Whitepaper

Ihr Guide zur MFA-Integration

Januar 2023

Inhalt

Einführung: Wie Sie Ihr Security-Standing im Zeitalter der Mega-Breaches stärken

Die Zahl raffinierter mehrstufiger Angriffe nimmt immer weiter zu, und bei einem Großteil davon spielen kompromittierte Zugangsdaten eine Schlüsselrolle. Ein aktueller Report kommt zu dem Schluss, dass E-Mail-basierte Attacken auf Unternehmen in der ersten Hälfte 2022 um 48 % zugenommen haben. Im Vergleich zum vorhergehenden Sechs-Monats-Zeitraum zielten mehr als zwei Drittel dieser Attacken darauf ab, Zugangsdaten zu stehlen (z. B. E-Mails mit bösartigem Link, die dafür designt waren, sensible Account-Daten zu stehlen). Die Angreifer gaben sich dabei als 265 unterschiedliche Unternehmen aus.

Die Cyberkriminellen machen sich die flächendeckende Einführung hybrider Arbeitsmodelle zunutze: Sie setzen vermehrt auf Social-Engineering-Attacken wie Phishing und missbrauchen gestohlene Daten, um die Accounts legitimer Benutzer zu übernehmen. Die Folge: Multi-Faktor-Authentifizierung (MFA) entwickelt sich mehr und mehr zur wichtigsten Abwehrmaßnahme, um sicherzustellen, dass jeder Benutzer auch wirklich der ist, der er zu sein vorgibt. MFA ermöglicht es Unternehmen, den Zugang zu ihren Ressourcen in der von Remote- und Hybrid-Arbeit geprägten Welt von heute zuverlässig zu schützen – einschließlich ihrer Web-basierten und mobilen Kunden- und Workplace-Anwendungen. Regierungen, Gesetzgeber und Unternehmen haben verstanden, wie wichtig MFA für die Einführung robuster Zero-Trust-Modelle („Niemals vertrauen. Immer verifizieren.“) ist.

Kurz: MFA ist heute ein integraler Bestandteil robuster, Identity-basierter Security-Strategien. Oder, um es an einem konkreten Beispiel festzumachen: Eine im Januar 2022 vom „Office of Management and Budget“ des US-Präsidenten erlassene Executive Order definiert Phishing-resistente MFA als eine zentrale Anforderung

bei der Modernisierung der Cybersecurity in den US-Bundesbehörden. Regierungen, Unternehmen und Cyberkriminelle entwickeln sich stetig weiter. Damit ändern sich auch die Vorgaben an die MFA – etwa mit Blick auf den Siegeszug der passwortlosen Authentifizierung oder die zunehmende Bedeutung von (verwalteten und nicht verwalteten) Devices für die Bewertung des Security-Standings.

Dieser Guide soll Ihnen bewährte Best Practices vermitteln, um das volle Potenzial Ihrer MFA-Lösung zu erschließen – einschließlich des Upgrades auf passwortlose Authentisierung. Dabei gehen wir auch auf die Ergebnisse einer Umfrage ein, die wir gemeinsam mit IDG durchgeführt haben, und die die Schlüsselrolle des Identity & Access Managements (IAM) in modernen Authentisierungs- und Security-Umgebungen unterstreicht. Und wir werden darüber sprechen, welche Prioritäten und Trends in anderen Unternehmen besonders hoch im Kurs stehen. Zusätzlich werden wir diesen Guide nutzen, um für Sie die wichtigsten Elemente zusammenzufassen, die es beim Design einer MFA-Lösung zu bedenken gilt. Dazu gehören beispielsweise:

- die Implementierung Phishing-resistenter Technologien
- das Verständnis von Policies und Compliance-Vorgaben; und
- die Berücksichtigung neuer Access-Anforderungen.

Aufsetzend auf unseren Beobachtungen bei der Zusammenarbeit mit Entwicklungs- und Produktteams beenden wir den Guide mit praktischen Tipps für Leser, die aktuell MFA für ihre eigenen Anwendungen entwickeln.

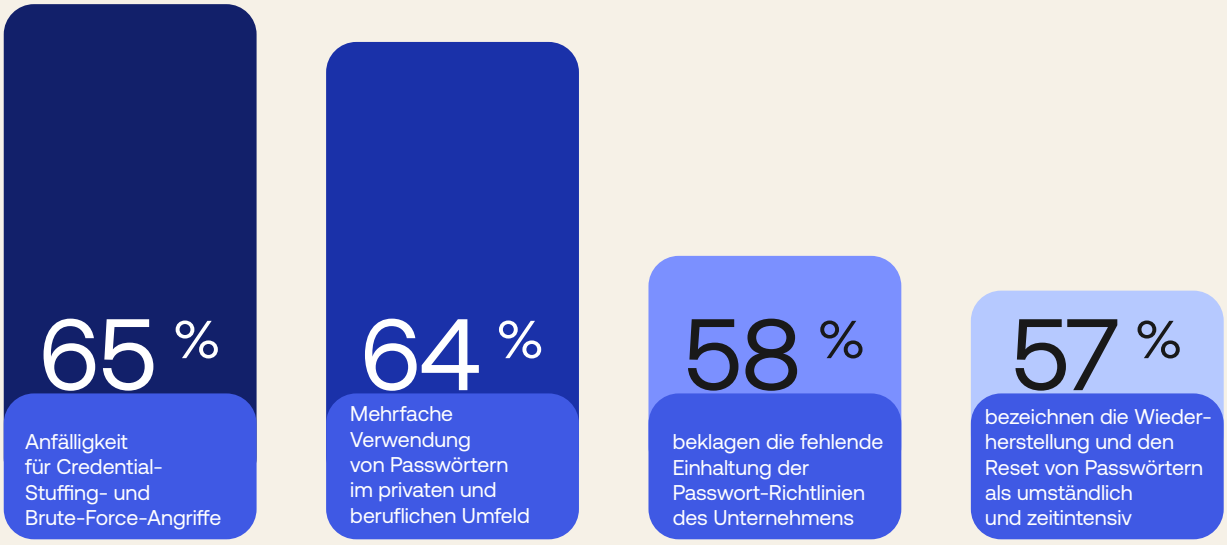
Integrieren Sie Phishing-resistente MFA als integralen Bestandteil Ihrer IAM-Strategie

