

Passkeys vs. 2FA: Warum der entscheidende Unterschied nicht im Komfort liegt

Von Thomas Faß · 3. Juni 2026 · aktualisiert 8. September 2026

Passkeys bieten strukturell besseren Schutz als klassische Zwei-Faktor-Authentifizierung (2FA), weil sie durch Public-Key-Kryptografie und Domain-Bindung phishing-resistent sind: Es gibt kein Passwort und keinen Code, den man abfangen oder auf einer gefälschten Seite eingeben könnte. 2FA bleibt ein wichtiger Fortschritt gegenüber reinen Passwörtern, ist aber je nach Methode – besonders SMS-Codes – weiterhin angreifbar.

Das Wichtigste in Kürze

- „Phishing-resistent“ ist seit Juli 2025 ein definierter Begriff, kein Adjektiv. NIST SP 800-63B-4 beschreibt ihn als die Fähigkeit des Verfahrens, die Preisgabe von Anmeldegeheimnissen an einen falschen Gegenüber zu verhindern – „without relying on the vigilance of the claimant“, also ohne auf die Wachsamkeit des Nutzers zu bauen. Verfahren mit manueller Eingabe eines Codes, also auch die Authenticator-App, erfüllen das ausdrücklich nicht.
- Passkeys bieten strukturell besseren Schutz als klassische 2FA, weil sie durch Public-Key-Kryptografie und Domain-Bindung phishing-resistent sind.
- Es gibt kein Passwort und keinen Code, den man abfangen oder auf einer gefälschten Seite eingeben könnte.
- 2FA bleibt ein wichtiger Fortschritt gegenüber reinen Passwörtern, ist aber je nach Methode – besonders SMS-Codes – weiterhin angreifbar.
- Der entscheidende Unterschied ist die Phishing-Resistenz, nicht der Komfort.

Kurz gesagt: Passkeys sind sicherer als klassische 2FA. Sie basieren auf den FIDO-Standards und sind von Natur aus phishing-resistent – der private Schlüssel verlässt das Gerät nie und ist an die jeweilige Domain gebunden. Klassische 2FA, vor allem per SMS-Code, bleibt anfällig für Phishing und SIM-Swapping. Dieser Vergleich zeigt den Unterschied im Detail und wann welches Verfahren sinnvoll ist.

Die digitale Landschaft ist von exponentiellem Wachstum und einer zunehmenden Vernetzung geprägt, was die Notwendigkeit robuster Authentifizierungsmechanismen verstärkt. Mit der Verlagerung kritischer Infrastrukturen und sensibler Daten in Online-Umgebungen steigt das Risiko von Cyberangriffen signifikant. Authentifizierung ist der erste und oft kritischste Verteidigungsmechanismus gegen unbefugten Zugriff.

Der Verizon Data Breach Investigations Report zeichnet dabei ein differenzierteres Bild, als oft zitiert wird. In der Ausgabe 2025 ist die Ausnutzung von Schwachstellen als Einstiegsweg um 34 Prozent gegenüber dem Vorjahr gewachsen und erreicht 20 Prozent. Der Missbrauch von Zugangsdaten bleibt der häufigste Einstiegsweg überhaupt – die Verwendung gestohlener Zugangsdaten ist in der Neuberechnung aber von 38 auf 31 Prozent gesunken. Der Weg über Anmeldedaten wird also nicht häufiger; er bleibt schlicht der

wichtigste. Diese Entwicklungen verdeutlichen, dass herkömmliche Sicherheitsmaßnahmen oft nicht mehr ausreichen, um digitale Identitäten effektiv zu schützen. Die digitale Sicherheit ist ein dynamisches Feld, in dem Innovationen nicht nur eine Option, sondern eine notwendige Antwort auf die sich ständig weiterentwickelnden Bedrohungen darstellen. Unternehmen, die nicht adaptieren, riskieren, ins Hintertreffen zu geraten.

Kurze Historie: Von Passwörtern zu Multi-Faktor-Ansätzen

Traditionell basierte die Authentifizierung auf Passwörtern, die als „etwas, das man weiß“ kategorisiert werden. Diese Methode hat sich jedoch als unzureichend erwiesen und ist anfällig für eine Vielzahl von Angriffen, darunter Brute-Force-Attacken, Wörterbuchangriffe, Credential Stuffing (durch Wiederverwendung von Passwörtern) und insbesondere Phishing. Die menschliche Tendenz zu schwachen oder wiederverwendeten Passwörtern stellt die größte Schwachstelle dar, da der Mensch oft das schwächste Glied in der Authentifizierungskette ist. Selbst komplexe Passwörter können durch Täuschung oder Diebstahl kompromittiert werden. Die grundlegende Anfälligkeit von Passwörtern als alleiniger oder primärer Authentifizierungsfaktor ist die ursächliche Triebkraft für die Entwicklung und Adoption stärkerer, passwortloser Methoden. Es geht nicht nur darum, Passwörter besser zu machen, sondern sie zu ersetzen.

Als Reaktion auf diese Schwachstellen etablierte sich die Multi-Faktor-Authentifizierung (MFA), deren häufigste Form die Zwei-Faktor-Authentifizierung (2FA) ist. 2FA erfordert zwei unterschiedliche Nachweise der Identität, um den Zugriff zu gewähren. Diese Entwicklung markiert einen kontinuierlichen Fortschritt in der Authentifizierung, um den Schutz digitaler Identitäten zu verbessern und die Benutzerfreundlichkeit nicht zu vernachlässigen. Der Anstieg von Phishing-Angriffen und Zugangsdaten-Diebstahl zeigt, dass bestehende Sicherheitsmaßnahmen, einschließlich vieler 2FA-Formen, nicht ausreichen, um mit der Raffinesse der Angreifer Schritt zu halten. Dies führt zu einem kontinuierlichen Druck auf die Entwicklung neuer, widerstandsfähigerer Authentifizierungstechnologien, die „phishing-resistent“ durch Design sind.

Zwei-Faktor-Authentifizierung (2FA): Der etablierte Standard mit bekannten Herausforderungen

Die wachsende Bedeutung robuster Authentifizierung in einer vernetzten Welt. Die digitale Landschaft ist von exponentiellem Wachstum und einer zunehmenden Vernetzung geprägt, was die Notwendigkeit robuster Authentifizierungsmechanismen verstärkt. Mit der Verlagerung kritischer Infrastrukturen und sensibler Daten in Online-Umgebungen steigt das Risiko von Cyberangriffen signifikant. Authentifizierung ist der erste und oft kritischste Verteidigungsmechanismus gegen unbefugten Zugriff.

