heise Business Services

Powered by okta

DIE PREKÄRE ZUKUNFT DER DIGITALEN IDENTITÄT

Zwischen Datensicherheit und Kundenerlebnis

Warum eine sichere, komfortable und datensparsame Authentifizierung schwierig, aber nicht unmöglich ist

Editorial

Ein Kunde ist heutzutage ziemlich anspruchsvoll. Er erwartet, dass ein Unternehmen oder eine Behörde all seine Anforderungen bei digitalen Prozessen erfüllt, ohne Fragen zu stellen. Egal, ob es sich zum Beispiel um Online-Shops, Kfz-Werkstätten, Sportvereine, Banken oder Krankenkassen handelt. Er wünscht sich einen sicheren und einfachen Online-Zugang zu seinem Kundenprofil – kann der Anbieter das nicht erfüllen, steigt das Risiko, dass sich der Kunde künftig beim Wettbewerber umsieht.

Firmen und Institutionen sind also gefragt, ihren Kunden und Besuchern über alle Kanäle, Apps und Dienste hinweg einfache und sichere Zugriffe zu ermöglichen. Diese Herausforderung lässt sich mit einem Customer Identity and Access Management (CIAM) bewältigen. Ein solches Konzept kann in Kundenanwendungen, -Webseiten und -portale eingebettet werden, um die Identität der Kunden zu überprüfen und ihre Zugriffsrechte zu regeln.

In diesem eBook erklären wir zunächst, wie ein CIAM das Kundenerlebnis verbessert. Dann zeigen wir, wie Hacker versuchen, Kundenkonten zu kompromittieren, und mit welchen Mitteln Unternehmen das verhindern können. Anschließend gehen wir darauf ein, dass Verbraucher mehr Kontrolle über ihre Daten fordern, bevor ein Okta-Manager Fragen zum Identitätsmanagement von Kunden beantwortet.

Viel Vergnügen bei der Lektüre!

Heise Medien GmbH & Co. KG
Abt. Heise Business Services
Hans-Pinsel-Straße 10b
85540 Haar bei München

Registergericht:
Amtsgericht Hannover HRA 26709

Persönlich haftende Gesellschafterin:
Heise Medien Geschäftsführung GmbH

Registergericht:
Amtsgericht Hannover, HRB 60405

Geschäftsführer:
Ansgar Heise, Beate Gerold

Verantwortlich für den Inhalt:
Heise Business Services
Thomas Jannot, tj@heise.de

Layout: Oliver Eismann, www.olivereismann.de

Inhalt

Über den Autor

Dr. Klaus Manhart ist freier Fachautor für IT und Wissenschaft und schreibt seit mehreren Jahrzehnten Beiträge für namhafte IT-Zeitschriften und Wissenschaftsjournale. Schwerpunkte im Bereich IT-Journalismus sind Business-Computing, Big Data/Analytics, Cloud-Computing, Artificial Intelligence und Security-Themen.

Mit Identitäts-Management Kunden schützen

Der Schutz der Kundenidentität ist zum Schlüsselfaktor jedes sicheren und kundenfreundlichen Unternehmens geworden. Customer Identity and Access Management (CIAM) bewahrt Unternehmen vor Problemen mit Zugangsdaten seiner Kunden – und sorgt daneben für eine gute Customer Experience.

Im Zeitalter der Digitalisierung ist die Identifizierung von Kunden und der Schutz ihrer Daten für jedes Unternehmen von zentraler Bedeutung. Kunden verlangen heute eine persönliche Customer Experience und wollen ihre sensiblen Daten gut gesichert wissen. Zudem erfordern gesetzliche Regularien wie die DSGVO umfangreiche Vorkehrungen gegen Datenkompromittierung. Die digitale Identität einer Person muss deshalb technisch durch starke Authentifizierungssysteme gesichert sein.

Für Hacker sind solche Authentifizierungssysteme und die digitalen Identitäten der Kunden lukrative Angriffsziele und eine begehrte Beute. Sie wenden immer raffiniertere Methoden an, um die persönlichen Informationen zu stehlen und diese Daten – unter Vorspiegelung einer falschen Identität – für ihre kriminellen Zwecke zu nutzen.

Die Konsequenzen eines solchen Identitätsdiebstahls können gravierend sein. Gelingt den Cyber-Angreifern ein Datenklau, können sie sich Zugang zu sensiblen und personenbezogenen Daten verschaffen und sich mit einer fremden Identität ausweisen. Die Möglichkeiten, die sich damit eröffnen, sind vielfältig und sorgen oft für hohen Schaden: Sie reichen von der einfachen Bestellung von Waren unter falscher Identität über die Manipulation von Aktienkursen bis hin zur Nutzung der gestohlenen Daten für kriminelle „Geschäftsmodelle".

Praktisch erfolgen solche Identitätsangriffe in vielerlei Formen – von manuell durchgeführten Attacken bis hin zu groß angelegten Ansätzen, die umfangreiche Automatisierungsfunktionen und Brute-Force-Taktiken einsetzen. Der Okta-Bericht „The State of Secure Identity 2022", der im nächsten Beitrag vorgestellt wird, zeigt, mit welchen Methoden Hacker arbeiten, wie sie ihre Angriffe durchführen und welche Maßnahmen Unternehmen ergreifen können.

Eine starke Identifizierung ist für Unternehmen und Behörden wichtig, um Daten zu schützen und das Vertrauen der Nutzer zu erlangen. (Foto: matrosovv, Adobe Stock)

Identitäten schützen mit IAM

Um ihre Daten zu schützen, Vertrauen aufzubauen und Kunden ein hochwertiges digitales Erlebnis zu bieten, sollten IT-Sicherheitsverantwortliche auf eine starke Identifizierung setzen. Die meisten Unternehmen haben dies erkannt: In einer Okta-Umfrage geben 80 Prozent aller befragten Unternehmen an, dass Identität für ihre gesamte Sicherheitsstrategie wichtig ist. Weitere 19 Prozent gehen sogar so weit, Identität als geschäftskritisch zu bezeichnen.

Die Relevanz von Identitätsschutz hat auch Gartner kürzlich in seinem Report „7 Top Trends in Cybersecurity for 2022" festgestellt. Dort heißt es, dass der „Missbrauch von Anmeldeinformationen" eine bevorzugte Methode von Angreifern ist, um auf Systeme zuzugreifen und ihre Ziele zu erreichen.

Unternehmen sollten deshalb ihre Systeme, Daten, Mitarbeiter und Kunden besser schützen. Traditionelle Herangehensweisen bei einer Identitätsprüfung, die für weniger komplexe Zeiten entwickelt wurden, sollten geändert werden. Wie das am besten geschehen soll, erfahren Sie in den folgenden Beiträgen.

Als Sicherheitslösung haben sich für diesen Zweck breitflächig Identity- und Access-Management-Systeme (IAM) etabliert. Diese Authentifizierungswerkzeuge schützen jedes Unternehmen vor Identitätsproblemen und -diebstahl. Die richtigen Benutzer erhalten zur richtigen Zeit Zugriff auf die richtigen Ressourcen. Gleichzeitig hat das IT-Team alle Logins im Blick und im Griff. Solche Systeme optimieren somit alle Prozesse rund um die Verwaltung von Identitäten und der Zugangskontrolle.