Identitäts-basierte Angriffe können heute die unterschiedlichsten Formen annehmen, darunter Malware, Hacking und Phishing. Die Konsequenzen sind der Diebstahl von Zugangsdaten, die Kompromittierung von Accounts und der Diebstahl von Daten. Um diesen Bedrohungen einen Riegel vorzuschieben, müssen Unternehmen ihr Security-Standing verbessern – und die erste Verteidigungslinie sind die digitalen Identitäten. Unternehmen, die sich dabei auf Legacy-Technologien wie On-Premises betriebene Apps und Firewalls verlassen, haben den zunehmend raffinierten Angriffen von heute nur wenig entgegenzusetzen. Sie verlassen sich beim Schutz ihres Unternehmens und ihrer Mitarbeitenden letztlich auf langsame, komplexe und fragmentierte Frameworks.

Aber sehen wir uns die Zahlen näher an: Unsere gemeinsam mit IDG unter IT- und Security-Verantwortlichen durchgeführte Umfrage beleuchtet einige konkrete Herausforderungen und Fakten rund um die sichere Authentisierung.

Die wichtigsten Bedenken bei der Verwendung von Passwörtern

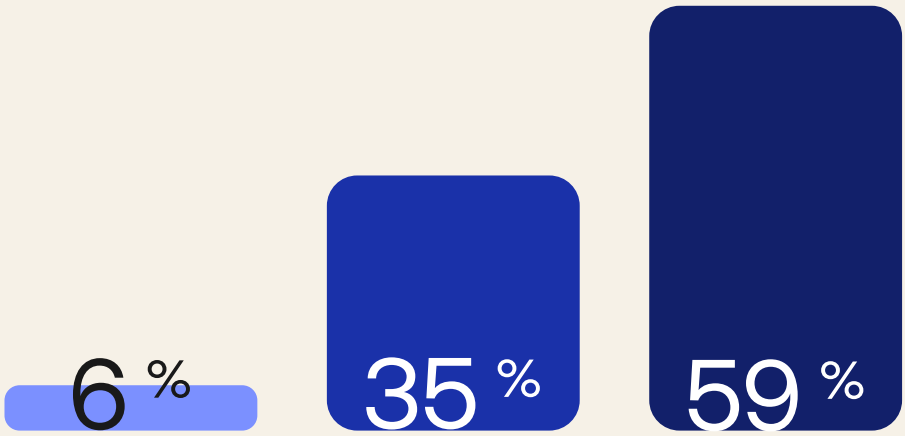
1.000+ Mitarbeitende	**70 %**
500-999 Mitarbeitende	**52 %**



Erkenntnis: Die Befragten nennen mehrere potenzielle Gefahren im Zusammenhang mit Passwörtern – darunter gestohlene Zugangsdaten oder die Mehrfachnutzung von Passwörtern für dienstliche und private Accounts.

Welcher MFA-Level für Unternehmen am sinnvollsten ist

VP IT oder höher	**73 %**
IT-Leiter/IT-Manager	**53 %**



Grundlegend: Nur Passwort und Sicherheitsfrage

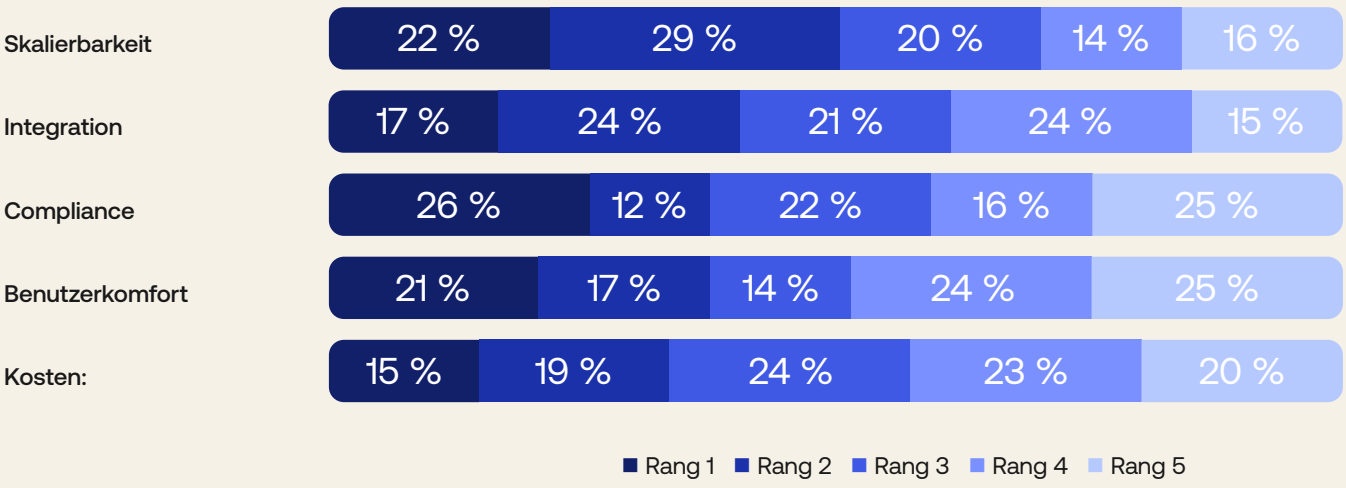
Mittel: SMS-/Voice-/ E-Mail-Verifizierung

Stark: Passwortlos, YubiKey, Smartcard, Biometrie

Erkenntnis: Mehr als die Hälfte (59 %) der Befragten gibt an, die stärkste MFA-Lösung auf dem Markt sei für ihr Unternehmen am besten geeignet.