Die Notwendigkeit einer starken Authentifizierung wird durch die steigende Anzahl von Cyberangriffen unterstrichen. Wie wenig Zeit dabei bleibt, hat Verizon im Data Breach Investigations Report 2024 gemessen: Nach dem Öffnen einer Phishing-Mail vergehen im Median 21 Sekunden bis zum Klick auf den Link – und danach nur weitere 28 Sekunden, bis die Zugangsdaten eingegeben sind. Weniger als eine Minute von der geöffneten Mail bis zum abgegriffenen Passwort. Wer in dieser Zeitspanne auf Aufmerksamkeit setzt, setzt auf das Falsche. Diese Entwicklungen verdeutlichen, dass herkömmliche Sicherheitsmaßnahmen oft nicht mehr ausreichen, um digitale Identitäten effektiv zu schützen. Die digitale Sicherheit ist ein dynamisches Feld, in dem Innovationen nicht nur eine Option, sondern eine notwendige

Antwort auf die sich ständig weiterentwickelnden Bedrohungen darstellen. Unternehmen, die nicht adaptieren, riskieren, ins Hintertreffen zu geraten.

Definition und grundlegende Prinzipien von 2FA

2FA ist eine elektronische Authentifizierungsmethode, bei der einem Benutzer der Zugriff auf eine Website oder Anwendung erst nach erfolgreicher Präsentation von genau zwei verschiedenen Nachweistypen gewährt wird. Es ist die häufigste Form der Multi-Faktor-Authentifizierung (MFA), die generell mehr als einen Faktor erfordert.

Die zur Verifizierung der Identität verwendeten Faktoren können aus drei Kategorien stammen:

- Wissen (Something You Know): Dies umfasst Passwörter, PINs oder Sicherheitsfragen.
- Besitz (Something You Have): Hierzu zählen physische Objekte wie Smartphones, Hardware-Token oder Bankkarten.
- Inhärenz (Something You Are): Dies bezieht sich auf biometrische Merkmale wie Fingerabdrücke, Gesichtserkennung oder Netzhautscans.

Das grundlegende Prinzip von 2FA beruht auf der Annahme, dass ein Angreifer unwahrscheinlich alle erforderlichen Faktoren für den Zugriff erlangen kann. Selbst wenn ein Passwort kompromittiert wird, bietet die zweite Ebene des Nachweises einen Schutzmechanismus.

Gängige 2FA-Methoden im Detail

SMS-basierte OTPs (One-Time Passwords):

- Funktionsweise: Ein numerischer Einmalcode wird per SMS an das registrierte Mobiltelefon des Benutzers gesendet, der dann zusätzlich zum Passwort eingegeben werden muss.
- Komfort: Diese Methode ist weit verbreitet und einfach zu nutzen, da fast jeder ein Mobiltelefon besitzt und keine zusätzliche App benötigt wird.
- Bekannte Schwachstellen: Trotz ihrer Bequemlichkeit gelten SMS-OTPs als die am wenigsten sichere 2FA-Methode. Sie sind anfällig für:
 - SIM-Swapping-Angriffe: Hierbei können Angreifer Mobilfunkanbieter dazu bringen, die Telefonnummer des Opfers auf eine neue SIM-Karte zu übertragen, um SMS-Codes abzufangen.
 - Phishing-Angriffe: Benutzer können durch gefälschte Websites dazu verleitet werden, sowohl ihr Passwort als auch den SMS-OTP einzugeben.
 - Abfangen von Nachrichten: SMS-Nachrichten können über Schwachstellen in Mobilfunknetzen (z. B. SS7-Schwachstellen) abgefangen werden.
 - Verzögerungen/Blockaden: SMS-Codes können verzögert ankommen oder ganz blockiert werden, was zu Frustration führt.

Authenticator-Apps (TOTP/HOTP):

- Funktionsweise: Apps wie Google Authenticator oder Authy generieren zeitbasierte (TOTP) oder ereignisbasierte (HOTP) Einmalcodes, die sich ständig ändern. Das Schlüsselmaterial zur Codegenerierung wird sicher in der App gespeichert.
- Erhöhte Sicherheit: Diese Methode ist deutlich sicherer als SMS-OTPs, da die Codes lokal auf dem Gerät generiert werden und keine Mobilfunkverbindung erforderlich ist, was sie resistenter gegen Abfangen macht.
- Offline-Fähigkeit: Codes können auch ohne Netzwerk- oder Mobilfunkverbindung generiert werden.
- Vorteile: Sie ermöglichen die Verwaltung mehrerer 2FA-Konten in einer einzigen App und bieten oft Backup- und Wiederherstellungsfunktionen.

Hardware-Sicherheitstoken:

- Funktionsweise: Physische Geräte (z. B. YubiKeys) generieren Codes oder führen kryptographische Operationen durch. Sie sind oft USB-, NFC- oder Bluetooth-basiert und müssen physisch mit dem Gerät des Benutzers verbunden werden.
- Höchste Sicherheit: Hardware-Token bieten eine sehr hohe Resistenz gegen Phishing und Manipulation, da der private Schlüssel auf dem Token gespeichert ist und das Gerät nicht verlassen kann. Sie sind ideal für regulierte oder hochsichere Umgebungen.
- Potenzielle Komforteinschränkungen: Sie erfordern eine anfängliche Investition in Hardware und können für Benutzer unpraktisch sein, wenn das Token vergessen oder verloren wird.

Biometrische Faktoren (Fingerabdruck, Gesichtserkennung):

- Funktionsweise: Diese Faktoren nutzen einzigartige physische Merkmale des Benutzers zur Verifizierung und sind oft direkt in Smartphones oder Laptops integriert.
- Komfort: Sie bieten eine sehr schnelle und intuitive Anmeldung.
- Inhärente Sicherheit: Biometrische Daten gelten als sehr schwer zu knacken. Bei einer Kompromittierung können die Auswirkungen jedoch schwerwiegend sein, da biometrische Daten nicht einfach geändert werden können. Die Fortschritte in der KI-gestützten Bildgenerierung wecken zudem Bedenken hinsichtlich der potenziellen Umgehung von Gesichtserkennungssystemen.

Vorteile von 2FA gegenüber reinen Passwörtern

Der Einsatz von 2FA bietet gegenüber der reinen Passwortauthentifizierung mehrere klare Vorteile:

- Stärkere Sicherheit: 2FA erhöht die Kontosicherheit erheblich, da Angreifer zwei Anmeldeinformationen stehlen müssen, um in ein System einzudringen. Selbst wenn ein Passwort kompromittiert wird, bietet die zweite Ebene Schutz.
- Schutz vor Phishing (eingeschränkt): Während 2FA-Codes abgefangen werden können, erschwert die zusätzliche Ebene den direkten Zugriff nach einem Phishing-Angriff auf das Passwort.
- Einhaltung von Industriestandards: 2FA ist oft eine Anforderung oder starke Empfehlung von Aufsichtsbehörden in verschiedenen Branchen (z. B. Finanzwesen, Gesundheitswesen), um Compliance-Standards zu erfüllen.

