MULTIFAKTOR-AUTHENTIFIZIERUNG: BEST PRACTICES ZUM SCHUTZ MODERNER DIGITALER UNTERNEHMEN

Optimierung von Kosten, Benutzerfreundlichkeit und Sicherheit durch einen Wechsel von Passwörtern und klassischer 2FA zur MFA

WHITEPAPER

INHALTSÜBERSICHT

ZUSAMMENFASSUNG

Kompromittierte Anmeldeinformationen stellen weiterhin eins der größten Sicherheitsrisiken in Unternehmen dar. Diese Tatsache ist nicht weiter verwunderlich, da viele Unternehmen zur Authentifizierung von Benutzern immer noch auf die Einfaktor-Variante mit Passwörtern setzen. Andere Unternehmen sind auf die klassische Zweifaktor-Authentifizierung (2FA) umgestiegen. Der Einsatz von Hard Token kann jedoch die Benutzererfahrung schmälern, die Akzeptanz erschweren und sehr kostspielig sein. Deshalb empfiehlt sich der Wechsel zu einem benutzerfreundlicheren und kostengünstigeren Authentifizierungsmodell, das mehr Sicherheit bietet. In diesem Whitepaper wird die Step-up-Multifaktor-Authentifizierung (MFA) ausführlich diskutiert und als erstklassiges Verfahren zur Benutzerauthentifizierung empfohlen.

Die Step-up-MFA ist ein dynamisches Authentifizierungsmodell, bei dem der Benutzer, ein Kunde oder ein Mitarbeiter, zusätzliche und richtlinienbasierte Authentifizierungsschritte je nach Bedarf ausführen muss. Typische Beispiele für Step-up-MFA:

- Ein Kunde, der sich mit einem Passwort auf einer Onlinebanking-Website angemeldet hat, möchte Geld überweisen. Die Mobile App der Bank sendet eine Push-Benachrichtigung an das zuvor vom Kunden als vertrauenswürdig angegebene Gerät, um die nötige zusätzliche Absicherung zu schaffen.
- Eine leitende Angestellte möchte während des Afrika-Urlaubs ein Geburtstagsgeschenk für ihr Kind kaufen und muss sich zur Bestätigung der Transaktion mit ihrem Fingerabdruck auf ihrem iPhone authentifizieren.
- Ein Elternteil eines Teenagers wird per Benachrichtigung dazu aufgefordert, einem neuen Fernsehsender zuzustimmen, der dem Kabel-TV-Paket der Familie hinzugefügt wurde.
- Eine Kundin, die sich von zu Hause über ihr iPad bei einem Onlineshop anmeldet, sieht keine sichtbaren Authentifizierungsschritte, bis sie ihre Einstellungen ändern muss.
- Ein Mitarbeiter versucht vom Büro aus auf eine native SaaS-Anwendung zuzugreifen. Da er sich im Firmennetzwerk befindet, braucht er keine zusätzliche Authentifizierung.
- Eine Kundin möchte einen neu erworbenen Smart-Thermostat mit dem Konto ihrer Hausautomationsplattform verknüpfen. Sie verwendet eine App auf ihrem Android-Smartphone, um die Anmeldeinformationen an den Thermostat weiterzuleiten, und wird darüber benachrichtigt, dass der Thermostat gerade installiert wird. Zudem wird sie aufgefordert, diesen vertraulichen Vorgang zu bestätigen.

In diesem Whitepaper stellen wir Best Practices für die Bereitstellung einer Step-up-MFA bei Kunden und in Unternehmen vor. Der Fokus liegt dabei auf einem risikobasierten Ansatz, bei dem die dynamische Step-up-Multifaktor-Authentifizierung mit passiven kontextbezogenen Mechanismen wie geografischer Standort und Uhrzeit kombiniert wird. Ein risikobasiertes Konzept sorgt für eine ganzheitliche Bewertung der Benutzer, ihrer Computing-Umgebung und der Art der Transaktion, die sie durchzuführen versuchen. Das Ziel besteht darin, angemessene Authentifizierungs- und Autorisierungsverfahren anzuwenden.

Vorteile des risikobasierten Step-up-MFA-Ansatzes:

- Für jede Transaktion wird nur die minimal erforderliche Authentifizierungsstufe verlangt. Auf diese Weise kann eine optimale Benutzererfahrung gewährleistet werden.
- Wenn die Kosten für Mechanismen, die eine höhere Sicherheit bieten, nutzungsbasiert sind, können risikobasierte Modelle sehr kosteneffizient sein, da teurere Optionen nur im Bedarfsfall eingesetzt werden.
- Die Betrugserkennung wird im Vergleich zu herkömmlichen binären Regelsätzen verbessert.
- Es entsteht eine flexible, zukunftssichere Architektur, die sich an neue Technologien und Datensätze anpassen lässt.

In diesem Whitepaper erfahren Sie …

- alles wichtige rund um das Thema Authentifizierung, einschließlich Begriffen, Mechanismen und Signalen.
- wie Sie die richtigen MFA-Mechanismen für Ihre Umgebung auswählen.
- wie Sie ein risikobasiertes Modell auf die Step-up-MFA anwenden.
- welche Best Practices bei der Step-up-MFA empfehlenswert sind, einschließlich Risikoanalyse, Auswahl der Authentifizierungsfaktoren, Datenschutz, Sperrfunktionen, Registrierung, Benutzer-Opt-in, vorübergehende Aufhebung und Umgehungslösungen, Selfservice, native Anwendungen, Erstauthentifizierung und mehrere Kontaktpunkte/Kanäle.

AUTHENTIFIZIERUNG IM ÜBERBLICK

In der Regel werden Authentifizierungsmechanismen in folgende Kategorien unterteilt:

1. Etwas, das man weiß (z. B. Passwort oder PIN)
2. Etwas, das man hat (z. B. Kreditkarte, Mobiltelefon oder Token)
3. Etwas, das man ist (z. B. Fingerabdruck oder andere biometrische Daten)

In der Theorie geht die Multifaktor-Authentifizierung einen Schritt weiter als die Zweifaktor-Authentifizierung, da Benutzer sich mit zwei oder mehr Faktoren authentifizieren müssen (Kombination aus „Etwas, das man weiß" mit „Etwas, das man hat"). Siehe Abbildung 1. In der Praxis ist es jedoch ebenso sinnvoll, mehrere Authentifizierungsfaktoren desselben Typs zu verwenden, solange die Kompromittierung eines Faktors nicht bedeutet, dass auch andere Faktoren kompromittiert werden.

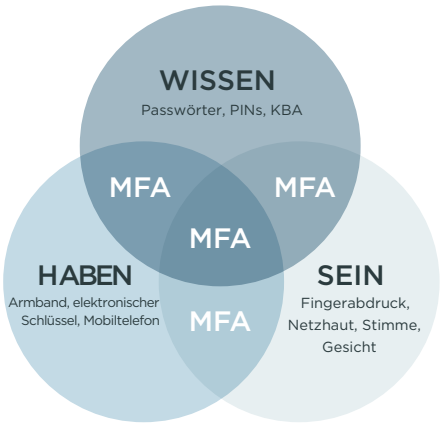

Abbildung 1: Bei der MFA müssen sich die Benutzer mit mindestens zwei Kategorien authentifizieren.

