yubico

WHITE PAPER

Die dunkle Seite Ihrer Strategie zur Authentifizierung per Mobilgerät

Warum Sie die alte MFA in die Wüste schicken und eine moderne, Phishing-resistente MFA in einem großen Maßstab einführen müssen

Inhalt

10–24 %

Angriffsdurchdringungsrate für die Authentifizierung per Mobilgerät[10]

82 %

der Sicherheitsverletzungen sind auf das **menschliche Element** zurückzuführen: soziale Angriffe, Fehler, Missbrauch oder Diebstahl von Zugangsdaten[11]

1 Mio. USD

Kosten pro Jahr allein für **Passwortzurücksetzungen**[12]

92 %

der Unternehmen wurden Opfer von **Phishing**[13]

Nicht alle Arten der MFA sind gleich

Trotz der zunehmenden Flut und Raffinesse von Cyberangriffen verlassen sich Unternehmen weiterhin auf **veraltete Authentifizierungsmethoden**, wie Benutzernamen und Passwörter und mobile Authentifikatoren, um den Zugriff auf kritische und sensible Anwendungen und Daten zu sichern. Ein aktueller Google Cloud-Bericht zeigt, dass 50 % der Verstöße bei Cloud-Umgebungen in Unternehmen im 4. Quartal 2022 auf schwache Passwörter zurückzuführen sind.[1]

Unternehmen stehen vor dem zunehmenden Druck von Regulierungsbehörden und Cyberversicherer, die Cybersicherheit durch Multi-Faktor-Authentifizierung (MFA) zu stärken und den Authentifizierungsprozess um ein oder mehrere zusätzliche Beweise zu ergänzen. Obwohl jede Form der MFA eine bessere Sicherheit bietet als eine passwortbasierte Authentifizierung allein, ist es eine Tatsache, dass **nicht alle Arten der MFA gleich sind**.

Ältere mobile MFA wie SMS, Einmal-Passcodes (OTP) und Push-Benachrichtigungs-Apps sind sehr anfällig für Kontoübernahmen durch Phishing, Social Engineering und Man-in-the-Middle-Angriffe (MITM). Dennoch entscheiden sich bis zu 53 % der Unternehmen für die Authentifizierung per Mobilgerät als MFA-Formfaktor.2 Warum ist das so? Weil sich die meisten Unternehmen der **Sicherheitsrisiken durch Authentifizierung per Mobilgerät nicht bewusst** sind.

Heutzutage kostet ein Datenschutzvorfall in den USA durchschnittlich 9,44 Millionen US-Dollar und weltweit 4,35 Millionen US-Dollar3, aber Cyberangriffe können auch das Vertrauen untergraben, kritische Infrastrukturen lahmlegen, den Kernbetrieb stören, die Cyberversicherungsprämien erhöhen und zum Verlust von geistigem Eigentum führen. Erfolgreiche Cyberangriffe sind der Grund dafür, dass Regulierungsbehörden jetzt ausdrücklich eine **Phishing-resistente MFA** vorschreiben. Dazu gehören die Executive Order 14028 des Weißen Hauses4, das Office of Management and Budget (OMB) Memo 22-095 und das National Security Memorandum/NSM-86 in den USA, NIS27 für die EU und der globale Standard PCI DSS v4.08. Und dennoch herrscht in der Branche immer noch Verwirrung darüber, welche Formen der MFA wirklich sicher oder Phishing-resistent sind.

Die bittere Wahrheit ist, dass **keine Form der Authentifizierung per Mobilgerät vor Phishing schützt**. Darüber hinaus kann der ROI Ihrer MFA-Strategie hinsichtlich **Kosten, User Experience, Abdeckung** und sogar der Fähigkeit, eine Brücke in eine **passwortlose** Zukunft zu schlagen, stark variieren, je nachdem, für welchen MFA-Ansatz Sie sich entscheiden.

In diesem Whitepaper decken wir die **fünf größten Irrtümer bei der Authentifizierung per Mobilgerät** auf, um Ihnen zu helfen, Ihre langfristige MFA-Strategie neu zu bewerten und den Wechsel zu einer zeitgemäßen MFA zu erwägen. Wir zeigen Ihnen, dass **bisherige mobile MFA nicht mehr funktioniert**, und wie Sie eine moderne, Phishing-resistente MFA mit einem geschätzten **ROI von bis zu 203 %** erreichen können.[9]

Veraltete Lösungen für die Authentifizierung per Mobilgerät verursachen **Sicherheitslücken** und Probleme bei der Benutzerfreundlichkeit, wenn sie **in großem Umfang** eingesetzt werden

Gängige Formen der Authentifizierung per Mobilgerät

Die häufigsten Formen der Authentifizierung per Mobilgerät hängen von einem **menschlichen Element** ab, sei es eine manuelle Eingabe einer Ausgabe (Code) oder die Genehmigung einer Anmeldeanfrage. Das menschliche Element der Authentifizierung kann direkte Auswirkungen auf Sicherheitsrisiken, Benutzerproduktivität und Supportkosten haben, wenn die Lösung keine optimale User Experience bietet. Tatsächlich lassen sich **82 % der Datenschutzverletzungen auf das menschliche Element zurückführen**: soziale Angriffe, Diebstahl von Zugangsdaten, Missbrauch oder Fehler.[14]

Einmalpasswörter oder -Passcodes (OTP)

Code gültig für eine Transaktion

Per SMS, E-Mail, Voice oder App gesendet

Code-Eingabe durch Benutzer

Zeitbasiertes Einmalpasswort (TOTP)

Mit HMAC generierter Code, der sich alle paar Sekunden oder Minuten ändert, geteiltes Geheimnis, Zeitstempel

Per SMS, E-Mail, Voice oder App gesendet

Code-Eingabe durch Benutzer

Push-Authentifizierung

Bei einem Authentifizierungsversuch wird eine Warnung an das Mobilgerät des Benutzers gesendet