Herausforderungen und Limitationen von 2FA

Dieselbe Norm sagt ausdrücklich, welche Verfahren die Anforderung **nicht** erfüllen — und begründet es: „Authenticators that involve the manual entry of an authenticator output (e.g., out-of-band and OTP authenticators) SHALL NOT be considered phishing-resistant because the manual entry does not bind the authenticator output to the specific session being authenticated.“

Das trifft nicht nur die SMS. Es trifft auch die Authenticator-App auf dem Diensthandy, die in vielen Unternehmen als der sichere Weg gilt. Wie überzeugend die Aufforderung zur Code-Eingabe inzwischen aussehen kann, zeigt das [KI-gestützte Phishing](#). Der Grund ist nicht die Übertragung, sondern die manuelle Eingabe: Ein Code ist an keine Sitzung gebunden, deshalb kann ein falscher Gegenüber ihn weiterreichen und sich damit selbst anmelden.

Zum Mobilfunknetz als Übertragungsweg formuliert NIST eine ausdrückliche Warnung: „Verifiers SHOULD consider risk indicators (e.g., device swap, SIM change, number porting, other abnormal behavior) before using the PSTN to deliver an out-of-band authentication secret.“ Für E-Mail lässt die Formulierung keinen Spielraum: „Email SHALL NOT be used for out-of-band authentication.“

Trotz der unbestreitbaren Vorteile ist 2FA nicht ohne Herausforderungen und Limitationen:

- **Benutzerakzeptanz und Reibung:** Viele Benutzer empfinden 2FA als unbequem, da es zusätzliche Schritte und möglicherweise mehrere Geräte erfordert. Dies kann zu „MFA-Müdigkeit“ und einer geringeren Akzeptanz führen. Die Notwendigkeit, zusätzliche Schritte durchzuführen oder ein zweites Gerät zu verwenden, wird als lästig empfunden. Die Akzeptanz von Sicherheitsmaßnahmen hängt stark von ihrer Benutzerfreundlichkeit ab. Wenn 2FA als zu umständlich wahrgenommen wird, kann dies die Adoptionsrate senken und Benutzer dazu verleiten, weniger sichere Alternativen zu wählen oder die Funktion zu deaktivieren. Dies untergräbt die beabsichtigte Sicherheitsverbesserung in der Praxis. Ein technisch überlegenes System, das nicht genutzt wird, ist ineffektiv.
- **Geräteabhängigkeit:** Viele 2FA-Methoden sind auf ein sekundäres Gerät (z. B. Smartphone) angewiesen. Bei Verlust, Beschädigung oder leerem Akku kann der Zugriff auf Konten verwehrt sein.
- **Implementierungskosten:** Für Unternehmen können erhebliche Kosten für die Anschaffung von Hardware-Token, die Einrichtung und Verwaltung von Systemen sowie die Schulung der Mitarbeiter anfallen. SMS-OTPs verursachen zudem Transaktionsgebühren. Dies führt zu einem erhöhten Management-Aufwand und kann insbesondere kleinere Unternehmen zögern lassen oder zu suboptimalen Implementierungen führen, die wiederum Sicherheitslücken schaffen.

- **Nicht narrensicher:** Trotz erhöhter Sicherheit ist 2FA nicht vollständig unverwundbar. SIM-Swapping und ausgefeilte Phishing-Techniken können bestimmte 2FA-Methoden umgehen. Auch Authenticator-Apps können bei fehlenden Retry-Limits für Brute-Force-Angriffe anfällig sein. Obwohl 2FA als „zweite Sicherheitsebene“ vermarktet wird, ist es wichtig zu verstehen, dass es sich um eine Verbesserung der Passwortsicherheit handelt, nicht um eine vollständige Eliminierung der inhärenten Schwachstellen. Die Abhängigkeit von einem „Shared Secret“ (Passwort) bleibt bestehen, und der zweite Faktor kann je nach Methode selbst Schwachstellen aufweisen. Die Schwachstellen des ersten Faktors (Passwort) und die potenziellen Angriffsvektoren auf den zweiten Faktor (insbesondere SMS/E-Mail) bedeuten, dass ein Angreifer mit ausreichend Aufwand oder durch Ausnutzung menschlicher Schwächen immer noch einen Weg finden kann, die Authentifizierung zu umgehen. Unternehmen und Benutzer müssen verstehen, dass traditionelles 2FA eine wichtige Risikominderung darstellt, aber keine vollständige Beseitigung aller Authentifizierungsrisiken. Dies schafft die Notwendigkeit für fundamental sicherere Ansätze wie Passkeys.
- **Kompatibilität mit Legacy-Systemen:** Die Integration von 2FA in bestehende, ältere Systeme kann eine Herausforderung darstellen und zusätzliche Konfiguration oder Anpassung erfordern.

Passkeys: Die passwortlose Zukunft der Authentifizierung

Passkeys sind eine innovative Authentifizierungsmethode, die darauf abzielt, die Sicherheit zu erhöhen und gleichzeitig die Benutzerfreundlichkeit zu verbessern, indem sie die Abhängigkeit von Passwörtern reduziert.

Definition und technische Grundlagen

Ein Passkey ist ein FIDO-Authentifizierungs-Credential, das auf FIDO-Standards basiert. Es ermöglicht Benutzern, sich bei Apps und Websites mit demselben Prozess anzumelden, den sie zum Entsperren ihres Geräts verwenden (Biometrie, PIN oder Muster). Passkeys sind kryptographische FIDO-Anmeldeinformationen, die an das Konto eines Benutzers auf einer Website oder Anwendung gebunden sind. Sie ersetzen Passwörter durch kryptographische Schlüsselpaare für eine Phishing-resistente Anmeldesicherheit und eine verbesserte Benutzererfahrung.

Passkeys nutzen asymmetrische Kryptographie (Public-Key-Kryptographie), die zwei separate Schlüssel verwendet: einen öffentlichen Schlüssel und einen privaten Schlüssel. Der private Schlüssel wird sicher in einer dedizierten sicheren Enklave auf dem Gerät des Benutzers (z. B. einem Hardware-Sicherheitsmodul oder dem sicheren Speicher des Betriebssystems) gespeichert und verlässt das Gerät niemals. Der öffentliche Schlüssel hingegen wird an den Server der Website oder Anwendung gesendet und dort gespeichert. Ein Angreifer, der nur den öffentlichen Schlüssel besitzt, kann sich nicht als Benutzer ausgeben, da der private Schlüssel für die Authentifizierung erforderlich ist. Passkeys verlagern den Authentifizierungsansatz von „etwas, das man weiß“ (Passwort) zu „etwas, das man hat“ (Gerät) und „etwas, das man ist“ (Biometrie/PIN). Dieser fundamentale Wandel verringert die Abhängigkeit vom anfälligen menschlichen Gedächtnis und der Anfälligkeit für Social Engineering-Angriffe, indem die Sicherheit auf kryptographische, hardwaregestützte Prozesse verlagert wird. Dies stellt eine robustere und zukunftssichere Grundlage für die digitale Identität dar.

Passkeys basieren auf den offenen FIDO-Standards, insbesondere FIDO2, das die W3C Web Authentication (WebAuthn) Spezifikation und die Client-to-Authenticator Protocols (CTAP) der FIDO Alliance umfasst. WebAuthn definiert eine Standard-Web-API, die in Browser und Plattformen integriert wird und FIDO-Authentifizierung in den Browser bringt. CTAP ermöglicht die Kommunikation zwischen dem Client (Browser/App) und externen Authentifikatoren (z. B. FIDO-Sicherheitsschlüssel, mobile Geräte) über USB, NFC oder BLE.