Im Allgemeinen steigt durch die Kombination mehrerer Authentifizierungsfaktoren auch die Gewissheit, dass der Benutzer, der gerade versucht sich zu authentifizieren, tatsächlich die Person ist, die er vorgibt zu sein. Selbst wenn ein Faktor kompromittiert wird, ist die Wahrscheinlichkeit gering, dass auch andere Faktoren kompromittiert werden.

Authentifizierungsmechanismen lassen sich außerdem danach unterscheiden, ob sie denselben Kanal nutzen, in dem der Benutzer auf die Anwendung zugreift, oder einen separaten Kanal, der speziell für die Authentifizierung gedacht ist.

Bevor wir im Detail auf die einzelnen Authentifizierungsmechanismen eingehen, sollten wir die Begriffe definieren, die im weiteren Verlauf dieses Whitepapers verwendet werden.

BEGRIFFSDEFINITION

Bei der Beschreibung von Authentifizierungsmodellen werden viele verschiedene – und teilweise widersprüchliche – Begriffe verwendet. In diesem Whitepaper gelten folgende Definitionen:

- **Authentifizierung** beschreibt den Prozess, mit dem die Echtheit einer vorgegebenen Identität überprüft und die Gültigkeit der Anmeldeinformationen verifiziert wird.
- Eine **Anmeldeinformation** ist etwas, auf das der Benutzer Zugriff hat (etwas, das er „hat" oder „weiß") und das in einem Authentifizierungsprotokoll verwendet werden kann. Damit sich ein Benutzer mit einer Anmeldeinformation authentifizieren kann, muss sie ihm erst zugewiesen oder mit ihm verknüpft worden sein.
- Als **Identifizierung** wird der Prozess beschrieben, mit dem Informationen zu einem Benutzer erfasst und dazu genutzt werden, mit einer gewissen Sicherheit festzustellen, dass er derjenige ist, der er vorgibt zu sein.
- Der **Identitätsnachweis** ist Teil des Registrierungsverfahrens, bei dem die Identität eines Kunden bestätigt wird, bevor für diesen Konten erstellt oder Anmeldeinformationen erzeugt werden.
- Der **Level of Assurance bzw. LoA** beschreibt das Maß an Gewissheit, dass ein Benutzer die Person ist, die er vorgibt zu sein, wenn er zur Angabe einer digitalen Anmeldeinformation aufgefordert wird. Ausschlaggebend für den LoA ist die Phase in der Identitätsüberprüfung und -nachweis erfolgen und Anmeldeinformationen erzeugt werden, sowie die Qualität des eigentlichen Authentifizierungsprozesses. Letzteres umfasst die Qualität/den Typ der Anmeldeinformation und die Belastbarkeit des Authentifizierungsmechanismus. LoA-Modelle enthalten üblicherweise vier verschiedene Kategorien, die jeweils genau definierte Anforderungen in Bezug auf den Identitätsnachweis und die Details der Authentifizierungsmechanismen aufweisen.
- **Multifaktor-Authentifizierung bzw. MFA** bezieht sich auf die Verwendung von mindestens zwei verschiedenen Anmeldeinformationen bei der Authentifizierung des Benutzers. Der Einsatz mehrerer Faktoren/Anmeldeinformationen sorgt in der Regel für einen höheren LoA im Hinblick auf den Benutzer. Die Zweifaktor-Authentifizierung (2FA) ist ein MFA-Beispiel, bei dem zwei verschiedene Anmeldeinformationen eingesetzt werden.
- **Registrierung** ist der Prozess, bei dem der Benutzer mit seinen Anmeldeinformationen und seinem Identitätsdatensatz verknüpft und entsprechende Anmeldeinformationen an den Benutzer ausgegeben werden.

AUTHENTIFIZIERUNGSMECHANISMEN

Als nächstes beschäftigen wir uns mit den unterschiedlichen Authentifizierungsmechanismen, die in einer Step-up-MFA-Sicherheitsarchitektur verwendet werden können. Einige Authentifizierungsmechanismen erfordern einen direkten Benutzereingriff, andere wiederum werden passiv erfasst (und verbessern dadurch die Usability).

PASSWÖRTER

Ein Passwort ist ein geheimer Schlüssel, der nur dem Benutzer und dem Server bekannt ist, bei dem sich der Benutzer authentifizieren muss. Passwörter sind heutzutage das Standardverfahren zur Authentifizierung im Internet. In isolierten Systemen stellen Passwörter jedoch keine akzeptable Authentifizierungslösung dar, weil sie nicht besonders benutzerfreundlich und darüber hinaus anfällig für großflächige Sicherheitsverletzungen und Phishing-Angriffe sind.

HARDWARE-TOKEN

Hierbei handelt es sich um kleine Hardwaregeräte, die vom Benutzer mitgeführt werden, um den Zugriff auf Netzwerkdienste zu autorisieren. Das Gerät kann eine Chipkarte sein oder in ein Objekt integriert sein, das sich leicht mitführen lässt, z. B. ein Schlüsselanhänger oder ein USB-Laufwerk. Das Token enthält einen Algorithmus (einen Timer oder einen Zähler) und einen Seed-Datensatz, mit dessen Hilfe eine Pseudozufallszahl erstellt wird. Diese Zahl muss vom Benutzer eingegeben werden, um nachzuweisen, dass er sich im Besitz des Tokens befindet. Der Server, von dem der Benutzer authentifiziert wird, muss ebenfalls über eine Kopie des Seed-Datensatzes, des verwendeten Algorithmus und der korrekten Uhrzeit jedes Tokens verfügen.

Bei einer neueren Variante von Hardware-Token werden kleine Geräte in den USB-Anschluss eines Computers gesteckt. Wenn der Benutzer sich authentifizieren muss, drückt er eine Taste auf dem Gerät. Dadurch wird ein Einmalpasswort (OTP, One-Time Passcode) generiert und an den Server weitergeleitet, um die manuelle Eingabe durch den Benutzer zu imitieren.

SOFTWARE-TOKEN

Diese Token sind softwarebasierte Sicherheitsanwendungen, die üblicherweise auf einem Smartphone ausgeführt werden und ein Einmalpasswort für die Anmeldung generieren. Software-Token haben einige entscheidende Vorteile gegenüber Hardware-Token. So ist es unwahrscheinlicher, dass ein Benutzer sein Smartphone zu Hause vergisst, als dass ihm ein Einmalpasswort-Hardware-Token abhanden kommt. Sollte der Benutzer sein Mobiltelefon doch einmal verlieren, wird er den Verlust höchstwahrscheinlich melden, sodass das Software-Token einfach deaktiviert werden kann. Software-Token lassen sich außerdem einfacher und kostengünstiger vertreiben als Hardware-Token, die eigens übergeben werden müssen.