Per SMS oder In-App gesendet

Benutzer genehmigt oder verweigert den Zugriff

Authentifizierungs-App

Authentifizierungs-App auf einem Mobilgerät installiert

App generiert TOTP-basierten Code

Code-Eingabe durch Benutzer

Die fünf größten Irrtümer im Zusammenhang mit der Authentifizierung per Mobilgerät

Im Folgenden finden Sie die fünf größten Irrtümer bei der Authentifizierung per Mobilgerät, die Unternehmen dem Risiko von Kontoübernahmen und erhöhten Betriebs- und Investitionskosten aussetzen, wenn sie nicht behoben werden:

MYTHOS	TATSACHE
Die Authentifizierung per Mobilgerät ist Phishing-resistent →	**Jede Form der Authentifizierung per Mobilgerät kann gehackt werden**
Die Authentifizierung per Mobilgerät ist kosteneffektiv →	**Sie ist teurer, als Sie denken**
Die Authentifizierung per Mobilgerät ist benutzerfreundlich →	**Die Verwendung und Verwaltung der Authentifizierung per Mobilgerät ist komplex**
Die Authentifizierung per Mobilgerät bietet eine 360°-Abdeckung →	**Die Authentifizierung per Mobilgerät führt zu Sicherheitslücken bei der MFA**
Die Authentifizierung per Mobilgerät ist zukunftssicher →	**Die Authentifizierung per Mobilgerät unterstützt keine neuen Vorschriften oder Abläufe ohne Passwort**

> Jede Form der MFA ist besser als nur ein Benutzername und ein Passwort, aber die meisten MFA-Methoden sind trotzdem anfällig für Phishing. Wir haben schnell erkannt, dass wir für alle Mitarbeiter eine stärkere Authentifizierung benötigten, die Phishing-resistent ist. YubiKeys waren da einfach am sinnvollsten."
>
> **Daniel Jacobson** |
> Senior Director of IT | Datadog

Irrtum Nr. 1: Die Authentifizierung per Mobilgerät ist Phishing-resistent

Die Realität: Jede Form der Authentifizierung per Mobilgerät kann gehackt werden

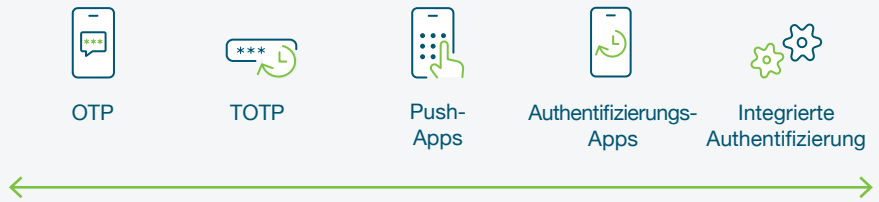
Der Hauptgrund für den Einsatz von MFA ist Sicherheit, aber auch wenn einige Formen der Authentifizierung per Mobilgerät sicherer sind als andere, **ist keine Form der Authentifizierung per Mobilgerät Phishing-resistent.**

Phishing-resistente MFA-Prozesse basieren auf einer kryptografischen Überprüfung zwischen Geräten oder zwischen dem Gerät und einer Domäne, wodurch sie ideal gegen Versuche geschützt sind, den Authentifizierungsprozess zu gefährden oder zu untergraben (z. B. Phishing, Brute-Force-Angriffe).

Der Fachpublikation (SP) 800-63 des National Institute of Standards and Technology (NIST) zufolge **erfüllen derzeit nur zwei Authentifizierungsmethoden die Kriterien für Phishing-resistente MFA**: PIV/Smartcard und FIDO2/WebAuthn.

Die heutigen Cyberbedrohungen zielen zunehmend auf ältere MFA-Systeme ab, darunter

Sicherheitsspektrum der Authentifizierung per Mobilgerät



Passwörter und mobile Authentifikatoren, die anfällig für moderne Cyberbedrohungen sind. Im Jahr 2022 führte ein Social-Engineering-Angriff auf den Messaging-Dienst Twilio zur Kompromittierung der Twilio-Plattform und ihrer Kunden, wodurch die Sicherheit der in dieser Zeit angebotenen OTP-Dienste untergraben wurde.[15] In den Jahren 2022 und 2023 wurden Phishing-Angriffe und gestohlene Zugangsdaten verwendet, um auf sensible Systeme (z. B. Uber[16]) oder Daten (z. B. American Airlines[17]) oder über Zugangsdaten Dritter (z. B. AT&T[18], Chick-fil-A[19]) zuzugreifen.

MFA ist von entscheidender Bedeutung, aber nicht alle MFA-Methoden sind gleich. Twitter verwendete die anwendungsbasierte MFA, die eine Authentifizierungsanforderung an das Smartphone eines Mitarbeiters sendete. Dies ist eine gängige Form der MFA, die aber umgangen werden kann. Während des Twitter-Hacks haben die Hacker die MFA überwunden, indem sie die Twitter-Mitarbeiter davon überzeugten, die anwendungsbasierte MFA während der Anmeldung zu authentifizieren. Die sicherste Form der MFA ist ein physischer Sicherheitsschlüssel oder eine Hardware-MFA, bei der ein USB-Stick zur Authentifizierung von Benutzern an einen Computer angeschlossen wird. Diese Art von Hardware-MFA hätte die Hacker gestoppt und Twitter implementiert sie jetzt anstelle der anwendungsbasierten MFA.

New York Department of Financial Services
Twitter Investigation Report
Oktober 2020

Wenn die Authentifizierung auf Wissen oder Menschen basiert, ist das Risiko schon vorprogrammiert. Menschen machen Fehler. Sie können dazu verleitet werden, Autorisierungsanfragen zu genehmigen, OTP-Codes einzugeben oder Software zu installieren. Kein noch so gutes Sicherheitstraining kann die Risiken moderner Phishing-Angriffe auf die Authentifizierung per Mobilgerät eliminieren. Schon das Mobilgerät selbst ist ein Risikofaktor:

1. Manipulation

Es gibt keine Garantie dafür, dass der private Schlüssel auf einem sicheren Element auf dem Mobilgerät landet.

