2024

Was Sie schon immer über die MFA-Einführung und die Authentifikatoren wissen wollten...

Die neuesten Trends rund um sichere Anmeldeprozesse

okta

Es war nicht schwer, die Welt von den Vorteilen der Multi-Faktor-Authentifizierung (MFA) zu überzeugen.

Die Sicherheitsbranche war sich von Anfang einig, dass MFA als Schutz vor den ständig anbrandenden Passwort-basierten Attacken unverzichtbar ist. Viele Unternehmen nutzten MFA zunächst jedoch nur zur Absicherung ihrer besonders wertvollen Systeme.

Während der Pandemie wurde MFA breitflächig eingeführt. Im Zuge des massenhaften Wechsels ins Homeoffice beobachtete Okta innerhalb weniger Monate eine Zunahme der MFA-Nutzung von 15 %. Mittlerweile müssen die meisten Okta-Administratoren sowie die Mehrheit der Benutzer für den Zugriff auf ihre beruflichen Anwendungen eine MFA-Abfrage passieren. Parallel dazu verlangen immer mehr Behörden und Standardisierungsorganisationen weltweit, dass Unternehmen den Zugriff mit diesen stärkeren Anmeldemethoden absichern.

Der diesjährige Secure Sign-in Trends Report zeigt eine starke Zunahme bei der Nutzung passwortloser, Phishing-resistenter Anmeldemethoden. Im Januar 2024 meldeten sich 5 % der Benutzer unserer Workforce Identity Cloud-Plattform nicht ein einziges Mal mit einem Passwort an. Diese gering erscheinende Zahl ist ein Hinweis auf ein riesiges und bislang latentes Potenzial und ein deutlicher Hinweis darauf, dass passwortlose Authentifizierung hier und jetzt verfügbar ist. Sie ist eine echte Alternative. Wenn diese Okta-Kunden es geschafft haben, können Sie das auch.

Daher gehen wir davon aus, dass die nächste Welle der MFA-Implementierungen nicht von Sicherheitspuristen oder weitblickenden Entscheidungsträgern vorangetrieben wird, sondern durch eine Nachfrage nach besseren User Experiences und höheren Sicherheitsanforderungen. Sobald Sie passwortlose Authentifizierung erlebt haben, sei es als Mitarbeiter oder Kunde, wollen Sie nicht mehr zurück.

Ich hoffe, Sie finden unsere Themen spannend. Viel Spaß bei der Lektüre.

Todd McKinnon
CEO von Okta

Inhaltsverzeichnis

03 **Eine Anmerkung zur Ermittlung der MFA-Nutzung**

06 **Zusammenfassung der wichtigsten Erkenntnisse**

07 **Einführung**

09 **So verwenden Sie die Daten**

11 **Aktueller Stand bei der MFA-Nutzung**

13 MFA-Nutzung im Zeitverlauf

15 MFA-Nutzung nach Region

17 MFA-Nutzung nach Branche

19 MFA-Nutzung nach Unternehmensgröße

21 MFA-Nutzung nach Benutzertyp

23 MFA-Nutzung nach Authentifikatortyp

27 **Datengestützte Bewertung des Benutzerkomforts und der Sicherheit von Authentifikatoren**

29 Zeitaufwand für Authentifizierungsabfragen

33 Zeitaufwand für die Registrierung eines Authentifikators

35 Fehlerquote bei Authentifizierungsabfragen

37 Anteil Phishing-resistenter Authentifizierung

39 Anteil Phishing-resistenter Authentifizierung mit Warnfunktion

41 Brute-Force-Fehlerquote bei Authentifizierungsabfragen

43 Umfrage zu Authentifikator-Kennzahlen

47 Bewertung der Performance und Akzeptanz von Authentifikatoren

49 **Der Weg in die Zukunft**

51 **Methodik**

Eine Anmerkung zur Ermittlung der MFA-Nutzung

Die hier genannten Daten und Schlussfolgerungen bilden die Entscheidungen von Unternehmen, ihren Administratoren und Mitarbeitern in Bezug auf Authentifizierung ab. Auch wenn wir regelmäßig von Benutzern sprechen, handelt es sich meist um Mitarbeiter in einem beruflichen Umfeld, deren Authentifizierungsoptionen von Unternehmensrichtlinien vorgegeben werden.

Es gibt mehrere Methoden zur Messung der MFA-Nutzung (Multi-Faktor-Authentifizierung), die in der Tabelle unten aufgeführt sind. Für diese Untersuchung haben wir die tatsächliche MFA-Nutzung gemessen, d. h. den Anteil der Benutzer, die sich innerhalb eines bestimmten Zeitraums per MFA angemeldet haben.

Messungsoption	Definition
Rate der MFA-Paketoptionen	Anteil der Kunden, die eine SKU mit MFA-Option gekauft haben
Registrierungsrate auf Tenant-Ebene	Anteil der Tenants und Okta-Kunden, die eine MFA-Option konfiguriert haben
Registrierungsrate auf Benutzerebene	Anteil der Benutzer, die sich für MFA-Authentifikatoren registriert haben
MFA-Nutzung auf Benutzerebene	**Anteil der Benutzer, die sich innerhalb eines bestimmten Zeitraums per MFA angemeldet haben**

Zudem erfassten wir die MFA-Nutzungsdaten auf Benutzerebene, da wir hier die Nutzungsrate messen wollten:

Erfassungsoption	Definition
MFA-Nutzungsrate auf Tenant-Ebene	Anteil der Okta-Tenants, deren Benutzer sich innerhalb eines Monats mindestens einmal per MFA angemeldet haben
MFA-Nutzungsrate auf Benutzerebene	**Anteil der Benutzer, die sich innerhalb eines Monats per MFA angemeldet haben**
MFA-Nutzungsrate auf Ereignisebene	Anteil der erfolgreichen Anmeldeereignisse, die innerhalb eines Monats eine MFA-Abfrage nutzten

Bei dieser Untersuchung wurden nur direkte MFA-Authentifizierungsereignisse in der Okta Workforce Identity Cloud (WIC) berücksichtigt. Wenn Benutzer sich ausschließlich über die MFA-Option eines anderen Identity-Anbieters authentifizieren und sich per Enterprise Federation oder Social Login mit Okta verbinden, werden sie nicht von unserer MFA-Nutzungsrate abgebildet. Aus diesem Grund ist es wahrscheinlich, dass die gemeldete MFA-Nutzungsrate etwas geringer ist als die Gesamtrate der MFA-Nutzung unter unseren Kunden. Für unsere Untersuchung wurden Test-Accounts ausgeschlossen. Alle Nutzungs- und Metrik-Daten stammen von Orgs/Tenants, die ein Abonnement in einer Produktionsumgebung einsetzen.

Benutzerkomfort und Sicherheit von Authentifikatoren

Wir verstehen die Hürden für die MFA-Nutzung jedoch nur, wenn wir zuerst einige grundsätzliche Fragen beantworten: Können wir ein Framework entwickeln und einen systematischen, quantitativen Überblick über die Eigenschaften des Authentifikators erhalten? Können wir mithilfe datengestützter Erkenntnisse unsere Kunden über bessere Schutzmöglichkeiten informieren und unsere Produktentwicklung optimieren?

Für diese Aufgabe haben wir Authentifikatoren im Hinblick auf Benutzerkomfort und Sicherheit bewertet, wie Tabelle 2 zeigt. Die Messung dieser Kriterien ist schwierig, da die Logik- und UI-Abläufe (Benutzeroberfläche) der jeweiligen Authentifikatoren variieren und stark angepasst werden können. Für einen konsistenten Überblick nutzten wir die Okta Identity Engine (OIE), die besser konzipierte und flexiblere Identity-Experiences und -Abläufe ermöglicht.

Wir ermittelten die Eigenschaften der folgenden Authentifizierungsmethoden: Passwort, E-Mail, Hardware-Token (One-Time Password, OTP), Soft-Token (OTP), Push-Nachrichten, Sicherheitsfrage, SMS, Voice-OTP, Okta FastPass, FIDO2 WebAuthn sowie Smartcard. Sofern nicht anders angegeben, erfassten wir die Daten mithilfe der Okta Identity Engine im Januar 2024 bei Mitarbeitern von Unternehmen, die ein Okta-Abonnement nutzen.

Wir haben bei den Datenerfassungsmethoden besonders darauf geachtet, dass sie einen aussagekräftigen Vergleich der einzelnen Authentifikatoren erlauben. Dieser Bericht geht auch auf Bedingungen ein, die diese Vergleiche erschweren, und erklärt die Konsequenzen für unsere Ergebnisse. Wir haben auch die monatlichen Unterschiede in den Daten untersucht, um sicherzustellen, dass die allgemeinen Trends langfristig konsistent sind.

Zusammen-fassung der wichtigsten Erkenntnisse

Der Wachstumstrend bei der MFA-Implementierung setzt sich fort

Stand Januar 2024 stieg die MFA-Implementierung bei Okta Workforce Identity Cloud-Kunden auf 66 %, wobei 91 % der Administratoren MFA nutzen.

Nutzungsraten unterscheiden sich stark nach Branche und Unternehmensgröße

Behörden und Bildungseinrichtungen verzeichneten bei der Nutzungsrate eine Zunahme von 5 % im Jahresvergleich. Diese Zahl kann angesichts der neuesten US-Präsidentendekrete und Gesetzesänderungen weiter steigen.

Phishing-resistente Authentifikatoren kommen stark in Fahrt

Die Nutzungsrate Phishing-resistenter Authentifikatoren ist signifikant gestiegen. Die Nutzungsrate bei FIDO2 WebAuthn stieg von 2 % (2023) auf 3 % (2024), während die Nutzung von Okta FastPass im gleichen Zeitraum von 2 % auf 6 % sprang.

Passwortlose Authentifizierung ist angekommen

Durch die zunehmende Implementierung moderner Authentifizierungsverfahren in Unternehmen geht die Zahl der Okta-Kunden, die immer noch auf Passwörter setzen, endlich zurück. Etwas weniger als 5 % der Benutzer verwendeten im Januar 2024 kein Passwort für ihre Anmeldeprozesse.

Starke Sicherheit und hervorragende User Experience schließen sich nicht gegenseitig aus

Die Benutzung Phishing-resistenter Authentifikatoren ist äußerst komfortabel. Bei unserer Untersuchung der Performance lagen FastPass und FIDO2 WebAuthn an der Spitze, da sie sicherer und bequemer als andere Optionen sind, selbst wenn wir praxisnähere Kriterien anlegen.

Einführung

„MFA (Multi-Faktor-Authentifizierung) gilt heute gemeinhin als die vielleicht wichtigste präventive Sicherheitskontrolle. Sie bietet starken Schutz vor verschiedenen Angriffstechniken wie Password Spraying, Wiederverwendung kompromittierter Passwörter und zum Teil sogar Phishing. Eine der zentralen Herausforderungen ist die schwierige Implementierung, sodass viele Unternehmen – kleine ebenso wie große – trotz unbestreitbarer Vorteile damit immer noch nicht vorangekommen sind.“[1]

Multi-Faktor-Authentifizierung sichert die Anmeldeprozesse von Benutzern zuverlässig ab.

Einer der schwierigsten Kompromisse beim Identitäts- und Zugriffsmanagement ist die Entscheidung, welche Reibungspunkte Sie den Endbenutzern zumuten wollen, um den Zugriff auf die Anwendungen und Daten des Unternehmens abzusichern. Zu wenige Reibungspunkte würden Angreifern eine Chance geben, während zu viel Aufwand dazu führen würde, dass Mitarbeiter auf nicht genehmigte Anwendungen ausweichen, wodurch neue Risiken entstehen.

Doch angesichts der wachsenden Zahl schwerwiegender Sicherheitsvorfälle und der damit verbundenen steigenden Kosten akzeptieren immer mehr Unternehmen, dass starke Authentifizierung insbesondere bei der Absicherung von Remote-Zugriffen auf Ressourcen unverzichtbar ist. Die Herausforderung besteht nun darin, maximal sichere Authentifizierung und minimale Reibungspunkte für Endbenutzer zu vereinen.

In diesem Bericht untersuchen wir die Vielzahl von Ansätzen, mit denen moderne Unternehmen die Identity ihrer Benutzer überprüfen und unbefugte Zugriffe verhindern. Auf Basis der anonymisierten Daten zu Milliarden monatlichen Authentifizierungen bei Okta-Kunden haben wir den aktuellen Stand der Authentifizierung bewertet, Trends identifiziert und die verschiedenen Ansätze je nach Branche, Region und Unternehmensgröße analysiert.

Der diesjährige Bericht zeigt, dass wir uns zwar in die richtige Richtung bewegen, dabei aber nicht schnell genug vorankommen. Während der COVID-Pandemie beobachteten wir bei der MFA-Implementierung eine sprunghafte Zunahme von 15 %, da Unternehmen ihre Homeoffice-Arbeitsplätze absichern mussten. Umso enttäuschender ist die Feststellung, dass die MFA-Nutzung trotz dieses guten Starts seit 2023 im Jahresvergleich nur um 2 % gestiegen ist. Stand Januar 2024 melden sich 66 % aller Benutzer per MFA an.

Wir scheinen an einem Wendepunkt angelangt zu sein. Das US-Präsidentendekret zur Verbesserung der nationalen Cybersicherheit tritt in Kraft und Unternehmen sowie Cloud-Anbieter beschleunigen die Umstellung ihrer Benutzer auf sicherere Authentifizierung. Gleichzeitig starten führende Technologieunternehmen wie Salesforce, GitHub, Okta und Microsoft Projekte, mit denen sie MFA für privilegierte Accounts durchsetzen. Dadurch wird das Interesse an der Entwicklung und Implementierung von Authentifizierungsverfahren steigen, die hohe Sicherheit ohne Reibungspunkte für Benutzer bieten.

Mit diesem Bericht möchten wir IT- und Sicherheitsexperten einen datengestützten Blick auf die heute verfügbaren Lösungen geben und das Gerücht zerstreuen, dass starke Authentifizierung zwingend mit zusätzlichem Aufwand für Benutzer einhergeht. Im Gegenteil: Passwortlose Phishing-resistente Authentifizierung lässt sich sicherer und gleichzeitig einfacher benutzen.

Sofern nicht anders angegeben, basieren alle Daten und Schlussfolgerungen in diesem Bericht auf anonymisierten Okta-Daten.