MOBILE AUTHENTIFIZIERUNG

Software-Token nutzen die Fähigkeit von Mobiltelefonen, Einmalpasswörter zu generieren, und können sich das jeweilige Kommunikationsnetz zunutze machen. Ein Benutzer kann beweisen, dass er sich im Besitz seines Telefons befindet (das zuvor mit diesem Benutzer verknüpft wurde), indem eine Nachricht an das Gerät gesendet wird. Einmalpasswörter können per SMS an das Telefon gesendet (und dann vom Benutzer in eine Anmeldemaske eingegeben) werden, eine App kann eine Authentifizierungsaufforderung über die Benachrichtigungsdienste des mobilen Betriebssystems empfangen oder das Mobiltelefon kann angerufen werden. Eine Mobile App erklärt dem Nutzer, warum er sich authentifizieren muss und was er dabei möglicherweise implizit oder explizit autorisiert. Es besteht ein großer Unterschied ob Sie sich „bei Ihrem Bankkonto anmelden“ oder ob Sie „Ihr gesamtes Guthaben überweisen“.

Die Option Einmalpasswort-per-SMS hat den Vorteil, dass der Benutzer kein modernes Smartphone für mobile Anwendungen benötigt. Sie hat aber auch einige Nachteile:

- Das National Institute of Standards and Technology (NIST) hat die Sicherheit von SMS-Nachrichten als Zweitfaktor geringer eingestuft, als ursprünglich angenommen.
- Die Technologie ist nicht für Sicherheitszwecke entwickelt worden
- und stützt sich unter anderem auf die Nummernübertragung durch die jeweiligen Netzbetreiber.
- Sie bietet keinen Schutz vor Phishing-Angriffen, wobei die Angreifer allerdings in Echtzeit vorgehen müssen.
- Außerdem bietet sie nicht die Zustellungsgarantie, die bei der Authentifizierung erforderlich ist. Eine Verzögerung von wenigen Minuten kann bereits dazu führen, dass das Konto eines Benutzers gesperrt wird.

BIOMETRISCHE AUTHENTIFIZIERUNG

Methoden der biometrischen Authentifizierung umfassen Netzhaut-, Iris-, Fingerabdruck- und Fingervenenscans, Gesichts- und Stimmerkennung sowie die Erkennung der Hand- und Ohrläppchengeometrie. Mobile Geräte können das bevorzugte Modell der biometrischen Erkennung ermöglichen, wobei die Mustervorlage auf dem Gerät, statt auf dem Server gespeichert sein kann. Die neuesten Smartphones bieten Hardwareunterstützung für biometrische Daten, z. B. TouchID auf dem iPhone. Biometrische Faktoren können explizite Aktionen des Benutzers erfordern, etwa beim Scannen eines Fingerabdrucks, oder implizit sein, z. B. wenn die Stimme des Benutzers analysiert wird, während er mit dem Helpdesk spricht.

Die FIDO-Allianz hat eine standardisierte Architektur definiert, mit deren Hilfe die lokale Authentifizierung eines Benutzers an einem Gerät (Laptop, Telefon usw.) an einen Server kommuniziert werden kann. Wenn die lokale Authentifizierung anhand biometrischer Daten erfolgt (z. B. durch einen Scan des Fingerabdrucks eines Benutzers mit einem Smartphone-Sensor oder durch einen Gesichtsscan), bietet das FIDO-Modell den Vorteil, dass die biometrische Mustervorlage nicht auf dem Server gespeichert werden muss. Gleichzeitig würden auch die mit diesem Speichervorgang verbundenen Risiken entfallen.

GERÄTE-IDENTIFIZIERUNG

Die Geräte-Identifizierung ist ein Verfahren, bei dem ein Geräte-Fingerabdruck erstellt wird, der dem Gerät relativ eindeutig zugeordnet werden kann. Mit der Zeit ermöglicht dieser Fingerabdruck dem Authentifizierungsserver, das Gerät wiederzuerkennen und zu erkennen, wenn der damit verknüpfte Benutzer versucht, sich mit einem anderen Gerät zu authentifizieren – was möglicherweise ein Hinweis für betrügerische Aktivitäten darstellt. Lösungen zur Geräte-Identifizierung erstellen einen Fingerabdruck, der auf Merkmalen wie dem geografischen Standort, der OS-Version, dem verwendeten Browser oder anderen gerätespezifischen Daten basiert. Die einfachste Methode der Geräte-Identifizierung ist der Einsatz eines langlebigen Cookies, der vom Authentifizierungsserver im Browser des Mobilgeräts erstellt wird. Anwendungen zur Geräte-Identifizierung eignen sich am besten für Unternehmen mit einer großen Zahl von Benutzern, die über das Internet auf sensible Informationen zugreifen.

KONTEXTBEZOGENE AUTHENTIFIZIERUNG

Dieser Prozess nutzt kontextbezogene Informationen wie den geografischen Standort, die IP-Adresse, die Uhrzeit und Geräte-IDs, um die Echtheit der Identität eines Benutzers zu bestimmen. Üblicherweise wird der aktuelle Kontext eines Benutzers mit zuvor aufgezeichneten Kontextdaten abgeglichen, damit Widersprüchlichkeiten ermittelt und potenzielle Betrugsaktivitäten erkannt werden können. Diese Prüfung wird im Hintergrund vollzogen, sodass der Benutzer nichts davon merkt. Für einen Angreifer können sie jedoch eine erhebliche Hürde darstellen. Bei der mobilen Standortbestätigung von Visa wird beispielsweise der Standort des Benutzer-Mobilgeräts ermittelt. Dadurch kann verifiziert werden, dass sich ein Benutzer in der Nähe des Standorts befindet, an dem seine Kreditkarte verwendet wird. Die Wahrscheinlichkeit einer betrügerischen Aktivität ist höher, wenn die Transaktion nicht an dem Ort erfolgt, an dem sich das Mobiltelefon befindet. In diesem Beispiel wird statt eines separaten Authentifizierungskanals der Anwendungskanal als Kontext zur Ermittlung potenzieller Betrugsfälle genutzt.

Es gibt viele andere Authentifizierungsmechanismen, einschließlich X.509-basierte Zertifikate, die sich aufgrund der unterschiedlichen Anforderungen bei der Bereitstellung und Implementierung besser für den Einsatz in Unternehmen, als bei Kunden eignen.

AUTHENTIFIZIERUNGSSIGNALE

Eine Voraussetzung für die kontextbezogene Authentifizierung ist die (in der Theorie) passive Erfassung diverser Signale zu den Benutzern und zu ihrem Kontext. Zu diesen Authentifizierungssignalen können ihr Standort (physisch und im Netzwerk), ihre Computing-Umgebung und die Ressourcen gehören, auf die sie zuzugreifen versuchen.