2. Abfangen

Der OTP-Code oder private Schlüssel könnte abgefangen werden.

3. Identitätsdiebstahl

Es ist unmöglich, den Besitznachweis zu gewährleisten.

Im Jahr 2020 zielte eine kleine Gruppe von Teenagern mit einem Spear-Phishing-Angriff auf Twitter-Mitarbeiter ab, um sich Zugang zu den Anmeldedaten und Authentifizierungs-App-Codes der Mitarbeiter zu verschaffen. Anschließend griff sie auf das interne Netzwerk zu, um hochkarätige Kryptowährungskonten zu beschlagnahmen und die Öffentlichkeit um über 118.000 Dollar in Bitcoin zu betrügen.[20] In einem anderen Fall demonstrierte ein White-Hat-Hacker, dass es nur 16 Dollar und ein paar Sekunden braucht, um vollständig und unsichtbar Social-Media-Konten zu übernehmen, die durch OTP-basierte MFA geschützt waren.[21]

Eine von Google, der NYU und der UCSD durchgeführte Analyse von 350.000 realen Hijacking-Versuchen ergab, dass ein SMS-basiertes OTP nur 76 % der gezielten Angriffe und eine mobile Push-App nur 90 % der gezielten Angriffe abwehrte.[22] Mit anderen Worten: Die **Authentifizierung per Mobilgerät erreicht eine Angriffsdurchdringungsrate von 10 bis 24 %.** Das Risiko des Abfangens von SMS ist sogar so hoch, dass das NIST dazu aufrief, SMS als Authentifizierungsmethode zu verwerfen.[23]

Wenn Sie davon bisher noch nichts wussten, sind Sie nicht allein. Nur 22 % der von Yubico befragten Personen sind sich bewusst, dass die Sicherheit bei der SMS-basierten Authentifizierung ein Problem darstellen könnte.[24] Obwohl OTP-Authentifikatoren die am wenigsten sichere Form der Authentifizierung per Mobilgerät bilden, werden sie in 58 % der Unternehmen am häufigsten bereitgestellt.[25]

Jeder mobile Authentifikator kann gehackt werden

Eine Kontoübernahme liegt vor, wenn sich ein Hacker mit einer der folgenden Methoden erfolgreich Zugang zu den Anmeldedaten eines Benutzers verschafft:

Phishing

Eine Form von Social Engineering, bei der Angreifer Benutzer dazu bringen, sensible Informationen preiszugeben oder Malware zu installieren.

Man-in-the-Middle-Angriff (MITM)

Angreifer fangen Zugangsdaten über einen Proxyserver ab, leiten die Kommunikation zwischen zwei Parteien heimlich weiter und verändern sie möglicherweise.

Malware

Softwarebasierter Angriff, der in böswilliger Absicht entwickelt wurde, um sich Zugang zu einem Netzwerk zu verschaffen oder Daten und Systeme zu beschädigen.

OAuth-Phishing

Hacker nutzen schädliche Drittanbieteranwendungen als Mittel zum Zugriff. Wenn Benutzer Dritten Zugriff auf ein Konto gewähren, kann der Hacker mit einem OAuth-Token anstelle eines Passworts Zugriff erhalten.

MFA- oder Push-Müdigkeit

Social-Engineering-Angriff, bei dem wiederholt 2FA-Anfragen gestellt werden, um Benutzer zu zwingen, die Identität des Betrügers zu bestätigen und Zugang zu Konten zu gewähren. Benutzer akzeptieren aus Gewohnheit, aus Versehen oder um Benachrichtigungen zu stoppen.

SIM-Swapping

Zielt auf eine Schwachstelle in einigen Formen der 2FA ab, bei der ein Anruf oder eine Textnachricht an ein Mobiltelefon gesendet wird. Dabei wird die Möglichkeit ausgenutzt, dass SIM-Karten (Subscriber Identity Module) von Mobilfunkanbietern von Gerät zu Gerät mit unterschiedlichen Telefonnummern portiert werden können.

Credential Stuffing

Gestohlene Zugangsdaten werden verwendet, um sich über groß angelegte automatische Anmeldeanfragen unbefugten Zugang zu verschaffen.

Brute-Force-Angriff

Systematischer Angriff mit allen möglichen Passwörtern und Passphrasen, bis das/die richtige gefunden wird.

Wie eine gefälschte Anmeldeseite die herkömmliche MFA aushebelt

1 Opfer

Jack erhält von einem Angreifer eine gefälschte URL per E-Mail oder über einen Social-Media-Post.

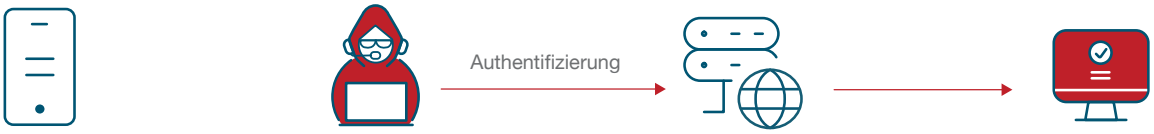
2 Gefälschte Anmeldeseite

Jack klickt auf den Link, der ihn zu einer gefälschten Website führt, die wie die echte Website aussieht.

Zugangsdaten (UN/PW)

6 Anmeldung auf gefälschter Website erfolgreich

Sekunden später gibt Jack diesen Code auf der gefälschten Website ein und kann sich dort anmelden.



5 Out-of-Band

Die echte Website löst den SMS-Code aus, der an Jacks Telefon gesendet wird.