Glossar

Authentifizierung: Authentifizierung (engl. authentication) ist der Prozess der Feststellung der Identität eines Nutzers. Bei der Authentifizierung wird festgestellt, dass die Person, mit der kommuniziert wird, tatsächlich diejenige ist, die sie vorgibt zu sein. Die einfachste und heute immer noch weiter verbreitete Authentifizierungsmethode ist die Abfrage eines Passworts.

IAM: Identity Access Management (Identitäts- und Zugriffsmanagement) ist ein Sammelbegriff für Tools, Prozesse und Richtlinien, mit denen Nutzeridentitäten – in der Regel von unternehmenseigenen Mitarbeitern – geprüft und Zugänge gewährt werden. Außerdem dient IAM der Einschränkung unbefugter Zugriffe. Damit umfasst IAM zwei verwandte Aktivitäten: zum einen die Authentifizierung und zum anderen die Autorisierung (= Gewährung des Zugangs zu Ressourcen für authentifizierte Nutzer)

CIAM: Customer Identity Access Management (Kundenidentitäts- und Zugriffsmanagement) ermöglicht es einem Unternehmen, den Kundenzugriff auf Anwendungen zu kontrollieren, die Kundenidentität festzustellen und Profilinformationen sicher zu erfassen sowie zu verwalten. Mit CIAM können Unternehmen gezieltes Marketing betreiben, eine nahtlose Authentifizierung für den Kundensupport bereitstellen und Business-Intelligence-Analysen durchführen, um Kunden mit neuen Produktfunktionen und -aktualisierungen besser zu bedienen.

CIAM – Nutzerfreundlichkeit ist ein Muss

Während IAM für die Identitätsprüfung von Mitarbeitern konzipiert ist, hat sich für die Verifizierung der Kunden-Accounts Customer Identity and Access Management (CIAM) durchgesetzt. Der Hauptunterschied zwischen einem mitarbeiter-orientierten IAM und einem CIAM ist, dass sich das CIAM sehr stark auf die User Experience konzentrieren muss. Stehen bei den IAM-Systemen im Enterprise-Bereich Compliance- und Gesetzesvorgaben sowie Prozessabläufe auf Basis von Standardisierung und Kontrolle im Vordergrund, ist im Consumer-Bereich die Kundenerfahrung entscheidend.

Der Kunde möchte in seiner Customer Experience möglichst nicht an Barrieren stoßen und ein grenzenloses Erlebnis haben. Das erfordert hoch modulare, flexible und offene Systeme, die sich über Schnittstellen in andere Lösungen wie Unternehmensportale integrieren und an individuelle Anforderungen anpassen lassen.

Besonders wichtig sind einfache Anmelde- und Registrierungsverfahren wie Social Login oder SMS-Text. Damit Interessenten im Consumer-Umfeld nicht vorzeitig abspringen, ist schon bei der Registrierung neuer Accounts eine niedrige Eintrittsbarriere von zentraler Bedeutung. Kunden-Login-Systeme dürfen deshalb Besucher, die sich zum ersten Mal an einem System anmelden, nicht überfordern.

Ein Beispiel für eine sehr einfache Authentifizierung ist die Anmeldung über Social Media Accounts, bei der die Kunden ihre digitale Identität gleich mitbringen. Weil die Nutzer keine langen Registrierungsformulare ausfüllen müssen, kann dies die Anzahl der Registrierungen enorm steigern.

State of Secure Identity 2022: Wie Hacker Kundendaten klauen

Angreifer werden immer besser darin, Kundenkonten zu kompromittieren – und fügen damit Unternehmen großen Schaden zu. Der aktuelle State of Secure Identity Report von Okta zeigt, wie Cyber-Kriminelle vorgehen, und hilft Unternehmen, Bedrohungen der Kundenidentität zu verstehen und abzuwehren.

Mit der zunehmenden Raffinesse von Cyber-Angreifern steigen die Attacken auf Zugangsdaten von Mitarbeitern und Kunden an. Einen entsprechend großen Anteil bei allen Security-Vorfällen nehmen dementsprechend geleakte Accounts ein: Etwa die Hälfte der Sicherheitsverletzungen beginnen laut dem Data Breach Investigation Report 2022 von Verizon mit gestohlenen Zugangsdaten. Bei Angriffen auf Webanwendungen wurden sogar über 80 Prozent der Sicherheitsverletzungen geleakten Zugangsdaten zugeschrieben.

Begehrt sind neben den Kontodaten der Mitarbeiter vor allem auch diejenigen der Kunden. Angreifer erhalten bei einem erfolgreichen Diebstahl von Kundenzugangsdaten nicht nur Zugriff auf Ressourcen wie Treuepunkte und Privilegien. Sie können auch in großem Ausmaß wertvolle demografische und personenbezogene Daten erlangen – die zum Teil strengsten Vorschriften unterliegen.

Abbildung 1: Beispiel eines tatsächlichen Angriffs auf eine Finanzorganisation in Südamerika, die mehr als zwei Monate dauerte. Innerhalb dieses Zeitraums war der Credential-Stuffing-Traffic (grün) regelmäßig fünf- bis zehnmal höher als die legitime Benutzeranmeldung (blau).

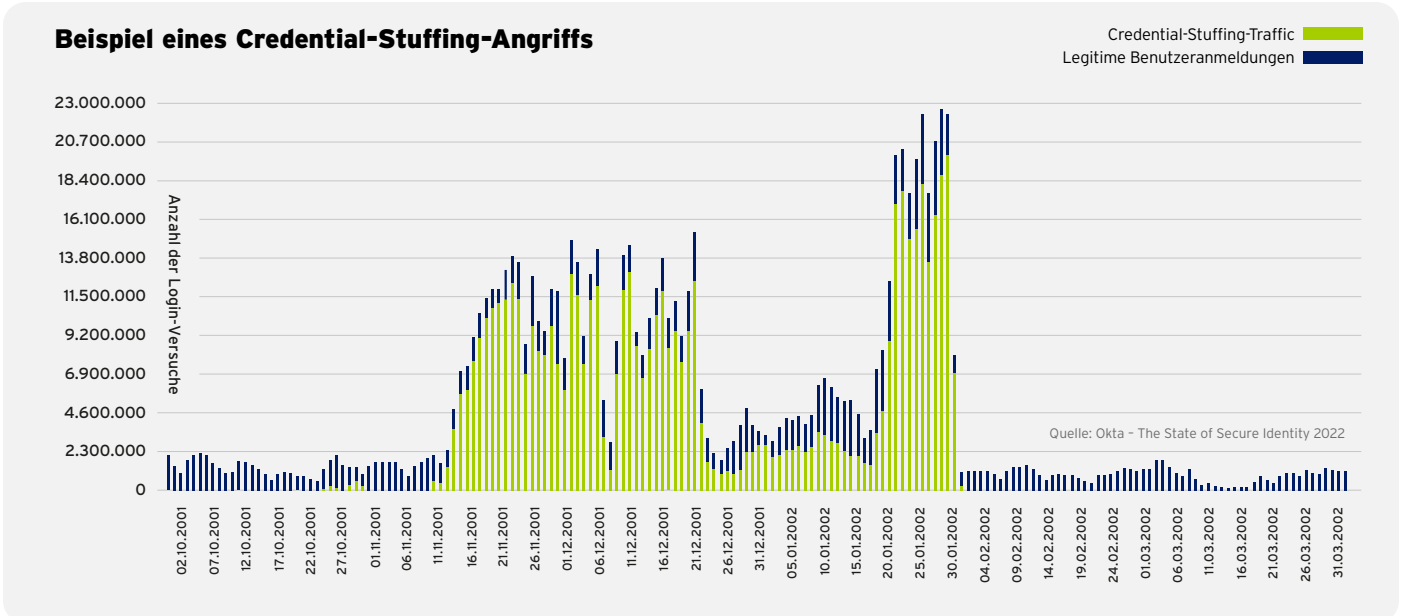
Gelingt die kriminelle Übernahme von Kundenkonten, kann dies für Unternehmen schwerwiegende Konsequenzen haben. Ihnen entstehen nicht nur Kosten für die Untersuchung und Beseitigung des Missbrauchs, sie müssen im Falle einer Datenschutzverletzung auch mit strengen behördlichen Strafen, Reputationsschäden sowie einem Vertrauensverlust der Nutzer rechnen.