Signale können wie folgt gesammelt werden:

- Über Webseiten, auf denen sich die Benutzer authentifizieren
- Über die Mobilgeräte, die zur MFA genutzt werden
- Über andere Netzwerkhardware
- Über Anwendungen (oder vorgeschaltete Gateways)
- Über andere Sensoren, die sich in der Nähe der Benutzer befinden (z. B. tragbare Geräte, Smartwatches)

Nachdem die Signale erfasst und zusammengeführt wurden, können sie von der Risiko- und Richtlinieninfrastruktur auf untypische Muster analysiert werden, die möglicherweise auf einen Angriff oder betrügerische Aktivitäten hinweisen. Diese Analyse kann folgendermaßen durchgeführt werden:

- **Kontextbezogen** – Signalwerte werden jeweils mit einer vorgegebenen Liste zulässiger oder unzulässiger Werte verglichen (z. B. um die Anmeldung mit einer IP-Adresse aus Usbekistan zu unterbinden).
- **Verhaltensbezogen** – Signalwerte werden jeweils mit einem erwarteten Wert abgeglichen, der auf einem zuvor etablierten Muster basiert (z. B. wenn ein Mitarbeiter häufig geschäftlich nach Usbekistan reist und sich deshalb im Gegensatz zu allen anderen Mitarbeitern per MFA aus Usbekistan anmelden darf).
- **Korrelativ** – Signalwerte werden jeweils mit einem anderen erfassten Signalwert verglichen, um Widersprüchlichkeiten zu ermitteln (z. B. wenn sich ein Mitarbeiter laut Laptop-IP in den USA, aber laut seinem Mobiltelefon in Kanada befindet).

AUSWAHL DES RICHTIGEN STEP-UP-MFA-MECHANISMUS

Wie wählen Sie den richtigen Step-up-MFA-Mechanismus für Ihre Umgebung aus? Beachten Sie bei Ihrer Entscheidung folgende Variablen:

- **Stärke:** Maximale Anzahl an „false positives“? Maximale Anzahl an „false negatives“?
- **Vorteile für die IT:** Lässt sich die Authentifizierungsmethode leicht implementieren? Sind zusätzliche IT-Ressourcen erforderlich? Funktioniert die Methode über mehrere Kanäle hinweg (z. B. online, Telefon)?
- **Vorteile für die Benutzer:** Lässt sich die Authentifizierungsmethode leicht anwenden? Werden die Endbenutzer den neuen Prozess akzeptieren? Kann davon ausgegangen werden, dass die Benutzer Geräte haben, die einen solchen Mechanismus unterstützen? Werden die Benutzer unzumutbar beeinträchtigt? Könnten sich die Benutzer Sorgen um den Datenschutz machen?
- **Branchenspezifische Vorteile:** Gibt es bei dieser Authentifizierungsmethode Aspekte, die sie für bestimmte Branchen oder Funktionsbereiche besonders vorteilhaft macht? Wenn Mitarbeiter beispielsweise Handschuhe bei der Arbeit tragen müssen, sind biometrische Daten nicht die beste Wahl.
- **Anschaffungskosten:** Steigen die Kosten pro Benutzer jedes Mal, wenn Sie einen Benutzer hinzufügen? Wie hoch sind die Wiederbeschaffungskosten, sowohl für das Gerät als auch für den damit verbundenen Verwaltungsaufwand?
- **Implementierungskosten:** Was sind die Kosten für die Implementierung des Authentifizierungsmechanismus? Ist Clienthardware oder -software erforderlich? Wenn ja, wie werden diese den Kunden bereitgestellt und wie hoch sind die entsprechenden Kosten?

ANWENDUNG EINES RISIKOBASIERTEN MODELLS AUF DIE STEP-UP-MFA

Bei der risikobasierten Step-up-Authentifizierung wird das Risiko bestimmter Handlungen dynamisch auf der Grundlage folgender Faktoren beurteilt:

- Aktueller Authentifizierungsstatus des Benutzers
- Mit der jeweiligen Ressource verbundenes Risiko
- Kontext der Zugriffsanfrage; bei Bedarf kann der Benutzer aufgefordert werden, sich mit einem weiteren Faktor zu authentifizieren, wenn das Ergebnis der Berechnung unter einem bestimmten Schwellenwert liegt

In diesem Modell wird die Step-up-Authentifizierung in der Regel durch atypische und ungewöhnliche Kontexte (z. B. eine Anmeldung aus Usbekistan) oder Verhaltensmuster (z. B. eine versuchte Transaktion mit einem Wert über 100.000 €) ausgelöst.

Wie in Abbildung 2 auf der nächsten Seite veranschaulicht, muss sich ein Benutzer mit einem vorgegebenen Faktor authentifizieren, z. B. einem Passwort, wenn er Zugriff auf eine bestimmte Ressource erhalten möchte. Während der Authentifizierung erfasst und überprüft das System außerdem Authentifizierungssignale. Nur wenn bei dieser Überprüfung unerwartete und ungewöhnliche Ergebnisse gefunden werden, wird der Benutzer dazu aufgefordert, sich mit dem zweiten Faktor zu authentifizieren.

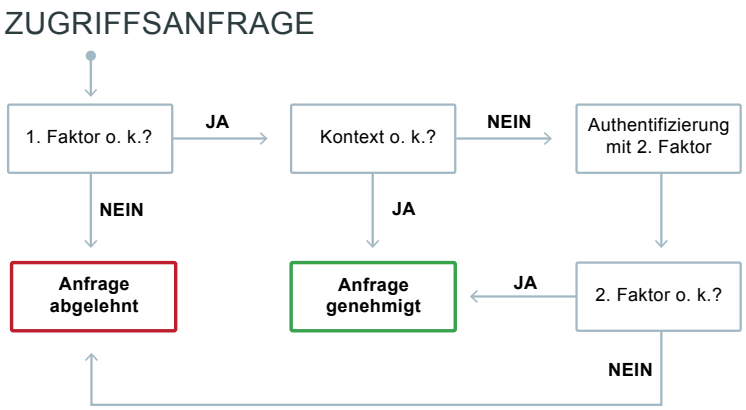

Abbildung 2: Die risikobasierte Step-up-MFA wird durch untypisches Verhalten oder einen ungewöhnlichen Kontext ausgelöst. Erst wenn die Kontextinformationen, die über den ersten Authentifizierungsfaktor erhoben werden, auf etwas Ungewöhnliches schließen lassen, wird vor dem Zugriff ein zweiter Authentifizierungsfaktor verlangt.

Ein wesentlicher Vorteil der risikobasierten Step-up-Multifaktor-Authentifizierung ist die bessere Usability. Der zweite Faktor bei der Authentifizierung muss nur bei Bedarf angegeben werden. Ausschlaggebend sind dabei die Ergebnisse der Überprüfung passiver Kontextinformationen.

Abbildung 3 zeigt Bildschirmaufnahmen einer mobilen Banking-App, die eine Variante der Step-up-MFA verwendet. Einige Elemente der App, wie die Telefonnummern der Filialen, stehen Benutzern auch ohne Authentifizierung zur Verfügung. Versucht der Benutzer sensiblere Features wie die Überweisungsfunktion aufzurufen, wird er jedoch aufgefordert, sich zu authentifizieren.

