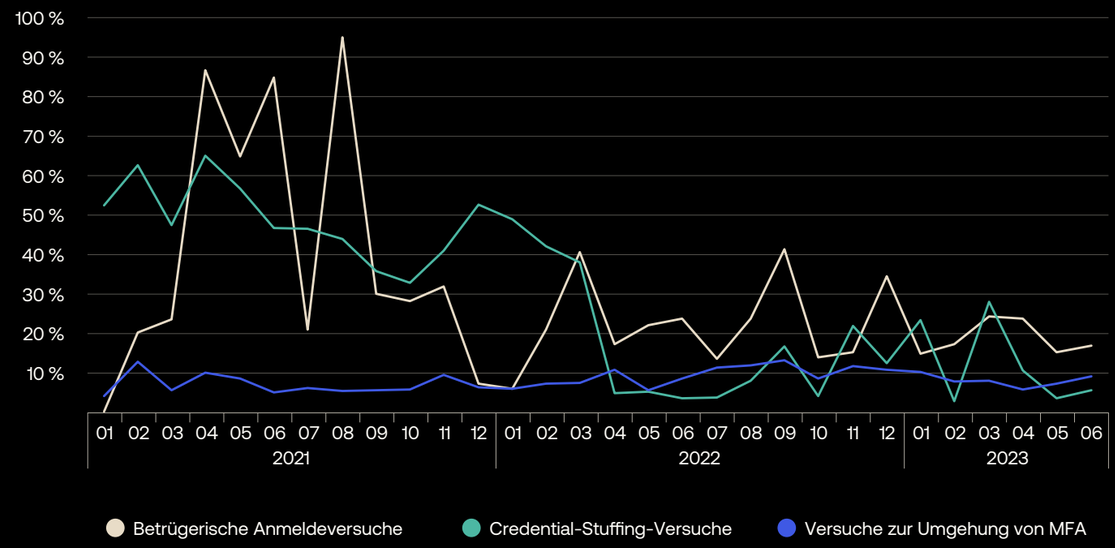


Tabelle 24: Japan

Überblick über Identity-Threat-Trends für Unternehmen mit Hauptsitz in Japan

	2021	2022	1H2023
Betrügerische Anmeldeversuche	16,5 %	33,9 %	43,6 %
Credential-Stuffing-Versuche	4,1 %	2,7 %	2,4 %
Versuche zur Umgehung von MFA	25,3 %	16,6 %	21,2 %

Abbildung 40: 30-monatiger Überblick über die täglichen Identity-Threats in Unternehmen mit Sitz in Japan

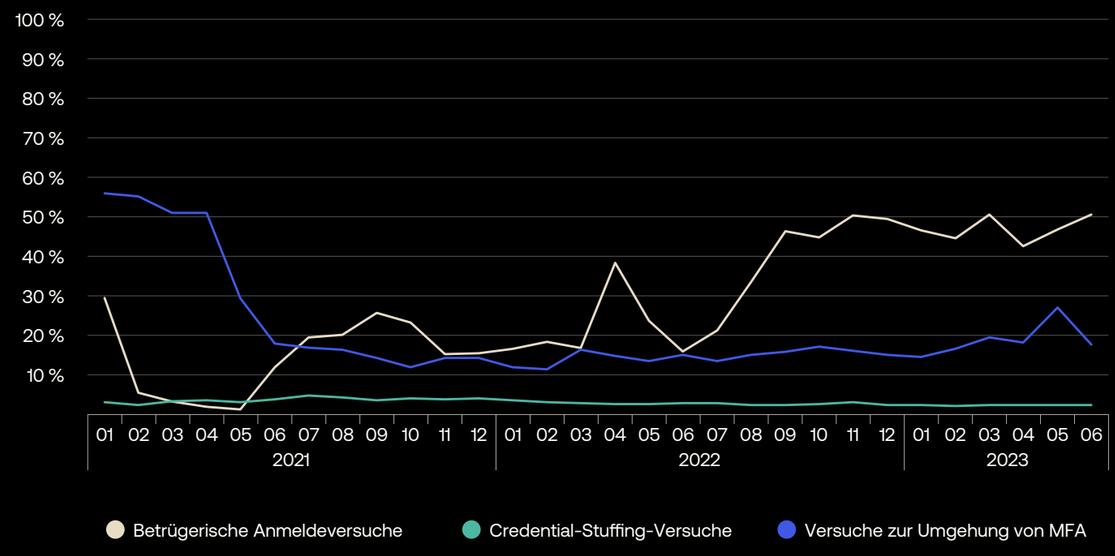


Tabelle 25: Australien und Neuseeland

Überblick über Identity-Threat-Trends für Unternehmen mit Hauptsitz in Australien oder Neuseeland

	2021	2022	1H2023
Betrügerische Anmeldeversuche	53,0 %	29,1 %	26,7 %
Credential-Stuffing-Versuche	57,1 %	26,6 %	14,8 %
Versuche zur Umgehung von MFA	4,3 %	8,7 %	9,1 %

Tabelle 26: Südostasien

Umfasst potenziell folgende Länder: Brunei, Indonesien, Kambodscha, Laos, Malaysia, Myanmar, Osttimor, Philippinen, Singapur, Thailand und Vietnam.