Stellenwert der Kriterien bei der Auswahl einer MFA-Lösung

Wir haben die Unternehmen gebeten, alle fünf Kriterien zu klassifizieren – vom wichtigsten zum unwichtigsten



Erkenntnis: 51 % bewerten Skalierbarkeit als einen der zwei wichtigsten Faktoren bei der Auswahl einer MFA-Lösung.

Bewerten Sie das Sicherheits-niveau der verschiedenen Authentisie-rungsfaktoren

Vereinfacht gesprochen, überprüft die Authentisierung die Identität anhand von drei Faktor-Typen:

- Etwas, das Sie wissen (ein Passwort)
- Etwas, das Sie besitzen (eine persönliche Smartcard zur Verifizierung der Identität)
- Etwas, das Sie sind (ein Fingerabdruck)

Um ein höheres Maß an Sicherheit zu erreichen, kombiniert MFA zwei oder mehr dieser Faktor-Typen. Die gängigste Variante ist die Kombination eines Passworts mit einem Zeit-basierten Token, einer Push-Benachrichtigung auf eine Mobile-App oder einem biometrischen Faktor. Es gibt aber auch andere MFA-Ansätze. Sie alle haben spezifische Vor- und Nachteile.

Auf dem Markt sind unterschiedliche Arten von Authentifikatoren unterschiedlicher Stärke verfügbar. Hier bei Okta klassifizieren wir die Stärke der Authentifikatoren folgendermaßen:

NIEDRIG: Passwörter, Sicherheitsfrage, One-Time-Passwort (OTPs) via SMS, Voice oder E-Mail, und OTP-Anwendungen wie Authy und Google Authenticator

MITTEL: Mobile Push-Benachrichtigungen und OTPs mit physikalischem Token

HOCH: Personal Identity Verification-(PIV-) oder Common Access Card-(CAC-)Smartcards, FIDO 2.0 / WebAuthn + CTAP2

Das Sicherheitsniveau ist für Unternehmen, die ihre MFA verbessern möchten, aber nicht der einzige entscheidende Faktor. Die Authentifikatoren müssen sich auch einfach bereitstellen lassen und für Mitarbeitende und Kunden leicht zu bedienen sein. Und sie müssen einen zuverlässigen Schutz vor gängigen Angriffen wie Man-in-the-Middle (MitM) und Adversary-in-the-Middle (AitM) bieten. Aber letztlich gibt es keine Alternative zu einer robusten Security mit hochsicheren Faktoren.

SMS als Faktor anzubieten, mag ein probater Weg sein, um Benutzer einfach und schnell an Ihre MFA anzubinden. Aber das Sicherheitsniveau der Lösung ist nicht besonders hoch. Viele gängige Sicherheitsprobleme – etwa SIM-Hijacking oder hoch skalierte „Smishing-&-Vishing“-Attacken – sind in der Lage, die Sicherheitsmechanismen der SMS-Authentisierung zu umgehen. Daher empfehlen wir dringend die Verwendung stärkerer MFA-Faktoren wie Okta Verify Push oder biometrischer Faktoren (via WebAuthn oder, im Falle von U.S.-Regierungsbehörden, PIV-/CAC-Smartcards).

Best Practices für eine starke MFA

1. Definieren Sie Ihre MFA-Policies mit Bedacht und überprüfen Sie sie regelmäßig

Bevor Sie eine MFA-Lösung implementieren, sollten Sie sich einen Überblick über die Security-Risiken und die konkreten Bedrohungen, denen Ihr Unternehmen ausgesetzt ist, verschaffen. Welche Ressourcen und welche Angriffsvektoren bereiten Ihnen besonders viel Kopfzerbrechen? Ihre Policy sollte durchdacht und Risiko-basiert konfiguriert sein, um bei besonders riskanten Zugriffen automatisch eine strengere Authentisierung anzustoßen.

So kann die Policy zum Beispiel sicherstellen, dass bei Zugriffen über ein unbekanntes Netzwerk alle acht Stunden ein zweiter Faktor angefordert wird, oder den zweiten Faktor nur dann abfragen, wenn es sich um ein neues Gerät oder einen neuen Standort handelt. Vielleicht gibt es bei Ihnen auch eine bestimmte Gruppe von User-Accounts mit besonders umfangreichen Zugriffsrechten auf sensible Daten – und diese erfordern eine strengere Policy. Ein typisches Beispiel könnten die Entwickler in Ihrem Unternehmen sein, die auf Ihren Code zugreifen können, oder das Management mit weit gefassten Zugriffsrechten auf sensible Daten. Sie können für diese Gruppen strengere Faktor-Typen vorgeben, oder sie auffordern, zusätzliche MFA-Prompts zu beantworten. Mitunter ist es auch überlegenswert, MFA für besonders sensible Aktivitäten innerhalb einer Anwendung zu implementieren. Feingranulare Kontrollmechanismen für hochgradig sensible Aktionen (etwa die Zustimmung zu einem Einkauf oder einer Überweisung) minimieren nicht nur Ihre Risiken, sondern erleichtern auch die Einhaltung geltender Compliance-Vorgaben.

Letzten Endes sollte die zusätzliche Verifikation aber stets so transparent und so komfortabel wie möglich sein. So garantieren Sie eine hochwertige User-Experience, ohne Abstriche bei der Sicherheit in Kauf zu nehmen.