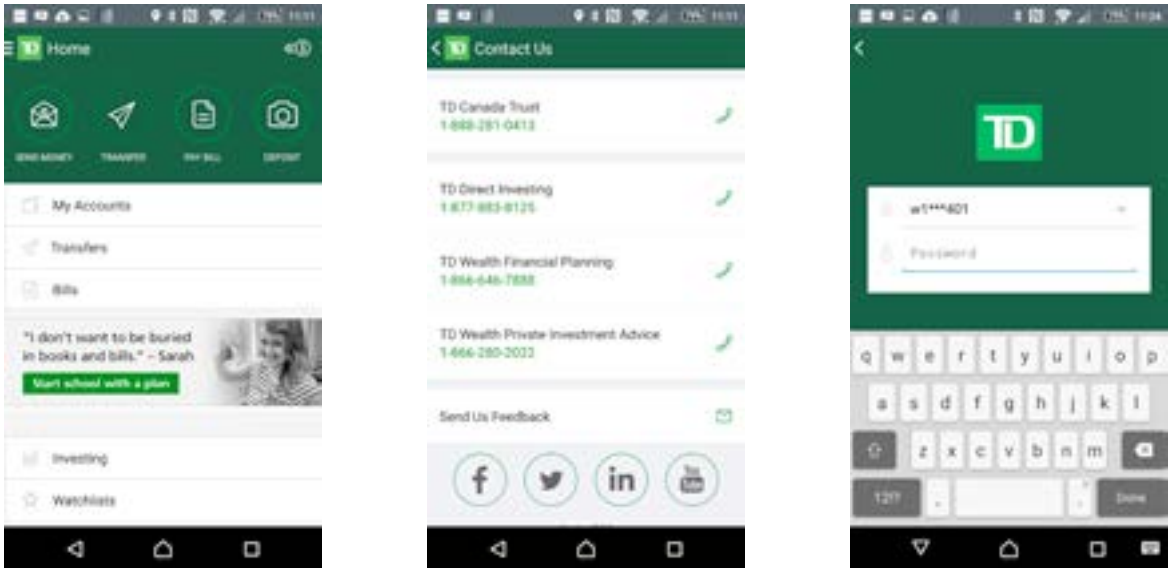

Abbildung 3: Das risikobasierte Step-up-Modell der MFA wird nur durch sensible Elemente einer Banking-App ausgelöst, z. B. Überweisungen.

Eine britische Bank entschied sich gegen das Step-up-Modell. Die Bank wählte stattdessen eine Authentifizierungsmethode mit der höchstmöglichen LoA für alle Benutzer, unabhängig davon, welchen Vorgang sie in der App ausführen möchten. Die Entscheidung gegen eine Step-up-Authentifizierung, bei der ein zusätzlicher Schritt nur im Fall eines veränderten Risikoprofils erforderlich ist, wurde damit begründet, dass diese Funktion die Kunden verwirren könnte. Deshalb fiel die Wahl auf ein einfacheres Modell.

BEST PRACTICES FÜR DIE STEP-UP-MFA

Ping Identity hat folgende Best Practices für die Step-up-MFA auf der Grundlage von Branchentrends, Gesprächen mit Kunden, die das Verfahren implementiert haben, und unserer eigenen Erfahrungen und Analysen zusammengetragen.

RISIKOANALYSE

Ein risikobasiertes Authentifizierungsmodell setzt voraus, dass das mit verschiedenen Anwendungsressourcen und -transaktionen verbundene Risiko bekannt ist. Mit dem Memorandum M-04-04 der US-Bundesbehörde Office of Management and Budget (OMB), „E-Authentication Guidance for Federal Agencies" (Leitfaden zur elektronischen Authentifizierung für Bundesbehörden) wird ein Modell zur Risikobewertung definiert, das für den Verbrauchermarkt eingesetzt werden kann:

Das Risiko eines Authentifizierungsfehlers ist eine Funktion mit zwei Faktoren:

1. Potenzieller Schaden oder potenzielle Auswirkungen
2. Die Wahrscheinlichkeit, dass dieser Schaden/diese Auswirkungen auftreten

Schadens- und Auswirkungskategorien umfassen:

- Unannehmlichkeiten, Belastung oder Schädigung von Ansehen bzw. Ruf
- Finanzielle Verluste oder staatliche Haftbarkeit
- Beeinträchtigung von staatlichen Programmen oder öffentlichen Interessen
- Nicht autorisierte Freigabe sensibler Informationen
- Persönliche Sicherheit
- Zivil- oder strafrechtliche Verstöße

Die Risikobewertung sollte durch die Abteilungen Marketing, Sicherheit und Compliance durchgeführt werden. Das Resultat sollte ein gemeinsam vereinbartes zulässiges Gesamtrisiko sein. Wenn die Ressourcen nach Risiko kategorisiert wurden, kann für jede Kategorie der notwendige Level of Assurance (LoA) festgelegt werden. Anschließend können anhand der LoA-Werte Authentifizierungsfaktoren und -modelle gewählt werden.

Im folgenden Beispiel einer Risikoanalyse implementierte eine britische Bank ein konditionales Modell: Dabei wendete die Bank diese Logik an: „Bei der Authentifizierung mit bestimmten Mechanismen kann der Benutzer folgende Aktionen durchführen." Den verschiedenen Authentifizierungsmechanismen, die den Benutzern geboten wurden, wies die Bank jeweils eine Stärke zu (Wert von 0–40). Beispiel:

- Ein physisches Kartenlesegerät, kombiniert mit einer Benutzer-PIN zur Erzeugung eines Einmalpassworts, erhielt die Stärke 40.
- Eine mobile Anwendung, die Einmalpasswörter generiert, wurde mit einer Stärke von 35 bewertet.
- Ein Passwort erhielt die Stärke 20.

Für jeden Wert liegt eine Liste zulässiger Aktionen vor (z. B. Kontostand abrufen, Überweisung tätigen), die der Benutzer durchführen kann, wenn er sich mit dem entsprechenden Mechanismus authentifiziert hat. Dies ist nicht die einzige Methode, um eine Risikoanalyse durchzuführen. Die grundlegende Voraussetzung besteht jedoch darin, verschiedenen Anwendungsressourcen die möglichen Authentifizierungsmechanismen zuzuordnen.

DIE WAHL DER AUTHENTIFIZIERUNGSFAKTOREN

Bei der Auswahl der geeigneten Authentifizierungsfaktoren gibt es nicht den universeller Ansatz, der alle Eventualitäten abdeckt. Eine überschaubare Anzahl von Benutzern, die auf äußerst sensible Ressourcen zugreifen, benötigt möglicherweise ganz andere Faktoren, als eine große Anzahl von Benutzern, die auf weniger risikobehaftete Inhalte zugreifen. Hilfreiche Tipps bei der Auswahl der geeigneten Authentifizierungsfaktoren für Ihre Anwendung finden Sie in Abschnitt 3 dieses Dokuments, „Auswahl der richtigen Step-up-MFA-Mechanismen".