Überblick über Identity-Threat-Trends für Unternehmen mit Hauptsitz in Südostasien

	2021	2022	1H2023
Betrügerische Anmeldeversuche	47,3 %	15,2 %	16,2 %
Credential-Stuffing-Versuche	73,4 %	55,8 %	24,3 %
Versuche zur Umgehung von MFA	16,2 %	34,7 %	3,5 %

Abbildung 41: 30-monatiger Überblick über die täglichen Identity-Threats in Unternehmen mit Sitz in Australien oder Neuseeland

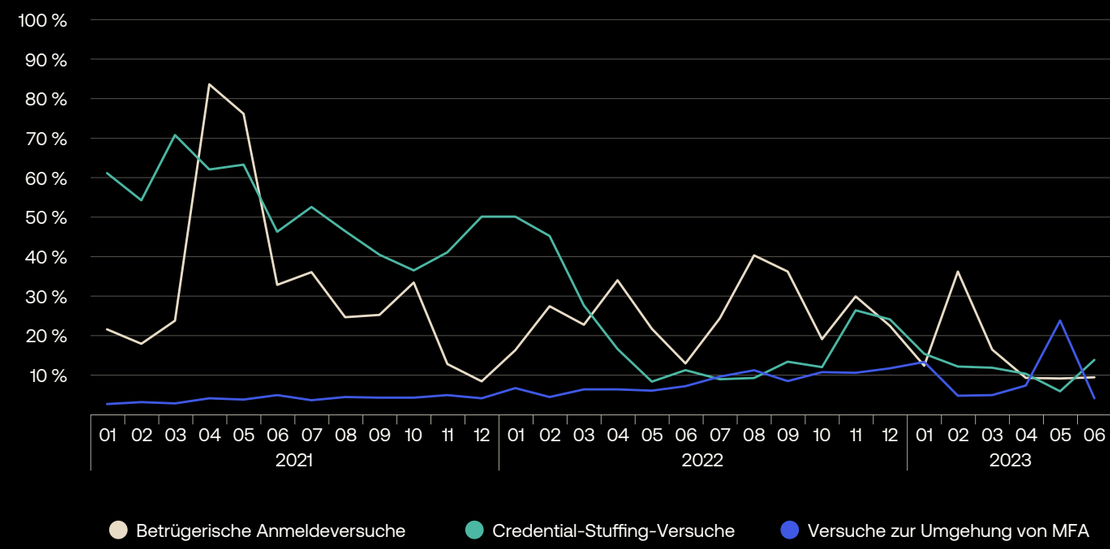
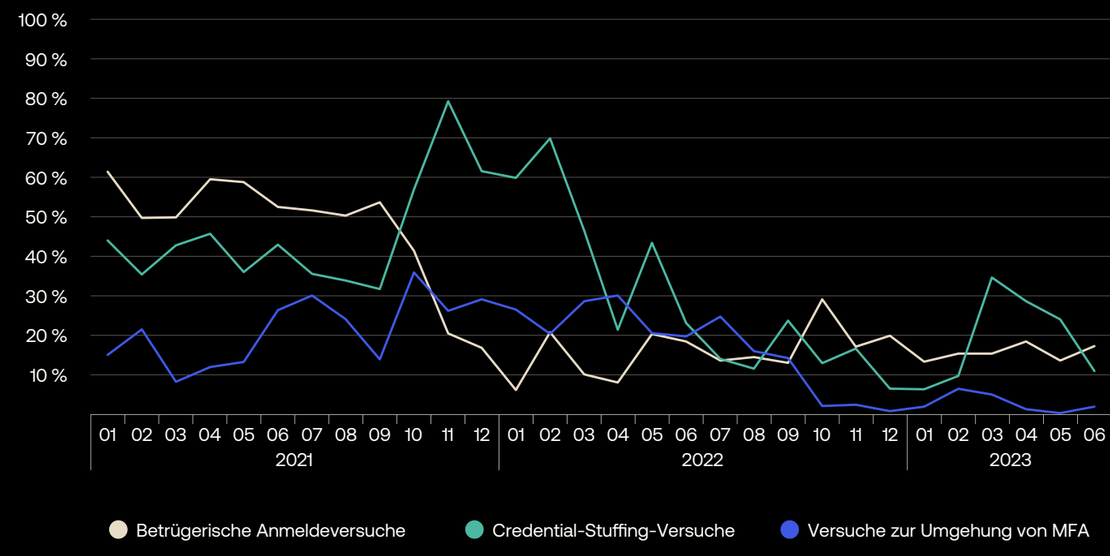


Abbildung 42: 30-monatiger Überblick über die täglichen Identity-Threats in Unternehmen mit Sitz in Südostasien



okta

Okta GmbH
Salvatorplatz 3
80333 München
info_germany@okta.com
+49 (89) 2620 3329