2. Berücksichtigen Sie bei der Planung unterschiedlichste Zugangsszenarien

Für Benutzer mit Internetzugang, aber eingeschränktem oder gar keinem Service ihres Mobilfunkanbieters – etwa in einem WLAN-fähigen Flugzeug, einem Haus auf dem Land oder im Keller eines Betongebäudes – sind Voice- und SMS-basierte Faktoren oft keine Option. In diesen Fällen ist Okta Verify mit Push oder ein One-Time-Password (OTP) die bessere Alternative, da diese Kommunikation über die Internetverbindung des Telefons verschlüsselt erfolgt. Hardware-Devices, die Event- oder Zeit-basierte One-Time-Passwords (TOTP) generieren, benötigen gar keinen Kommunikationskanal und sind schwer zu manipulieren oder zu kopieren. Die Bereitstellung dieser physischen Devices ist jedoch relativ kostspielig. Hinzu kommt, dass die Mitarbeiter sie leicht zu Hause vergessen oder verlieren können. Daher sind diese Faktor-Typen nicht die beste Wahl, wenn es gilt, externe, zeitlich befristete Partner oder Positionen mit hoher Fluktuation anzubinden.

Unternehmen sollten eine MFA-Lösung implementieren, die eine möglichst breite Palette von Szenarien abdeckt. Eine Lösung von der Stange, die in allen Einsatzbereichen überzeugt, gibt es in der Regel aber nicht. Die folgenden Tipps helfen Ihnen, Ihren Anwendern einen zuverlässigen Schutz und eine hochwertige User-Experience zu bieten:

- Lassen Sie Anwender stets zwischen mehreren Faktoren wählen. So haben sie jederzeit einen Plan B. Handelt es sich bei einem Faktor um ein Passwort, sollten Sie sicherstellen, dass kompromittierte Passwörter frühzeitig identifiziert werden. So können Sie Anwender im Ernstfall rasch sperren und die Verwendung der gestohlenen Passwörter unterbinden.
- Implementieren Sie ausschließlich starke, Phishing-resistente Faktor-Typen. Treiben Sie, wenn möglich, die Einführung von passwortloser MFA oder (im Falle von US-Regierungsbehörden) von PIV-/CIC-Smartcards voran.
- Validieren Sie vor der Authentisierung die Herkunft von Web-URLs. Zugangsdaten sollten stets mit der Domäne verknüpft sein, von der der Zugangs-Request stammt.
- Wenn es Ihre Hardware unterstützt, sollten Sie den Anwendern gestatten, Biometrie als sekundären Faktor zu verwenden (etwa Windows Hello oder Touch ID). So sorgen Sie für eine hochwertige User-Experience und erhalten ein höheres Maß an Gewissheit darüber, dass der Anwender auch wirklich der ist, der er zu sein vorgibt.

3. Setzen Sie im Rahmen Ihrer MFA-Policy hochsichere und Phishing-resistente Authentisierungsfaktoren für sensible Apps durch

Wie bereits erwähnt, sind nicht alle Authentifikatoren Phishing-resistent. Die verschiedenen Faktoren bieten einen unterschiedlich robusten Schutz vor Social-Engineering-Angriffen. Letzten Endes bedeutet für den Angreifer aber jeder Faktor zusätzliche Kosten und Mehraufwand beim Versuch, einen Account zu übernehmen. So lassen sich SMS-basierte OTPs relativ einfach abfangen. Push-Authentifikatoren bieten einen besseren Schutz vor statischen, auf Zugangsdaten abzielenden Angriffen als Authentifikatoren, die sich ausschließlich auf OTPs verlassen.

Kombiniert man Push mit einer Number Challenge, bei der der Benutzer, der eine Push-Anfrage verifiziert, aufgefordert wird, eine auf der Anmeldeseite angezeigte Ziffernfolge zu identifizieren, erreichen Sie ein hohes Maß an Schutz vor einer Vielzahl gängiger Angriffstechniken, einschließlich „MFA Fatigue“-Angriffen. Hardware-basierte Authentifikatoren bieten das höchste Maß an Sicherheit.

Die zuverlässigste Definition der Phishing-Resistenz liefert uns das US National Institute of Standards and Technology (NIST). Gemäß der Definition des NIST setzt Phishing-Resistenz voraus, dass der zu authentifizierende Kanal kryptographisch mit der Ausgabe des Authentifikators verknüpft ist. Vereinfacht gesprochen bedeutet dies, dass die Domäne (d. h. die Adresse) der Website, bei der Sie sich anmelden, mit Ihrem Authentifikator verknüpft ist. Auf diese Weise wird sichergestellt, dass Ihre Anmeldedaten nicht an eine Phishing-Webseite weitergeleitet werden.

Die Okta Plattform unterstützt mehrere Faktoren, die dieser Definition gerecht werden. Okta unterstützt roamende FIDO2 WebAuthn-Authentifikatoren (d.h. Security-Keys) und Device-gebundene FIDO2 WebAuthn-Authentifikatoren (z.B. FaceID, TouchID oder Windows Hello). Außerdem unterstützen wir die Verwendung von PIV-Smartcards innerhalb der Sign-on-Policy einer App, um auf spezifische Anwendungen zuzugreifen. Je nachdem, für welches Deployment-Modell Sie sich entschieden haben, kann auch Okta FastPass (unser Device-gebundener, passwortloser Authentifikator) diese Definition erfüllen. Die obligatorische Verwendung von mindestens einem Phishing-resistenten Authentifikator eliminiert die Gefahr, die von raffinierten Phishing-Angriffen, Social Engineering und AitM-Attacken ausgeht.

