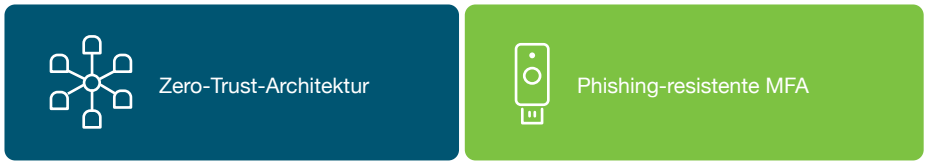
yubico

Aufbau eines Unternehmens, das Konto-übernahmen mit Phishing-resistenter MFA verhindert

Wichtige Überlegungen zur Überprüfung von Passkeys im Rahmen einer gerätegebundenen Unternehmensstrategie

Benutzerorientierte Authentifizierung – die neue Grenze der Unternehmens-authentifizierung

Passwörter sind in jeder Phase des traditionellen IAM-Identitätslebenszyklus fest verankert. Leider sind gestohlene Passwörter aber einer der größten Bedrohungsvektoren, die die Online-Sicherheit gefährden. In letzter Zeit wurden jedoch wichtige Vorschriften für Regierungsbehörden sowie private Organisationen eingeführt, um die Cybersicherheit gegen Phishing-Angriffe zu stärken, indem die hochgradig anfällige passwortbasierte Multi-Faktor-Authentifizierung durch eine Phishing-resistente Multi-Faktor-Authentifizierung (MFA) ersetzt und idealerweise auf eine passwortlose Authentifizierung umgestellt wird, bei der Passwörter gänzlich wegfallen.

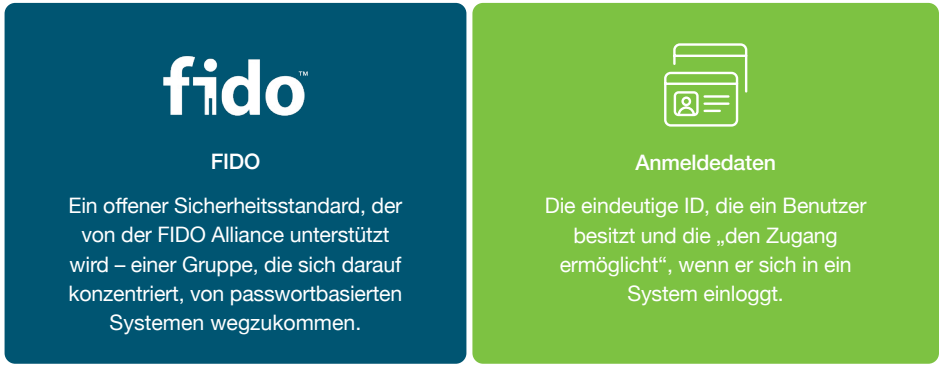


Mit den jüngsten Fortschritten bei passwortloser und neuer gerätebasierter Authentifizierung hat sich die Art und Weise, wie ein Unternehmen die Identitäts-nachweise eines Benutzers während seines gesamten Lebenszyklus erstellen und verwalten kann, weiterentwickelt.

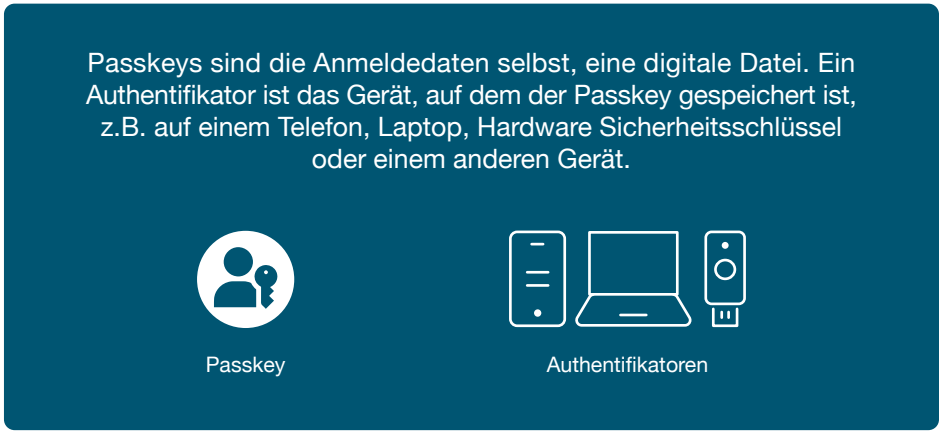
Üblicherweise denken Unternehmen an eine Phishing-resistente Authentifizierung und nicht an Phishing-resistente Benutzer. Der Unterschied besteht darin, Authentifizierungsereignisse als Zeitpunkte zu betrachten, zu denen sie sich bei sensiblen Systemen, Apps und Diensten anmelden, anstatt darüber nachzudenken, wie Benutzer leben und arbeiten. Benutzer wechseln im Laufe ihres Tages häufig zwischen Plattformen (Apple, Google, Microsoft) und Geräten (Smartphones, Laptops, Tablets) sowie zwischen privaten und geschäftlichen Apps und Diensten. Unternehmen müssen darüber nachdenken, ihre Benutzer mit einer Art von Authentifizierung auszustatten, die Phishing-Resistenz bietet, unabhängig von dem Geschäftsszenario (Remote-Arbeiter, Umgebungen mit Einschränkungen für Mobilgeräte, gemeinsam genutzte Arbeitsstationen, Drittanbieter aus der Lieferkette usw.) oder den Plattformen oder Geräten, die sie verwenden.