Um solche Identitätsverletzungen zu verhindern, sollten IT- und Security-Verantwortliche verstehen, warum und wie Hacker Systeme zum Customer Identity and Access Management (CIAM) attackieren. Der aktuelle Bericht „State of Secure Identity 2022" von Okta will Licht ins Dunkel bringen. Der Report liefert einen Überblick zu Angriffen auf die Identität von Kunden und stellt Strategien zur Risikominderung vor. Die Erkenntnisse basieren auf Selbstauskünften von Kunden der Auth0-Zugangsmanagement-Plattform, die inzwischen von Okta übernommen wurde.

Credential Stuffing – zehnmal höherer Traffic

Angriffe auf Kundendaten und CIAM-Dienste gibt es in vielen Formen – von präzisen, manuell erzeugten „Hands-on-Keyboard"-Attacken bis hin zu groß angelegten Ansätzen, die umfangreiche Automatisierungsfunktionen und Brute-Force-Taktiken einsetzen.

Die häufigste Cyber-Angriffsmethode auf CIAM-Dienste ist laut dem Report Credential Stuffing. Bei diesen Attacken werden zuvor geleakte oder illegal erlangte Anmeldedaten für den unbefugten Zugang bei anderen Diensten massenhaft ausprobiert. Laut dem Report bestehen 34 Prozent des gesamten Datenverkehrs im Okta-Netzwerk aus solchen Aktionen – das sind fast zehn



Milliarden Versuche allein im ersten Quartal 2022. Dabei verzeichnete das Okta-Netzwerk mit mehr als 300 Millionen Versuchen pro Tag zwei der größten Ausbrüche von Credential Stuffing, die jemals auf der Plattform registriert wurden.

Credential-Stuffing-Angriffe können durch eine große Zunahme der Anmeldeversuche und durch einen plötzlichen und starken Anstieg fehlgeschlagener Anmeldeversuche identifiziert werden (siehe Abb. 1). Solche Attacken sind für Unternehmen und Kunden nicht nur ein großes Risiko. Sie belasten die IT-Infrastruktur auch enorm, was zu Latenzen in den Anwendungen und Reibungsverlusten bei den Benutzern führen kann.

Credential Stuffing – Unterschiede der Branchen, Zeiten, Länder

Nicht alle Branchen sind von Credential-Stuffing-Attacken gleich stark betroffen (Abb. 2). Während in den meisten Branchen eine Rate von weniger als 10 Prozent für diese Angriffsart registriert wurde, machten die Attacken in anderen Fällen den Großteil der Anmeldeversuche aus. Beispielsweise waren im Einzelhandel/E-Commerce mehr als 80 Prozent des Login-Verkehrs mit hoher Sicherheit Credential-Stuffing-Versuche. Auch im Finanzdienstleistungs- und Unterhaltungsbereich war solche Angriffe für mehr als 50 Prozent der Login-Aktivität verantwortlich. Wie sich solche Attacken praktisch vermeiden lassen, zeigt das Fallbeispiel einer Versicherung, das im nächsten Beitrag vorgestellt wird.

Auch über die Zeit unterscheiden sich die Angriffe. Abb. 3 zeigt, dass die Gesamtrate der Credential-Stuffing-Angriffe gegen Ende des Jahres 2021 zunahm und dass dieses höhere Niveau in den ersten Monaten des Jahres 2022 Bestand hatte – einschließlich eines neuen Allzeithochs Mitte Januar. Die Angriffsrate sank bis Mitte März, bevor es im April schon wieder einen neuen Rekord gab.

Beim Vergleich einzelner Länder zeigen sich ebenfalls deutliche Unterschiede. In Deutschland – wie in den meisten europäischen Ländern – ist normaler Traffic an der Tagesordnung. Hinweise auf anhaltendes Credential Stuffing gibt es nur auf niedriger Ebene, unterbrochen von größeren Angriffen (Abb. 4). Ein bemerkenswerter Unterschied besteht darin, dass das „Hintergrund"-Volumen des Angriffsverkehrs im Verhältnis zu den erwarteten Ausfällen relativ hoch ist.

In krassem Gegensatz zu dem, was in Europa beobachtet wurde, stehen die USA. Während des gleichen Beobachtungszeitraums macht Credential Stuffing in den Vereinigten Staaten den größten Anteil an Anmeldeversuchen aus (Abb. 5) – 61 Prozent insgesamt und ein Anstieg auf 85 Prozent der Anmeldeereignisse während der Angriffs ganz rechts in der Abbildung. Credential Stuffing übertrifft damit deutlich andere Angriffsarten und den normalen Datenverkehr (38 Prozent).

Multi-Faktor-Authentifizierung umgehen

Als effektive Möglichkeit, Kontoübernahmen durch Credential-Stuffing-Angriffe zu verhindern, gilt die Multi-Faktor-Authentifizierung (MFA). Dabei werden mehrere Faktoren zur Prüfung der Identität eingesetzt.