4. Überprüfen Sie sorgfältig die Compliance-Vorgaben

Die meisten IT-Compliance-Standards, etwa PCI DSS, SOX und HIPAA, schreiben eine robuste Authentifizierung der Benutzer vor – und sind damit einer der wichtigsten Treiber für die MFA-Einführung. Um diese und ähnliche Standards zu erfüllen, müssen Sie deren Anforderungen genau kennen. Nur so können Sie Ihre Konfiguration und Ihre Policies entsprechend anpassen. So erfordern beispielsweise die PCI und die HIPAA eine starke Authentifizierung, die mindestens zwei von drei starken Authentifizierungsverfahren unterstützt. Der SOX-Standard konzentriert sich weniger auf die Technologie als vielmehr auf die Bestehung eines Audits. Auch dabei müssen Sie aber nachweisen, dass die Finanz- und Buchhaltungsdaten Ihres Unternehmens sicher sind. Zur IT-Compliance gehört es, die einschlägigen Normen umzusetzen und deren Einhaltung zu dokumentieren. Stellen Sie im Rahmen Ihrer Konfigurations- und Implementierungsprozesse auch eine sorgfältige Dokumentation der Abläufe sicher. So können Sie bei einem Audit jederzeit alle geforderten Nachweise erbringen. Ihr künftiges Ich (und Ihr Unternehmen) werden es Ihnen danken.

5. Integrieren Sie MFA mit Blick auf die zunehmend hybride Workforce

Immer mehr remote und hybrid agierende Mitarbeitende und Partner greifen heute auf Ressourcen in der Cloud zu. Eine starke Security ist damit unerlässlich. Idealerweise sollten neue Mitarbeitende vor Ort im Office eingewiesen werden, wo die Kollegen aus der IT persönlich verfügbar sind. Aber die Remote-Modelle von heute bergen mit Blick auf die MFA-Implementierung und das Troubleshooting neue Herausforderungen.

Um die MFA-Einführung zu beschleunigen, haben sich Faktoren bewährt, mit denen die Mitarbeitenden sofort loslegen können (etwa im Mobilgerät integrierte Biometrie-Scanner oder Mobile-App-Authentifikatoren wie Okta Verify) – eine zeitnah verfügbare Alternative zu Hardware-Tokens, die ihnen zugesandt werden müssen. So können Ihre Neueinsteiger schneller auf die Ressourcen zugreifen, die sie für einen erfolgreichen Start brauchen.
Beim Remote-Onboarding neuer Mitarbeiter setzen einige Unternehmen heute auf virtuelle Sessions, und senden neuen Kollegen die Setup-Informationen an die private E-Mail-Adresse, damit sich diese einlesen können, obwohl sie noch gar keinen Zugang zu ihrem Unternehmens-Account haben.

6. Rechnen Sie damit, dass Devices verloren gehen

Immer mehr Unternehmen führen BYOD-(Bring-Your-Own-Device-) Modelle ein und ermöglichen es Mitarbeitern, über private Mobilgeräte auf Unternehmensdaten zuzugreifen. Diese nicht zentral gemanagten Geräte gehen jedoch mit einigen erheblichen Sicherheitsrisiken einher.
In vielen Unternehmen mit BYOD-Policy werden diese Geräte für Angriffe missbraucht – ein gefährlicher Bedrohungsvektor, den es zu schließen gilt.

Dedizierte Device-Assurance-Policies ermöglichen es Ihnen, im Rahmen der Authentisierungsrichtlinien auch sicherheitskritische Device-Attribute zu überprüfen – etwa die Betriebssystemversion, die Festplattenverschlüsselung und die Jailbreak-/Root-Erkennung. Damit dient die Device-Assurance-Policy als zusätzliche Security-Ebene, die über die Authentifizierungsrichtlinie hinaus den Security-Status des Geräts überwacht.

Ein weiterer wichtiger Aspekt ist es, dass Mitarbeitende regelmäßig Unternehmensdaten auf ihre Desktops und Laptops herunterladen. Daher sollten Ihre Benutzer nach der Eingabe ihres Passworts stets eine zusätzliche MFA-Challenge beantworten müssen, um ihren Rechner zu entsperren.
Die meisten Compliance-Richtlinien geben den Einsatz einer MFA-Lösung vor – und die Option, diese auf Device-Ebene zu implementieren, minimiert das Risiko Desktop-bezogener Angriffe und schützt sensible Daten, wenn ein Laptop verloren geht oder gestohlen wird.

Doch alles, was ein Benutzer hat, kann er auch verlieren. Daher sollte das Playbook Ihres IT-Helpdesks klare Prozesse für den Umgang mit verlorenen Devices vorgeben. Stellen Sie sicher, dass jedes Mal, wenn ein für die MFA verwendetes Gerät als verloren gemeldet wird, die folgenden Schritte ablaufen:

- Schließung aller offenen Sessions und Aufforderung des Benutzers, sich neu zu authentifizieren
- Trennung des Geräts vom Benutzerkonto und den Zugriffsrechten des Benutzers
- Remotes Löschen der Unternehmensdaten auf dem Mobilgerät (wie es typischerweise auf unternehmenseigenen Geräten geschieht)

Darüber hinaus ist es wichtig, die Aktivitäten des Benutzerkontos vor dem Zeitpunkt des Device-Verlusts mit Blick auf ungewöhnliche Aktivitäten zu überprüfen. Wenn Sie etwas Verdächtiges bemerken, sollten Sie die Möglichkeit eines Angriffs in Betracht ziehen und die Situation entsprechend eskalieren. Sobald Sie die vorrangigen Security-Bedenken ausgeräumt haben, sollten Sie sich darauf fokussieren, den Mitarbeitenden mit einem Ersatzgerät oder einem neuen Zugang wieder einsatzfähig zu machen. Oft genügt beispielsweise ein Anruf beim IT-Helpdesk, um die Identität des Mitarbeiters zu prüfen. So kann dieser wieder produktiv arbeiten, während Sie neue Faktoren für ihn implementieren.

7. Setzen Sie sich mit Adaptiver MFA auseinander

Eine mehrstufige MFA lässt Ihnen die Kontrolle, wann und wie die Multi-Faktor-Authentisierung angewendet werden soll. Allerdings sollten Sie bei der Konfiguration höchste Sorgfalt walten lassen. Selbst bei klar definierten Policies und Kriterien ist es mitunter empfehlenswert, die Zugangsentscheidungen dynamisch anhand des Benutzer- oder Device-Kontexts zu treffen.