Die Einführung von Passkeys

Passkeys wurden von der FIDO Alliance eingeführt, um die passwortlose Anmeldung für Verbraucher und Unternehmen zu beschleunigen. Passkeys sind inzwischen auf jeder wichtigen Plattform verfügbar, einschließlich Google, Apple, Microsoft und Webbrowsern. Die Entwicklung von Passkey-Lösungen hat neue Sicherheitsereignisse für die Unternehmens-identität in jedem Unternehmen geschaffen.



Organisationen und ihre Benutzer verwechseln oft den Passkey mit dem Authenticator, in dem er gespeichert ist. Passkeys sind einfach FIDO2-Anmeldedaten, und können auf einem Smartphone oder anderen Gerät wie Tablets oder Laptops gespeichert sein. Alternativ können sie auf tragbaren Geräten gespeichert sein, die speziell für die Sicherheit entwickelte Authenticatoren sind, wie z.B. FIDO-Hardware-Sicherheitsschlüssel..



Sicherung von Unternehmensbenutzern

Benutzer haben unterschiedliche Authentifizierungsanforderungen

Nicht alle Unternehmensbenutzer erledigen jeden Tag die gleiche Arbeit. Je nach den Anforderungen des Unternehmens kann es sein, dass ein Benutzer aus der Ferne auf einem Laptop arbeiten, während einer Besprechung über sein Telefon auf seine E-Mails zugreifen oder in einer Produktionshalle einen gemeinsamen Arbeitsplatz nutzen muss. Unternehmensbenutzer haben unterschiedliche Arten von Authentifizierungsanforderungen – daher sollten sie auch unterschiedliche Authentifikatorentypen verwenden. Ein Unternehmensbenutzer kann ein Remote- oder Hybridarbeiter sein oder in einer mobil eingeschränkten Umgebung arbeiten, in der Mobiltelefone einfach keine Option sind. Sie können auch an gemeinsam genutzten Arbeitsstationen arbeiten, an denen sich verschiedene Benutzer sicher an- und abmelden müssen, alle auf demselben Computerterminal.

Daher kann der Typ des Authentifikators, auf dem der Benutzer seine Passkeys speichern muss, je nach der Sensibilität seiner Aufgaben oder der Art der Daten oder Systeme, auf die er zugreifen muss, unterschiedlich sein. Hardware-Sicherheitsschlüssel sind tragbare Authentifikatoren, die speziell für die Sicherheit entwickelt wurden. Sie ermöglichen Benutzern ein sicheres und nahtloses Arbeiten in einer Vielzahl von Unternehmensszenarien. Alternativ dazu sind Plattform-Authentifikatoren in allgemeine Geräte wie Smartphones und Laptops integriert. Und schließlich bieten auch mobile Anwendungen, wie z. B. Authentifizierungs-Apps, Lösungen zur Benutzerauthentifizierung. Alle diese Authentifikatoren gehen in Bezug auf Sicherheit und Benutzerfreundlichkeit Kompromisse ein. Es liegt an dem Unternehmen zu enscheiden, welches Maß an Sicherheit es benötigt und mit welchem Risiko es sich abfinden kann.

Sicherheitsschlüssel

Gerätegebundene Zugangsnachweise mit Attestierung

Plattform-Authentifikatoren

In Ihre Geräte integrierte Authentifikatoren

Authentifizierungs-Apps von Drittanbietern

Anwendungen, die Benutzerauthentifizierungs-lösungen bereitstellen

Unterschiedliche Passkey-Klassen

Passkey ist nicht gleich Passkey

Passkeys sind sicherer als Passwörter und begünstigen die schnelle Umstellung auf eine passwortlose Authentifizierung, die mehr Sicherheit und Effizienz ermöglicht.
Es gibt zwar unterschiedliche Passkey-Implementierungen, die jeweils ihre eigenen Sicherheits- und Nutzungskompromisse aufweisen, aber nicht alle Passkeys sind gleich und nicht alle sind ideal für das Unternehmen geeignet.