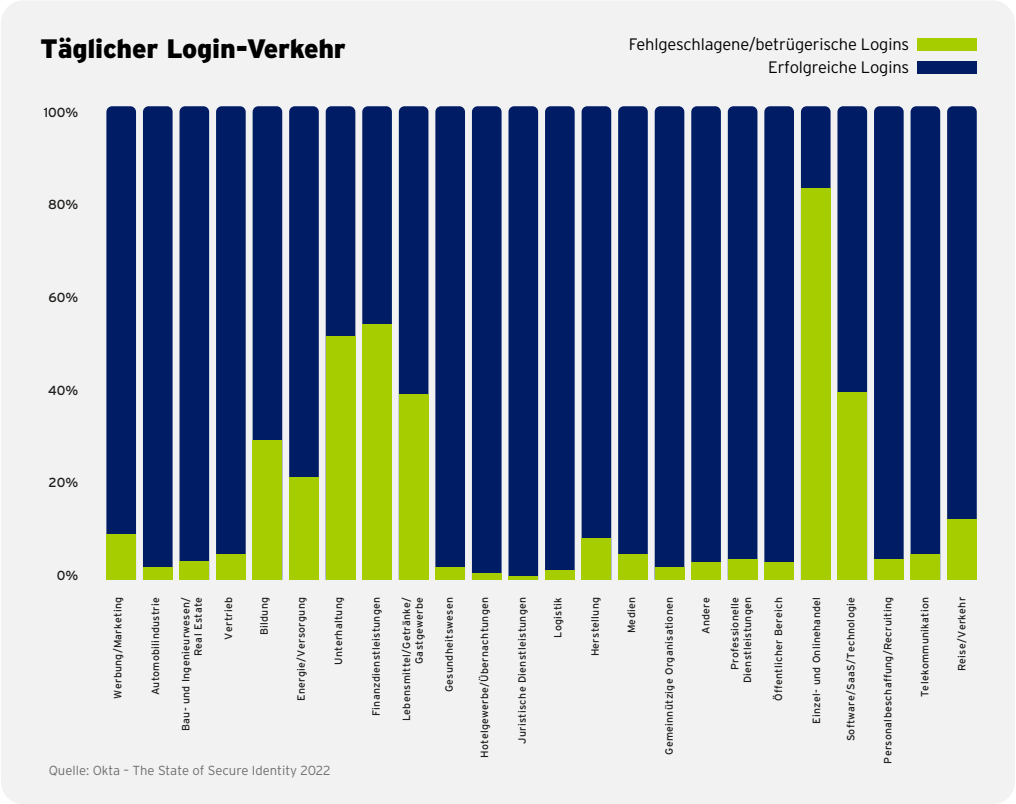


Abbildung 2: Credential-Stuffing-Angriffsversuche sortiert nach Branchen in den ersten 90 Tagen des Jahres 2022.

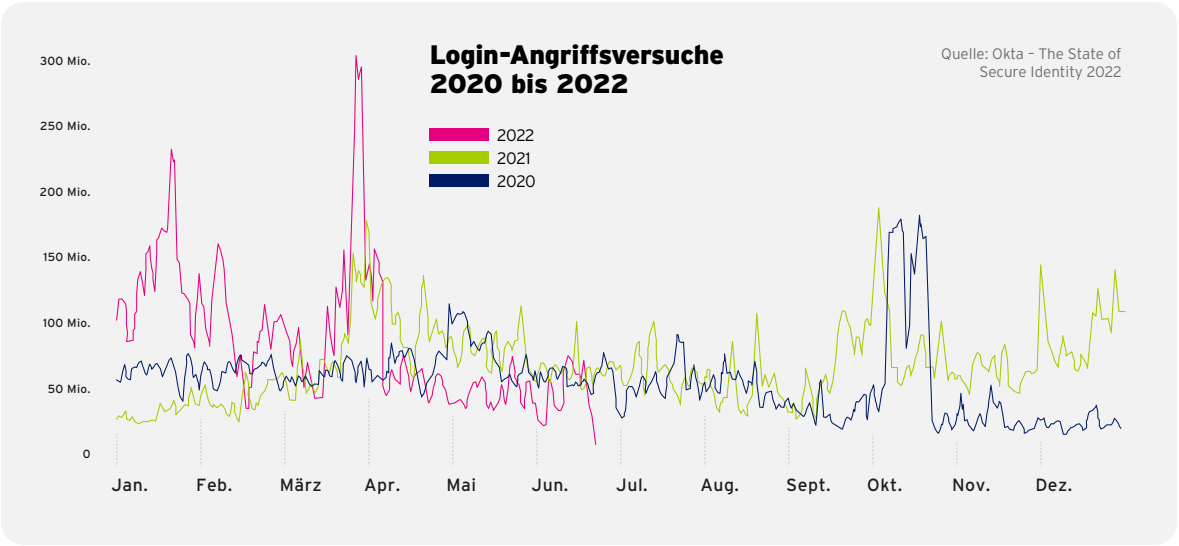


Abbildung 3: Zeitlich gesehen macht Credential Stuffing den größten Anteil des Angriffsverkehrs aus.

Erfolgreiche Angriffe auf MFA sind zwar schwierig – doch die einzelnen Sicherheitsmerkmale von MFA können durchaus geknackt werden. Allerdings wird eine Kompromittierung von MFA immer schwieriger, je mehr dieser Merkmale eingesetzt werden. Wer also MFA mit mehreren Faktoren im Einsatz hat, ist relativ sicher.

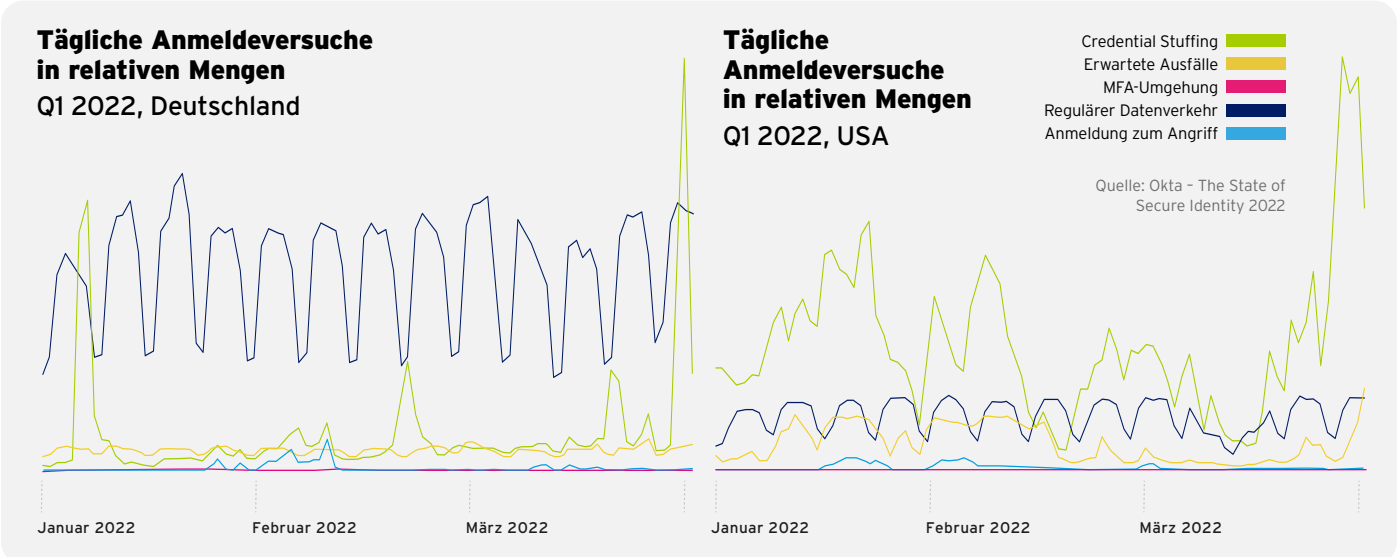
Dennoch berichtet der Report von gelegentlichen MFA-Angriffen. Die häufigste Angriffsmethode auf MFA ist Brute Force, bei der der Authentifizierungscode erfolgreich erraten wird. Eine andere ist, dass der Benutzer getäuscht oder gezwungen wird, die MFA-Prozedur abzuschließen, obwohl er sie nicht imitiert hat. Inzwischen sind auch mehrere Tools verfügbar, die solche Angriffe einfacher machen. Oft kennen zudem hochmotivierte und gut ausgestattete Bedrohungsakteure Techniken, wie sie MFA umgehen können, und bieten diese käuflich an.