Adaptive MFA basiert auf der Analyse von Zugriffsmustern und – darauf aufsetzend – auf der Anpassung der Policy für einzelne Benutzer und Gruppen. So wird für einen Anwender, der viel reist und häufig im Ausland seine E-Mails checkt, nur selten ein zweiter Authentisierungsfaktor erforderlich sein. Bei einem Mitarbeiter hingegen, der niemals verreist, wird schon beim ersten internationalen Zugriff eine MFA-Challenge erfolgen. Risiko-basierte Policies, etwa die mehrstufige Authentisierung beim versuchten Zugriff über einen unautorisierten Proxy oder das automatische Blockieren von Zugriffen über bekanntermaßen bösartige IPs, können auch über verdächtige Events ausgelöst werden. Adaptive MFA ist ein mächtiges Werkzeug, um mit der Zeit automatisch dynamische Policies zu entwickeln – Policies, die Ihrem Unternehmen den Schutz bieten, den es benötigt, und die flexibel genug sind, um den individuellen Anforderungen jedes Anwenders Rechnung zu tragen.

8. Planen Sie Ihr Deployment

Komplexe Deployments und Policies funktionieren nur selten vom ersten Tag an. Wenn ein neuer Prozess auf alle Mitarbeitenden ausstrahlt, sollten Sie seine Wirksamkeit ab dem Rollout durchgehend kontrollieren, und vorbereitet sein, die Policies auf der Basis Ihrer Beobachtungen anzupassen. Planen Sie das Deployment so, dass die MFA-Lösung zunächst für Ihre IT- und Security-Teams ausgerollt wird. Dann können Sie schrittweise weitere Benutzergruppen anbinden. Machen Sie sich so früh wie möglich mit den Audit-Funktionalitäten vertraut – sie werden schon bald eine unschätzbare Hilfe beim Troubleshooting und bei der Anpassung der Policy-Konfiguration sein.

Wenn Sie beispielsweise MFA für eine bestimmte Gruppe oder bestimmte Anwender ausrollen, helfen Ihnen die Audit-Werkzeuge, die Einführung und Verwendung punktuell zu prüfen. Versuchen Sie, einen Feedback-Mechanismus für Ihre Anwender einzuführen. Ihre Anwender werden sich nicht immer die Zeit nehmen, ein schriftliches Feedback zu geben. Aber mit einem Audit-Trail erhalten Sie zumindest ein gewisses Maß an Transparenz über die User-Experience. Hat ein Benutzer drei Anläufe gebraucht, um sein OTP einzugeben? Hat er schließlich aufgegeben? Diese Probleme sind oft ein Indiz für eine fehlerhafte Konfiguration, fehlendes Wissen auf Seiten der Anwender oder ein Szenario, dass im ersten Rollout-Plan einfach nicht vorgesehen war. Wenn Sie die Audit-Werkzeuge nutzen und auf das Feedback der Anwender hören, erhalten alle Stakeholder die Gewissheit, dass die Lösung funktioniert, wie sie soll, und dass alle Policies erfolgreich umgesetzt werden.

9. Schulen Sie Ihre Anwender

Zu den wichtigsten Security-Best-Practices in der digitalen Welt von heute gehört es, sich durch den Einsatz von MFA vor den Gefahren unsicherer Passwörter zu schützen. Einige Anwender werden dies als aufwändig empfinden, und glauben, dass sie dieser zusätzliche Schritt unnötig viel Zeit kostet. Daher ist es wichtig, dass jeder Ihrer Kollegen – vom Management über das IT- und Security-Team bis hin zu den Endanwendern – vom ersten Tag an versteht, warum Sie MFA einführen. Wenn das gesamte Unternehmen eingebunden wird, müssen Sie sich nicht um die Akzeptanz der Lösung sorgen, und jeder versteht, dass er auf diese Weise zur Sicherheit aller beiträgt. Schulungen helfen Ihren Mitarbeitenden, zu verinnerlichen, dass ein besserer Schutz manchmal einen zusätzlichen Handgriff lohnt.

Ein typischer Ansatz ist es, dass die IT die anstehenden Veränderungen per E-Mail ankündigt. Ein anderer sind simulierte Phishing-Trainings, bei denen die IT zu beweisen versucht, dass selbst die aufmerksamsten Kollegen zur Preisgabe ihrer Zugangsdaten bewogen werden können. Wenn Sie Ihren Mitarbeitenden darüber hinaus auch Screenshots, FAQs und Kontaktinformationen an die Hand geben, machen Sie es ihnen leicht, bei Bedarf Hilfe anzufordern.

Verstehen und härten Sie Ihre Prozesse zur Konto-Wieder-herstellung.

Multi-Faktor-Authentisierung ist immer nur so sicher wie die hinterlegten Prozesse zur Konto-Wiederherstellung. Bei einigen viel beachteten Attacken der jüngeren Vergangenheit missbrauchten Angreifer gezielt Schwachstellen bei der Konto-Wiederherstellung, um Accounts zu übernehmen.

Nehmen wir ein fiktives Unternehmen namens Acme. Die Webanwendung von Acme unterstützt MFA über eine auf dem Smartphone des Benutzers installierte Soft-Token-App. Für den Fall, dass er nicht auf das Soft-Token auf seinem primären Gerät zugreifen kann, darf der Anwender eine Backup-Telefonnummer als alternativen zweiten Faktor zur Konto-Wiederherstellung angeben. Wie stark dieser zweite Faktor ist, hängt ganz davon ab, wie robust die Prozesse des Telekommunikationsproviders bei der Authentisierung und der SMS-Weiterleitung sind. Wird es einem Angreifer gelingen, sich als der Anwender auszugeben – und einen Support-Mitarbeiter zu überzeugen, Anrufe oder SMS auf eine von ihm kontrollierte Nummer weiterzuleiten?