Unternehmen müssen ein ausgewogenes Verhältnis zwischen Usability, Kosten und Sicherheit finden, um die Benutzererfahrung ihrer Kunden zu verbessern. Je nach gewählten Authentifizierungsfaktoren kann die Benutzererfahrung stark variieren – manche Faktoren erfordern einen Eingriff, andere laufen komplett im Hintergrund. Bei einem risikobasierten Modell kann man sicherstellen, dass der Benutzer sich nur explizit authentifizieren muss, wenn dies absolut notwendig ist. Standardmäßig kommt die passive, kontextbezogene Authentifizierung zum Einsatz.

Eine flexible MFA-Lösung ermöglicht einen Wechsel zwischen den unterstützten Modi. Wenn ein Mobiltelefon beispielsweise offline ist oder der Benutzer einen Roaming-Dienst in Anspruch nimmt, kann auf ein Einmalpasswort ausgewichen werden. Insbesondere bei Kunden steigt die Akzeptanz, wenn Sie für die Step-up-Mechanismen mehrere Optionen bieten. Nicht alle Benutzer verfügen über Telefone, die sich für mobilgerätbasierte Mechanismen eignen. Andere Mechanismen kommen möglicherweise für Benutzer mit Behinderung nicht infrage. Zudem gibt es Benutzer, die neuen Technologien generell kritisch gegenüberstehen.

Die folgende Abbildung enthält eine Übersicht der von Google unterstützten MFA-Mechanismen. Diese Mechanismen decken die unterschiedlichen Präferenzen und Beschränkungen der Benutzer ab und dienen als Alternative, wenn der primäre Modus nicht verfügbar ist.
Hardware-Token bieten zwar mehr Sicherheit als Software-Token-Modelle für Mobilgeräte, sind jedoch aufgrund der hohen Kosten und geringen Usability weniger empfehlenswert.

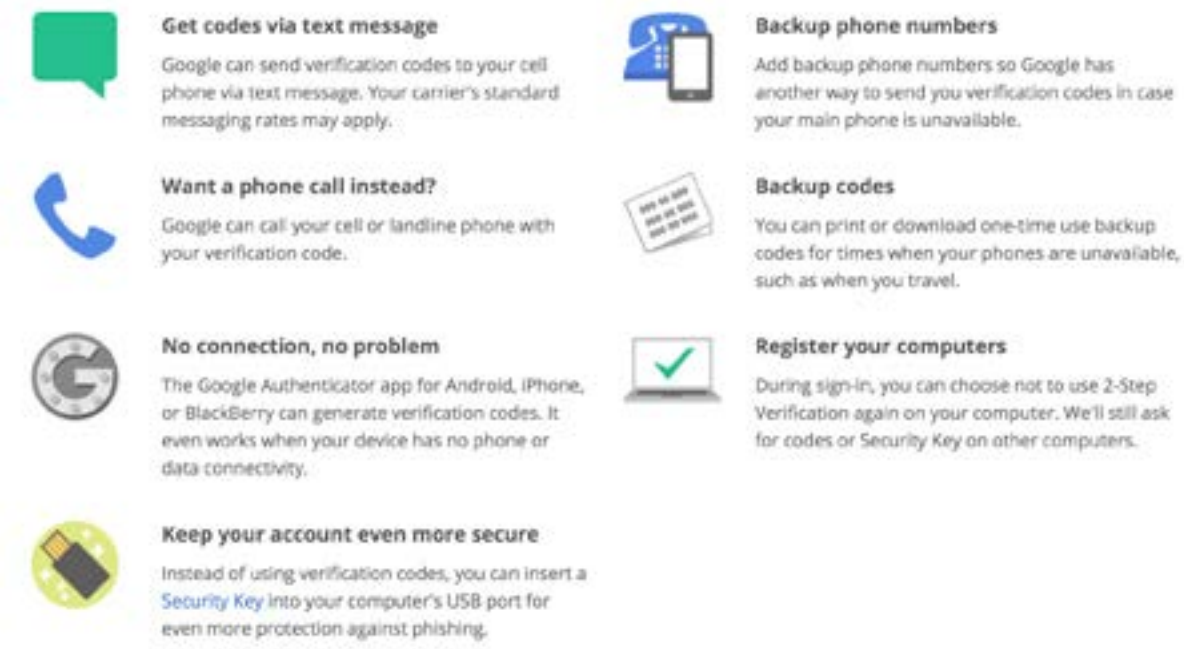

Abbildung 4: Google unterstützt eine Vielzahl primärer und alternativer MFA-Mechanismen, um den Präferenzen und Beschränkungen seiner Benutzer gerecht zu werden.

Abbildung 5: Twitter integriert MFA-Funktionen in seine Mobile App.

In einer Mobile App für Verbraucher sollten MFA-Funktionen in die vorhandenen nativen Anwendungen integriert werden, damit der Benutzer keine separate Authentifizierungsanwendung herunterladen muss. Wie in Abbildung 5 gezeigt, können Benutzer der Twitter-App in den Einstellungen eine Verifizierung in zwei Schritten („2-step verification") aktivieren. In der offiziellen Twitter-App werden Benutzer aufgefordert, bestimmte Vorgänge zu bestätigen, z. B. die Anmeldung auf ihrem Konto über ein zuvor unbekanntes Gerät.

Dies setzt voraus, dass die mobile MFA-Lösung ein SDK bietet, mit dem die Authentifizierungsfunktionalität in vorhandene Unternehmensanwendungen integriert werden kann.

DATENSCHUTZ

Je nach Authentifizierungsmechanismus müssen mehr oder weniger potenziell sensible Benutzerdaten gesammelt werden. Bei einem Modell mit Einmalpasswort per SMS müssen die Benutzer z. B. ihre Telefonnummer bereitstellen. Immer wenn personenbezogene Daten erfasst werden, sollte der Benutzer über den Verwendungszweck informiert werden. Lösungen zur Geräte-Identifizierung erstellen eine Art Fingerabdruck individueller Geräte. Dieser Fingerabdruck könnte dazu missbraucht werden, das Verhalten einzelner Kunden über mehrere Anwendungen hinweg nachzuverfolgen. Europäische Datenschutzbestimmungen beschränken die Benutzerinformationen, die gesammelt werden dürfen. In einigen Regionen sind Unternehmen daher verpflichtet, Kunden den Widerruf von Anwendungen zur Geräte-Identifizierung zu ermöglichen.

Um die Privatsphäre der Benutzer zu schützen, müssen Opt-in-MFA-Modelle und mehrere Optionen für den verwendeten MFA-Mechanismus bereitgestellt werden. Auf dem Verbrauchermarkt müssen Benutzer flexibel über ihre personenbezogenen Daten entscheiden können und ein gewisses Maß an Kontrolle erhalten. Dies spielt auch im Unternehmen eine wichtige Rolle. Da die Datenschutzeinstellungen für Verbraucher zunehmend erweitert werden, nehmen Mitarbeiter veraltete IT-Sicherheitsrichtlinien nicht mehr ohne weiteres hin.