3 Angreifer

Auf dieser gefälschten Website gibt Jack seinen Benutzernamen und sein Passwort ein und denkt, er würde sich auf der echten Website anmelden.
Der Angreifer schnappt sich die Zugangsdaten, die Jack eingegeben hat.

4 Webportal für Kunden

Der Angreifer gibt diese Informationen dann auf der echten Website ein. Aber selbst wenn es eine 2FA oder MFA gibt, wie z. B. SMS, kann Jacks Konto geknackt werden.

7 Angreifer meldet sich erfolgreich bei der echten Website an

Der Angreifer schnappt sich nun die von Jack eingegebene SMS-Zeichenfolge und gibt sie auf der echten Website ein, um sich erfolgreich anzumelden. Er kann das Passwort für Jacks Konto und seine Handynummer aktualisieren und Jack damit komplett aussperren.

Gerätekosten

Die Gesamtbetriebskosten des Geräts müssen berücksichtigt werden

1 Mio. USD

geben große Unternehmen jährlich für Personal und Infrastruktur aus, um Passwörter von Mitarbeitern zurückzusetzen

5,2 Mio. USD

an Produktivität verliert das durchschnittliche Unternehmen jährlich aufgrund von Kontosperrungen

300 %

Anstieg der Cyber-versicherungsprämien in allen Hochrisikobranchen

> „Wenn unsere Prämien um ein Drittel fallen und die anderer um 20 % oder mehr steigen, ist das ein wirklich großer Gewinn. Ich schätze, dass unsere Prämien fast die Hälfte von dem betragen, was andere zahlen müssen."
>
> **Brent Deterding** | CISO | Afni

Irrtum Nr. 2: Die Authentifizierung per Mobilgerät ist kosteneffektiv

Die Realität: Sie ist teurer, als Sie denken

Die Einführung der Authentifizierung per Mobilgerät gilt als relativ kostengünstig, sodass viele Unternehmen davon überzeugt sind, eine bezahlbare Lösung für die Authentifizierung gefunden zu haben. Die Authentifizierung per Mobilgerät ist jedoch mit vielen versteckten Kosten verbunden.

Wenn Sie von Ihren Mitarbeitern die Authentifizierung per Mobilgerät verlangen, kann es sein, dass Sie nach bundesstaatlichem Recht oder Gewerkschaftsvorschriften nicht verlangen dürfen,dass Mitarbeiter die Mobilitätskosten selbst tragen.[26] Daher müssen Sie die **Gesamtkosten des Gerätebesitzes berücksichtigen**: Hardware, wiederkehrende Servicekosten, Geräteverwaltung-slösungen, Sicherheitslösungen und sogar die Kosten für den Austausch von Geräten, um mit der Nachfrage nach neuen Geräten Schritt zu halten. Einige Unternehmen bieten außerdem eine monatliche Aufwandsentschädigung an, um die unternehmensweite Nutzung persönlicher Geräte zu unterstützen.

Selbst in BYOD-Situationen bleiben die **Governance- und Supportkosten** für die Legacy-Authentifizierung hoch. Forrester hat herausgefunden, dass große Unternehmen jährlich bis zu 1 Million US-Dollar für Personal und Infrastruktur ausgeben, um Anfragen zum Zurücksetzen von Passwörtern durch Mitarbeiter zu bearbeiten – und Passwörter stellen nur den ersten Faktor bei der 2FA- oder MFA-Authentifizierung dar.[27] Schätzungsweise 10 % der Geräte gehen jedes Jahr in Unternehmen verloren, werden gestohlen oder gehen kaputt – ein weiterer Faktor, der die Kosten für die Authentifizierung per Mobilgerät erhöht (ganz zu schweigen von den Risiken).[28]

Während Sicherheitsteams kostspielige Anstrengungen unternehmen, um Passwortrichtlinien in großem Umfang einzurichten und zu verwalten, sind Benutzer, die Probleme mit der Legacy-Authentifizierung haben, nicht **produktiv**. Dazu gehören vergessene Passwörter, Kontosperrungen, Richtlinien zum Zurücksetzen von Passwörtern, zeitraubende Workflows zur Erstellung und Eingabe von OTP/TOTP/Push-App-Codes oder die Notwendigkeit, neue Geräte zu registrieren. Authentifizierung ist ein unternehmenskritischer Service. Wenn Mitarbeiter nicht in der Lage sind, sich bei den von ihnen verwendeten Apps oder Portalen anzumelden, können sie ihre Arbeit nicht erledigen. Tatsächlich verliert das durchschnittliche Unternehmen jährlich aufgrund von Kontosperrungen 5,2 Mio. US-Dollar an Produktivität.[29]

Wie im Sicherheitsabschnitt erwähnt, entstehen die höchsten Kosten im Zusammenhang mit der Legacy-Authentifizierung durch Risiken, darunter das Risiko von **Compliance-Verstößen oder Datenschutzverletzungen, der Unterbrechung des Betriebs, der Bedrohung kritischer Infrastrukturen und des Verlusts von geistigem Eigentum**. Wenn komplexe Aufgaben wie gemeinsam genutzte Arbeitsplatzgeräte und Remote-Arbeit hinzukommen, wachsen diese Risiken noch weiter. Einer kürzlich durchgeführten Umfrage zufolge bezeichnen 40 % der Führungskräfte Cyberbedrohungen als das Geschäftsrisiko Nr. 1 – ein Risiko mit dem Potenzial, einem Unternehmen schwere Schäden zuzufügen und im schlimmsten Fall eine Wiederherstellung unmöglich zu machen.[30]

Infolge des mit Cyberbedrohungen verbundenen Schadenspotenzials sind die **Cyber-versicherungsprämien** in Hochrisikobranchen um bis zu 300 % gestiegen, und mittlerweile gelten neue Untergrenzen und Ausschlüsse sowie MFA als Grundvoraussetzung.[31] Es liegt an Ihnen als Unternehmen, die Effektivität der Cybersicherheit, einschließlich der MFA-Strategie, nachzuweisen, um Ihr Sicherheitsprofil für Cyberversicherer attraktiver zu gestalten. Der Contact-Center-Spezialist Afni konnte seine Cyberversicherungsprämien um 30 % senken, indem er demonstrierte, wie YubiKeys sein Risikoprofil reduziert.