[1] https://media.defense.gov/2023/Oct/04/2003313510/-1/-1/0/ESF%20CTR%20IAM%20MFA%20SSO%20CHALLENGES.PDF

So verwenden Sie die Daten

Dieser Bericht stellt ein Framework zum Messen des Benutzerkomforts sowie der Sicherheit verschiedener Authentifikatoren bereit. Wir haben Antworten auf wichtige Fragen gesucht, die CIOs, CSOs und politischen Entscheidern die Gründe für die unterschiedlichen MFA-Nutzungsraten zeigen sollen. Zu diesen Fragen gehören:

- Wie hat sich die MFA-Nutzung im Laufe der Zeit geändert?
- Beeinflussen Branche, Standort oder Größe eines Unternehmens die MFA-Nutzungsrate?
- Welche wahrnehmbaren Komforteigenschaften sind für die MFA-Akzeptanz wichtig?
    - Wie viel Zeit müssen Benutzer für die Authentifizierung mit einem bestimmten Authentifikator typischerweise aufwenden?
    - Wie viel Zeit müssen Benutzer für die Einrichtung/Registrierung eines bestimmten Authentifikators typischerweise aufwenden?
    - Wie oft kommt es bei bestimmten Authentifikatoren zu Authentifizierungsfehlern?
- Welche wahrnehmbaren Sicherheitseigenschaften sind für die MFA-Akzeptanz wichtig?
    - Wir groß ist der Anteil bestimmter Authentifikatoren bei Phishing-resistenten Authentifizierungsabläufen?
    - Wie oft greifen Bedrohungsakteure bei Brute-Force-Angriffen Accounts mit bestimmten Authentifikatoren an?

Die Antworten auf diese Fragen helfen IT- und Sicherheitsverantwortlichen, die Kosten und Vorteile unterschiedlicher Authentifikatoren abzuwägen und die beste Lösung für ihr Unternehmen und dessen Benutzer zu finden.

“Okta nutzt schon seit mehreren Jahren die Vorteile passwortloser Phishing-resistenter Authentifizierung. In den 12 Monaten seit dem letzten Secure Sign-in Trends Report haben wir umfangreich in den Phishing-Schutz investiert, wobei wir den gesamten User Lifecycle abdecken – von der Benutzerregistrierung über Zugriffe bis zur Account-Wiederherstellung. Damit haben wir bewiesen, dass das möglich ist.“

David Bradbury
Chief Security Officer

okta

Aktueller Stand bei der MFA-Nutzung

MFA ist ein zentraler Bestandteil jeder hochsicheren Unternehmensumgebung. Bei der Anmeldung mit MFA müssen Benutzer zwei oder mehr unterschiedliche Faktoren zur Überprüfung ihrer Identity angeben, z. B. einen Wissensfaktor (etwas, das Sie kennen, z. B. ein Passwort), einen Besitzfaktor (etwas, das Sie besitzen, z. B. ein registriertes Gerät) oder einen Inhärenzfaktor (etwas, das Sie sind, z. B. ein biometrisches Merkmal).

Auch wenn MFA für sichere Anmeldungen als unverzichtbar gilt, wird die Nutzung durch mehrere interne und externe Faktoren beeinflusst. In diesem Abschnitt betrachten wir die Nutzungsraten über einen bestimmten Zeitraum hinweg sowie nach Region, Branche, Unternehmensgröße, Authentifikatortyp und Benutzertyp (Benutzer mit und ohne Administratorrechte). Die Ergebnisse dienen sowohl dem Vergleich mit anderen Unternehmen und Branchen als auch der Erkennung von Verbesserungsmöglichkeiten.

Abgrenzung von Faktor oder Authentifikator

Dieser Bericht nutzt die Begriffe „Authentifikator“ und „Faktor“ entsprechend den Definitionen des National Institute of Standards and Technology (NIST):

Authentifikator: Etwas, das eine berechtigte Person besitzt oder kontrolliert und als Identitätsnachweis nutzt.

Faktor: Eine Authentifizierungseigenschaft, z. B. ein Wissensfaktor (etwas, das Sie wissen, z. B. ein Passwort oder eine Sicherheitsfrage), ein Besitzfaktor (etwas, das Sie besitzen, z. B. ein registriertes Gerät) oder ein Inhärenzfaktor (etwas, das Sie sind, z. B. Ihr Fingerabdruck).

Hinweis: Jeder Authentifikator besitzt einen oder mehrere Faktoren. Häufig werden die Begriffe verwechselt, z. B. wenn „Faktor“ als „Authentifikator“ verwendet wird oder ein Authentifikator mehrere Faktoren besitzen kann. Beispielsweise kann Okta FastPass sowohl einen Besitzfaktor (ein registriertes Gerät) als auch einen Inhärenzfaktor (mit biometrischer Verifizierung) bereitstellen.

Aktueller Stand bei der MFA-Nutzung

MFA-Nutzung im Zeitverlauf

Abbildung 1 zeigt die MFA-Nutzungsraten für Okta Workforce Identity Cloud-Kunden (diejenigen, die ihren Mitarbeitern, Auftragnehmern und Partnern mit Okta sicheren Zugriff auf Unternehmensressourcen gewähren) von Oktober 2019 bis Januar 2024. Jeder Datenpunkt stellt die MFA-Nutzung im jeweiligen Monat dar.

Wie im Bericht von 2023 erwähnt, stieg die MFA-Nutzungsrate von Februar bis März 2020 sprunghaft von 35 % auf 50 % an, da Unternehmen sich auf Homeoffice-Arbeit umstellten und einen Perimeter schützen mussten, der nun weit über das Unternehmensnetzwerk hinausging. Seither stieg die MFA-Nutzung von 2020 bis 2023 pro Jahr um 6 % und im Jahr 2024 um 2 %. Stand Januar 2024 melden sich 66 % aller Benutzer per MFA an.

Diese Wachstumsrate hält nicht mit der Zunahme Identity-basierter Attacken Schritt. Im Jahr 2024 beobachteten wir mehrere Ereignisse, bei denen Bedrohungsakteure User Accounts und Maschinen-Accounts ohne aktivierte Multi-Faktor-Authentifizierung angriffen. Als Reaktion darauf schreiben nun viele Cloud-Anbieter MFA für privilegierte Accounts (und teilweise für sämtliche Accounts) vor.

Wichtige Erkenntnis

Da immer mehr Unternehmen MFA für privilegierte Accounts erzwingen, werden sich wahrscheinlich mehr Service Provider diesem Trend anschließen. IT- und Sicherheitsexperten sollte das motivieren, die breitere MFA-Implementierung in ihren Unternehmen zu beschleunigen.

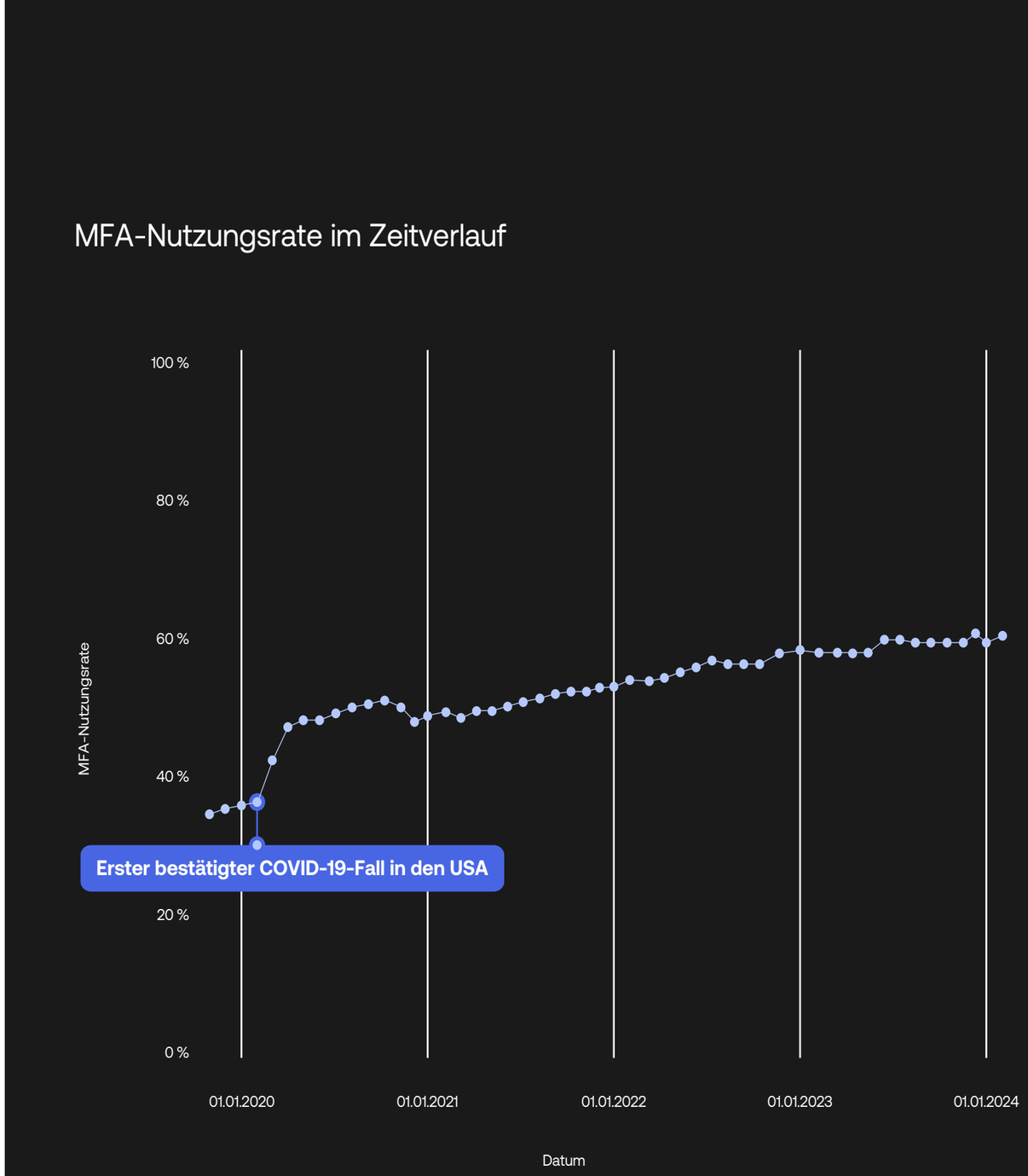

Abbildung 1: MFA-Nutzungsraten von Oktober 2019 bis Januar 2024. Die Daten zeigen die Nutzung von Okta Workforce Identity Cloud durch die Belegschaft und enthalten keine Daten für Okta Customer Identity Cloud (ehemals Auth0) oder kundenorientierte Use Cases der Okta-Plattform. Ebenfalls nicht enthalten sind Daten von Okta FedRAMP-Kunden (Federal Risk and Authorization Management Program) der Stufen High und DoD Impact Level 4.

Aktueller Stand bei der MFA-Nutzung

MFA-Nutzung nach Region

Im Bericht von 2023 stellten wir fest, dass die MFA-Nutzung in allen Weltregionen relativ einheitlich war, und gingen davon aus, dass sich dieser Trend auch im Jahr 2024 fortsetzen würde. Unabhängig vom Standort implementieren Okta-Kunden MFA häufiger für Benutzer als bei jedem anderen Mitbewerber-Service.

Unsere Daten bestätigten diese Annahme und zeigten MFA-Nutzungsraten zwischen 61 % und 68 % für die Regionen AMER (Nord-, Mittel- und Südamerika), APAC (Asien-Pazifik) und EMEA (Europa, Nahost und Afrika). Wir beobachteten im AMER- und EMEA-Raum eine Steigerung von 3 % bei der Nutzungsrate im Vergleich zu 2023 und einen Rückgang von 1 % in der APAC-Region.

Wichtige Erkenntnis

Wir können die Schlussfolgerung ziehen, dass (innerhalb der von uns abgedeckten Regionen) der Standort eines Unternehmens und seiner Benutzer Region (zumindest bei aggregierte Daten) kein entscheidender Faktor für die MFA-Implementierung ist.

MFA-Nutzungsrate nach Region

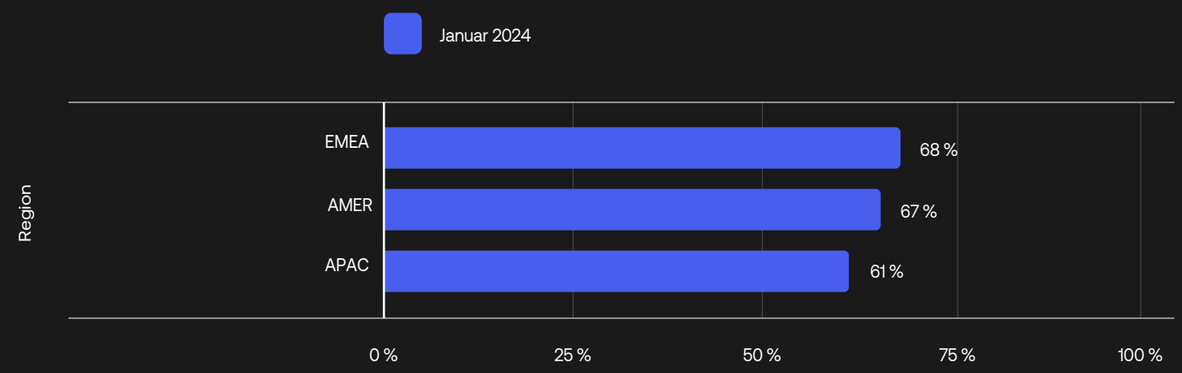

Abbildung 2: MFA-Nutzungsrate in den Regionen AMER (Nord-, Mittel und Südamerika), APAC (Asien-Pazifik), EMEA (Europa, Nahost und Afrika).

Aktueller Stand bei der MFA-Nutzung

MFA-Nutzung nach Branche

Auch im Jahr 2024 verzeichnen wir große Unterschiede bei der MFA-Nutzung nach Branche, wobei die Differenz zwischen der Branche mit der stärksten (Technologie) und der geringsten Nutzung (Transport und Logistik) auf 50 Prozentpunkte gestiegen ist. Wie so oft agiert der Technologiesektor als Early Adopter und verzeichnet weiterhin die höchste MFA-Nutzungsrate (88 %) unter den Okta Workforce Identity Cloud-Kunden.

Im letzten Jahr beobachteten wir bei fast allen Branchen eine stärkere MFA-Nutzung. Bei Behörden (von 48 % auf 55 %)[2] und im Bildungssektor (von 64 % auf 69 %) stieg die MFA-Nutzung im Jahresvergleich um 5 %. Beide Sektoren sind stark reguliert, zeigten ursprünglich nur eine relativ geringe MFA-Nutzung und holen nun auf. Wir rechnen damit, dass die aktuellen Dekrete des US-Präsidenten sowie neue Gesetze diesen Trend noch beschleunigen werden. Gleichzeitig verzeichneten wir einen Rückgang der MFA-Nutzung im Bereich Kunst, Unterhaltung und Freizeit (von 57 % auf 53 %) sowie im Versicherungssektor (von 77 % auf 71 %). Diese Branchen gehörten zu denen, die bei der Authentifizierung in großen Geschäftspartner-Netzwerken auf eine gute User Experience Wert legen (z. B. Versicherungsmakler). Angesichts der Daten, auf die diese kleinen Unternehmen zugreifen, finden wir es jedoch unwahrscheinlich, dass politische Entscheidungsträger ein Passwort allein oder MFA mit einer Kombination aus Passwort und SMS langfristig als ausreichend ansehen werden. Dieser Bericht stellt mehrere Möglichkeiten für reibungslose User Experiences vor, bei denen die Sicherheit nicht vernachlässigt wird.