Wie Passkeys funktionieren: Ein nahtloser und sicherer Prozess

Die Funktionsweise von Passkeys lässt sich in mehreren Schritten beschreiben:

- **Generierung von Schlüsselpaaren:** Wenn ein Benutzer einen Passkey für einen Dienst einrichtet, generiert sein Gerät ein öffentliches-privates Schlüsselpaar. Der öffentliche Schlüssel wird an den Server gesendet und dort gespeichert.
- **Speicherung des privaten Schlüssels:** Der private Schlüssel wird sicher in einer dedizierten sicheren Enklave auf dem Gerät des Benutzers (z. B. Hardware-Sicherheitsmodul oder sicherer Speicher des Betriebssystems) gespeichert und verlässt das Gerät niemals.
- **Authentifizierung über Biometrie/PIN:** Wenn sich ein Benutzer bei einer Website oder App anmelden möchte, sendet der Server eine kryptographische Herausforderung (Nonce) an das Gerät des Benutzers. Das Gerät signiert diese Herausforderung mit dem privaten Schlüssel. Diese digitale Signatur wird an den Server zurückgesendet, der sie mit dem zuvor gespeicherten öffentlichen Schlüssel verifiziert. Ist die Signatur gültig, wird der Zugriff gewährt. Der Benutzer autorisiert diesen Vorgang mit der gleichen Methode, die er zum Entsperren seines Geräts verwendet (Biometrie wie Fingerabdruck oder Gesichtserkennung, oder eine PIN).
- **Cross-Device-Synchronisierung:** Passkeys können sicher über die Cloud (z. B. iCloud Keychain, Google Password Manager) über die Geräte eines Benutzers hinweg synchronisiert werden – die Nutzung bleibt damit über Geräte hinweg nahtlos. Alternativ können sie an ein bestimmtes Hardware-Token gebunden sein (gerätegebundene Passkeys).

Die inhärente Phishing-Resistenz von Passkeys

„Phishing-resistent“ ist keine Marketingvokabel. Das US-amerikanische National Institute of Standards and Technology hat den Begriff in seinen Digital Identity Guidelines festgeschrieben – **NIST SP 800-63B-4, „Authentication and Authenticator Management“, Juli 2025**. Die Definition lautet dort: Phishing-Resistenz ist „the ability of the authentication protocol to prevent the disclosure of authentication secrets and valid authenticator outputs to an impostor verifier ... **without relying on the vigilance of the claimant**“.

Der letzte Halbsatz ist der entscheidende. Ein Verfahren gilt erst dann als phishing-resistent, wenn es **nicht** davon abhängt, dass der Nutzer aufmerksam ist – dieselbe Haltung, die einer [Zero-Trust-Architektur](#) zugrunde liegt: nicht auf Vertrauen bauen, sondern auf Prüfung. Genau das ist der Unterschied zu jeder Schulung: Awareness setzt Wachsamkeit voraus, die Norm verlangt ein Verfahren, das ohne sie auskommt.

Für die höchste Vertrauensstufe formuliert die Norm: „AAL3 authentication requires the use of a cryptographic authenticator with a non-exportable private key that provides phishing resistance.“ **Nicht exportierbar** heißt: nicht weitergebbar. Einen Code kann man vorlesen, weiterleiten, auf einer falschen

Seite eintippen. Einen nicht exportierbaren privaten Schlüssel kann man nicht herausgeben – auch dann nicht, wenn man es wollte.

Für die mittlere Stufe gilt: „Verifiers SHALL offer at least one phishing-resistant authentication option at AAL2.“ Für US-Bundesbehörden ist die Sache entschieden: „Federal agencies SHALL require their staff, contractors, and partners to use phishing-resistant authentication to access federal information systems.“ Als Verfahren erkennt die Norm zwei Wege an: Channel Binding und Verifier Name Binding.

Passkeys sind von Natur aus Phishing-resistent. Dies liegt daran, dass sie an die Identität einer bestimmten Website oder App gebunden sind. Der Browser oder das Betriebssystem stellt sicher, dass ein Passkey nur mit der Website oder App verwendet werden kann, die ihn erstellt hat. Dies verhindert, dass Benutzer auf betrügerische Websites gelockt werden, da die Domain-Bindung überprüft wird. Es gibt keine Passwörter zu stehlen und keine Anmeldedaten, die für Angriffe verwendet werden könnten.

Passkeys verschieben die Verantwortung für den Phishing-Schutz vom Benutzer auf das System. Während traditionelle 2FA-Methoden oft immer noch auf die Fähigkeit des Benutzers angewiesen sind, Phishing-Versuche zu erkennen und das „Shared Secret“ (Passwort) zu schützen, eliminieren Passkeys diese Abhängigkeit. Der technische Mechanismus der Domain-Bindung schützt den Benutzer automatisch, selbst wenn dieser auf einen Phishing-Link klickt. Dies ist ein fundamentaler Unterschied in der Sicherheitsarchitektur, der die Angriffsfläche drastisch reduziert, die durch menschliches Fehlverhalten entsteht.

Vorteile von Passkeys: Sicherheit und Benutzerfreundlichkeit im Einklang

- Überlegene Sicherheit:
- Phishing-Resistenz: Wie oben erläutert, sind Passkeys immun gegen Phishing, da sie an die Domain gebunden sind und keine Passwörter übertragen werden.
- Schutz vor Credential Stuffing und Replay Attacks: Da jeder Passkey einzigartig für jede Website/App ist und keine Passwörter wiederverwendet werden, sind sie gegen Credential Stuffing und Replay Attacks immun.
- Geringere Angriffsfläche auf dem Server: Server speichern nur den öffentlichen Schlüssel, der für Angreifer nutzlos ist. Dies reduziert den Wert von Server-Breaches erheblich.

Verbesserte Benutzererfahrung:

- Schneller, reibungsloser Login: Benutzer müssen keine Benutzernamen und Passwörter mehr eingeben. Die Anmeldung erfolgt mit einem einfachen Tap oder Biometrie/PIN, was den Prozess deutlich beschleunigt und vereinfacht. Microsoft berichtete im Mai 2025, dass Anmeldungen mit Passkeys dreimal häufiger gelingen als mit Passwort – rund 98 Prozent gegenüber etwa 32 Prozent – und achtmal schneller sind als die Kombination aus Passwort und Multifaktor-Verfahren.
- Kein Passwortmanagement: Die Notwendigkeit, komplexe Passwörter zu merken oder zu verwalten, entfällt, was den „cognitive load“ für Benutzer reduziert.
- AutoFill UI: Passkeys bieten eine nahtlose Integration in Browsern und auf mobilen Geräten.