Irrtum Nr. 3: Die Authentifizierung per Mobilgerät ist benutzerfreundlich

Die Realität: Die Verwendung und Verwaltung der Authentifizierung per Mobilgerät ist komplex

Da es kaum Hindernisse für die Implementierung gibt und Benutzer mit mobilen Authentifizierungs-methoden bestens vertraut sind, wird häufig davon ausgegangen, dass die Authentifizierung per Mobilgerät benutzerfreundlich oder einfach ist.

Die Wahrheit ist jedoch, dass Passwörter allein bereits eine Belastung für Benutzer und IT darstellen. In Kombination mit der Authentifizierung per Mobilgerät werden diese Herausforderungen bei der Benutzerfreundlichkeit nicht eliminiert, sondern eher noch verschärft.

Wissensbasiert
Schwer zu verwenden und zu merken, leicht zu manipulieren

Authentifikator-Verfügbarkeit
Mobilfunknetz, Akku, Besitz

Verzögerungen bei der Authentifizierung
Mehrstufig, OTP-Verzögerung, Fehlerrate, erneute Authentifizierung

MFA-Müdigkeit
Gedankenlose Genehmigung von Push-Authentifizierungsanfragen

Umweltaspekte
Handschuhe, Masken, Umgebungen mit Einschränkungen für Mobilgeräte

IT-Komplexität
Verwaltung von Passwortrichtlinien, Geräteregistrierung und -verwaltung, MFA-Integration

Laut einer branchenübergreifenden Studie geben 43 % der Unternehmen an, dass die **User Experience** das größte Hindernis bei der Nutzung der MFA darstellt.[32] Da der durchschnittliche Mitarbeiter 50–120 Passwörter[33] verwaltet, für die jeweils Richtlinien für das Erzwingen von Rücksetzungen und Zeitüberschreitungen gelten, müssen sich Benutzer mitunter Hunderte Male pro Tag authentifizieren – und das nur, wenn die MFA wie erwartet funktioniert. Vergessene Passwörter, OTP-Verzögerungen oder mobile Geräte, die verloren gehen, nicht aufgeladen oder offline sind, stehen auf einem ganz anderen Blatt.

Obwohl die Endbenutzererfahrung für die Mitarbeitererfahrung und Produktivitätsmetriken von entscheidender Bedeutung ist, müssen Überlegungen zur Benutzerfreundlichkeit auch für die **IT- und Helpdesk-Mitarbeiter** gelten. Aus der IT-Perspektive geben 41 % der Unternehmen an, dass die Komplexität ein Hindernis für die Einführung von MFA darstellt.[34] Die mobile MFA erfordert die Unterstützung von Passwörtern und Authentifizierung per Mobilgerät im gesamten Unternehmen, wodurch die Registrierung neuer Geräte, Schulungen, die Integration der MFA in neue Apps, die Geräteverwaltung und Helpdesk-Anfragen für das Zurücksetzen von Passwörtern oder verlorene Geräte komplexer werden.

Plattform-Authentifikatoren sind nicht portabel

Im Zuge der Abkehr von der herkömmlichen Authentifizierung entscheiden sich einige Unternehmen für Plattform-Authentifikatoren, d. h. Authentifikatoren, die als Trusted Platform Modules (TPM) oder sichere Elemente in Smartphones und Laptops integriert sind. Plattform-Authentifikatoren stützen sich auf ein vom Benutzer bereitgestelltes biometrisches Merkmal (Gesicht oder Fingerabdruck) als Authentifizierungsfaktor, der in Kombination mit einem besitzbasierten Authentifikator für hohe Sicherheit und Phishing-resistente FIDO2-Authentifizierung verwendet werden kann.

Plattform-Authentifikatoren können zwar eine gute Option für Benutzer mit nur einem Gerät sein, doch der durchschnittliche Mitarbeiter verwendet heute mindestens zwei Geräte für die Arbeit, ganz zu schweigen von gemeinsam genutzten Arbeitsplatzgeräten. Da das kryptografische Material für Plattform-Authentifikatoren in das Gerät selbst eingebettet ist, verhindert diese Form der Authentifizierung die **Portabilität**. Dadurch wird es schwieriger, zwischen Geräten zu wechseln, auf gemeinsam genutzte Arbeitsplatzgeräte zuzugreifen oder in Umgebungen mit Einschränkungen für Mobilgeräte zu arbeiten.

Irrtum Nr. 4: Die Authentifizierung per Mobilgerät bietet eine 360°-Abdeckung

Die Realität: Die Authentifizierung per Mobilgerät führt zu Lücken bei der MFA

Zwar können Unternehmen der MFA Priorität einräumen oder sie sogar vorschreiben, doch es gibt fast immer Lücken, die die Authentifizierung per Mobilgerät nicht füllen kann. Wo Lücken ohne eine umfassende MFA-Strategie bestehen, verwenden die meisten Unternehmen einfach Benutzernamen und Passwort.

Die Authentifizierung per Mobilgerät führt zu Lücken bei der MFA

Gleichstellung

Es gibt auch Benutzer, die kein Smartphone haben oder in Bereichen mit geringer Konnektivität leben.

Gewerkschafts-beschränkungen

Gewerkschaftsvorschriften können die Verwendung von persönlichen Mobilgeräten für Unternehmenszwecke, einschließlich der Authentifizierung, einschränken.

Präferenz

Mitarbeiter können sich weigern, ihre eigenen Telefone für die Authentifizierung per Mobilgerät zu verwenden.