Wichtige Erkenntnis

Wir wollten den Fortschritt im Behördensektor besonders herausstellen. Unternehmen, die Dienstleistungen für Behörden oder einen anderen regulierten Sektor anbieten, sollten MFA zumindest für privilegierte Accounts implementieren. Der Bericht von 2023 zeigte, dass die MFA-Nutzungsrate bei Behörden um mehr als 16 Prozentpunkte hinter dem privaten Sektor liegt. In diesem Jahr stieg die MFA-Nutzung in Behörden um 7 Prozentpunkte auf 55 %, einer der größten Sprünge in unseren Daten. Da nun die neuen US-Präsidentendekrete in Kraft treten[3] und die US-amerikanische Behörde CISA (Cybersecurity and Infrastructure Security Agency) ausdrücklich MFA und Phishing-resistente Authentifizierung befürwortet, sehen wir im US-Behördensektor einen echten Fortschritt.

[2] Einige Behördenmitarbeiter nutzen PIV-Karten (Personal Identity Verification) oder Smartcards zur Authentifizierung mit einer Drittanbieterlösung und greifen per Enterprise Federation auf Okta zu. Die MFA-Nutzungsrate im Behördensektor von derzeit 55 % deckt dieses Anwendungsszenario nicht ab, sodass die tatsächliche MFA-Nutzung höher liegen kann. Okta führte Smartcards als nativen Authentifikator im Jahr 2023 ein. Wir empfehlen Behördenkunden den Wechsel von X.509-Föderation zur Smartcard-Authentifizierung, um fortschrittliche Funktionen wie Authentifizierungsrichtlinien auf Anwendungsebene und Okta Device Access nutzen zu können.

[3] https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/information-technology-category/it-security/executive-order-14028

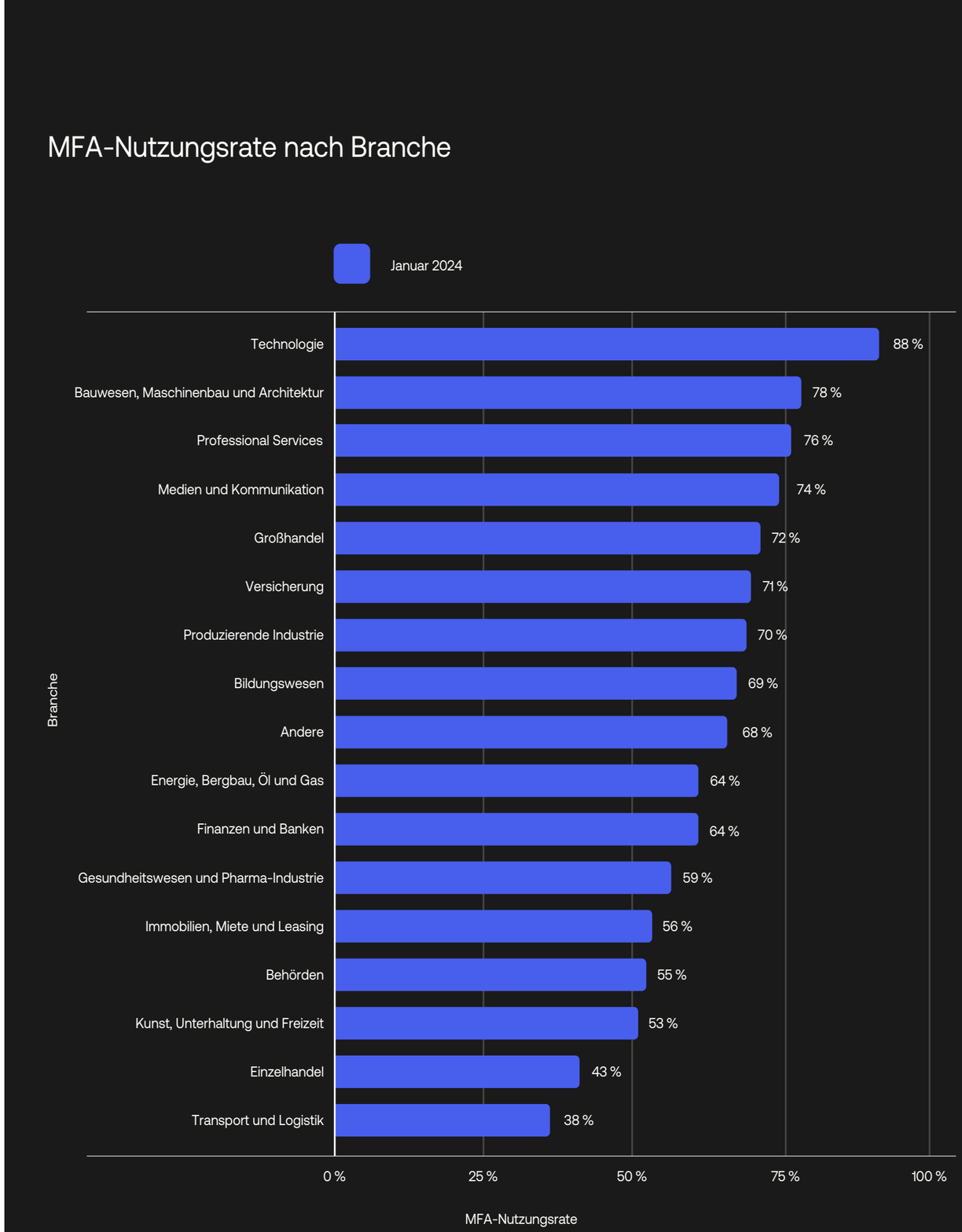

Abbildung 3: MFA-Nutzungsraten nach Branche, absteigend nach Rate.

Aktueller Stand bei der MFA-Nutzung

MFA-Nutzung nach Unternehmensgröße

Nach Unternehmensgröße betrachtet sehen wir eine annähernd umgekehrte Korrelation zwischen der Anzahl von Mitarbeitern und der MFA-Nutzungsrate: Je größer das Unternehmen, desto geringer die MFA-Nutzung. Firmen mit weniger als 300 Mitarbeitern haben in der Tendenz die höchste MFA-Nutzungsrate (≥82 %), während die Nutzungsrate bei Unternehmen mit mehr als 20.000 Mitarbeitern am geringsten war (59 %). Allerdings beobachten wir bei Letzteren im Jahresvergleich eine überdurchschnittliche Steigerung (5 %).

Der Unterschied zwischen kleinen und großen Unternehmen lässt sich auf mehrere Faktoren zurückführen: Ebenso wie bei Behörden und Finanzinstituten ist der Austausch veralteter Infrastruktur bei großen Unternehmen sehr aufwändig, was die Implementierung moderner Identity-Frameworks verzögert. Großunternehmen setzen auch häufiger auf mehrere Identity-Anbieter und können andere MFA-Lösungen als Okta nutzen (unser Bericht bezieht sich ausschließlich auf MFA mit der Okta-Plattform).

Wichtige Erkenntnis

Die fehlende zentrale Übersicht über IAM (Identity and Access Management) sorgt bei großen oder kleinen Unternehmen gleichermaßen für Probleme. Großunternehmen reagieren stärker auf Sicherheitsereignisse, die das Kundenvertrauen erschüttern, und sollten zur umfassenden MFA-Nutzung angehalten werden.

MFA-Nutzungsrate nach Unternehmensgröße

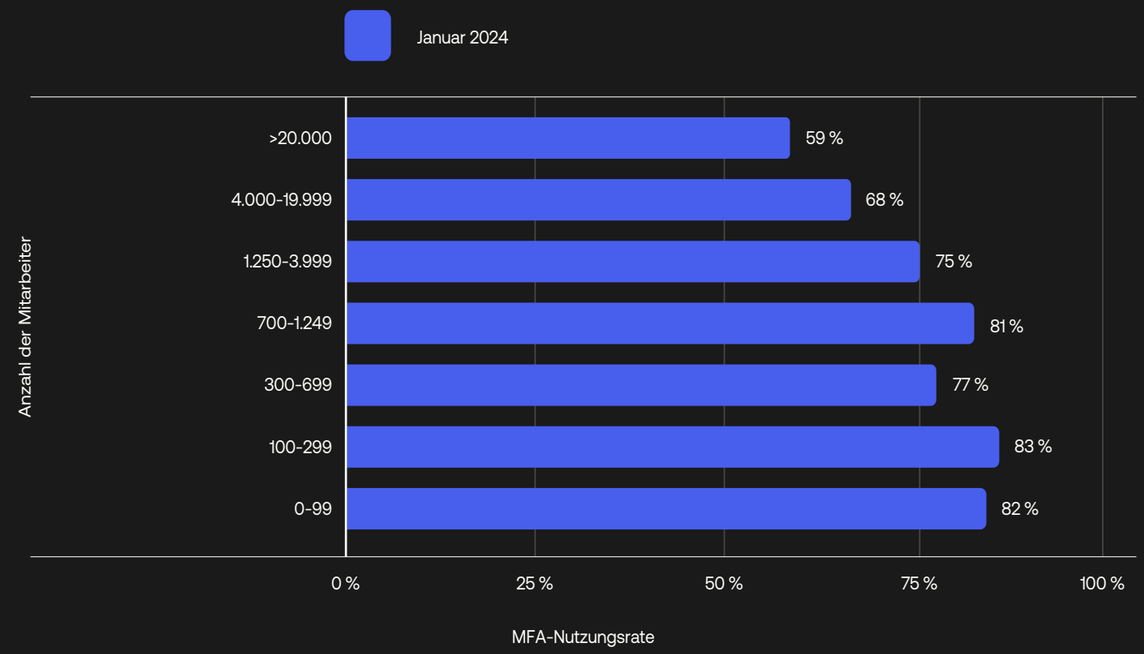

Abbildung 4: MFA-Nutzungsraten bei Unternehmen unterschiedlicher Größen, absteigend nach Anzahl der Mitarbeiter.

Aktueller Stand bei der MFA-Nutzung

MFA-Nutzung nach Benutzertyp

Bei der Analyse der MFA-Nutzung durch Okta-Administratoren definieren wir diese als Personen mit mindestens einer Administratorrolle bei Okta. Dazu gehören alle Mitarbeiter vom IT-Helpdesk bis hin zu IAM- und Sicherheitsteams. Diese MFA-Nutzungszahlen liegen bei sehr guten 91 % und sind im Vergleich zum letzten Jahr um 1 % gestiegen. Administratoren sind häufig auch Vorreiter bei der Nutzung Phishing-resistenter MFA. Die Nutzung von FIDO2 WebAuthn stieg unter Benutzern mit Administratorberechtigungen im letzten Jahr von 8 % auf 9 %, während der Anteil von Okta FastPass von 5 % auf 13 % wuchs.

Seit August 2024 verlangt Okta im Rahmen des Okta Secure Identity Commitment von Kunden die MFA-Nutzung für den Zugriff auf Administrator- und Verwaltungskonsolen.[4] Vor der MFA-Durchsetzung für die WIC-Admin-Konsole beobachteten wir eine hohe, aber keine umfassende Nutzung.[5] Um unser Ziel – eine hundertprozentige Nutzung – zu erreichen, konzentrieren wir uns auf die zahlreichen Benutzer mit Administratorrechten.

Damit unsere Kunden möglichst wenig beeinträchtigt werden, erfolgt die Durchsetzung schrittweise entsprechend der Komplexität bestehender Anmeldeprozesse. Einige Administratoren melden sich direkt bei Okta WIC an, während andere Identity-Anbieter-Föderation oder Integrationen mit PAM-Software (Privileged Access Management) nutzen. Okta verhindert mittlerweile die Erstellung von Ein-Faktor-Richtlinien für Direktzugriff auf die Okta-Admin-Konsole und erzwingt MFA für den Konsolenzugriff bei 62 % der aktuellen Okta Workforce Identity Cloud-Tenants.

Wir hoffen, dass privilegierte Benutzer erkennen, wie einfach die Anmeldung mit passwortlosen Phishing-resistenten Authentifikatoren ist, und dass es in Folge zu einer breiteren MFA-Nutzung bei allen Benutzern kommt.

Wichtige Erkenntnis

Da Okta für den Zugriff auf Administrator-Anwendungen MFA erzwingt, werden IT- und Sicherheitsexperten motiviert, die globale Authentifizierungsstrategie ihres Unternehmens genau zu prüfen. Wir empfehlen unseren Kunden, bei dieser Gelegenheit die Anmelderichtlinien für alle Verwaltungskonsolen und andere gefährdete oder geschäftskritische Anwendungen auf den Prüfstand zu stellen.

Dieser Rollout kann mit anwendungsspezifischen Authentifizierungsrichtlinien erleichtert werden, die starke Authentifizierung nur bei besonders gefährdeten oder geschäftskritischen Anwendungen vorschreiben, während Mitarbeiter bei weniger gefährdeten Anwendungen schwächere Authentifizierungsmethoden nutzen dürfen. Bei dieser Strategie können Administratoren die Sicherheit ihres Unternehmens verbessern, ohne Geschäftsprozesse zu beeinträchtigen.

[4] https://support.okta.com/help/s/blog/a674z000000147HAAQ/mfa-enforcement-for-the-admin-console?language=en_US

[5] Bitte beachten Sie, dass der Anteil der Administratoren, die MFA für den Zugriff auf die Okta-Admin-Konsole nutzen, sich von der MFA-Nutzungsrate für Administratoren unterscheidet. Die erste Kennzahl zeigt lediglich den Zugriff auf die Okta-Admin-Konsole, während die zweite den Zugriff auf sämtliche Anwendungen berücksichtigt. Zudem müssen Administratoren sich bei der ersten Kennzahl für jeden Zugriff auf die Admin-Konsole per MFA authentifizieren, während bei der zweiten nur eine MFA-Authentifizierung im Monat notwendig ist.

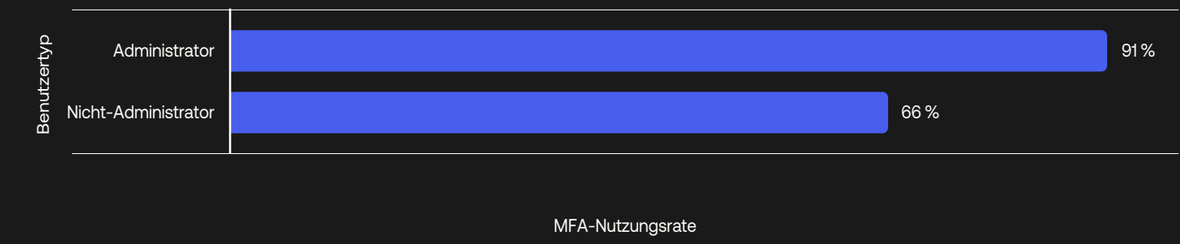

Abbildung 5: MFA-Nutzungsrate für Administratoren und Nicht-Administratoren.