Da jeder sekundäre Faktor zuverlässig zu ersetzen sein muss, müssen Unternehmen sichere Austauschprozesse entwickeln. Welcher Ansatz am besten geeignet ist, hängt ganz von den konkreten Umständen ab. Die folgenden Best Practices sollten Sie aber in jedem Fall berücksichtigen:

Die Wiederherstellung der primären und sekundären Faktoren sollte unabhängig erfolgen.
Es ist wichtig, die Wiederherstellung des sekundären Faktors vollständig von der Wiederherstellung des primären Faktors zu entkoppeln. Sonst können Sie sich in dem Moment, wo ein Angreifer die Kontrolle über den ersten Authentisierungsfaktor erlangt, nicht mehr auf den zweiten Faktor verlassen, da dieser einfach mit dem kompromittierten Faktor zurückgesetzt werden kann. Der Wiederherstellungsprozess für den zweiten Faktor muss vollständig vom Wiederherstellungsprozess für das Passwort getrennt sein. Wenn die Wiederherstellung also zum Beispiel über eine E-Mail-Nachricht erfolgt, sollte der zweite Faktor über einen anderen Kanal wiederhergestellt werden.

Ziehen Sie einen Administrator hinzu.
Ein Administrator kann in einer Reihe von Szenarien intelligente, hochsichere Authentisierungsverfahren implementieren. In Enterprise-Szenarien sind Unternehmen in einer sehr guten Position, um die eigenen Mitarbeitenden auf der Basis von Shared Secrets zu authentisieren – etwa mit Fragen zu deren Aufgabenfeld oder Profil, zum Unternehmen oder zu den Beziehungen zu Kollegen. Ein bewährter Ansatz ist es auch, den Vorgesetzten eines Mitarbeiters zu bitten, diesen zu authentisieren, und die IT dann zu autorisieren, die MFA zurückzusetzen.

In Verbraucherszenarien kann ein Administrator einen Benutzer über eine Reihe von Shared Secrets abfragen. So erfassen beispielsweise Bankanwendungen für Verbraucher beim Onboarding eine große Anzahl von obskuren persönlichen Fakten, die als Shared Secrets für die Wiederherstellung von Konten herangezogen werden. Aktuelle Ereignisse in der Historie des Anwenders – etwa zum Einsatz der App oder zu den Interaktionen mit dem Unternehmen – lassen sich ebenfalls als Shared Secrets verwenden. Die Bewertung der Shared Secrets kann über das Internet oder via Voice automatisiert erfolgen. In der Regel ist dieses Verfahren sicherer als die Abfrage durch einen menschlichen Ansprechpartner, da es weniger anfällig für Social Engineering ist.

Integrieren Sie einen zweiten sekundären Faktor als Backup.
In vielen Szenarien ist ein automatisiertes Verfahren zur Wiederherstellung des zweiten Faktors erforderlich (zum Beispiel bei Produkten, die von einer hohen Anzahl von Benutzern verwendet werden, so dass eine persönliche Betreuung zu kostenintensiv wäre, oder wenn es gilt, die laufenden Kosten zu senken). Wenn Sie für jeden Benutzer bereits beim Onboarding mehr als einen sekundären Faktor einrichten, ermöglichen Sie es ihm, im Notfall den sekundären Faktor wiederherzustellen, indem die Authentifizierung über einen zweiten sekundären Backup-Faktor abgeschlossen wird. Ein gängiges, einfaches und günstiges Verfahren ist es, dem Benutzer eine physische oder ausdruckbare Karte mit einem Satz von Codes auszuhändigen, die lediglich einmal verwendbar sind und als zweiter sekundärer Backup-Faktor dienen.

Schützen Sie Logins vor Brute-Force- und Credential-Stuffing-Angriffen

Mit der einfachen Verfügbarkeit preiswerter Rechenleistung steigt auch die Anfälligkeit von Authentifizierungssystemen für Brute-Force-Angriffe. Mit einigen einfachen Techniken lässt sich die Sicherheit Ihrer MFA im Falle einer Kompromittierung eines Passworts aber erheblich verbessern.

Analysieren Sie Log-Files und Alarmmeldungen.
Erfassen und analysieren Sie nicht erfolgreiche Anmeldeversuche mit dem sekundären Faktor. Kommt es zu mehreren fehlgeschlagenen Second-Factor-Challenges, sollten Sie den Benutzer oder einen Administrator auf das verdächtige Verhalten hinweisen – und den User auffordern, ein neues Token zu registrieren.

Verwenden Sie Out-of-Band-Token.
Ein sekundärer Faktor, der über einen vom ersten Faktor separaten Kanal verifiziert wird, bietet zusätzlichen Schutz vor Brute-Force-Angriffen und Phishing. So sendet ein beliebter neuer Faktor dem Anwender eine Push-Benachrichtigung auf sein Mobiltelefon, die Details zur Authentifizierungsanfrage enthält, sowie einen Prompt, der ihn auffordert, den Request anzunehmen oder abzulehnen. Dieser Kanal ist mit klassischen Brute-Force-Verfahren nicht zu knacken.