SPERRFUNKTION

Wenn Sie den App-Zugriff eines Benutzers sperren, schaffen Sie unweigerlich eine negative Benutzererfahrung. Außerdem kann eine Kontosperre finanzielle Auswirkungen haben, wenn sie beispielsweise einen Kunden daran hindert, einen Kaufvorgang abzuschließen. Ebenso kann die Produktivität beeinträchtigt werden: ein Mitarbeiter, der keinen Zugriff mehr auf seine Arbeitsanwendungen hat, kann seine Aufgaben nicht mehr ordnungsgemäß ausführen.

Die Sperrfunktion sollte immer nur im Notfall eingesetzt werden. Es gibt bessere Optionen. Wenn ein Benutzer sein Passwort beispielsweise wiederholt falsch eingibt, können Sie sein Passwort im Rahmen einer Multifaktor-Authentifizierung zurücksetzen – statt den Zugang komplett zu sperren. Das Modell der kontinuierlichen Authentifizierung macht es noch unwahrscheinlicher, dass eine Sperrung überhaupt angewendet werden muss. Je mehr Authentifizierungssignale erfasst und analysiert werden, desto weniger fällt ein untypischer Wert (der Anlass für eine Sperrung geben könnte) möglicherweise ins Gewicht.

REGISTRIERUNG

Ein Authentifizierungsmechanismus ist immer nur so stark wie das Registrierungsverfahren, das die Anmeldeinformationen bereitstellt. Ein gründlicher Registrierungsprozess, bei dem die Anmeldeinformationen eng mit den individuellen Benutzern verknüpft werden, ist absolut erforderlich.

In mobilen Systemen, bei denen der Authentifizierungsserver den Benutzer bereits mit dem ersten Faktor bestätigt hat (z. B. einem Passwort), ist die Anzeige eines QR-Codes ein effektiver und nützlicher Mechanismus. Abbildung 6 zeigt das Beispiel eines QR-Codes, der beim PingID-Registrierungsverfahren eingesetzt wird. Der Benutzer scannt den Code mit der zuvor heruntergeladenen und installierten Anwendung (eine spezielle Authentifizierungsanwendung oder eine integrierte Funktion in einer vorhandenen Anwendung). Da der QR-Code Informationen zur Identität des Kunden referenziert, wird die Anwendung mit dem entsprechenden Kundenkonto verknüpft.

Abbildung 6: Die Mobile App PingID nutzt einen QR-Code bei der Geräteregistrierung.

BENUTZER-OPT-IN

Bei manchen Benutzergruppen kann es unpraktisch sein, die Step-up-MFA für alle User vorzuschreiben. Möglicherweise verfügt nicht jeder Benutzer über ein Telefon, das eine mobile Authentifizierung unterstützt. Manche Benutzer betrachten neue Technologien eventuell mit Skepsis und möchten sie nicht sofort einsetzen. Die Step-up-Multifaktor-Authentifizierung sollte als Methode zum Schutz von Kundendaten statt von Unternehmensdaten vermarktet werden.

Es ist wichtig, Kunden über den Nutzen der MFA aufzuklären. Am effektivsten ist es wahrscheinlich, wenn Sie Opt-in-Anreize bieten. Angebote mit erweiterten Services können Kunden dazu bewegen, MFA-Lösungen zu nutzen. Eine US-Bank bietet Kunden z. B. an, die täglichen und wöchentlichen Höchstbeträge für Überweisungen zu erhöhen, wenn sie sich für den MFA-Service registrieren. Google bietet einen Bonus für Benutzer, die der Einführung der Step-up-MFA im Rahmen einer Sicherheitsprüfung zustimmen (siehe Abbildung 7).

Abbildung 7: Google schafft Anreize für die Nutzung der Step-up-MFA durch die Benutzer.

Im Unternehmen, in denen die Multifaktor-Authentifizierung eventuell obligatorisch ist, sollten Sie einen gestaffelten Umstieg ermöglichen, der den Mitarbeitern die Möglichkeit bietet, die MFA einige Male oder bis zu einem bestimmten Datum aufzuschieben.

VORÜBERGEHENDE AUFHEBUNG UND UMGEHUNGSLÖSUNGEN

Entwickeln Sie sichere und gründliche Ausnahmeprozesse und alternative Zugangsmethoden für häufige Szenarien wie vergessene Passwörter oder verlorene und gestohlene MFA-Anmeldeinformationen.

Sie könnten den Benutzern die Möglichkeit bieten, auf die Step-up-MFA zu verzichten, wenn sie sich bei einer Anwendung mit einem bekannten und vertrauenswürdigen Gerät anmelden, auf dem die Multifaktor-Authentifizierung schon einmal durchgeführt wurde. Alternativ können Sie für vertrauenswürdige Gerätemodelle einen risikobasierten Ansatz wählen, bei dem die Benutzer nicht explizit auf den MFA-Schritt verzichten.

Wie in Abbildung 8 gezeigt, setzt Google das Modell mit den vertrauenswürdigen Gerätemodellen ein, um die Einblendung von Step-up-Aufforderungen zu minimieren.

Abbildung 8: Google nutzt das Modell der vertrauenswürdigen Geräte zur Umgehung der MFA.

Führen Sie ein Verfahren für verlorene oder gestohlene Geräte ein, bei dem die Benutzer sicheren Zugriff auf die Anwendung erhalten oder ein neues Gerät registrieren können. Sie können u. a. folgende Wiederherstellungsmethoden nutzen:

- Senden einer Reset-E-Mail an die hinterlegte Adresse
- Wissensbasierte Authentifizierung (KBA, Knowledge-based Authentication)
- Wiederherstellungscodes auf Papier (müssen von den Benutzern an einem sicheren Ort aufbewahrt werden)

Keine ausreichende Sicherheit bieten Wiederherstellungsprozesse mit Fragen, deren Antworten per Google- oder Facebook-Suche einfach herauszufinden sind – z. B. „Wo sind Sie zur Schule gegangen?“

SELFSERVICE

Sie können Ihre Effizienz steigern, indem Sie den Benutzern die Möglichkeit bieten, ihre MFA-Mechanismen und Geräte selbst zu verwalten. Selfservice MFA-Mechanismen können in Anmeldungs-, Wiederherstellungs- und Widerrufsphasen eine wichtige Rolle spielen und kostspielige Eingriffe durch die Verwaltung reduzieren. Selfservice-Mechanismen können Benutzern außerdem mehr Kontrolle über ihre Authentifizierungsinformationen sowie die Möglichkeit zur Einsichtnahme bieten, was sich insgesamt positiv auf den Datenschutz auswirken kann.

NATIVE ANWENDUNGEN

Zur Authentifizierung von Benutzern nativer Anwendungen haben sich OAuth 2.0 oder OpenID Connect 1.0 bewährt. Nach der erstmaligen Installation der nativen Anwendung (oder etwas später) ruft diese ein Browserfenster auf (keine Webansicht) und lädt die Anmeldeseite auf dem entsprechenden Server. Nach der Authentifizierung werden die Token wieder an die native Anwendung zurückübertragen, um eine Nutzung bei entsprechenden API-Aufrufen zu ermöglichen.