Rechtliches

Viele Unternehmen dürfen rechtlich nicht verlangen, dass Mitarbeiter Unternehmens-Apps oder MFA auf privaten Geräten installieren oder verwenden, was zu Kosten für unternehmenseigene Geräte führt.

Eingeschränkter Zugang

Die Authentifizierung per Mobilgerät kann nicht in Bereichen mit Einschränkungen für Mobilgeräte verwendet werden, z. B. in Callcentern, Fertigungshallen oder Reinräumen.

Verfügbarkeit

Die Authentifizierung per Mobilgerät, die vom Akku des Geräts, dem Mobilfunksignal und der Anwesenheit des Geräts abhängt, ist gefährdet, wenn das Gerät vergessen, verloren oder gestohlen wird.

IT-Hindernisse

Die Authentifizierung per Mobilgerät kann durch den unerwarteten Verlust eines Geräts, die Notwendigkeit, ein neues Gerät zu registrieren, oder die Notwendigkeit, mehrere Geräte zu registrieren oder einzurichten, um die Anmeldung auf jedem Gerät zu unterstützen, unterbrochen werden.

Risiko

Die meisten Unternehmen sind sich bewusst, dass bestimmte Benutzergruppen und Authentifizierungsszenarien, darunter privilegierter Zugriff und Remote-Arbeit, ein höheres Risiko darstellen und dass ein solches Risiko eine stärkere Authentifizierung erfordert als die Authentifizierung per Mobilgerät.

> “Die passwortlose Anmeldung stellt eine enorme Veränderung in der Art und Weise dar, wie sich Milliarden von Benutzern, sowohl Unternehmen als auch Verbraucher, sicher bei ihren Windows 10-Geräten anmelden und sich bei auf Azure Active Directory basierenden Anwendungen und Diensten authentifizieren.”
>
> **Alex Simons** |
> Corporate Vice President PM,
> Microsoft Identity Division

Allein in den letzten zwei Jahren wurde der Druck zur Einführung einer Phishing-resistenten MFA in mehrere Vorschriften und Standards aufgenommen:

- Executive Order 14028 des Weißen Hauses[35] / Office of Management and Budget (OMB) Memo 22-09[36]
- National Security Memorandum/ NSM-8[37]
- NIS2[38]
- PCI DSS v4.0[39]
- FTC-Standards[40]

Irrtum Nr. 5: Die Authentifizierung per Mobilgerät ist zukunftssicher

Die Realität: Die Authentifizierung per Mobilgerät unterstützt keine neuen Vorschriften oder moderne, Phishing-resistente Abläufe ohne Passwort

MFA-Investitionen müssen Unternehmen Schutz bieten, der sich mit den Risiko- und Compliance-Anforderungen weiterentwickelt. Um zukunftssicher zu sein, sollte die MFA-Investition die wachsende regulatorische Anforderung an die **Phishing-resistente MFA**, die Notwendigkeit der Implementierung von **Zero Trust** und moderne Anmeldeabläufe wie die **passwortlose Authentifizierung** berücksichtigen.

Die **passwortlose Authentifizierung** wurde entwickelt, um **die mit Passwörtern verbundenen Schwachstellen in Bezug auf Sicherheit und Benutzerfreundlichkeit zu beseitigen. Allerdings können nicht alle Implementierungen beides leisten.** Das Senden eines OTP-Codes per SMS ist eine einfache, passwortlose Implementierung, aber weder sicher noch Phishing-resistent. Eine Smartcard ist eine sichere, Phishing-resistente passwortlose Implementierung, aber weder einfach noch kostengünstig.

Die Zukunft der passwortlosen Authentifizierung ist FIDO2/WebAuthn, die Kombination aus Phishing-resistenten FIDO-Zugangsdaten, auch **Passkey** genannt, und der WebAuthn-API, die eine einfachere und sicherere Anmeldung bei Websites und Apps von gängigen Geräten aus ermöglicht. Ein **Passkey** enthält jedoch nur die Zugangsdaten selbst (eine digitale Datei). Er verbirgt sich im **Authentifikator** auf einem Telefon, Laptop, Hardware-Schlüssel oder einem anderen Gerät. Und hier liegt der wesentliche Unterschied.

Ein **synchronisierter Passkey** befindet sich auf einem Smartphone, Tablet oder Laptop, wo er kopiert und mit vielen Geräten synchronisiert werden kann. Wie wir bei der Authentifizierung per Mobilgerät gesehen haben, macht diese „Mobilität“ die Verwendung einfach, aber nicht immer sicher oder einfach zu verwalten. Ein synchronisierter Passkey ist anfällig, da er so einfach freigegeben werden kann (an neue Geräten in einem Cloud-Konto oder über AirDrop), was die Kontrolle der Identität und des Risikos erschwert.

Ein **hardwaregebundener Passkey** befindet sich auf einem USB-Stick, der von alltäglichen Geräten getrennt bleibt, aber dennoch eine einfache Authentifizierung auf Geräten und Plattformen ermöglicht – eine zukunftssichere, passwortlose Lösung, die sowohl **einfach als auch sicher** ist. Weitere Informationen zu Passkeys finden Sie hier.

Wie bei der Authentifizierung per Mobilgerät verstärkt die Entwicklung hin zur passwortlosen Authentifizierung die Notwendigkeit, die verwendeten Geräte vom Authentifikator zu trennen. Ein hardwaregebundener Passkey ist eine portable Vertrauensbasis als Nachweis dafür, dass Sie über das spezielle Hardwaregerät verfügen, das das im Benutzerkonto registrierte kryptografische Material enthält. In Kombination mit einer PIN erfüllt er echte Multi-Faktor-Aut hentifizierungsanforderungen, indem er **etwas, das Sie kennen,** mit **etwas, das Sie sind**, und **etwas, das Sie haben** kombiniert.