Aktueller Stand bei der MFA-Nutzung

MFA-Nutzung nach Authentifikatortyp

Die Okta Identity Cloud ist Plattform-unabhängig und ermöglicht Kunden die Nutzung von Technologien ihrer Wahl. Okta bietet verschiedenste First-Party- und Third-Party-MFA-Authentifikatoren für alle Use Cases an. Authentifikatoren können entsprechend ihren Mechanismen in drei Kategorien unterteilt werden: Passwort-Authentifizierung, klassische MFA-Authentifikatoren und Phishing-resistente MFA-Authentifikatoren.

Klassische MFA-Authentifikatoren sind E-Mail-Adressen, Hardware-Token, Push- und SMS-Nachrichten, Sicherheitsfragen sowie Soft-Token. Phishing-resistente MFA-Authentifikatoren sind beispielsweise Okta FastPass, FIDO2 WebAuthn und Smartcards. Wie in Tabelle 1 zu sehen, nennen wir für jeden Authentifikatortyp so viele Angebote wie möglich. Falls die Authentifizierungsdaten jedoch nicht nach Authentifikatortyp unterteilt werden konnten oder kundenspezifische Optionen umfassten, haben wir sie in die Kategorie „Andere“ sortiert und bei der Untersuchung nicht berücksichtigt.

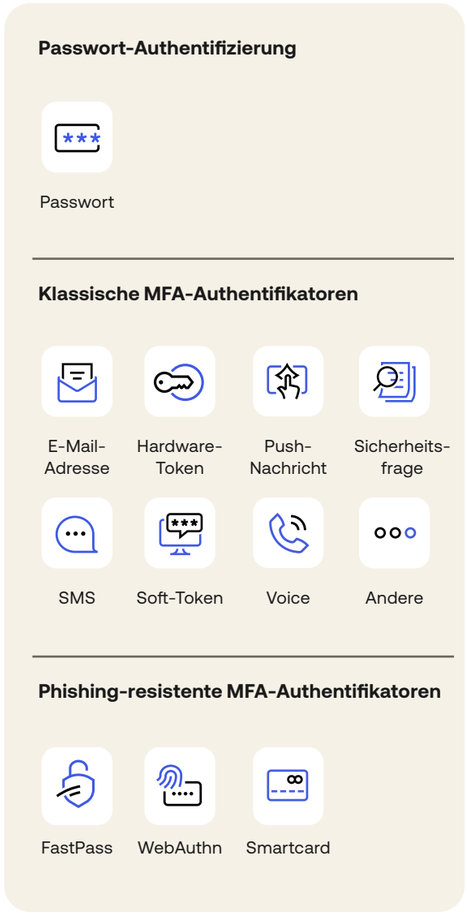

Tabelle 1: Authentifikatortypen und ihre Eigenschaften

Die Tabelle zeigt die Authentifikatortypen, die zur Bewertung der Nutzung, des Benutzerkomforts und der Sicherheit von MFA untersucht wurden, sowie wichtige Eigenschaften der einzelnen Authentifikatoren.

Authentifikatortyp	Von Okta unterstützte, bei dieser Untersuchung berücksichtigte Authentifikatoren	Bezeichnungen der Authentifikatoren, die zur Bewertung von Benutzerkomfort und Sicherheit berücksichtigt wurden	Art des Faktors	Sicherheitsniveau
Passwort	Passwort	Passwort	Wissen	Schwach
E-Mail-Adresse	Kombination aus E-Mail-Code und Link (Magic Link)	Kombination aus E-Mail-Code und Link	Besitz	Schwach
Hardware-Token	YubiKey OTP, RSA SecurId, kundenspezifisches TOTP	YubiKey OTP	Besitz	Mittel
Push-Nachricht	Okta Verify-App, Push-Methode, Duo Authenticator	Okta Verify-Push-Nachricht	Besitz Besitz + Biometrie	Mittel
Sicherheitsfrage	Sicherheitsfragen	Sicherheitsfragen	Wissen	Schwach
SMS	SMS, Duo Authenticator	SMS	Besitz	Schwach
Soft-Token	Okta Verify OTP, Google Authenticator, RSA SecurId, kundenspezifisches TOTP, Duo Authenticator	Okta Verify OTP, Google Authenticator	Besitz	Schwach
Voice	Sprachauthentifizierung per Telefon, Duo Authenticator	Sprachauthentifizierung per Telefon	Besitz	Schwach
FastPass	Okta Verify-App, FastPass-Methode	Okta FastPass	Besitz Besitz + Biometrie	Hoch
WebAuthn	WebAuthn-Authentifikatoren (Kombination aus Mac Touch ID, Android Fingerprint, Windows Hello, YubiKey, Google Titan, PassKey), Duo Authenticator	WebAuthn-Authentifikatoren (Kombination aus Mac Touch ID, Android Fingerprint, Windows Hello, YubiKey, Google Titan, PassKey)	Besitz Besitz + Biometrie	Hoch
Smartcard	Smartcard	Kombination aus PIV und CAC	Besitz + Wissen	Hoch

Es überrascht nicht, dass Passwörter auch weiterhin aktiv von Mitarbeitern genutzt werden. Wir verzeichnen jedoch auch eine Zunahme bei passwortloser Authentifizierung, die von weniger als 2 % im Januar 2023 auf fast 5 % im Januar 2024 stieg. Dabei ist die Push-Nachricht (29 %) der beliebteste MFA-Authentifikator, gefolgt von SMS (17 %) und Soft-Token (14 %).

Die Nutzungsrate bei klassischen MFA-Authentifikatoren hat im Vergleich zum Vorjahr zwar zugenommen, die Änderungen waren jedoch nur gering (1,3 % insgesamt). Bei der MFA-Nutzung von SMS verzeichneten wir eine sehr kleine Zunahme von 1,2 % über die letzten drei Jahre, obwohl die allgemeine MFA-Nutzungsrate im gleichen Zeitraum um 14 % stieg. Im Gegensatz dazu sehen wir bei Phishing-resistenten Authentifikatoren eine erhebliche Zunahme. So stieg die Nutzungsrate bei WebAuthn von 2 % (2023) auf 3 % (2024) der Benutzer, während die Nutzungsrate bei Okta Verify FastPass im gleichen Zeitraum von 2 % der Benutzer auf 6 % sprang.

Es gibt drei zentrale Gründe für die Zunahme Phishing-resistenter Authentifikatoren. Erstens: Die stetig wachsende Bedrohung durch Phishing-Angriffe. So beobachtete das Okta-Security-Team beispielsweise, dass die Zahl der Phishing-Angriffe mit nachgeahmten Unternehmen von Februar 2023 bis Januar 2024 um 50 % stieg. Parallel dazu hat Zscaler anhand von Daten der eigenen Netzwerksicherheitsprodukte eine Zunahme von 58 % bei Phishing-Angriffen beobachtet.[6]

Zweitens: Die Verfügbarkeit Phishing-resistenter Optionen. Okta unterstützt verschiedene Phishing-resistente Authentifikatoren wie FastPass und FIDO2 WebAuthn. Die vereinfachte Zugriff mit dieser Technologie hat direkte Auswirkungen auf ihre Nutzung. Im Rahmen des kostenlosen Upgrades auf die Okta Identity Engine wurde FastPass, die in Okta Verify integrierte passwortlose und Phishing-resistente Anmeldemethode, für alle Kunden bereitgestellt. Wir stellten fest, dass 7 % der neuen oder migrierten OIE-Tenants, die zwischen Februar 2023 und Januar 2024 ein Upgrade auf OIE durchgeführt hatten, innerhalb der ersten 90 Tage FastPass ausprobiert hatten.

Drittens: Wir können damit rechnen, dass die Nutzung Phishing-resistenter Faktoren durch gesetzliche Vorgaben weiter beschleunigt wird. So müssen beispielsweise Behörden in Australien für die Vorschriften Essential Eight Maturity Level 2 und 3 Phishing-resistente Authentifizierungsmethoden implementieren.

Wichtige Erkenntnis

OIE bietet mehr Flexibilität bei der Verwaltung von Anmeldevorgängen. So können Administratoren mit Anmelderichtlinien für Anwendungen individuelle Regeln für den Zugriff auf Anwendungen konfigurieren und Benutzern in Okta FastPass einen passwortlosen, Phishing-resistenten Authentifikator anbieten. Wir empfehlen Okta-Kunden, stärkere Authentifikatoren zu evaluieren und zu implementieren, da dies den Komfort für die Administratoren verbessert und zudem zahlreiche Vorteile für die Benutzer bietet. Beispielsweise ist bekannt, dass die Authentifizierung per SMS nur geringe Sicherheit bietet, für SIM-Swapping-Angriffe anfällig ist und mit höheren Betriebskosten verbunden ist. Die besten Ergebnisse erreichen Sie, wenn IT- und Security-Teams das Upgrade gemeinsam durchführen, um schnell den größten Mehrwert zu erzielen und die beste Authentifizierungsstrategie für das Unternehmen zu finden.

[6] https://www.zscaler.com/blogs/security-research/phishing-attacks-rise-58-year-ai-threatlabz-2024-phishing-report

MFA-Nutzungsrate nach Authentifikator

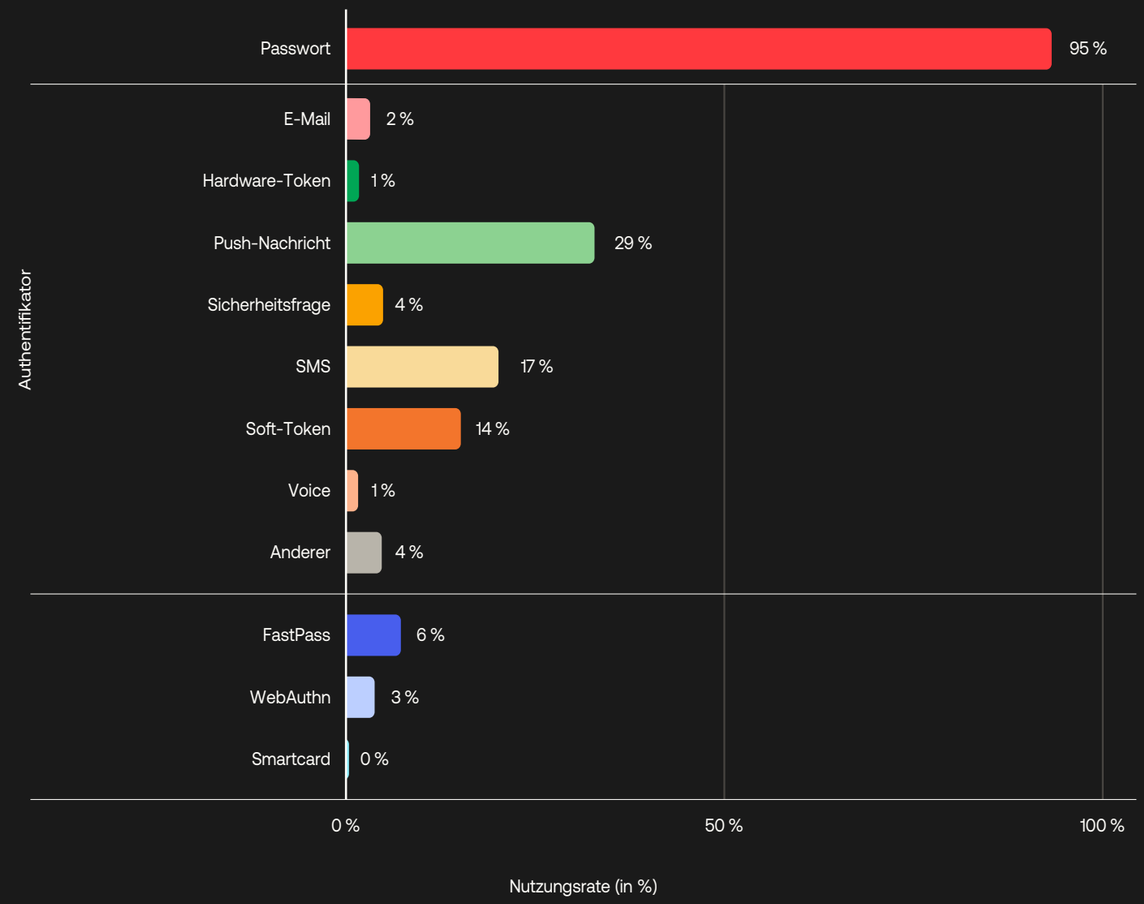

Abbildung 6: MFA-Nutzungsraten für Authentifikatoren, die in Okta Workforce Identity Cloud verfügbar sind. Die Summe der Nutzungsrate für jeden Authentifikator ist höher als die MFA-Nutzungsrate, da Benutzer sich mit mehreren Authentifikatoren authentifizieren können.

Datengestützte Bewertung des Benutzerkomforts und der Sicherheit von Authentifikatoren

Auch wenn die MFA-Nutzung Fahrt aufnimmt, gibt es immer noch Hürden, die überwunden werden müssen. Damit CIOs, CSOs und politische Entscheider überlegte Entscheidungen zu Authentifikatoren treffen können, ist es sinnvoll, die jeweiligen Vor- und Nachteile zu verstehen.

Dazu haben wir ein Framework entwickelt, mit dem der Benutzerkomfort und die Sicherheit von Authentifikatoren bewertet werden kann. Die Bewertungskategorien finden Sie in Tabelle 2. Mithilfe der daraus gewonnenen, datengestützten Erkenntnisse können IT- und Sicherheitsverantwortliche ihre Unternehmen besser schützen und die Produktentwicklung anpassen.

Wenn Sie unseren Secure Sign-in Trends Report 2023 gelesen haben, wird Ihnen dieser Abschnitt sehr bekannt vorkommen. Für den Bericht für das Jahr 2024 haben wir die Kennzahlen aktualisiert, ohne dass es jedoch zu großen Veränderungen gekommen ist – die Zeit für das Eingeben eines Passworts oder den Erhalt eines E-Mail-Codes variiert nicht groß. Bei der diesjährigen Untersuchung berücksichtigten wir jedoch mehr Benutzer und Ereignisse, da mehr Unternehmen zu OIE migriert sind. Zudem haben wir die Rückmeldungen von Okta-IT- und Sicherheitsexperten genutzt, um die relativen Kennzahlengewichtungen anzupassen und die Umfragemethodik insgesamt zu verbessern. Trotz der überarbeiteten und praxisnäheren Kriterien kommen wir bei der Nutzung eines Phishing-resistenten Authentifikators zu den gleichen Vorteilen. Wir haben jetzt auch Metrikdaten für die Authentifizierung per Smartcard berücksichtigt. Wir sind der Meinung, dass die Erkenntnisse aus diesem Bericht allen Verantwortlichen helfen, die moderne Authentifizierungsmethoden wie FastPass oder WebAuthn evaluieren sollen.