Zum Zeitpunkt der Token-Ausstellung kann der Anbieter die Multifaktor-Authentifizierung erzwingen. Je nachdem, um welche Art von nativer Anwendung es sich handelt, lässt sich die MFA selbst für die erstmalige Installation und Einrichtung per Richtlinie vorschreiben. Da die Authentifizierung in einem Browserfenster und nicht in der Benutzeroberfläche der Anwendung durchgeführt werden sollte, kann dieselbe Anmeldeseite, Step-up-Richtlinie und -Architektur genutzt werden, die für die normale Webanwendung erstellt wurde.

Mithilfe sogenannter Aktualisierungs-Token sorgt OAuth für ausgedehnte Sitzungen mit nativen Anwendungen. Es kann daher vorkommen, dass der Benutzer über lange Zeiträume hinweg nicht zur Anmeldung aufgefordert wird. Bei der Verwendung von langlebigen Aktualisierungs-Token kann es sinnvoll sein, den Anmeldevorgang um MFA-Schritte zu erweitern. Dadurch wird die native Anwendung noch enger mit dem entsprechenden Benutzer verknüpft, was wiederum das Risiko der langlebigen Token verringert.

Sie können außerdem ein Step-up-MFA-Modell für native Anwendungen implementieren. Wenn die Anwendung bei einer Anfrage für eine bestimmte Funktion ein Token präsentiert, kann die API den mit dem Token verknüpften LoA überprüfen. Sollte der Wert nicht ausreichend sein, kann die API die Anfrage ablehnen und die Anwendung benachrichtigen, dass ein neues Token (mit einem höheren LoA) benötigt wird. Die Anwendung leitet diese Anforderung an die Anmeldeseite weiter, damit der entsprechende Step-up-Ablauf ausgelöst wird.

Zusätzlich kann die API ähnliche kontextbezogene Informationen erfassen (z. B. IP-Adresse, Uhrzeit, Anwendungsverhalten) und in die Risiko-Engine einspeisen.

Abbildung 9: In der Erwartung, dass Passwörter in der Zukunft ggf. nicht mehr als erste Anmeldeinformation vom Authentifizierungsserver angefordert werden, trennte Google die Eingabe von Benutzername und Passwort auf seiner Anmeldeseite.

ERSTAUTHENTIFIZIERUNG

Die Sicherheitsprobleme, die sich aus der Verwendung von Passwörtern ergeben, lassen sich durch die MFA mindern. Dennoch werden Passwörter vermutlich auf absehbare Zeit als standardmäßiger erster Faktor, also als erste Anmeldeinformation, die der Benutzer an den Authentifizierungsserver sendet, bestehen bleiben. Aktuell werden Benutzername und Passwort in der Regel auf demselben Bildschirm eingegeben.

Auf lange Sicht könnte es jedoch sein, dass der Authentifizierungsserver nicht mehr nach einem Passwort als erste Anmeldeinformation fragt. Dann könnten Kontextdaten oder andere Mechanismen ausreichen und Passwörter obsolet werden. Bei der Entwicklung der Benutzererfahrung sollten sich Unternehmen möglicherweise auf diese Zukunft einstellen. Google ist diesen Schritt schon gegangen. Wie in Abbildung 9 zu sehen ist, hat das Unternehmen die Abfrage von Benutzername und Passwort auf seiner Anmeldeseite im Mai 2015 voneinander getrennt.

Die Aufteilung in zwei Vorgänge – wie Benutzer ihre Identität angeben (linke Seite der Abbildung) und wie sie sich authentifizieren (rechte Seite der Abbildung) – ermöglicht mehr Flexibilität für zukünftige Authentifizierungskonzepte. Wenn Google irgendwann neue Authentifizierungsmethoden ohne Passwörter einführt, muss die erste Anmeldeseite nicht geändert werden. Das Authentifizierungskonzept auf der ersten Seite, ermöglicht zudem eine freie Wahl der Authentifizierungsmethode für eine bestimmte Kombination aus Benutzer und Kontext.

MEHRERE KONTAKTPUNKTE/KANÄLE

Wenn ein Unternehmen seinen Kunden mehrere Kanäle bietet, um mit Anwendungsressourcen und Daten zu interagieren, z. B. Web, Mobile Apps, Telefonie und Geschäftsniederlassungen, kann es für jeden Kanal unterschiedliche MFA-Lösungen wählen.

Eine US-Bank setzt für ihren Telefoniekanal zum Beispiel auf die passive Authentifizierung per Stimmerkennung. Auch die kanadische Bank Manulife gab kürzlich eine Aktualisierung ihrer IVR-System (Interactive Voice Response) durch die Bereitstellung von NLU- (Natural Language Understanding) und passiver Stimmerkennungstechnologien bekannt.

FAZIT

Unternehmen tun gut daran, ihre Benutzerauthentifizierung weiterzuentwickeln und zu verbessern, um die Einschränkungen von Passwörtern und klassischen Zweifaktor-Authentifizierungsmethoden hinter sich zu lassen. Die Multifaktor-Authentifizierung bietet mehr Sicherheit. Dabei sollten Unternehmen jedoch kontextbezogene Daten für eine dynamische Step-up-Authentifizierung nutzen.

Die kontextbezogene Authentifizierung gilt heute als komplementäre Lösung zu aktiven und expliziten Authentifizierungsfaktoren. Ping Identity geht jedoch davon aus, dass sich die kontextbezogene Authentifizierung künftig zur Norm entwickeln und der Einsatz expliziter Authentifizierungsmethoden zurückgehen wird. Risikobasierte Authentifizierungsarchitekturen kombinieren Step-up-MFA mit passiver kontextbezogener Authentifizierung und bieten dadurch eine optimale Mischung aus Kosteneffizienz, Usability und Sicherheit.

Für die Step-up-MFA empfiehlt Ping Identity diese fünf Best Practices:

- Die Step-up-MFA sollte durch passive kontextbezogene Authentifizierung ergänzt werden.
- Um zu bestimmen, wann die Step-up-MFA eingesetzt werden sollte, empfiehlt sich ein risikobasierter Ansatz auf der Grundlage von Transaktionsabfragen und kontextbezogenen Indikatoren.
- Die Step-up-MFA sollte in den meisten Kundenszenarien optional sein. Der Kunden-Opt-in sollte durch die Bereitstellung von Informationen zu den Vorteilen sowie durch Opt-in-Anreize gefördert werden. Das Risiko eines kundenseitigen Verzichts auf die Step-up-MFA sollte durch alternative Mechanismen verringert werden.
- Mitarbeiter sollten im Hinblick auf die genutzten Authentifizierungsmechanismen eine Wahl und mehrere Optionen haben. Wenn Mitarbeiter auf die Verwendung erweiterter aktiver Authentifizierungsmodi verzichten, sollten Unternehmen passive Alternativen bieten.
- Es sollten verschiedene MFA-Optionen unterstützt werden, um den Anforderungen unterschiedlicher Benutzergruppen gerecht zu werden, z. B. Benutzern mit Behinderungen oder technisch weniger versierten Benutzern.

Weitere Informationen erhalten Sie auf www.pingidentity.com.

#3001 | 06.2017 | v00c