YubiKey bietet einfache, Phishing-resistente MFA

Yubico hat den **YubiKey** entwickelt, einen Hardware-Sicherheitsschlüssel, der **Phishing-resistente Zwei-Faktor-, MFA- und passwortlose Authentifizierung** in einem großen Maßstab mit optimierter **User Experience** unterstützt.

Der YubiKey ist ein Multiprotokollschlüssel, der sowohl die Standards PIV/Smartcard als auch FIDO2/WebAuthn sowie OTP und OpenPGP unterstützt. Er lässt sich nahtlos in ältere und moderne Umgebungen integrieren und hilft Unternehmen dabei, **eine passwortlose Zukunft zu erreichen**, die von hardwaregebundenen Passkeys unterstützt wird.

Moderne Hardware-Sicherheitsschlüssel wie der YubiKey bieten einen Authentifizierungsprozess, der frei von menschlichem Versagen ist und Unternehmen einen Zero-Trust-Pfad eröffnet, der nachweislich das Risiko um 99,9 % senkt. Der YubiKey funktioniert im gesamten Unternehmen und an Orten, an denen die herkömmliche MFA nicht funktioniert. Er ist nicht auf externe Stromversorgung, Batterien oder Netzwerkverbindungen angewiesen.

Der YubiKey wurde entwickelt, um eine großartige **User Experience** zu bieten und Benutzern die sichere Anmeldung bei über tausend Produkten, Services und Anwendungen zu ermöglichen, darunter führende Identitäts- und Zugriffsmanagement-Plattformen (IAM), PAM-Lösungen (Privileged Access Management) und Cloud-Services, wobei zu keinem Zeitpunkt Geheimnisse zwischen den Diensten geteilt werden.

> “Ich wollte etwas, das absolut Phishing-resistent ist. Wenn wir uns schon die Mühe machen, einen Großteil unserer Infrastruktur für die Identitäts- und Zugriffsverwaltung neu zu gestalten, dann sollte sie auch zukunftssicher und widerstandsfähig sein.”[42]
>
> **Derek Pitts** |
> Director of Enterprise Security

Die wirtschaftlichen Auswirkungen von YubiKeys insgesamt[41]:

Höchste Sicherheit
Reduzieren Sie das Risiko um
99,9 %

Hohe Rendite
Erreichen Sie einen ROI von
203 %

Größerer Nutzen
Reduzieren Sie Support-Tickets um
75 %

Schneller
Verringern Sie die Authentifizierungszeit um mehr als das Vierfache
>4x

Cloudflare stoppt Phishing mit dem YubiKey

Cloudflare, eine der weltweit führenden Plattformen für die Bereitstellung von Internetinhalten und Sicherheit, hat 2020 mit dem YubiKey den Wechsel von der OTP-Technologie zu WebAuth/FIDO2 eingeleitet. Dabei wurde die Nutzung von YubiKeys in seiner sensibelsten Infrastruktur selektiv durchgesetzt, um die Benutzerakzeptanz und -interaktion zu fördern.

Als im Jahr 2022 ein ähnlicher Phishing-Angriff wie bei Twilio auf die Mitarbeiter von Cloudflare abzielte, spielte es keine Rolle, dass die Mitarbeiter dem Betrug zum Opfer fielen. Der Angriff wurde durch die Zero-Trust-Plattform von Cloudflare gestoppt, die vom YubiKey unterstützt wird. „Der Angreifer hat zwar versucht, sich mit dem kompromittierten Benutzernamen und Passwort in unsere Systeme einzuloggen“, schreibt das Cloudflare-Team in seinem Blog, „aber er konnte die Hardkey-Anforderung nicht umgehen“.

Der Einstieg ist ganz einfach

In diesem Whitepaper haben wir die dunkle Seite der Authentifizierung per Mobilgerät aufgedeckt, nämlich dass die einfache Nutzung oder Bereitstellung mit versteckten Risiken, Kosten, Problemen bei der Benutzerfreundlichkeit und Lücken einhergeht. Darüber hinaus haben wir untersucht, wie die Authentifizierung per Mobilgerät Unternehmen auf ihrem Weg zu Zero Trust und passwortlosem Arbeiten ausbremst.

Hat die Authentifizierung per Mobilgerät die sichere, einfache Lösung gebracht, die wir uns erhofft (oder erwartet) hatten? Nein. Doch zum Glück gibt es einen Weg, der nach vorne führt. Mit dem YubiKey ist es jetzt ganz einfach, eine Phishing-resistente MFA und passwortlose

Planung

Sicherstellung der Bereitschaft und Klärung von Anwendungsfällen und Benutzergruppen

Validierung

Bestätigung des Prozesses mit einer kleinen Gruppe von Benutzern vor der allgemeinen Umsetzung

Integration

Sicherstellung, dass die wichtigsten Apps und Services YubiKey-fähig sind

Einführung

Verteilung der Schlüssel an Benutzer per Komplettbereitstellungsservice oder über Vertriebspartner

Akzeptanz

Förderung der Akzeptanz durch bewährte Schulungen und Unterstützung

Messung

Berichterstattung zu Auswirkungen auf Sicherheit und Geschäftswert

Lösung bereitzustellen. Wir bieten einen einfachen 6-Schritte-Bereitstellungsleitfaden mit Best Practices, um die Implementierung moderner MFA in großem Maßstab zu beschleunigen:

Um das Rätselraten bei Planung, Einkauf und Lieferung zu beseitigen, bietet Yubico Professional Services und As-a-Service-Optionen an und arbeitet mit vielen Vertriebspartnern zusammen, um den Einstieg zu erleichtern.