Benutzerkomfort und Sicherheit von Authentifikatoren

Zeitaufwand für Authentifizierungs-abfragen

Zwei Möglichkeiten der Passwort-Eingabe

Wir haben den Zeitaufwand für die Passwort-Authentifizierung mit zwei verschiedenen Benutzeroberflächen-Konfigurationen berücksichtigt:

- **Bei einem Ablauf mit Benutzername/Passwort** wird Benutzern ein Feld für Benutzername und Passwort auf derselben Anmeldeseite angezeigt.
- **Bei einem Ablauf nur mit Passwort** geben Benutzer ihren Benutzernamen auf einer Seite ein und werden aufgefordert, auf der nächsten Seite ein Passwort einzugeben.

Der mittlere Zeitaufwand für die Authentifizierung per Passwort mit dem Nur-Passwort-Szenario eignet sich am besten für den Vergleich mit anderen Authentifikatoren, weil bei allen anderen MFA-Authentifikatoren vor der Abfrage kein Account angegeben werden muss. Dennoch werden wir im Diagramm beide Varianten verwendet.

Der Zeitaufwand für Authentifizierungsabfragen bezeichnet den mittleren Zeitaufwand des Benutzers bis zum erfolgreichen Abschluss einer Authentifizierungabfrage.

Dieser Zeitaufwand hat sich im Jahresverlauf nicht verändert. Bei der Password-Authentifizierung liegt der mittlere Zeitaufwand bei ca. sechs Sekunden. Wir gehen davon aus, dass diese Zeitangabe bei Passwörtern aufgrund der Nutzung von Passwortmanagern und der automatischen Ausfüllfunktion im Browser nach unten gezogen wird. Bei Authentifizierungsabläufen, die mit Passwörtern beginnen, verlängert das Eingeben eines OTP (One-Time-Passwort) den Zeitaufwand um mindestens 12 Sekunden – und sogar noch mehr, wenn das OTP per E-Mail oder Anruf übermittelt wird.

Unsere Daten zeigen, dass Authentifikatoren, die Besitz und Inhärenz (wie biometrische Daten) kombinieren, den geringsten Zeitaufwand verursachen (4 Sekunden). FIDO2 WebAuthn, Okta FastPass (das bereits im Namen darauf hinweist) und Smartcards ermöglichen wesentlich effizientere Authentifizierungsprozesse als alle anderen Authentifikatoren. Diese Geschwindigkeit bietet Unternehmen auch die Möglichkeit, häufiger erneute Authentifizierungen durchzuführen oder für den Zugriff auf vertrauliche Anwendungen vorzuschreiben. Beides sind wichtige Schutzmaßnahmen gegen Session-Hijacking-Angriffe.

Wichtige Erkenntnis

Wenn der Zugriff auf eine Mitarbeiteranwendung zwei unterschiedliche Faktoren erfordert (was die Mindestanforderung für NIST AAL2 ist), erreichen Sie den größten Benutzerkomfort (in Bezug auf den Zeitaufwand für die Abfrage) mit FIDO2 WebAuthn oder Okta FastPass, die zudem die beste Sicherheit (Phishing-Schutz) bieten.

Diese Authentifikatoren stellen einen Besitzfaktor sowie einen Inhärenzfaktor meist in weniger als vier Sekunden bereit – und sind damit wesentlich schneller als eine Kombination aus Passwort und OTP-Sicherheitsabfrage.

Zeitaufwand für Authentifizierungsabfragen

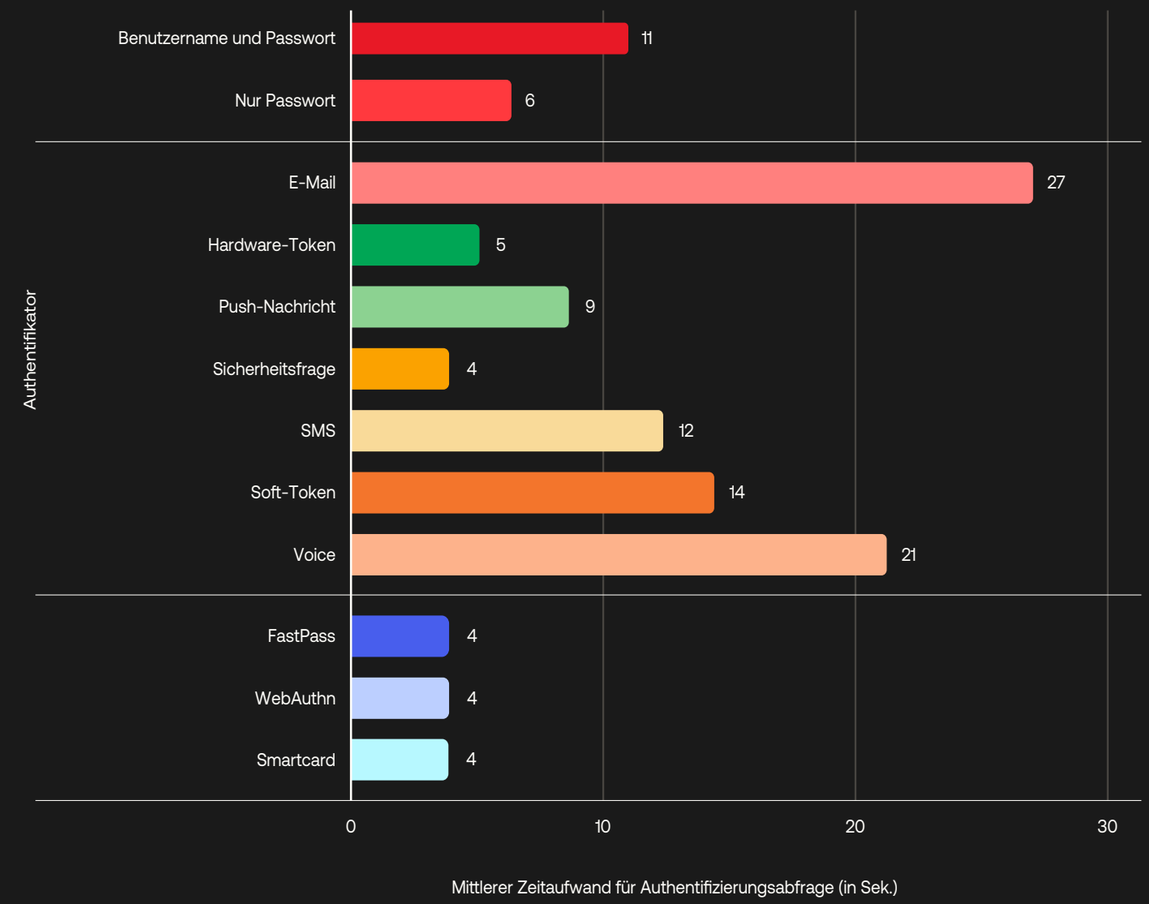

Abbildung 7: Mittlerer Zeitaufwand für Authentifizierungsabfragen mit den Authentifikatoren Passwort (Benutzername/Passwort und nur Passwort), E-Mail-Adresse, Hardware-Token, Push-Nachricht, Sicherheitsfrage, SMS, Soft-Token, Voice, FastPass, WebAuthn und Smartcard.

“Einfache MFA bietet keinen zuverlässigen Schutz vor Bedrohungsakteuren. Mit Okta FastPass ist es ein Kinderspiel, nicht nur die Sicherheit mit Phishing-resistenter MFA zu verbessern, sondern auch kontextbezogene Informationen zum Gerätestatus zu erhalten. Wenn Sie Phishing-resistente Authentifizierung implementieren und den Zugriff auf sensible Anwendungen nur für verwaltete Geräte zulassen, können Sie die möglichen Angriffsquellen drastisch minimieren. Zudem gewährleisten Sie mit Device Assurance-Kontrollen, dass diese Geräte gepatcht und die notwendigen Kontrollen zum Zeitpunkt des Zugriffs aktiv sind.

Sicherheit ist jedoch nicht nur ein immer strikterer Prozess. Wenn strikte Kontrollen die User Experience beeinträchtigen, arbeiten Sie damit gegen Ihr eigentliches Ziel. Deshalb haben wir auch passwortlose Authentifizierung implementiert. Mit Phishing-Schutz, verwalteten Geräten, biometrischer Benutzerverifizierung und Gerätestatus erreichen wir unter anderem AAL2 und verbessern gleichzeitig die alltägliche User Experience für unsere Endbenutzer.“

Andrew Meinert
Director of System Operations

HubSpot

Benutzerkomfort und Sicherheit von Authentifikatoren

Zeitaufwand für die Registrierung eines Authentifikators

Der Zeitaufwand für die Registrierung eines Authentifikators ist die mittlere Zeitspanne, die für die Registrierung eines Authentifikators benötigt wird – von der Anzeige der Registrierungsseite bis zum Abschluss der Registrierung, nachdem der Benutzer den angegebenen Anweisungen gefolgt ist.

Die Registrierung und Zurücksetzung von Authentifikatoren sowie die Password-Wiederherstellung stellen kurze Phasen erhöhter Risiken dar. Für jedes Registrierungs- oder Rücksetzungsereignis können (und sollten) Administratoren Regeln dazu durchsetzen, welche Administratoren für die Initiierung und Überprüfung der Benutzeridentität erforderlich sind. Für diesen Zweck empfehlen wir die Einrichtung Phishing-resistenter Authentifikatoren.

Der mittlere Zeitaufwand für die Registrierung eines Passworts liegt bei etwa 35 Sekunden – einschließlich Erstellung eines neuen Passworts, Bestätigung (bzw. erneute Eingabe) sowie die Auswahl, ob andere authentifizierte Geräte abgemeldet werden sollen. Die längste mittlere Registrierungszeit haben Sicherheitsfragen (40 Sekunden), da Benutzer hier eine Sicherheitsfrage wählen oder erstellen und anschließend die Antwort eingeben müssen.

Der Registrierungsprozess für Authentifikatoren ist bei Okta so gestaltet, dass Okta Verify OTP, Okta Verify Push und Okta FastPass gemeinsam mit der Okta Verify-App registriert werden können. Da in einem Schritt mehrere Authentifikatortypen registriert werden, liegt die mittlere Registrierungszeit bei ca. 38 Sekunden, einschließlich der Zeit für das Scannen eines QR-Codes sowie den Abschluss des Konfigurationsprozesses für Okta Verify. Bei Hardware-Token, Voice, SMS sowie FIDO2 WebAuthn ist der Zeitaufwand mit weniger als 25 Sekunden am kürzesten. Smartcard-Registrierungsprozesse umfassen die Offline-Benutzerverifizierung, Smartcard-Herstellung und ihren Versand. Es kann mehrere Woche dauern, bis die neue Smartcard angekommen ist. Die Okta Identity-Plattform kann diesen Prozess nicht erfassen.

Wichtige Erkenntnis

Bemerkenswert ist, dass wir gegenüber 2023 überall leichte Zunahmen beim Zeitaufwand für die Registrierung verzeichnen. Da dieser Schritt manuell erfolgt, kann das durch menschliche oder technische Faktoren begründet sein.

Unternehmen setzen zunehmend auf automatisierte Registrierungsprozesse, um die Benutzer zu entlasten. Beispielsweise gab Okta im April 2024 eine Partnerschaft mit YubiKey bekannt, sodass Administratoren vorab registrierte YubiKeys an die Privatanschriften von Mitarbeitern senden lassen können. Benutzer müssen dann nur noch den Schlüssel einstecken und eine PIN eingeben, sodass sie praktisch sofort loslegen können.

Zeitaufwand für die Registrierung eines Authentifikators

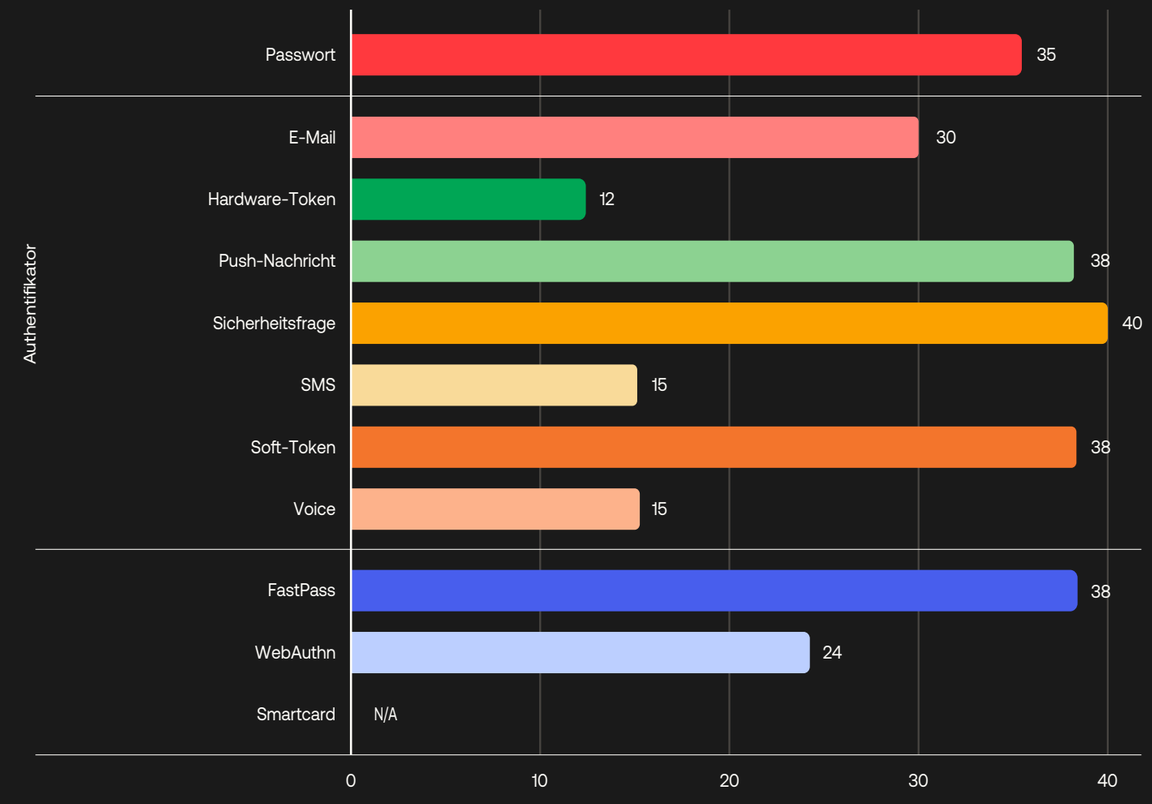

Abbildung 8: Mittlerer Zeitaufwand für die Registrierung der Authentifikatoren Passwort, E-Mail-Adresse, Hardware-Token, Push-Nachricht, Sicherheitsfrage, SMS, Soft-Token, Voice, FastPass, WebAuthn und Smartcard. Die Zeit für die Benutzerverifizierung wurde von dieser Analyse ausgenommen, da sie von Registrierungs- und Wiederherstellungsrichtlinien und nicht vom Authentifikator bestimmt wird.