- **Cross-Device- und Cross-Plattform-Kompatibilität:** Passkeys sind so konzipiert, dass sie geräte- und plattformübergreifend funktionieren. Apple, Google und Microsoft haben sich zur Interoperabilität über die FIDO Alliance verpflichtet und diese bereits umgesetzt, z. B. durch QR-Code-Scans für den Login auf anderen Geräten. Die gemeinsame Verpflichtung und aktive Implementierung von Passkeys durch diese großen Technologieunternehmen ist ein entscheidender Faktor für die breite Akzeptanz. Diese Zusammenarbeit überwindet traditionelle Ökosystem-Grenzen und schafft eine einheitliche, interoperable Infrastruktur, die für Endbenutzer und Entwickler gleichermaßen von Vorteil ist. Dies beschleunigt die „passwortlose Zukunft“ erheblich.
- **Reduzierter IT-Support-Aufwand:** Durch die Eliminierung von Passwörtern und die Vereinfachung des Anmeldeprozesses können Unternehmen den Aufwand für Passwort-Resets und damit verbundene Support-Anfragen reduzieren. Auch die Kosten für SMS-Integration entfallen.

Herausforderungen bei der Einführung und Akzeptanz von Passkeys

Obwohl Passkeys erhebliche Vorteile bieten, gibt es bei ihrer Einführung und Akzeptanz auch Herausforderungen:

- **Geräteabhängigkeit und Wiederherstellungsszenarien:**
- **Geräteverlust/-ausfall:** Wenn ein Benutzer sein primäres Gerät verliert oder es ausfällt, kann der Zugriff auf Passkeys verloren gehen.
- **Wiederherstellung:** Die Wiederherstellung von Passkeys ist oft immer noch an traditionelle Methoden (Passwörter, E-Mail, SMS) gebunden, was eine potenzielle Schwachstelle darstellt. Es bedarf robuster Backup-Lösungen. Die Abhängigkeit von traditionellen, weniger sicheren Methoden für die Passkey-Wiederherstellung stellt ein erhebliches Risiko dar, das die ansonsten überlegene Sicherheit von Passkeys untergraben kann. Wenn der sicherste Authentifizierungsmechanismus über einen unsicheren Kanal wiederhergestellt werden kann, ist die Sicherheit der gesamten Kette nur so stark wie das schwächste Glied in der Wiederherstellung. Dies erfordert von Unternehmen, die Sicherheit der Wiederherstellungskanäle zu stärken und alternative, sicherere Wiederherstellungsmethoden zu entwickeln oder zu nutzen.
- **Benutzeraufklärung und Akzeptanzbarrieren:**
- **Lernkurve:** Benutzer müssen lernen, wie Passkeys eingerichtet und verwendet werden, was eine Barriere darstellen kann.
- **Widerstand gegen Veränderungen:** Einige Benutzer sind möglicherweise resistent gegenüber der Änderung ihrer etablierten Passwortgewohnheiten.
- **Missverständnisse:** Die Verwendung von Biometrie kann fälschlicherweise den Eindruck erwecken, dass sensible Informationen an den Server gesendet werden, obwohl dies nicht der Fall ist.
- **Ökosystem-Reife und Kompatibilität mit Legacy-Systemen:**
- **Inkonsistente Unterstützung:** Obwohl die Unterstützung schnell wächst, sind Passkeys noch nicht auf allen Geräten, Websites oder in allen Credential Managern vollständig kompatibel. Ältere Geräte unterstützen möglicherweise keine Passkeys.

- **Legacy-Systeme:** Die Integration von Passkeys in ältere, nicht FIDO2-kompatible Systeme kann eine Herausforderung darstellen.
- **Potenzieller Vendor Lock-in bei bestimmten Implementierungen:** Einige Passkey-Implementierungen können zu einem Vendor Lock-in führen, bei dem es schwierig ist, Passkeys zwischen verschiedenen Plattformen (z. B. Apple und Android) zu übertragen. Die FIDO Alliance arbeitet jedoch an Standards wie dem Credential Exchange Protocol (CXP), um dies zu beheben.
- **Umgang mit geteilten Konten:** Das Teilen von Konten, wie es bei Familien häufig vorkommt, ist mit Passkeys schwieriger als mit Passwörtern.

Der direkte Vergleich: Passkeys schlagen 2FA in der Sicherheit

Die digitale Welt entwickelt sich ständig weiter, und mit ihr die Anforderungen an sichere und benutzerfreundliche Authentifizierungsmethoden. Während die Zwei-Faktor-Authentifizierung (2FA) einen wichtigen Fortschritt gegenüber der reinen Passwortnutzung darstellt, bieten Passkeys eine noch überlegenere Lösung. Ein detaillierter Vergleich beleuchtet die Stärken und Schwächen beider Ansätze in Bezug auf Sicherheit, Benutzerfreundlichkeit und technische Aspekte.

Sicherheit: Der entscheidende Unterschied

Im Bereich der Sicherheit übertreffen Passkeys traditionelles 2FA, insbesondere bei der Phishing-Resistenz. Während Passwörter und selbst per SMS versendete Einmalpasswörter (OTPs) anfällig für Phishing-Angriffe sind, sind Passkeys inhärent phishing-resistent. Der private Schlüssel eines Passkeys verlässt das Gerät nie und ist an eine bestimmte Domain gebunden, wodurch Betrugsversuche ins Leere laufen.

Ähnlich verhält es sich mit dem Schutz vor Credential Theft/Reuse und Replay Attacks. Traditionelles 2FA ist hier schwächer, da Passwörter gestohlen und OTPs potenziell abgefangen und wiederverwendet werden können. Passkeys hingegen nutzen einzigartige kryptografische Schlüsselpaare pro Dienst und reagieren auf zeitgebundene kryptografische Herausforderungen, was sie immun gegen solche Angriffe macht.

Auch die Angriffsfläche auf Server-Seite ist bei Passkeys deutlich geringer. Server speichern bei Passkeys lediglich den öffentlichen Schlüssel, der für Angreifer nutzlos ist, selbst wenn es zu einem Server-Hack kommt. Bei traditionellem 2FA müssen hingegen Passwörter oder deren Hashes gespeichert werden, was ein höheres Risiko darstellt. Die gerätabhängige Sicherheit des privaten Schlüssels ist bei Hardware-Token-basiertem 2FA hoch, bei SMS- oder App-basiertem 2FA jedoch variabler; Passkeys bieten hier durch die sichere Speicherung auf dem Gerät oder Hardware-Token ebenfalls ein hohes Maß an Sicherheit.

Benutzererfahrung: Einfacher und schneller

Für den Endnutzer bieten Passkeys einen klaren Komfortvorteil. Der Login-Prozess ist passwortlos; Benutzer entsperren ihr Gerät einfach per Biometrie oder PIN, was den Anmeldevorgang im Vergleich zur Eingabe eines Passworts und eines zweiten Faktors erheblich schneller und reibungsloser macht. Dies reduziert die Komplexität und Reibung deutlich und minimiert die sogenannte „MFA-Müdigkeit“.