In den ersten 90 Tagen des Jahres 2022 beobachtete Okta fast 113 Millionen Angriffe gegen MFA. Aufgrund des Aufwands, der erforderlich ist, um MFA erfolgreich zu umgehen, konzentrieren sich solche Angriffe in der Regel auf hochwertige Ziele. In der Tat zeigt die untersuchte Angriffsrate in verschiedenen Branchen, dass Hacker vorrangig Personalbeschaffung/Rekrutierung, den öffentlichen Sektor, den Einzelhandel/E-Commerce und Finanzdienstleister ins Visier nehmen.

Ein Beispiel für einen MFA-Angriff ist die jüngste Sicherheitsverletzung bei Uber. Dort akzeptierte ein Mitarbeiter eine von einem Hacker eingereichte Anfrage zur Zwei-Faktor-Authentifizierung, nachdem dieser im Dark Web Zugriff auf die Anmeldedaten des Mitarbeiters erhalten hatte. Da Angreifer bei der Kompromittierung auf diese wichtige Abwehrmaßnahme immer raffinierter werden, ist es entscheidend, dass MFA korrekt implementiert wird und dass starke sekundäre Faktoren ausgewählt werden.

Viele weitere Angriffsmethoden werden laut dem Report eingesetzt, um Zugangsdaten zu kompromittieren, sind aber im Vergleich zu Credential Stuffing we-

Abbildung 4 und 5: Die Verteilung der Anmeldeversuche für Deutschland in den ersten 90 Tagen des Jahres 2022 (Abb 4, links) und der Traffic der Anmeldeversuche für die USA während der ersten 90 Tage des Jahres 2022 (Abb. 5, rechts).



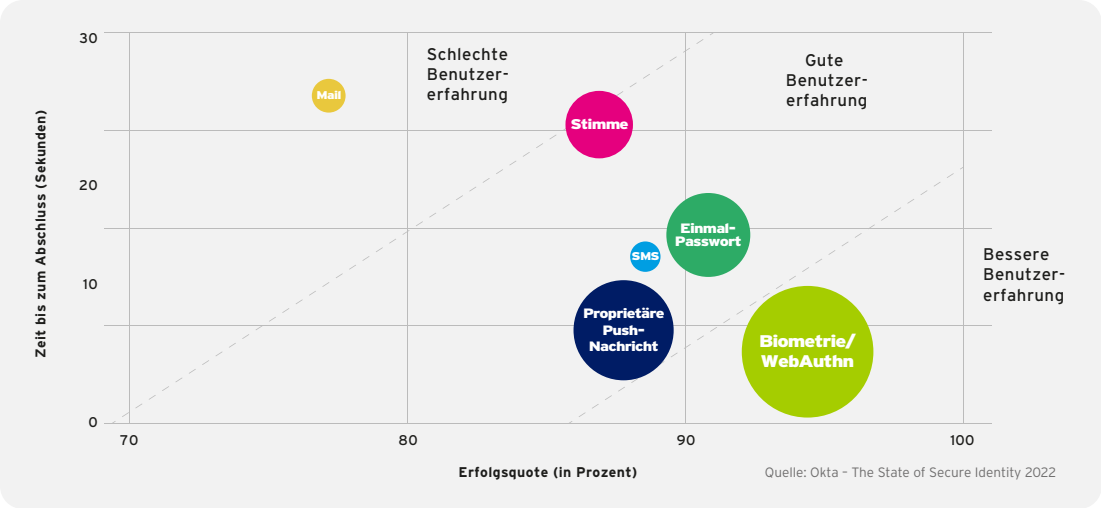


Abbildung 6: Die Sicherung von CIAM erfordert eine Verteidigungsstrategie, die viele komplementäre Tools und Techniken einsetzt. Die Größe der Blasen gibt die Stärke der Sicherheit an.

niger bedeutend. Passwort Spraying und Bot-Attacken sind Brute-Force-Methoden, bei der Angreifer automatisierte Tools verwenden, um Passwörter über viele verschiedene Konten hinweg auszuprobieren.

Injection-Angriffe fügen Code in ein Feld wie einen Benutzernamen ein, um schlecht implementierte Systeme, die Eingaben nicht bereinigen, auszunutzen. Beispielsweise kann der Code das Backend anweisen, die Passwortprüfung zu ignorieren und den Angreifer automatisch in der Benutzerdatenbank anzumelden – was häufig das Administratorkonto ist. Sobald ein Angreifer administrativen Zugriff hat, steht eine breite Palette von Angriffsaktionen zur Verfügung

Glossar

MFA: Multi-Faktor- oder Mehr-Faktor-Authentifizierung ist die Kombination von mehreren Sicherheitsmerkmalen zur Identifizierung einer Person – zum Beispiel Gesicht, Fingerabdruck und PIN. Eine Spezialform der MFA ist die Zwei-Faktor-Authentifizierung mit nur zwei Merkmalen. Das bekannteste Beispiel ist die Bankkarte (EC- oder Kreditkarte). Die Authentifizierung erfolgt dabei in der Regel über den Besitz der Karte (1. Faktor) zusammen mit einer PIN (2. Faktor). Eine MFA mit mehr als zwei Faktoren erhöht die Sicherheit erheblich, da jeder weitere Authentifizierungsfaktor zusätzlichen Aufwand erfordert, um ihn zu kompromittieren.

Credential Stuffing: Credential Stuffing ist eine Cyber-Attacke mit gestohlenen Zugangsdaten. Diese verwendet der Angreifer, um durch breit angelegte Anmeldeanfragen Zugang zu Benutzerkonten auf anderen Systemen zu erhalten. Dabei automatisiert der Angreifer die Anmeldungen für eine große Anzahl von zuvor entdeckten Credential-Paaren mit Hilfe von Automatisierungstools. Beispiel: Ein Angreifer kann eine Liste von Benutzernamen und Passwörtern aus geklauten Kundendaten eines Online-Shops benutzen, um zu versuchen, sich auf der Website einer Bank mit denselben Zugangsinformationen anzumelden – in der Hoffnung, dass viele Nutzer bei verschiedenen Online-Systemen die gleichen Passwörter verwenden.

CIAM-Bedrohungen vermeiden

Um sich gegen CIAM-Angriffe über Credential Stuffing, MFA-Kompromittierung oder andere Verfahren zu schützen, empfiehlt der Okta-Bericht ein ganzes Arsenal von Abwehrmaßnahmen. Grundsätzlich sollten mehrere Sicherheitstools kombiniert werden. Sie sollten auf verschiedenen Ebenen arbeiten und eine einheitliche Verteidigungslinie bilden. Dazu gehören eine professionelle Implementierung von MFA, die Verwendung von generischen Fehlermeldungen, die keine Systemdetails preisgeben, die Begrenzung fehlgeschlagener Anmeldeversuche und die Implementierung sicherer Praktiken für das Sitzungsmanagement.

Wann immer möglich – so der Report – sollte MFA zusammen mit spezifischen, sekundären Maßnahmen verwendet werden. Solche Maßnahmen helfen zum Beispiel, Konten zu identifizieren, die sich auf bereits verletzte Anmeldeinformationen stützen. Ein derart abgesichertes MFA erhöht den Zeit- und Arbeitsaufwand für den Angreifer drastisch.