Benutzerkomfort und Sicherheit von Authentifikatoren

Fehlerquote bei Authentifizierungs-abfragen

Die Fehlerquote bei Authentifizierungsabfragen ist definiert als die Anzahl der fehlgeschlagenen Authentifizierungsversuche geteilt durch die Gesamtzahl der Authentifizierungsversuche, die beim Okta-Backend-Server für einen bestimmten Authentifikator eingegangen sind.

Fehlgeschlagene Authentifizierungsversuche treten überraschend häufig auf. Dazu gehören Ereignisse, bei denen Benutzer ein falsches Passwort eingeben oder eine Sicherheitsfrage falsch beantworten, ein falsches OTP eingeben, eine Push-Abfrage verweigern oder eine falsche Authentifizierungssignatur mit einem biometrischen Authentifikator (z. B. Okta FastPass oder FIDO2 WebAuthn) angeben.

Die Fehlerquote bei Authentifizierungsabfragen ist gleichermaßen eine Kennzahl für Benutzerkomfort und Sicherheit, da ein fehlgeschlagenes Authentifizierungsereignis harmlos oder gefährlich sein kann. Eine höhere Rate harmloser Fehler bedeutet, dass Benutzer während der Authentifizierung mit einem bestimmten Authentifikator häufiger Fehler machen, was ihre Produktivität beeinträchtigt. Eine höhere Rate verdächtiger Fehler weist wiederum darauf hin, dass Angreifer diese Methode als leichteres Ziel betrachten. Die Unterscheidung zwischen einem harmlosen und einem gefährlichen Ereignis erfordert allerdings erweiterte Kenntnisse der Nutzungsmuster, die in den anonymisierten Daten für diesen Bericht nicht enthalten sind. Ihr Security-Team ist möglicherweise in der Lage, einen solchen Bericht für Ihre Umgebung bereitzustellen.

Unsere Daten zeigen, dass wissensbasierte Authentifikatoren für Benutzer die größte Belastung darstellen, gefolgt von verschiedenen OTP-Formen.

Das gewöhnliche Passwort verzeichnet die höchste Fehlerquote (fast 10 %), gefolgt von Soft-Token, per E-Mail versendeten Authentifizierungsabfragen sowie Sicherheitsfragen.

Die Authentifizierung per FIDO2 WebAuthn und Smartcard führt logischerweise zu weniger unbeabsichtigten Benutzerfehlern (d. h. Vertippern) und weniger verdächtigen Anmeldeversuchen, was entsprechend niedrige Fehlerquoten bedeutet. Diese Erkenntnisse haben jedoch einen Haken: Die Implementierung von WebAuthn und Smartcards erfolgt nicht wie bei den anderen Authentifizierungsmethoden. Prinzipbedingt erfolgt der Authentifizierungsprozess bei diesen Methoden auf dem Benutzersystem, sodass der Identity-Anbieter (Okta) nicht alle fehlgeschlagenen Ereignisse für diese Authentifikatoren erfassen kann. Wenn Benutzer sich beispielsweise mit FIDO2 WebAuthn bei einem Phishing-Proxy anmelden wollen und das Authentifizierungssystem eine Domain-Diskrepanz erkennt, gibt es keinen Mechanismus zum Senden dieser Informationen zurück an die Backend-Server des Identity-Anbieters. Dadurch hat der Administrator keine Möglichkeit, die korrekte Zahl gefährlicher Authentifizierungsversuche zu erfassen.

Wichtige Erkenntnis

Selbst wenn wir den Haken mit der WebAuthn-Fehlerquote berücksichtigen, können wir sehen, dass die Phishing-resistenten Authentifikatoren die beste User Experience bieten.

Fehlerquote bei Authentifizierungsabfragen nach Authentifikator

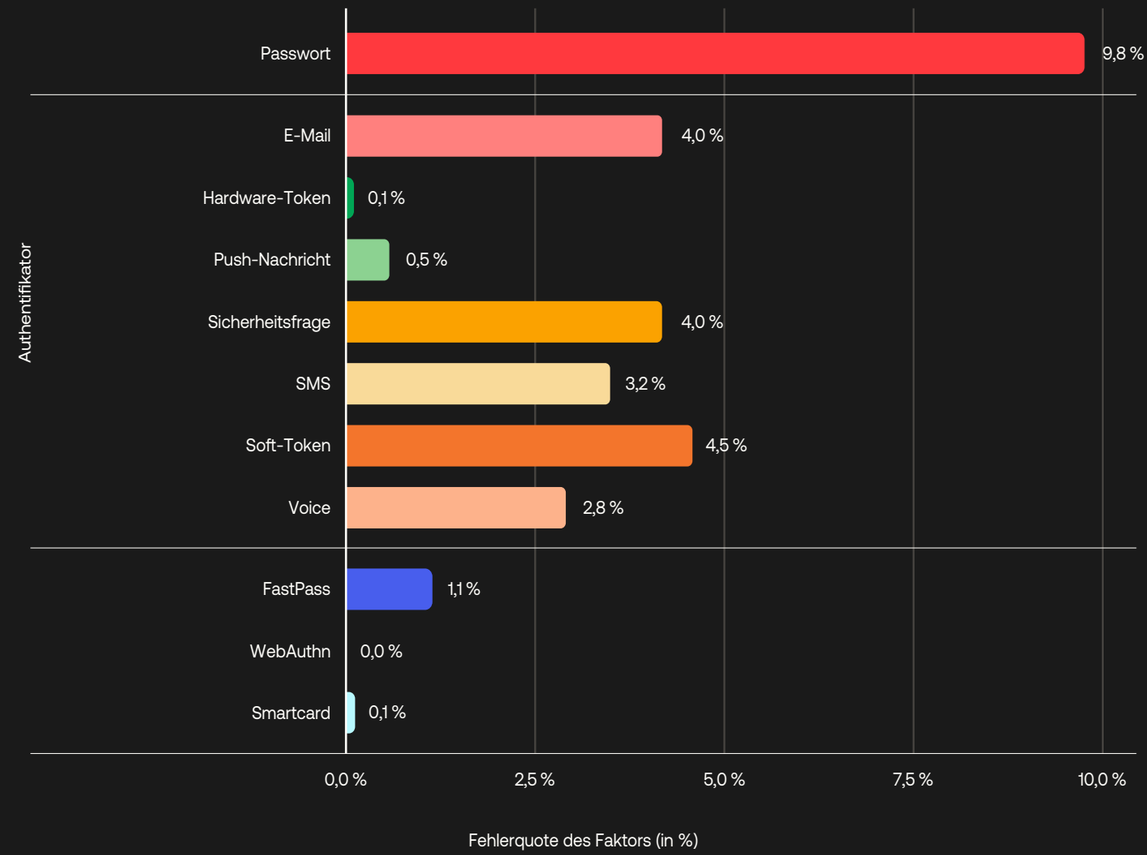

Abbildung 9: Fehlerquote bei Authentifizierungsabfragen mit den Authentifikatoren Passwort, E-Mail-Adresse, Hardware-Token, Push-Nachrichten, Sicherheitsfragen, SMS, Soft-Token, Voice, FastPass, WebAuthn und Smartcard.

Benutzerkomfort und Sicherheit von Authentifikatoren

Anteil Phishing-resistenter Authenti-fizierung

Der Anteil Phishing-resistenter Authentifizierung beschreibt den potenziellen Anteil von Benutzern, die mit einem Authentifikator geschützt werden, der die NIST-Definition für Phishing-Resistenz erfüllt.

Wenn ein Authentifikator nicht Phishing-resistent ist, liegt der Anteil Phishing-resistenter Authentifizierung bei Null. Ein Phishing-resistenter Authentifikator hat einen Anteil Phishing-resistenter Authentifizierung entsprechend dem Anteil der Benutzer, deren Browser und Betriebssysteme diese Funktionen unterstützen. Anhand dieser Kriterien zeigt sich, dass drei Authentifikatoren einen Anteil Phishing-resistenter Authentifizierung von über Null haben: Okta FastPass, FIDO WebAuthn und Smartcards.

FIDO 2 WebAuthn erlaubt Websites die Ergänzung ihrer Anmeldeseiten mit FIDO-basierter, Phishing-resistenter Authentifizierung auf unterstützten Browsern und Plattformen. Laut caniuse.com können 96 % aller Geräte WebAuthn auf ihren Browsern und Plattformen nutzen. Die Verfügbarkeit Phishing-resistenter WebAuthn-Authentifikatoren ist ein theoretischer und optimistisch angesetzter Wert, da diese nur von bestimmten Plattformen unterstützt werden. Daher kann ihr Anteil sehr viel geringer sein als der im Diagramm dargestellte optimale Anteil.

Okta FastPass bietet effektiven Schutz vor Anmeldedaten-Phishing-Angriffen, indem bei jedem Authentifizierungsversuch die Ursprungs-URL verifiziert wird. Dieser Phishing-Schutz ist unter Windows, macOS, Android und iOS verfügbar. In Bezug auf Belegschaften gehen wir davon aus, dass bei dem Browser- und Plattform-Mix von caniuse.com ca. 95 % der Benutzer die Phishing-Schutz-Funktion von FastPass nutzen können.

Wichtige Erkenntnis

WebAuthn und FastPass bieten Phishing-resistente Authentifizierung. Klassisch handelt es sich bei WebAuthn-Implementierungen um Anmeldedaten für einzelne Geräte in der Form von Roaming-Authentifikatoren (z. B. physische Sicherheitsschlüssel) oder um Plattform-Authentifikatoren (z. B. Face ID oder Windows Hello). Im vergangenen Jahr führten FIDO und große Betriebssystemanbieter Passkeys für mehrere Geräte (Multi-Device-Passkeys) als WebAuthn-Anmeldedaten ein, mit denen Benutzer sich auf unterschiedlichen Geräten synchronisieren können.

Alle WebAuthn-Implementierungen sind Phishing-resistent, wobei sie nicht alle einheitlich sind. Die Unterschiede zwischen Windows, macOS, iOS und Android können irritierend sein und die Benutzung erschweren. Die Einführung von Passkeys für mehrere Geräte erleichtert zwar Kunden die Authentifizierung erheblich, kann jedoch bei Mitarbeitern zu Problemen führen, wenn die Verwendung eines Passkeys auf unterschiedlichen Geräten laut Unternehmensrichtlinie untersagt ist. Hinzu kommt, dass einige Betriebs-systemanbieter vor Kurzem die Unterstützung von gerätegebundenem WebAuthn zugunsten von Multi-Device-Passkeys eingestellt haben, sodass eine einheitliche User Experience nicht gegeben ist.[7]

FastPass ist ebenfalls für Mitarbeiter und Sicherheitsmodelle optimiert und bietet starke Gerätebindung sowie Device Assurance-Statusprüfungen. Zudem ist ein einheitliches Design auf allen Plattformen (einschließlich Desktop und Mobilgeräte) gegeben, sodass Benutzer motiviert sind, die stärksten verfügbaren Authentifizierungsmethoden zu nutzen.

Da Smartcards spezialisierte Hardware benötigen, ist diese Technologie meist auf stark regulierte Branchen beschränkt, die sich eine einheitliche IT-Infrastruktur leisten können.

[7] https://passkeys.dev/device-support/

Anteil Phishing-resistenter Authentifizierung nach Authentifikator

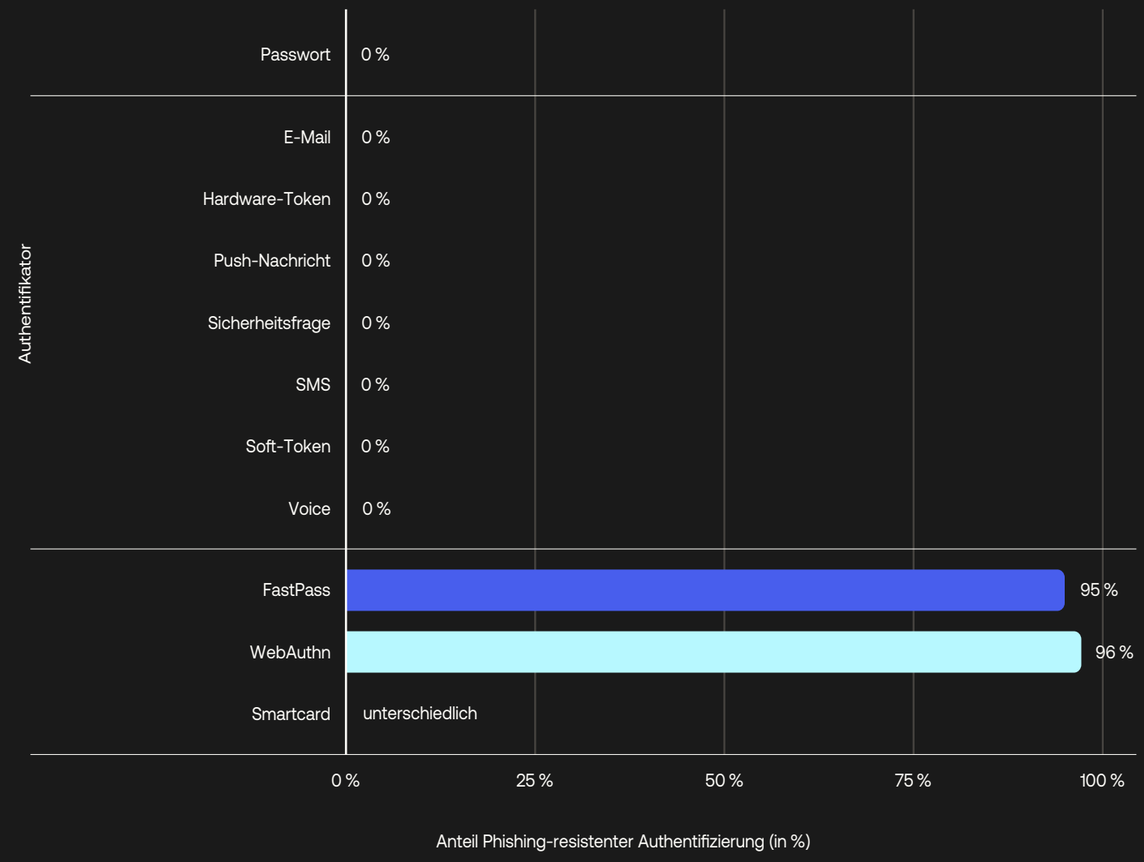

Abbildung 10: Anteil Phishing-resistenter Authentifizierung bei den Authentifikatoren Passwort, E-Mail-Adresse, Hardware-Token, Push-Nachrichten, Sicherheitsfragen, SMS, Soft-Token, Voice, FastPass, WebAuthn und Smartcard.

Benutzerkomfort und Sicherheit von Authentifikatoren

Anteil Phishing-resistenter Authentifizierung mit Warnfunktion

Der Anteil Phishing-resistenter Authentifizierung mit Warnfunktion bezeichnet die Benutzer, die potenziell von einem Authentifikator geschützt werden, der Anfragen mit fehlgeschlagenen Ursprungsprüfungen – ein typisches Anzeichen für AitM-Angriffe (Adversary-in-the-Middle) – erfassen kann.