Ein weiterer großer Vorteil ist, dass Passwort-Management komplett entfällt. Benutzer müssen sich keine komplexen Passwörter mehr merken oder diese verwalten, was den kognitiven Aufwand erheblich senkt.

Technische Aspekte: Standardisierung und Kompatibilität

Passkeys basieren auf offenen FIDO-Standards (insbesondere WebAuthn), was ihre Standardisierung und breite Akzeptanz fördert. Traditionelle 2FA-Methoden basieren oft auf diversen proprietären Implementierungen.

Der Implementierungsaufwand für Anbieter ist bei beiden Methoden als mittel einzustufen. Während bei traditionellem 2FA die Integration verschiedener Methoden und Legacy-Kompatibilität eine Rolle spielt, erfordert Passkey die WebAuthn API-Integration und Ökosystem-Support. Auch bei den Kosten für Anbieter zeigen Passkeys Vorteile, da sie keine SMS-Gebühren verursachen und den Supportaufwand für Passwort-Resets reduzieren.

Die Cross-Plattform/Geräte-Kompatibilität ist bei Passkeys dank der FIDO-Standards und der Zusammenarbeit großer Technologieunternehmen (wie Apple, Google, Microsoft) hoch – die Nutzung bleibt über Geräte und Ökosysteme hinweg nahtlos. Bei traditionellem 2FA ist dies oft variabler und geräte-/plattformspezifischer.

Eine wichtige Herausforderung bleibt die Wiederherstellung bei Geräteverlust. Bei beiden Methoden ist die Wiederherstellung oft noch an traditionelle, potenziell weniger sichere Fallback-Methoden gebunden, was eine Schwachstelle darstellen kann und robuste Backup-Lösungen erfordert.

Zusammenfassend lässt sich sagen, dass Passkeys eine signifikante Weiterentwicklung in der Authentifizierungslandschaft darstellen, die sowohl die Sicherheit als auch die Benutzerfreundlichkeit im Vergleich zu traditionellen 2FA-Methoden deutlich verbessert. Trotz einiger Herausforderungen bei der Einführung sind sie der Weg in eine passwortlose und sicherere digitale Zukunft.

Passkeys stellen in mehreren kritischen Sicherheitsaspekten eine überlegene Lösung gegenüber traditionellen 2FA-Methoden dar. Der Kern dieser Überlegenheit liegt in der fundamentalen Eliminierung des Passworts und der damit verbundenen Angriffsvektoren.

Ein wesentlicher Vorteil von Passkeys ist ihre inhärente Phishing-Resistenz. Im Gegensatz zu Passwörtern, die „etwas, das man weiß“ darstellen und durch Täuschung abgefragt werden können, basieren Passkeys auf kryptographischen Schlüsselpaaren, bei denen der private Schlüssel das Gerät des Benutzers niemals verlässt. Die Authentifizierung ist an die spezifische Domain oder App gebunden, was bedeutet, dass selbst wenn ein Benutzer auf einen Phishing-Link klickt, der Passkey auf der gefälschten Website nicht funktioniert, da die Domain-Bindung nicht übereinstimmt. Dies eliminiert den „menschlichen Faktor“ als primäre Schwachstelle bei Phishing-Angriffen, da der Benutzer nicht mehr die Verantwortung trägt, die Legitimität einer Website zu beurteilen, sondern das System dies automatisch übernimmt. Dies ist ein entscheidender Fortschritt gegenüber 2FA-Methoden wie SMS-OTPs, die weiterhin anfällig für Phishing und SIM-Swapping sind.

Darüber hinaus bieten Passkeys einen robusteren Schutz vor Credential Stuffing und Replay Attacks. Da für jede Website oder Anwendung ein einzigartiges Schlüsselpaar generiert wird, entfällt das Risiko der Passwortwiederverwendung vollständig. Dies ist ein erheblicher Vorteil, da die Wiederverwendung von

Passwörtern eine der Hauptursachen für weitreichende Sicherheitsverletzungen ist. Bei Passkeys gibt es zudem keine „Shared Secrets“ (Passwörter), die von Servern gestohlen und für Replay-Angriffe verwendet werden könnten. Die Server speichern lediglich den öffentlichen Schlüssel, der für Angreifer nutzlos ist, was die Angriffsfläche bei Datenlecks drastisch reduziert.

Die Überlegenheit von Passkeys erstreckt sich auch auf die Benutzerfreundlichkeit, die wiederum die Sicherheit positiv beeinflusst. Während traditionelle 2FA-Methoden oft als umständlich empfunden werden und zu „MFA-Müdigkeit“ führen können, was die Akzeptanz und damit die tatsächliche Nutzung reduziert, bieten Passkeys einen nahtlosen und schnellen Anmeldevorgang. Die Anmeldung erfolgt einfach durch das Entsperren des Geräts mittels Biometrie oder PIN, ähnlich wie bei der täglichen Nutzung des Smartphones. Diese verbesserte Benutzererfahrung kann zu einer höheren Adoptionsrate und damit zu einer insgesamt stärkeren Sicherheitslage für Benutzer und Organisationen führen. Passkeys brechen somit den traditionellen Kompromiss zwischen Sicherheit und Komfort auf.

Zusammenfassend lässt sich festhalten, dass die Architektur von Passkeys, die auf kryptographischen Prinzipien und der Eliminierung von Passwörtern basiert, eine fundamental sicherere Grundlage für die digitale Authentifizierung schafft. Während 2FA eine wichtige inkrementelle Verbesserung darstellt, adressiert es nicht die Wurzel des Problems – die Anfälligkeit von Passwörtern. Passkeys sind darauf ausgelegt, genau diese Schwachstelle zu beseitigen und bieten gleichzeitig eine überlegene Benutzererfahrung, was sie zur bevorzugten Wahl für die zukünftige digitale Sicherheit macht.

Passkeys als Brücke zur passwortlosen Welt: Strategien für die Übergangsphase

Passkeys bieten eine überlegene Sicherheit und Benutzerfreundlichkeit und sind darauf ausgelegt, Passwörter vollständig abzulösen. Die Transformation hin zu einer passwortlosen Zukunft erfordert jedoch einen strategischen Übergang, der sowohl technische Flexibilität als auch umfassende Benutzeraufklärung berücksichtigt.

Integration von Passkeys als starker zweiter Faktor

Auch wenn Passkeys letztendlich Passwörter ersetzen sollen, können sie in einer Übergangsphase als starker zweiter Faktor in bestehenden 2FA-Workflows eingesetzt werden. Dies ermöglicht eine flexible Migrationsstrategie, die Organisationen schrittweise von den Vorteilen der Passkey-Technologie profitieren lässt, ohne die gesamte Authentifizierungsinfrastruktur sofort umgestalten zu müssen.

Die Nutzung von Passkeys als zweiten Faktor, beispielsweise in Kombination mit einem Passwort, verbessert die Sicherheit erheblich, da sie die Schwachstellen von SMS-OTPs oder anderen abfangbaren Codes umgeht. Dies erlaubt es Unternehmen, die Vorteile der Passkey-Technologie zu nutzen, während sie ihre Infrastruktur und Benutzerbasis schrittweise an die passwortlose Zukunft anpassen. Passkeys stellen somit einen evolutionären Schritt dar, der eine flexible Integration in bestehende Systeme erlaubt.