Die Durchsetzung von starken Passwörtern mit einer bestimmten Mindestlänge, Komplexität und einem zeitlichen Wechsel auf der Grundlage der NIST-Empfehlungen (National Institute of Standards and Technology) sind weitere Möglichkeiten für CISOs, Unternehmen vor CIAM-Angriffen zu schützen. Daneben sollte auch die missbräuchliche Verwendung von Passwörtern überwacht werden und auf die Auslieferung von Produkten mit Standard-Anmeldedaten oder Klartextpasswörtern unterbunden werden.

Customer Identity Trends Report: Verbraucher fordern mehr Kontrolle über ihre Daten

Die Anzahl der Online-Konten steigt rasant, aber es wachsen auch das Misstrauen und die Verunsicherung seitens der Verbraucher, wenn es um die Sicherheit im Umgang mit ihren persönlichen Daten geht. Das zeigt der aktuelle Customer Identity Trends Report von Okta. Weder bei Regierung oder NGO, noch bei Technologie-Unternehmen hat die Mehrheit der Befragten ausreichend Vertrauen, was die Verwaltung digitaler Identitäten betrifft.

Mehr Kontrolle und Selbstbestimmung beim Verwalten ihrer persönlichen Daten – das ist es, was sich Verbraucher wünschen. Sie wollen selbst entscheiden, welche Daten erhoben und wie sie verwendet werden. Jüngere Altersgruppen sind der Studie zufolge sogar bereit, für mehr Kontrolle ihrer Daten ein Stück weit auf Komfort beim Anmeldeprozess zu verzichten.

Finanzdienstleister und Gesundheitswesen stehen besonders unter Druck

Nach Angaben der Befragten stehen besonders Finanzdienstleistungsunternehmen (86 Prozent), das Gesundheitswesen (83 Prozent) sowie der öffentliche Sektor (81 Prozent) unter Handlungsdruck. Denn diese Branchen verwalten täglich unzählige, sensible Nutzerdaten auf ihren Portalen. Insgesamt 83 Prozent der Umfrageteilnehmer sagen aus, dass sie immer häufiger Kompromisse zwischen dem Nutzererlebnis und der Datensicherheit eingehen zu müssen. 51 Prozent sind angesichts dieser Situation sogar bereit, mehr Geld auszugeben, wenn dadurch der Anmeldeprozess störungsfrei funktionieren würde.

Eine Vielzahl an Online-Konten macht die Datenspuren zum Problem

Für den Okta-Report wurden mehr als 20.000 Verbrauchern aus 14 Ländern befragt. Demnach verfügen 35 Prozent von ihnen im Schnitt über mehr als 20 aktive Online-Accounts für diverse Anwendungen oder Websites – in Europa sind es sogar 39 Prozent. Etwa 75 Prozent aller Befragten besitzen mehr als 10 aktive Accounts (Abb. 7). Die Befragten im Alter von 18 bis 39 Jahren haben im Durchschnitt etwa 26 aktive Konten, während 37 Prozent der Befragten in der Altersgruppe von 60+ weniger als 10 aktive Konten haben. Da es in der Umfrage um „aktive" Accounts ging, dürften es in Wahrheit noch viel mehr Accounts sein – denn viele User haben wahrscheinlich etliche nicht gepflegte Konten, die erst recht Sicherheitsrisiken mit sich bringen.

Alle Befragten gaben zudem an, allein in den drei Monaten vor der Erhebung durchschnittlich drei bis vier neue Konten angelegt zu haben. Mindestens 40 Prozent von ihnen hatten sogar fünf oder mehr Konten neu hinzugenommen. Nicht überraschend, dass die Anzahl der Accounts mit steigendem Alter abnimmt: In der Altersgruppe der über 60-Jährigen hatte man nur durchschnittlich etwa zwei Accounts neu in den zurückliegenden drei Monaten angelegt (Abb. 8).

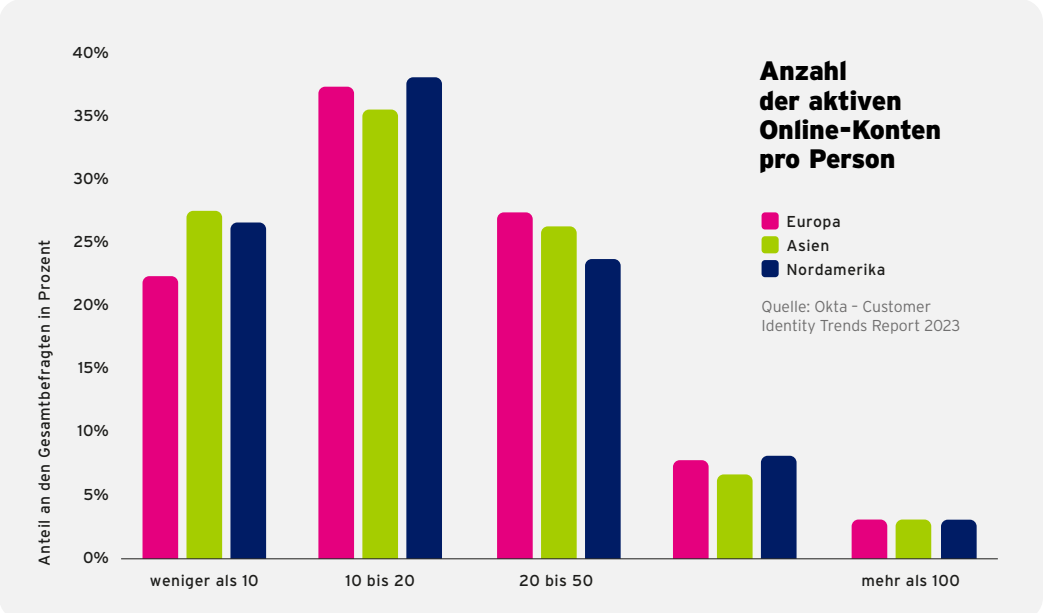
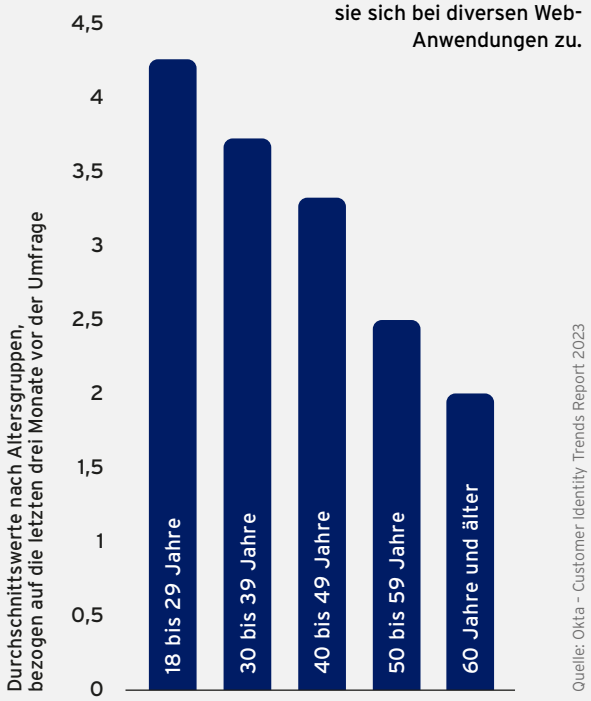


Abbildung 7: Mehr Konten, mehr Probleme: Fast 40 Prozent der Befragten in Europa haben durchschnittlich mehr als 20 aktive Online-Accounts für Web-Anwendungen.