YubiEnterprise Services*		Yubico Professional Services		
YubiEnterprise Subscription	YubiEnterprise Delivery	Deployment 360	Workshops	Implementierungsprojekte
Vereinfacht die Beschaffung, Aktualisierung und Unterstützung von YubiKeys durch Unternehmen	Lieferung an entfernte und Bürostandorte durch vertrauenswürdige Partner	Servicezeiten-Pakete	Kundenspezifische Inhalte	Technische Zusammenarbeit zur Implementierung von YubiKeys in Ihrer Umgebung

* YubiEnterprise Services sind für Unternehmen mit 500 oder mehr Benutzern verfügbar.

Quellen

1 Google Cloud, April 2023 Threat Horizons Report, (April 2023)

2 451 Research, 2021 Yubico und 451 Research Study, (April 2021)

3 IBM, 2022 Cost of Data Breach Report, (27. Juli 2022)

4 Das Weiße Haus, Executive Order on Improving the Nation's Cybersecurity, (12. Mai 2021)

5 OMB, M-22-09, (26. Januar 2022)

6 Das Weiße Haus, Memorandum on Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems, (19. Januar 2022)

7 Europäisches Parlament, NIS2-Richtlinie, (Februar 2023)

8 PCI, PCI DSS: v4.0, (März 2022)

9 Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)

10 Kurt Thomas und Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (17. Mai 2019)

11 Verizon, 2022 Data Breach Investigations Report, (24. Mai 2022)

12 Forrester Research, Inc., Optimize User Experience with Passwordless Authentication, (2. März 2020)

13 Egress, Email Security Risk Report 2023, (8 März 2023)

14 Verizon, 2022 Data Breach Investigations Report, (24. Mai 2022)

15 Pieter Arntz, Twilio data breach turns out to be more elaborate than suspected, (29. August 2022)

16 Lawrence Adams, Uber hacked, internal systems breached and vulnerability reports stolen, (16. September 2022)

17 Alicia Hope, American Airlines data breach linked to a phishing campaign exposed sensitive customer and employee personal information, (28. September 2022)

18 David Lumb, AT&T Vendor Data Breach Exposed 9 Million Customer Accounts, (9. März 2023)

19 WSOCTV, Chick-fil-A announces app data breach, tells customers how to protect personal information, (4. März 2023)

20 Twitter, An update on our security incident, (18. Juli 2020); New York State Department of Financial Services, Twitter Investigation Report, (aufgerufen am 14. September 2021)

21 Joseph Cox, A Hacker Got All My Texts for $16, VICE, (16. März 2021)

22 Kurt Thomas, Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking, (17. Mai 2019)

23 Rob Lemos, The state of two-factor authentication by text: What security pros need to know, (aufgerufen am 14. September 2021)

24 451 Research, 2021 Yubico und 451 Research Study, (April 2021)

25 LastPass und IDC, Enabling the Future of Work with EPM, Identity and Access Controls, (23. Februar 2022)

26 Shouse Labor Law Group, Cell phone reimbursement—when are workers entitled to it? (7. Januar 2022)

27 Forrester Research, Inc., Optimize User Experience with Passwordless Authentication, (2. März 2020)

28 LocknCharge, The True Cost of Lost or Missing Mobile Devices, (aufgerufen am 12. September 2021)

29 Ponemon Institute, 2019 State of Password and Authentication Security Behaviors Report, (aufgerufen am 14. September 2021)

30 PwC, PwC Pulse Survey: Managing business risks, (18. August 2022)

31 Ryan Smith, Cyber insurers raising premiums, lowering coverage limits – Bericht, (11. Oktober 2021)

32 451 Research, 2021 Yubico und 451 Research Study, (April 2021)

33 LastPass und IDC, Enabling the Future of Work with EPM, Identity and Access Controls, (23. Februar 2022)

34 451 Research, 2021 Yubico und 451 Research Study, (April 2021)

35 Das Weiße Haus, Executive Order on Improving the Nation's Cybersecurity, (12. Mai 2021)

36 OMB, M-22-09, (26. Januar 2022)

37 Das Weiße Haus, Memorandum on Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems, (19. Januar 2022)

38 Europäisches Parlament, NIS2-Richtlinie, (Februar 2023)

39 PCI SSC, PCI DSS v4.0, (März 2022)

40 James Dempsey, The FTC's rapidly evolving standards for MFA, (8. November 2022)

41 Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)

42 FIDO Alliance, Cloudflare embraces FIDO to help improve its own security, (2023)

43 Cloudflare, The mechanics of a sophisticated phishing scam and how we stopped it, (9. August 2022)

yubico

Über Yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO), Erfinder des YubiKey, bietet den Goldstandard für eine Phishing-resistente Multi-Faktor-Authentifizierung (MFA), die Kontoübernahmen vorbeugt und sichere Anmeldungen einfach und für jedermann möglich macht. Seit seiner Gründung im Jahr 2007 hat das Unternehmen federführend an der Festlegung globaler Standards für den sicheren Zugriff auf Computer, Mobilgeräte, Server, Browser und Internetkonten mitgewirkt. Yubico hat wesentlich zur Entwicklung der offenen Authentifizierungsstandards FIDO2, WebAuthn und FIDO Universal 2nd Factor (U2F) beigetragen und ist ein Pionier bei der Bereitstellung einer modernen, skalierbaren, hardwarebasierten Passkey-Authentifizierung für Kunden in über 160 Ländern.

Die Lösungen von Yubico ermöglichen eine passwortlose Anmeldung mit der sichersten Form der Passkey-Technologie. YubiKeys funktionieren out-of-the-box mit Hunderten von Verbraucher- und Unternehmensanwendungen und -diensten und vereinen starke Sicherheit mit Schnelligkeit und Benutzerfreundlichkeit.

Im Rahmen seiner Mission, das Internet für alle sicherer zu machen, spendet Yubico über die gemeinnützige Initiative Secure it Forward YubiKeys an Organisationen, die besonders gefährdete Personen unterstützen. Yubico hat seinen Hauptsitz in Stockholm und Santa Clara, Kalifornien. Für weitere Informationen über Yubico besuchen Sie uns bitte unter www.yubico.com