Empfehlungen für Unternehmen zur schrittweisen Migration

Für Unternehmen ist ein schrittweiser Ansatz zur Einführung von Passkeys ratsam. Dies minimiert Störungen und ermöglicht eine reibungslose Anpassung:

- **Pilotprojekte:** Beginnen Sie mit der Implementierung von Passkeys für nicht-kritische Anwendungen oder eine kleine Gruppe technisch versierter Benutzer. Dies hilft, Erfahrungen zu sammeln, die Implementierung zu testen und potenzielle Probleme vor einer breiteren Einführung zu identifizieren.
- **Koexistenz:** Eine Übergangsphase, in der Passwörter und traditionelle 2FA-Methoden weiterhin als Fallback oder für bestimmte Anwendungsfälle existieren, ist sinnvoll. Microsoft bietet beispielsweise die Möglichkeit, Passwörter für bestehende Konten zu löschen oder sie als Fallback in Edge zu speichern, während neue Konten standardmäßig passwortlos sind. Dies erlaubt es Benutzern, sich an die neue Methode zu gewöhnen und verringert das Risiko von Zugriffsverlusten.
- **Umfassende Benutzeraufklärung:** Eine kontinuierliche und umfassende Aufklärung der Benutzer ist entscheidend für den Erfolg der Einführung. Die Vorteile von Passkeys müssen klar kommuniziert und Missverständnisse (z. B. bezüglich der Biometrie-Übertragung) ausgeräumt werden. Die Bereitstellung von FAQs, Schritt-für-Schritt-Anleitungen und unterstützenden Materialien kann die Lernkurve erleichtern und den Widerstand gegen Veränderungen reduzieren.
- **Sichere Wiederherstellungsstrategien:** Robuste und sichere Kontowiederherstellungsmechanismen sind unerlässlich. Organisationen müssen sicherstellen, dass Benutzer bei Verlust ihres Geräts den Zugriff auf ihre Passkeys wiederherstellen können, ohne dabei die Sicherheitsvorteile zu untergraben. Dies ist ein Bereich, der weiterhin Aufmerksamkeit erfordert, da die Wiederherstellung oft noch auf traditionellen, potenziell weniger sicheren Methoden basiert. Die Abhängigkeit von diesen Fallback-Methoden stellt ein Paradox dar, da sie die ansonsten überlegene Sicherheit von Passkeys untergraben könnten. Daher ist es von entscheidender Bedeutung, auch die Sicherheit der Wiederherstellungskanäle zu stärken.

Die Rolle großer Tech-Unternehmen bei der Förderung von Passkeys

Die breite Akzeptanz und der Erfolg von Passkeys werden maßgeblich durch das Engagement großer Technologieunternehmen wie Apple, Google und Microsoft vorangetrieben. Diese Unternehmen integrieren Passkeys aktiv in ihre Betriebssysteme und Dienste und setzen sich für deren Interoperabilität ein.

- **Microsofts proaktiver Ansatz:** Microsoft hat eine führende Rolle eingenommen, indem es neue Microsoft-Konten standardmäßig passwortlos gestaltet und die Passwort-Autofill-Funktion aus der Microsoft Authenticator App entfernt. Dies ist ein starkes Signal und zwingt Benutzer indirekt zur Adoption sichererer Methoden.
- **Apples nahtlose Integration:** Apple hat Passkeys 2022 mit iOS 16 und macOS Ventura eingeführt; beide sind bis heute die Mindestvoraussetzung, iPadOS 16 ebenso. Innerhalb des Apple-Ökosystems ist die Nutzung dadurch nahtlos. Die Möglichkeit, Passkeys über iCloud Keychain zu synchronisieren, verbessert die Benutzerfreundlichkeit erheblich.
- **Googles Cross-Plattform-Fokus:** Google hat Passkeys in seinen Google Password Manager integriert, wodurch sie über alle Geräte hinweg zugänglich sind, die mit demselben Google-Konto angemeldet sind. Google ermöglicht auch die Erstellung und Nutzung von Passkeys in anderen Ökosystemen wie Windows und Apple.

- **Gemeinsame Interoperabilität:** Die gemeinsame Verpflichtung dieser Unternehmen durch die FIDO Alliance zur Interoperabilität und die Entwicklung von Standards wie dem Credential Exchange Protocol (CXP) sind entscheidend, um Vendor Lock-in zu vermeiden und einen reibungslosen Transfer von Passkeys zwischen verschiedenen Plattformen zu gewährleisten. Diese konzertierte Anstrengung schafft Vertrauen und beschleunigt die Adoption auf globaler Ebene, indem sie die Komplexität für den Benutzer reduziert und eine breite Kompatibilität sicherstellt.

Die Konvergenz der Tech-Giganten ist ein fundamentaler Treiber für die schnelle und erfolgreiche Ablösung von Passwörtern und unsicheren 2FA-Methoden. Diese Entwicklung ist nicht nur ein Trend, sondern ein entscheidender Faktor für die Etablierung von Passkeys als De-facto-Standard.

Fazit: Eine sicherere digitale Zukunft

Die vorliegende Analyse hat gezeigt, dass Passkeys eine signifikante Weiterentwicklung in der digitalen Authentifizierung darstellen und traditionelle 2FA-Methoden in mehreren Schlüsselbereichen übertreffen. Die inhärente Phishing-Resistenz von Passkeys, die durch die Public-Key-Kryptographie und die Domain-Bindung erreicht wird, eliminiert eine der größten Schwachstellen der passwortbasierten Authentifizierung. Im Gegensatz dazu, obwohl traditionelles 2FA eine wichtige zusätzliche Sicherheitsebene bietet, bleibt das zugrunde liegende Passwort eine Angriffsfläche, und bestimmte 2FA-Methoden sind selbst anfällig für Abfangen oder Umgehung.

Darüber hinaus bieten Passkeys eine überragende Benutzererfahrung, indem sie Passwörter vollständig eliminieren und den Anmeldevorgang durch die Nutzung von Biometrie oder PINs am Gerät vereinfachen und beschleunigen. Diese Kombination aus verbesserter Sicherheit und erhöhter Benutzerfreundlichkeit ist entscheidend für eine breite Akzeptanz und damit für eine effektivere Sicherheitslage. Die aktive Unterstützung und Implementierung durch große Technologieunternehmen wie Apple, Google und Microsoft unterstreicht das Potenzial von Passkeys, sich als neuer Standard für die digitale Authentifizierung zu etablieren und die passwortlose Zukunft voranzutreiben.

Empfehlungen für technisch orientierte Leser und Unternehmen zur Adoption von Passkeys

Für technisch versierte Anwender und Unternehmen ist es ratsam, die Einführung von Passkeys proaktiv zu planen und umzusetzen. Dies ist keine bloße Option mehr, sondern eine strategische Notwendigkeit, um den sich ständig weiterentwickelnden Cyberbedrohungen zu begegnen und die digitale Identität effektiv zu schützen.