Nach aktuellem Stand ist Okta FastPass der einzige Authentifikator, der bei Phishing-Versuchen, die zu einer fehlgeschlagenen Ursprungsprüfung führen, Server-seitige Ereignisse generieren kann. Wenn die fehlende Übereinstimmung des Domain-Namens oder von Cookies einer Phishing-Website erkannt wird, lehnt FastPass die Anfrage ab und warnt Endbenutzer sowie Administratoren. Dadurch nehmen Benutzer sowie Unternehmen die Bedrohungen stärker wahr und können böswillige Aktivitäten besser erkennen und stoppen.

FastPass ist die Rettung

Die folgende Fallstudie basiert auf den Erfahrungen eines Okta-Kunden, der Anfang 2023 OIE implementiert und FastPass eingeführt hatte:

An einem Abend im Juli 2024 erhielt einer unserer Mitarbeiter einen Anruf im Rahmen einer umfangreichen Social-Engineering-Kampagne, bei der hunderte Unternehmen angegriffen wurden. Der Anrufer hatte einen amerikanischen Akzent und eine tatsächlich vom Unternehmen genutzte Telefonnummer gefälscht. Er stellte sich als Mitarbeiter des IT-Teams vor und wies den Mitarbeiter an, sich bei einer Website anzumelden, die einer Unternehmens-Domain täuschend ähnlich sah. Der Benutzer verwendete jedoch Okta FastPass, das den Anmeldeversuch blockierte, da Domain und Zertifikat nicht mit der Okta Org des Kunden übereinstimmte. In den darauf folgenden fünf Minuten überzeugte der Bedrohungsakteur den Benutzer mehrmals, sich über die Phishing-Website anzumelden. Auch dies wurde jeweils von FastPass blockiert. Das Security-Team, das bereits durch die erfolglosen Social-Engineering-Versuche anderer Benutzer gewarnt war, konnte diese fehlgeschlagenen Versuche schnell im Systemprotokoll lokalisieren und reagieren. Dabei wurde sogar kurzfristig der Zugriff des angegriffenen Benutzers gesperrt. Am nächsten Morgen erhielt der angegriffene Benutzer wieder den notwendigen Zugriff und konnte weiterarbeiten.

Eine nachfolgende Untersuchung zeigte, dass die Warnmeldungen von FastPass den Kunden vor Account-Hacking durch den Social-Engineering-Akteur geschützt und die Beeinträchtigung der Mitarbeiterproduktivität minimiert hat.

Dabei ist FastPass nicht nur ein klassischer Authentifikator, sondern kann auch Gerätekontextinformationen wie Gerätemanagementstatus, Betriebssystemversion, Gerätesperrung, Datenträgerverschlüsselung und Jailbreaks/Rootzugriff erfassen. FastPass integriert sich auch Lösungen für UEM (Unified Endpoint Management) sowie EDR (Endpoint Detection and Response) wie Jamf, Microsoft Intune, Workspace One, CrowdStrike, Windows Security Center und Chrome Device Trust.[8] Dadurch ist gewährleistet, dass ein sich authentifizierendes Gerät verwaltet wird bzw. eine ausreichende Sicherheitshygiene nachweisen kann. Diese Kontextinformationen unterstützen die Bedrohungserkennung sowie die Durchsetzung von Authentifizierungsrichtlinien.

Wichtige Erkenntnis

Wir rechnen damit, dass Funktionen zur proaktiven Erkennung und Meldung von Social-Engineering- und AiTM-Phishing-Kampagnen noch wichtiger werden, weil die Erkennungs- und Reaktionsgeschwindigkeit beim Kampf gegen Cyberangriffe ein zentrales Alleinstellungsmerkmal sein wird. Unternehmen profitieren durch die Warnfunktionen von Okta FastPass nahezu in Echtzeit von Schutz und Erkennung von Phishing-Angriffen.

[8] https://support.okta.com/resource/device_context_deployment_guide

Anteil Phishing-resistenter Authentifizierung mit Warnfunktion nach Authentifikator

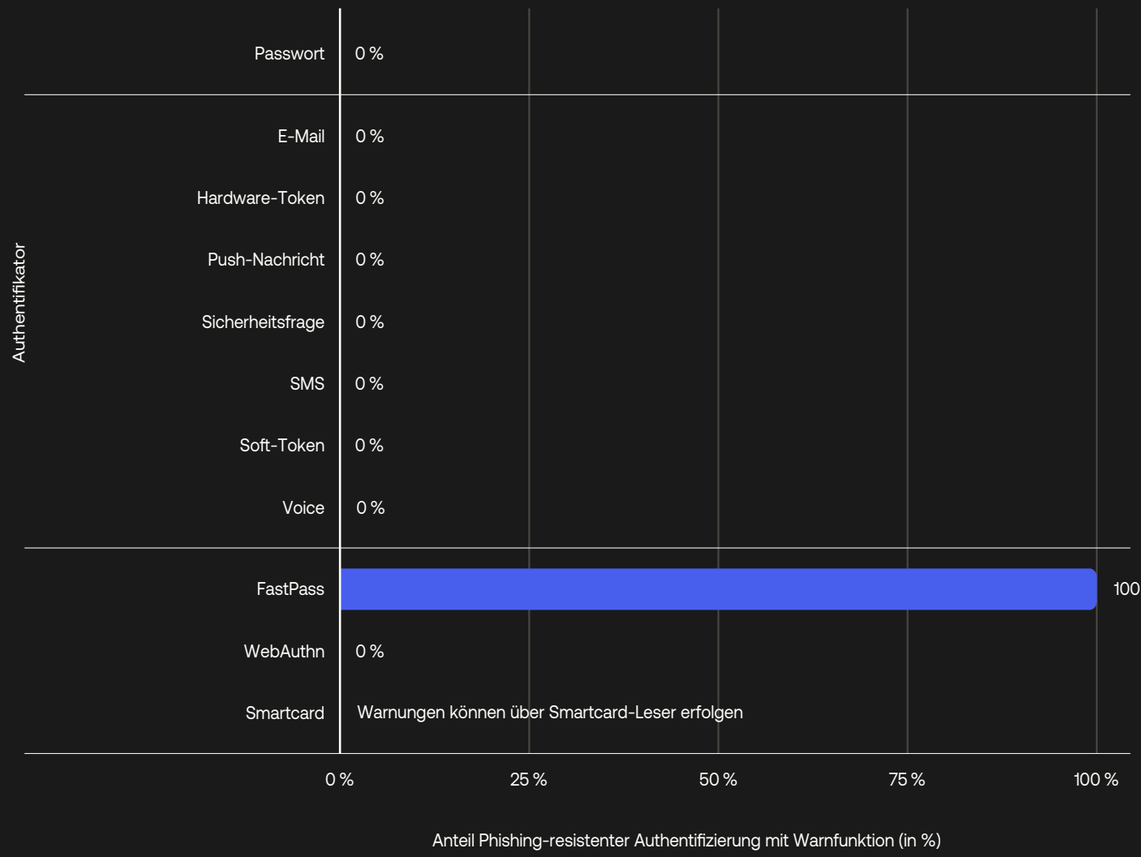

Abbildung 11: Anteil Phishing-resistenter Authentifizierung mit Warnfunktion bei den Authentifikatoren Passwort, E-Mail-Adresse, Hardware-Token, Push-Nachricht, Sicherheitsfrage, SMS, Soft-Token, Voice, FastPass und WebAuthn.

Benutzerkomfort und Sicherheit von Authentifikatoren

Brute-Force-Fehlerquote bei Authentifizierungs-abfragen

Die Brute-Force-Fehlerquote bezeichnet den Anteil der Benutzer mit mehr als N fehlgeschlagenen Authentifizierungsversuchen an einem Tag. Sie wird dargestellt als Anteil der Benutzer, die sich mit dem Authentifikator angemeldet haben.

Ein Brute-Force-Fehler tritt auf, wenn ein gefährlicher oder harmloser Benutzer sich mehr als N Mal nicht authentifizieren kann (wobei N ein Schwellenwert ist, der einen möglichen Brute-Force-Fehler definiert). Für die Analyse in diesem Bericht haben wir N=10 verwendet, da es äußerst unwahrscheinlich ist, dass ein legitimer Benutzer so viele Anmeldungen versuchen würde. Da Bedrohungsakteure das Erraten eines Passworts oder One-Time-Passworts automatisieren oder wiederholte Authentifizierungsabfragen generieren können, um Benutzer zum Gewähren des Zugriffs zu verleiten, spiegeln Brute-Force-Fehler stets eine Präferenz des Angreifers für Brute-Force-Angriffe gegen einen bestimmten Authentifikator wider.

Wie schon im Bericht von 2023 beschrieben, werden wissensbasierte Secrets immer noch am häufigsten von automatisierten Angreifer-Tools attackiert und schaffen gleichzeitig die größten Reibungspunkte für legitime Benutzer, die sich trotz häufiger Fehler mehrfach anzumelden versuchen. FIDO2 WebAuthn weist die geringste Brute-Force-Fehlerquote auf, hat jedoch den oben beschriebenen Haken, dass die Werte in Wirklichkeit höher sein können, weil prinzipbedingt möglicherweise nicht alle Fehler an Okta gemeldet werden.

FastPass funktioniert anders als andere Authentifikatoren und nutzt zwei verschiedene Analysemethoden. Mithilfe von Analysen im Hintergrund oder Authentifizierung im Hintergrund kann das Okta Sign-in-Widget automatisch überprüfen, ob FastPass auf dem Gerät konfiguriert ist und Benutzer ohne deren Interaktion authentifizieren kann. Interaktive Analysen oder Standard-Authentifizierung werden dagegen klassisch ausgelöst, sobald ein Benutzer sich mit einem FastPass-Authentifikator anmeldet. Die Authentifizierung im Hintergrund führt regelmäßige Geräte- und Benutzerprüfungen durch, ohne die Benutzer zu beeinträchtigen. Aus diesem Grund kann die FastPass-Abfrage häufiger als bei anderen Authentifikatortypen durchgeführt werden, was die Fehlerquote der Brute-Force-Abfrage sehr wahrscheinlich verbessert.

Wichtige Erkenntnis

Auch wenn Angriffe mit Umgehung der MFA zunehmen, richten sich klassische Brute-Force-Angriffe immer noch in erster Linie gegen wissensbasierte Authentifikatoren. Authentifikatoren, die auf Besitz- oder biometrischen Faktoren basieren, können die Wahrscheinlichkeit von Account-Hacking aufgrund von Brute-Force-Angriffen erheblich senken.

Brute-Force-Fehlerquote nach Authentifikator

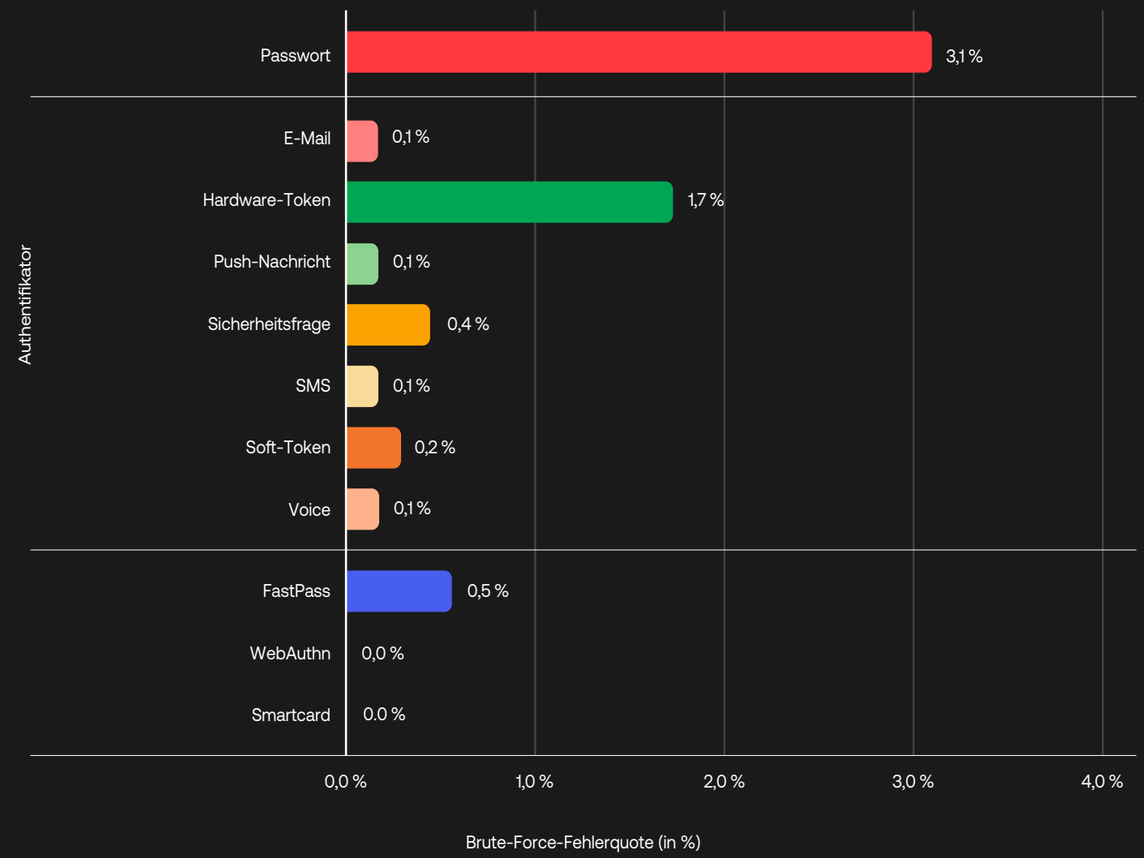

Abbildung 12: Brute-Force-Fehlerquoten bei Authentifizierung mit den Authentifikatoren Passwort, E-Mail-Adresse, Hardware-Token, Push-Nachricht, Sicherheitsfrage, SMS, Soft-Token, Voice, FastPass und WebAuthn. Die Daten wurden zwischen November 2023 und Januar 2024 erfasst.

Benutzerkomfort und Sicherheit von Authentifikatoren

Umfrage zu Authentifikator-Kennzahlen

Im letztjährigen Bericht nutzten wir metrische Gewichtungen zum Beschreiben der relativen Bedeutung der Authentifikator-Kennzahlen. Grundlage für die Gewichtung waren unsere internen Kenntnisse der Authentifikatoreigenschaften sowie ihrer Nutzung durch unsere Kunden.

Nach der Veröffentlichung des Berichts für 2023 suchten wir nach Möglichkeiten, die Kennzahlengewichtung praxisnaher zu gestalten. Zu diesem Zweck führten wir eine Umfrage unter Okta-IT- und Sicherheitsexperten durch, damit wir die relative Bedeutung jeder der Kennzahlen zu Benutzerkomfort und Sicherheit von Authentifikatoren verstehen. Anhand der Ergebnisse dieser Umfrage können wir die Daten aus unseren Protokollen mit den Rückmeldungen von Administratoren abgleichen, wie in Tabelle 2 dargestellt. Dies erlaubt präzisere Schätzungen, als sie früher möglich waren.