Anzahl der neu angelegten Online-Konten

Abbildung 8: Je jünger die Verbraucher sind, desto mehr neue Accounts legen sie sich bei diversen Web-Anwendungen zu.



Mit jedem neuen Web-Konto wächst auch der digitale Fußabdruck, dessen sind sich 71 Prozent der Befragten bewusst. 50 Prozent der deutschen Verbraucher ergreifen daher Maßnahmen, um digitale Spuren im Netz zu kontrollieren und zu verwalten.

Damit ist aber auch klar: Je mehr Accounts ein Nutzer hat, desto größer ist seine Anfälligkeit für Datenschutzverletzungen. Denn es liegt in der Natur des Menschen, dass viele Konten vergessen oder einfach nicht mehr gepflegt werden. Und somit kann ein Angriff auf diese Dienste einen Hacker mit einer großen Menge persönlicher Nutzerinformationen ausstatten.

Login: Passwörter sind Frustrationsquelle Nummer 1

Der Report zeigt außerdem: Passwörter sind der Hauptgrund für Frustration bei einer Online-Anmeldung. 65 Prozent aller befragten Verbraucher fühlen sich bei der Verwaltung einer Vielzahl von Benutzernamen und Passwörtern regelrecht überfordert. 64 Prozent geben an, dass sie sich mindestens einmal im Monat nicht bei einem Konto anmelden können, weil sie ihren Benutzernamen oder ihr Passwort vergessen haben. Etwa ein Drittel hat dieses Problem wöchentlich und eine von 20 Personen sieht sich täglich damit konfrontiert. Aber auch lange Eingabeformulare oder die permanente Aufforderung zu neuen Passwörtern stresst die Verbraucher zunehmend. In der Konsequenz geben daher viele ihre Konten einfach auf. 60 Prozent wären bereit, mehr Geld auszugeben, wenn dadurch der Anmeldeprozess reibungslos und sicher funktionieren würde.

Datensicherheit: Widerspruch zwischen Anspruch und Nutzung

Um der ständigen Unsicherheit in Bezug auf die Kontrolle ihrer Daten entgegenzuwirken, setzen deutsche Verbraucher auf Authentifizierungsmethoden, denen sie ein hohes Maß an Datensicherheit zuschreiben. Die am häufigsten verwendete Methode (rund 50 Prozent) ist die Anmeldung über einen Social Login, gefolgt von der Multi-Faktor-Authentifizierung (MFA) mit etwa 44 Prozent. Diese Methoden werden als selbstverständlich angesehen, wenn es darum geht, die Sicherheit ihrer Konten zu erhöhen.

Interessanterweise werden Benutzername und Passwort allgemein als die bequemste und sicherste Form der Authentifizierung genannt. In Branchen wie Einzelhandel, Finanzdienstleistungen, Reisen, Entertainment, öffentlicher Verwaltung und Gesundheitswesen ist diese traditionelle und gleichzeitig unsicherste Form der Authentifizierung immer noch am weitesten verbreitet. Was sich möglicherweise darauf zurückführen lässt, dass Verbraucher auf bestimmte Online-Dienste angewiesen sind, diese aber nicht immer über die bestmöglichen Sicherheitsstandards verfügen.

Fazit: Die Karten auf den Tisch legen

Der Customer Identity Trends Report von Okta zeigt, dass sich die Verbraucherreibungslose, personalisierte Online-Erlebnisse wünschen, wenn sie sich bei Apps anmelden oder Einkäufe tätigen. Gleichzeitig möchten sie kontrollieren, welche Daten sie weitergeben, und wünschen sich angemessene Sicherheitskontrollen, um diese zu schützen. Unternehmen sollten also in Zukunft den Nutzern gegenüber offenlegen, wie sie deren digitale Identitäten verwalten – einschließlich der Frage, warum ihre Daten benötigt werden und welche Sicherheitsmaßnahmen zum Schutz der Nutzerkonten getroffen werden.

Als Business-Partner, nicht als Verhinderer auftreten

Die Wahrscheinlichkeit von Cyber-Attacken auf Login-Daten wächst. Unternehmen sollten daher jetzt dringend dafür sorgen, ihre IT- und Datensysteme resilient gegen die dauerhafte Bedrohung zu machen. Sven Kniest, Vice President Europe von Okta erläutert, an welchen Stellschrauben Security- und IT-Entscheider ansetzen können.

Nicht erst seit dem Ukraine-Krieg haben Menge und Qualität der Cyberattacken merklich zugenommen. Viele Cyber-Kriminelle wollen inzwischen statt eines schnellen Gewinns einen möglichst großen Schaden anrichten. Welche Beobachtungen hat Okta dazu auf seiner eigenen Plattform gemacht?

Okta veröffentlicht jedes Jahr seinen State of Secure Identity Report, in dem die Anmeldedaten über die Okta-Plattformen – natürlich anonym und verschlüsselt – unter die Lupe genommen werden. Der Report bezieht sich konkret auf die ersten sechs Monate des jeweiligen Kalenderjahres. Wie schon in den letzten Jahren ergab der Bericht auch diesmal, dass die Gefahr von Cybersecurity-Attacken weiterhin wächst, sich weiter ausdifferenziert und demzufolge nicht zu unterschätzen ist. Ein Beispiel: Allein in der ersten Jahreshälfte 2022 konnte ein Drittel aller Login-Versuche weltweit auf Credential-Stuffing zurückgeführt werden. Jeder dritte Anmeldeversuch erfolgte also mittels gestohlener Daten. Vor allem im Bereich E-Commerce ist diese Art der Cyberkriminalität mit 80 Prozent besonders hoch.

Welche Lehren sollten Unternehmen daraus ziehen?

Einerseits ist das Ergebnis ernüchternd, andererseits zeigt es, dass eine funktionsfähige IAM-Strategie solche Angriffsversuche erfolgreich abwehren kann. Und die Erkenntnisse, die wir dank unserer Plattform gewonnen haben, können wir unseren Kunden direkt zur Verfügung stellen. Vor diesem Hintergrund wirken wir mit unserer Technologie zukünftigen Attacken nicht nur präventiv entgegen, sondern ermöglichen auch eine stetige Anpassung und Weiterentwicklung unserer IAM-Lösungen.

Welche Maßnahmen sollten Unternehmen aktuell vor allem im Blick haben? In welche Bereiche sollte investiert werden?

Es ist wichtig zu erkennen, dass alte Sicherheitsrichtlinien an Relevanz verloren haben. Heute hat die digitale Identität an sich eine viel stärkere Bedeutung

„Alte Sicherheitsrichtlinien haben heutzutage an Relevanz verloren. Dagegen kann Authentifizierung durch den Einsatz moderner Technologien recht simpel sein."