- **Priorisierung der Implementierung:** Unternehmen sollten die Einführung von Passkeys für ihre Dienste priorisieren, beginnend mit kritischen Anwendungen und schrittweise auf breitere Benutzergruppen ausweiten.
- **Umfassende Benutzeraufklärung:** Investitionen in die Aufklärung der Benutzer über die Vorteile und die korrekte Nutzung von Passkeys sind unerlässlich, um Akzeptanzbarrieren zu überwinden und Missverständnisse zu vermeiden.
- **Sichere Wiederherstellungsmechanismen:** Die Entwicklung robuster und sicherer Wiederherstellungsstrategien für den Verlust von Geräten oder Passkeys ist von größter Bedeutung, um die Überlegenheit von Passkeys nicht durch schwache Fallback-Methoden zu untergraben.

- Beobachtung der Ökosystem-Entwicklung: Es ist wichtig, die Weiterentwicklung der FIDO-Standards und die Implementierungen der großen Tech-Unternehmen genau zu verfolgen, um die Interoperabilität und die besten Praktiken zu gewährleisten.

Ihr nächster Schritt

Die Frage ist selten, ob Passkeys besser sind. Sie lautet, welche Anwendungen bei Ihnen heute noch an einem Code hängen, den ein Mitarbeiter am Telefon vorlesen könnte – und welche davon Zugriff auf Geld oder Kundendaten haben. Nicht nur im eigenen Haus: Auch Dienstleister mit Zugängen gehören auf diese Liste, wie die [Lieferketten-Sicherheit](#) zeigt. Diese Liste erstellen wir mit Ihnen, bevor über Werkzeuge gesprochen wird – mit Senior-Experten aus unserer [Cybersecurity-Expertise](#), gesteuert aus Deutschland.

Häufige Fragen

Sind Passkeys sicherer als eine Authenticator-App?

In der Regel ja. Auch App-basierte 2FA-Codes lassen sich über gefälschte Login-Seiten abphishen. Passkeys sind an die echte Domain gebunden und funktionieren auf einer Betrugsseite schlicht nicht – der Angriffsweg entfällt.

Was passiert bei Geräteverlust?

Passkeys lassen sich über die Plattform (z. B. Apple, Google, Microsoft) synchronisieren und wiederherstellen. Wichtig ist ein sauber eingerichteter Wiederherstellungspfad – sonst wird der Geräteverlust zum Aussperr-Risiko.

Ersetzen Passkeys 2FA komplett?

Perspektivisch ja, in der Übergangsphase oft nicht sofort. Viele Unternehmen führen Passkeys zunächst als starken Faktor neben bestehender 2FA ein und migrieren schrittweise.

Warum sind Passkeys phishing-resistent?

Weil ein Passkey an die echte Domain gebunden ist: Er funktioniert nur auf der legitimen Website und verweigert die Anmeldung auf einer gefälschten Seite. Es gibt kein Passwort und keinen Code, den ein Angreifer abfangen oder auf einer Phishing-Seite abgreifen könnte.

Wie funktioniert ein Passkey technisch?

Ein Passkey besteht aus einem Schlüsselpaar (Public-Key-Kryptografie): Der private Schlüssel bleibt sicher auf dem Gerät, der öffentliche liegt beim Dienst. Bei der Anmeldung beweist das Gerät den Besitz des privaten Schlüssels, ohne ein Geheimnis zu übertragen – abfangbar ist dabei nichts Wesentliches.

Warum gelten SMS-Codes als unsichere 2FA-Methode?

Weil SMS-Codes übertragen und umgeleitet werden können – etwa durch SIM-Swapping oder Abfangen – und weil sie sich auf einer gefälschten Seite abphishen lassen. SMS-2FA ist besser als nur ein Passwort, aber die schwächste der gängigen Methoden.

Wie führen Unternehmen Passkeys ein?

Schrittweise: Passkeys zunächst als zusätzliche, starke Option anbieten, parallel zu bestehenden Verfahren, und die Nutzung gezielt fördern. Große Plattformen treiben die Verbreitung, sodass Unternehmen auf etablierten Standards aufsetzen können.

Thematische Vertiefungen

[Zero Trust: Das Sicherheitskonzept für die vernetzte Welt](#)

[Cybersecurity-Expertise](#)

[KI im Kampf gegen Cyberkriminalität](#)

Quellen

- NIST SP 800-63B-4: Digital Identity Guidelines — Authentication and Authenticator Management, Juli 2025, 129 Seiten. Belegt wörtlich die Definition in Abschnitt 3.2.5 („without relying on the vigilance of the claimant“), die AAL3-Anforderung an einen nicht exportierbaren privaten Schlüssel, die AAL2-Pflicht, die Vorgabe für US-Bundesbehörden sowie den Ausschluss von OTP- und Out-of-Band-Verfahren samt Begründung. — <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.pdf>
- NIST SP 800-63B-4, HTML-Fassung — <https://pages.nist.gov/800-63-4/sp800-63b.html>
- Microsoft Security Blog: Pushing passkeys forward, 1. Mai 2025. Belegt wörtlich: „users signing in with passkeys are three times more successful at getting into their account than password users (about 98% versus 32%)“ und „Passkey sign-ins are eight times faster than a password and multifactor authentication“ — der Geschwindigkeitsvergleich läuft also gegen Passwort plus zweiten Faktor, nicht gegen das Passwort allein. — <https://www.microsoft.com/en-us/security/blog/2025/05/01/pushing-passkeys-forward-microsofts-latest-updates-for-simpler-safer-sign-ins/>
- Verizon: 2024 Data Breach Investigations Report, 100 Seiten. Belegt: Median von 21 Sekunden bis zum Klick nach dem Öffnen einer Phishing-Mail und weiteren 28 Sekunden bis zur Eingabe der Daten. — <https://www.verizon.com/business/resources/T78c/reports/2024-dbir-data-breach-investigations-report.pdf>
- Verizon: 2025 Data Breach Investigations Report, 117 Seiten. Belegt: Ausnutzung von Schwachstellen als Einstiegsweg bei 20 % und um 34 % gegenüber dem Vorjahr gewachsen; Verwendung gestohlener Zugangsdaten in der Neuberechnung von 38 % auf 31 % gesunken, Missbrauch von Zugangsdaten weiterhin häufigster Einstiegsweg. — <https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf>
- Apple Support: Sign in with passkeys on iPhone (Fassung iOS 16). Belegt die Mindestversionen iOS 16, iPadOS 16 und macOS Ventura für Passkeys. — <https://support.apple.com/guide/iphone/use-passkeys-to-sign-in-to-websites-and-apps-iphf538ea8d0/ios>

- [FIDO Alliance: Passkeys / WebAuthn \(Standard\)](https://fidoalliance.org/passkeys/) — <https://fidoalliance.org/passkeys/>