Anhand der Umfrageergebnisse konnten wir Werte zu Benutzerkomfort und Sicherheit der Authentifikatoren berechnen. Zuerst normalisierten wir die Kennzahlen jedes Authentifikators anhand der Maximal- und Minimalwerte in einen Bereich von 0 bis 1. So hat WebAuthn beispielsweise eine Fehlerquote von 1, während Passwörter den Wert 0 erhalten. Anschließend gewichteten wir diese Werte entsprechend ihrer Auswirkung auf Benutzerkomfort und Sicherheit des jeweiligen Authentifikators. Dadurch erhalten wir eine Übersicht mit realistischen Bedingungen und Prioritäten. Auf der nächsten Seite sehen Sie, wie Ihr bevorzugter Authentifikator abschneidet.

Wichtige Erkenntnis

Ein zentraler Erfolgsfaktor bei der Stärkung Ihrer Sicherheitsinfrastruktur besteht darin, die enge Abstimmung und Zusammenarbeit von Sicherheits- und IT-Verantwortlichen zu gewährleisten. Die Umfrage zur Kennzahlengewichtung kann bei der Wahl von Authentifizierungsmethoden effektiv Einigkeit bei wichtigen Überlegungen und Risiken herstellen.

Tabelle 2: Benutzerkomfort und Sicherheit von Authentifikatorkategorien

Implementierung		Benutzerkomfort		Sicherheit	
Kennzahl	**Gewichtung**	**Kennzahl**	**Gewichtung**	**Kennzahl**	**Gewichtung**
Nutzungsrate auf Benutzerebene	–	Zeitaufwand für Abfrage	7,33/10	Fehlerquote des Faktors	5,71/10
		Zeitaufwand für Registrierung	5,14/10	Fehlerquote von Brute-Force-Abfragen	7,14/10
		Fehlerquote des Faktors	6,25/10	Anteil Phishing-resistenter Authentifizierung	8,65/10
				Anteil Phishing-resistenter Authentifizierung mit Warnfunktion	7,47/10
Implementierungswerte von Authentifikatoren		**Benutzerkomfortwerte von Authentifikatoren**		**Sicherheitswerte von Authentifikatoren**	

“Der Versuch, Mitarbeiter zur Nutzung individueller und starker Passwörter zu zwingen, ist zum Scheitern verurteilt. Der Vorteil passwortloser MFA-Optionen ist ihr Benutzerkomfort und ihre Sicherheit – was nur selten einhergeht.

Sicherheitsvorteile sind nur dann relevant, wenn sie Unternehmensprozesse beschleunigen und Wachstumsmöglichkeiten schaffen. Passwortlose Authentifizierung erfüllt diese Anforderung voll und ganz. MFA-Faktoren, die auf Passwörter verzichten, sind schneller, einfacher, senken die Kosten und öffnen die Tür für stärkere Integrationspartnerschaften.“

Shana Uhlmann
IT-Leiterin und CISO

Tattarang

Benutzerkomfort und Sicherheit von Authentifikatoren

Bewertung der Performance und Akzeptanz von Authentifikatoren

Phishing-resistente Authentifizierung bietet hervorragende User Experiences

Was bedeutet die Summe dieser Beobachtungen für die Authentifikatoren eines Unternehmens, und wie können IT- und Sicherheitsverantwortliche die Nutzung komfortabler und sicherer Authentifikatoren durchsetzen?

In der IT-Sicherheit wird regelmäßig davon ausgegangen, dass Technikverantwortliche sich für Sicherheit auf Kosten des Benutzerkomforts entscheiden müssten.

Unsere Analyse zeigt, dass diese Wahl falsch ist. Auch wenn die Umfrage nicht die Präferenzen von Benutzern erfasst, zeigen die Rohdaten zur Authentifizierung, dass Phishing-resistente Authentifizierung hervorragende User Experiences bietet. Mit FastPass oder FIDO2 WebAuthn können Benutzer die Sicherheit ihrer Accounts verbessern, ohne beim Nutzungskomfort Abstriche machen zu müssen.

Wichtige Erkenntnis

Die Implementierung von MFA und passwortloser Authentifizierung in großem Maßstab ist mehr eine Frage der Unternehmenskultur als der Technik. Unternehmen benötigen Wahlmöglichkeiten und Flexibilität. Die Okta Identity-Plattform bietet verschiedene Optionen, die den individuellen Anforderungen Ihres Unternehmens Rechnung tragen. Sie können die Methodik und das Framework anwenden, das am besten für Sie passt. Wir hoffen, dass unser Ansatz bei der Definition der relativen Gewichtung von Authentifikatoreigenschaften sowie der Abstimmung dieser Kennzahlen mit wichtigen Stakeholdern Sie motiviert, die Nutzung stärkerer Authentifizierung in Ihrem Unternehmen zu propagieren.

Abbildung 7: Zeitaufwand für Authentifizierungsabfragen

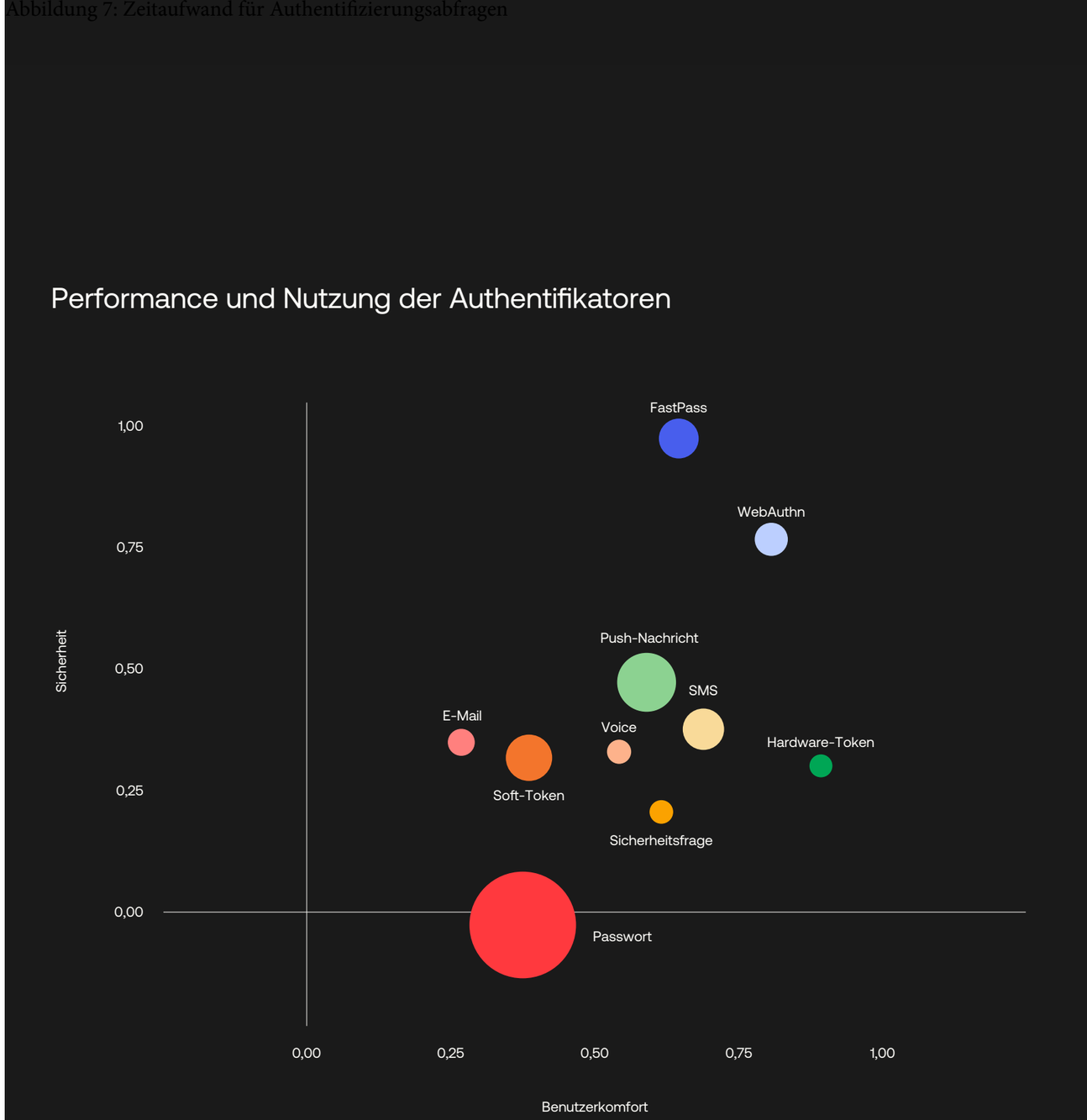

Abbildung 13: Performance und Nutzung der Authentifikatoren Passwort, E-Mail-Adresse, Hardware-Token, Push-Nachricht, Sicherheitsfragen, SMS, Soft-Token, Voice, FastPass und WebAuthn. Die Performance jedes Authentifikators wird durch Benutzerkomfort und Sicherheit in einer 2x2-Matrix dargestellt. Die Größe des Kreises stellt die Nutzungsrate des Authentifikators auf einer Skala von 0 % bis 100 % dar.

Der Weg in die Zukunft

Angesichts des Erfolgs der Angreifer bei Phishing- und Social-Engineering-Techniken in den letzten 12 Monaten sollte Phishing-resistente Authentifizierung eigentlich stärker vertreten sein. In den Monaten seit der Erfassung dieser Daten rückte eine Reihe schwerwiegender Sicherheitsereignisse dieses Problem ins Rampenlicht. Salesforce, GitHub, Okta und Microsoft haben die verpflichtende Nutzung von MFA für Teile ihrer Benutzerbasis eingeführt. Die Implementierung von FastPass unter Okta-Kunden nimmt stetig zu, und in den Vorständen werden Sorgen wegen neuer Phishing-Bedrohungen aufgrund der Evolution von KI laut. Wir können also optimistisch sein!

Phishing-resistente MFA ist sicher, komfortabel und mit überschaubarem Aufwand umsetzbar. Für Administratoren und Benutzer ist das eine Win-Win-Situation, denn diese Technologie schützt am besten vor den allgegenwärtigen Bedrohungen. Deshalb müssen wir unsere Unternehmen bei der Implementierung unterstützen. Wir bei Okta hoffen, dass Ihnen dieser Bericht die Möglichkeit gibt, Ihr Unternehmen mit Ihren Mitbewerbern zu vergleichen und Führungskräfte sowie Benutzer in Gesprächen vom Wechsel zu stärkerer und unkomplizierter Authentifizierung zu überzeugen.

Wenn Sie an individueller Beratung interessiert sind, kontaktieren Sie uns gern. Wir unterstützen Sie dabei, die Sicherheit Ihres Unternehmens und die Zufriedenheit Ihre Benutzer zu vergrößern.

Fünf Tipps zur Verbesserung Ihrer Authentifizierungsstrategie

Auch wenn der Wechsel zu einer starken Authentifizierungsstrategie häufig aufwändig erscheint, können Unternehmen diesen Weg mit relativ einfachen Schritten beginnen.

1. Legen Sie in Ihren Richtlinien fest, dass für die Anmeldung MFA und für den Administratorzugriff auf vertrauliche Anwendungen und Daten Phishing-resistente Authentifizierung erforderlich ist. Wir empfehlen dringend, die Phishing-resistenten Optionen und die Device Assurance-Funktionen unserer passwortlosen Authentifizierungslösung Okta FastPass zu verwenden.

2. Weisen Sie Ihre Führungskräfte und den Vorstand darauf hin, dass die Implementierung von MFA Priorität haben sollte. Da MFA enorm dazu beitragen kann, die wertvollsten Ressourcen und Informationen zu schützen, sollte die Implementierungsrate der Unternehmensführung bekannt sein.

3. Setzen Sie bei Zugriffen auf einen Zero-Trust-Ansatz. Bei diesem Ansatz werden die Zugriffsrechte entsprechend den Identity-Eigenschaften für die jeweilige Session und nach dem Least-Privilege-Prinzip gewährt. Gleichzeitig werden die Sicherheitsanforderungen der angeforderten Anwendung bzw. der Daten berücksichtigt.

4. Erstellen Sie dynamische Zugriffsrichtlinien, die Benutzerattribute, den Gerätekontext (ist das Gerät bekannt, verwaltet und bietet starke Sicherheit), Netzwerkattribute (ist das Netzwerk vertrauenswürdig) und die Konsistenz der Anfrage mit früherem Benutzerverhalten berücksichtigen.

5. Entwickeln Sie einen Plan, um die Nutzung von Passwörtern reduzieren bzw. langfristig auf die Nutzung von Passwörtern verzichten zu können.

Methodik

Für diesen Bericht nutzten wir Daten von Okta Workforce Identity Cloud. Wir haben Daten von Milliarden monatlichen Authentifizierungen und Verifizierungen aus Ländern auf der ganzen Welt anonymisiert und aggregiert. Unsere Kunden und ihre Mitarbeiter, Auftragnehmer, Partner und Kunden melden sich mit Okta auf Geräten, in Anwendungen und bei Diensten an, und mit unseren Sicherheitsfunktionen schützen sie zudem ihre vertraulichen Daten. Wir haben Kunden aus allen wichtigen Branchen und unterschiedlichen Unternehmensgrößen, von kleinen Firmen bis hin zu den weltgrößten Unternehmen.

Die Unternehmensgröße wird definiert durch die Anzahl der Vollzeitangestellten. Die Branchentaxonomie entspricht dem North American Industry Classification System (NAICS). Die Größe, Branche und geografische Region des Kunden werden von Drittanbieter-Ressourcen validiert.

Sofern nicht anders angegeben, bezieht sich dieser Bericht ausschließlich auf die Daten der Okta Workforce Identity Cloud und auf Use Cases im Bereich Workforce Identity. Es wurden keine Daten von Okta Customer Identity Cloud ausgewertet.

Über Okta

Okta ist das weltweit führende Identity-Unternehmen. Als ein führender unabhängiger Identity-Anbieter ermöglichen wir es unseren Partnern und Kunden, jede Technologie sicher zu nutzen – überall, mit jedem Gerät und jeder Anwendung. Die weltweit renommiertesten Marken vertrauen beim Schutz von Zugriff, Authentifizierung und Automatisierung auf Okta. Im Mittelpunkt unserer Okta Workforce Identity Cloud sowie der Okta Customer Identity Cloud stehen Flexibilität und Neutralität. Mit unseren individualisierbaren Lösungen und unseren über 7.000 vorkonfigurierten Integrationen können sich Führungskräfte und Entwickler ganz auf neue Innovationen und eine rasche Digitalisierung konzentrieren. Wir entwickeln eine Welt, in der Ihre Identity ganz Ihnen gehört. Weitere Informationen finden Sie unter okta.com/de.

okta

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