Achten Sie bei der Entwicklung auf Risiken, Usability und Kosten

Das Design eines MFA-Features wirkt sich in jedem Kontext unmittelbar auf die Sicherheit, die Usability und die Kosten aus. Ein besonders sicherer sekundärer Faktor bedeutet für Ihre Benutzer und Administratoren mitunter einen unnötigen Mehraufwand; dies kann die Akzeptanz der MFA für Ihr Produkt beeinträchtigen und so die Sicherheit verringern. Die folgenden Tipps helfen Ihnen, die richtige Balance zwischen Risiken, Usability und Kosten zu finden:

Bieten Sie ein breites Spektrum von Optionen für unterschiedliche Nutzergruppen an.
Unterschiedliche Nutzergruppen bedeuten unterschiedliche Risiko-Level und erfordern daher ein unterschiedliches Maß an Sicherheit. So haben Administratoren oft weiter gefasste Zugriffsrechte als gewöhnliche Benutzer. Daher werden Sie für Administratoren in der Regel besonders sichere sekundäre Faktoren vorsehen, und für die gewöhnliche Workforce eher auf den Bedienkomfort achten. In Verbraucherszenarien können die Sicherheit und die Usability je nach Benutzer einen ganz anderen Stellenwert haben. Dies kann sogar dazu führen, dass eine vertraute Option mit geringerem Security-Level (wie SMS) am Ende einen besseren Schutz bietet als eine hochsichere Option, die bei den Anwendern auf Widerstand stößt.

Unterstützen Sie die Authentisierung über föderierte Identitäten.
Föderierte Identitäten, auch bekannt als föderierter Single Sign-On (SSO), bezeichnen ein Verfahren, bei dem die Identität eines Benutzers über mehrere Identity-Management-Systeme hinweg verknüpft wird. Dies erlaubt es den Benutzern, schnell zwischen den verschiedenen Systemen zu wechseln, ohne Abstriche bei der Sicherheit in Kauf zu nehmen. Im Business-Umfeld implementieren viele Unternehmen die Authentifizierung und MFA für die von ihnen verwalteten Identitäten lokal – und föderieren sie dann an externe Ressourcen. Dies ermöglicht es Produktentwicklern, das Management von Policies und Security-Prozessen an ihre Kunden und Partner auszulagern. So können diese MFA unabhängig voneinander implementieren und mit Blick auf die oben beschriebenen Aspekte an ihre individuellen Vorgaben und Einschränkungen anzupassen. Auf diese Weise könnte ein Partner beispielsweise die Verwaltung der Konto-Wiederherstellung auf seine ganz spezifischen IT-Anforderungen abstimmen. Dieses Outsourcing bietet darüber hinaus den Vorteil, dass die Anwender über ein einziges Token auf alle Ressourcen zugreifen können.

Okta als Gamechanger

Der moderne Identity-Management-Ansatz von Okta kann Ihrem Unternehmen dabei helfen, die Kontrolle über das Management der Identitäten und die MFA zu übernehmen sowie Angriffe und andere potenzielle Schäden zuverlässig zu stoppen. Okta ermöglicht es Ihnen:

MFA für Ihre Workforce und Ihre Kunden schneller bereitzustellen.

- Implementieren Sie MFA einfach und schnell, mit mehr als 7.000 schlüsselfertigen Integrationen im Okta Application Network
- Integrieren Sie auch On-Premises-Anwendungen – mit Unterstützung von RADIUS, RDP, ADFS, und LDAP, sowie von Header-basierter Authentisierung und Kerberos über das Okta Access Gateway
- Stellen Sie die Weichen für intelligente, Kontext-basierte Zugangsentscheidungen auf Basis der Device- und Verbindungseigenschaften
- Reduzieren Sie durch Single-Sign-On und passwortlose Technologien Ihre Abhängigkeit von Passwörtern

Ihre Identitäten zu zentralisieren.

- Minimieren Sie die Komplexität beim Account-Management
- Vereinheitlichen Sie die Anwender-Zugriffe, um Passwörter zu vermeiden und jederzeit eine hochwertige Experience zu garantieren
- Minimieren Sie Risiken und vermeiden Sie einen Wildwuchs von Identitäten, indem Sie den Zugang zu Services über smarte SAML-Connections regeln

Ihre Angriffsfläche zu verkleinern und schneller auf kompromittierte Zugangsdaten zu reagieren.

- Automatisieren Sie die Provisionierung und Deprovisionierung, um das Onboarding nachhaltig zu beschleunigen und verwaiste Accounts zu vermeiden
- Erweitern Sie Ihre Security-Policy auch auf eigenentwickelte Anwendungen – zum Beispiel über SCIM, SDKs oder das breite Angebot an Okta APIs
- Stellen Sie sicher, dass stets die richtigen Zugriffsrechte zur richtigen Zeit für die richtigen Anwendungen gewährt werden – mit Workflows für Access-Requests und durchgängigem Management des Identity-Lifecycles

Wenn Sie sich davon überzeugen möchten, wie einfach es ist, Oktas Adaptive Multi-Factor Authentication zu administrieren und den Authentisierungsprozess zu managen, sehen Sie sich unsere Demo an.

Mehr über die Lösung Adaptive MFA von Okta erfahren Sie unter https://www.okta.com/de/products/adaptive-multi-factor-authentication/

Fazit
Ihre Roadmap zur erfol-greichen MFA

Multi-Faktor-Authentisierung ist unter Anwendungsentwicklern heute weltweit eine etablierte Best Practice, um den Zugang zu ihren Anwendungen zu schützen. Um das volle Potenzial der MFA zu erschließen, ohne die Arbeitsabläufe der Mitarbeitenden zu stören, ist hinter den Kulissen aber eine ganze Reihe von Maßnahmen erforderlich. Zu den Best Practices gehört es, die Second-Factor-Recovery-Flows zu analysieren, die Systeme gegen Brute-Force-Angriffe zu härten und die richtige Balance zwischen Security, Usability und Kosten zu suchen.

Ein moderner, automatisierter MFA-Ansatz hilft Unternehmen dabei, die Zugriffe auf Ihre Ressourcen zu kontrollieren, die Wiederherstellungsprozesse nachhaltig zu automatisieren und die Gefahr erfolgreicher Angriffe drastisch zu reduzieren.

Über Okta

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

Whitepaper

Ihr Guide zur MFA-Integration

okta

Okta GmbH
100 First Street
80333 München
info_germany@okta.com
+49 (89) 2620 3329