Sven Kniest,
Vice President Central & Eastern Europe von Okta

gewonnen, weil Cyberkriminelle es oft genau darauf abgesehen haben – wie das Beispiel Phishing-Attacken zeigt. Unternehmen müssen also sicherstellen, dass der Schutz aller Identitäten – egal ob Mitarbeiter oder Kunde – im Sinne eines Zero-Trust-Ansatzes technologisch möglich ist und gewährleistet wird. Das bedeutet konkret: Silolösungen abschaffen und ganzheitliche Standards und Plattformen implementieren.

Im Jahr 2022 sind besonders Energieunternehmen, aber auch Versicherungen oder der E-Commerce von Cyberangriffen betroffen. Wie sollten jetzt konkret die Identitätssysteme verbessert werden?

Der erste und wichtigste Schritt ist, einfache Grundlagen zu schaffen. Dazu gehört unter anderem die Absicherung aller Zugriffe durch einen zweiten Faktor. Moderne Technologien, zum Beispiel die Biometrie bzw. Gesichtserkennung, werden weitestgehend von den Nutzern akzeptiert und erhöhen die Sicherheit – und zwar ohne dadurch den Authentifizierungsprozess komplizierter zu machen.

Wie kommen die Unternehmen mit der Entwicklung einer CIAM-Strategie voran?

Viele Unternehmen haben bei diesem Thema noch eine weite Reise vor sich und müssen einiges tun – insbesondere wenn es um Kundenidentitäten in den Branchen Energie, Versicherung und E-Commerce geht. Häufig setzen Sicherheitsverantwortliche noch auf selbst programmierte Lösungen. Solche proprietären Systeme ziehen die User Experience durch komplizierte und unzureichende Sicherheitsvorgaben in Mitleidenschaft und setzen Unternehmen erhöhten Risiken aus. Als bessere Alternative bieten sich moderne, cloud-basierte Lösungen aus dem SaaS-Bereich an. Sie ermöglichen ein holistisches Identitätsmanagement und erhöhen gleichermaßen Nutzererfahrung und Sicherheit.

Wie kann es trotz aktuell knapper IT-Budgets dennoch gelingen, den Schutz der Mitarbeiter und Kundenidentitäten weitgehend zu verbessern? Welche wirtschaftlichen und organisatorischen Treiber sehen Sie?

Das Thema Digital Trust ist bei vielen Unternehmen relevant. Die Absicherung von Identitäten geht schließlich mit vielen Vorteilen einher. Auf der einen Seite wird die Sicherheit erhöht, auf der anderen Seite entsteht mittels einer verbesserten Nutzererfahrung Wachstumspotenzial für das Unternehmen an sich. Eine gut durchdachte CIAM-Strategie unterstützt die Kundenbindung und kann somit Umsatz und Wachstum fördern.

Wie relevant sind regulatorische Anforderungen beim Identitätsmanagement?

Regulatorische Anforderungen nehmen zweifellos eine wichtige Rolle ein. Heute sind zum Beispiel viele Cyberversicherungen schlicht unbezahlbar, wenn bei einem Unternehmen keine Multifaktor-Authentifizierung (MFA) implementiert wurde. Außerdem gab es schon genug Fälle, bei denen Firmen durch Attacken mit extremen betriebswirtschaftlichen Konsequenzen umgehen mussten. Und durch die steigende Bedrohungslage stehen IT-Security-Verantwortliche vor einer immer komplexer werdenden Aufgabe, solche Attacken zu verhindern. Das sind alles relativ einfache Beispiele, die den Mehrwert einer cloud-basierten Identitätsstrategie schnell klar werden lassen.

Obwohl in vielen IT-Systemen bereits Kundendaten verarbeitet werden, wird das Identitätsmanagement im Vergleich zur Security-Strategie immer noch stiefmütterlich behandelt. Warum ist das so?

Das hat mit Sicherheit verschiedene Gründe. Meine Vermutung ist, dass das Identitätsmanagement bei vielen Kundenplattformen von Anfang an etwas vernachlässigt wurde. Da bei der Entwicklung von vielen Apps Geschwindigkeit und Agilität elementar sind, hat man den Stellenwert von Identitätsmanagement häufig verkannt oder nicht richtig eingeordnet. Hinzukommt: CISOs wurden vielfach nur bedingt oder zu spät in die Weiterentwicklung von Kundenplattformen eingebunden. Das ist heute anders. Identitätsmanagement genießt eine wachsende Bedeutung.

Mitarbeiter und Kunden beklagen oft aufwändige Authentifizierungsprozesse. Was könnte ganz konkret ohne großen Aufwand verbessert werden?

Authentifizierung ist durch den Einsatz von modernen Technologien recht simpel, wenn diese eingesetzt und genutzt werden. Letztendlich muss ein Authentifizierungsprozess möglichst reibungslos und einfach sein, um vom Nutzer akzeptiert zu werden. Das gilt für Mitarbeiter genauso wie für Kunden. Ein gutes Beispiel hierfür ist das Single-Sign-On-Verfahren (SSO), bei dem Nutzer sich einmalig zentral authentifizieren und innerhalb von Sekunden Zugang zu allen Apps kommen, die sie brauchen. Dadurch wird das ständige An- und Abmelden eliminiert. Auch Social Login, also die Authentifizierung durch bereits existierende Nutzerdaten externer Unternehmen wie Meta (Facebook, Instagram) oder Apple, vereinfacht den Login-Prozess um ein Vielfaches, ohne dabei die Sicherheit zu beeinträchtigen.

Welche Tipps geben Sie CISOs an die Hand, die aktuell über die Einführung einer CIAM-Strategie nachdenken?

Ich habe spontan drei Tipps parat:

1. **CISOs sollten als Business-Partner und nicht als Verhinderer auftreten. Sie sind gut beraten, Identitätsmanagement immer als holistischen Wachstumstreiber zu betrachten.**
2. **Gegenüber Entscheidungsträgern sollten CISOs die KPIs und den Mehrwert der Einführung von Identitätsmanagement klar und verständlich kommunizieren – etwa durch steigende Sign-Up-Rates oder nachweisliche Eliminierung von Bot-Accounts.**
3. **Das Thema Security müssen CISOs immer aus der Sicht von Kunden denken. Das bedeutet, dass die Kundenerfahrung im Zentrum stehen sollte und Identitätsmanagement so verwaltet und gestaltet wird, dass Kundenwünsche stets im Vordergrund stehen.**

Über Okta

Okta ist einer der führenden Identitätsanbieter weltweit. Wir geben jedem die Möglichkeit, jede Technologie sicher zu nutzen – überall, auf jedem Gerät und in jeder App. Die vertrauenswürdigsten Marken vertrauen auf Okta, um sicheren Zugang, Authentifizierung und Automatisierung zu erhalten. Mit Flexibilität und Neutralität im Zentrum unserer Okta Workforce Identity und Customer Identity Clouds können sich Führungskräfte und Entwickler auf Innovationen konzentrieren und den digitalen Wandel beschleunigen. Und das dank anpassbarer Lösungen und mehr als 7.000 vorgefertigter Integrationen. Wir bauen eine Welt auf, in der die Identität Ihnen gehört.

Erfahren Sie mehr unter okta.com/de/.

okta

Kontakt

Okta GmbH

Oskar-von-Miller-Ring 20
80333 München

Tel. 089 2620-3329
www.okta.com/de