Synchronisierte Passkeys

Gerätegebundene Passkeys
(auch als hardwaregebunden bezeichnet)

Synchronisierte Passkeys

Entwickelt für Verbraucher, nicht für Unternehmen

Synchronisierte Passkeys sind kopierbare Zugangsdaten, die auf allen mit dem Benutzerkonto verbundenen Geräten kopiert werden, einschließlich Smartphones, Laptops und Tablets. Synchronisierte Passkeys können mit einem anderen Benutzerkonto geteilt oder in dieses kopiert werden. Dies kann zu einigen abschreckenden Schwachpunkten für das Unternehmen führen. Synchronisierte Passkeys bergen große Risiken und Sicherheitslücken in wichtigen Unternehmensszenarien, wie Remote-Arbeit, Sicherheit in der Lieferkette, Compliance und Komplexität des Supports.

Erfahren Sie mehr über die Fallstricke von synchronisierten Passkeys für Unternehmen.

Gerätegebundene Passkeys

Für Unternehmensbenutzer entwickelt

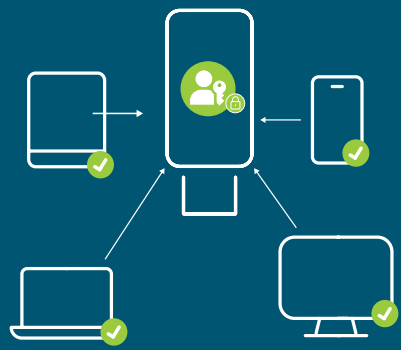
Gerätegebundene Passkeys bieten Unternehmen im Vergleich zu synchronisierten Passkeys eine bessere Kontrolle über ihre FIDO-Zugangsdaten.

Es gibt jedoch verschiedene Arten von gerätegebundenen Passkeys. Es gibt gerätegebundene Passkeys, die sich in alltäglichen Geräten wie Smartphones und Laptops befinden. Gerätegebundene Passkeys, die in Hardware-Sicherheitsschlüsseln enthalten sind, bieten bekanntermaßen die höchste Sicherheit und liefern Unternehmen die Bescheinigung, mit der sie die Sicherheit ihrer Zugangsdaten nachweisen können. Hardware-Sicherheitsschlüssel ermöglichen es Unternehmen, vertrauenswürdige Prozesse zur Verwaltung des Lebenszyklus von Zugangsdaten aufzubauen. Sicherheitsschlüssel ermöglichen es Unternehmensbenutzern, neue Geräte zu registrieren, sich bei ihren unternehmensweiten Passkey-Anbietern zu authentifizieren und andere gerätegebundene Zugangsdaten (wie Windows Hello oder Okta Fastpass) zu registrieren, da jeder Benutzer über tragbare, Phishing-resistente Zugangsdaten verfügt, um sich im Rahmen dieser Prozesse einfach und sicher zu authentifizieren. Diese Lösung reduziert das Risiko für den Helpdesk und ermöglicht es Unternehmen, die strengsten Anforderungen in jeder Branche zu erfüllen.

Synchronisierte Passkeys im Vergleich zu gerätegebundenen Passkeys

Synchronisierte Passkeys

Diese werden auf einem Smartphone, Tablet, Laptop oder einem anderen Gerät verwendet, wo sie auf vielen anderen Geräten kopiert und synchronisiert werden können.



Gerätegebundene Passkeys

Diese werden auf einem USB-Key oder einer anderen Hardware verwendet, sind von alltäglichen Geräten getrennt und bieten ein höheres Sicherheitsversprechen.

Nutzen Sie alle Vorteile mit der Passkey-Toolbox

Unterschiedliche Passkey-Implementierungen für synchronisierte und gerätegebundene Passkeys

Benutzern stehen im Wesentlichen drei Arten von Authentifikatoren zur Verfügung, die sie zur Authentifizierung mit den darin enthaltenen Passkeys verwenden können. Die erste Passkey-Lösung auf dem Markt und der Goldstandard für die Authentifizierung sind Hardware-Sicherheitsschlüssel. Diese Sicherheitsschlüssel ermöglichen es Benutzern, sich mit Passkeys zu authentifizieren, die auf ihrem Gerät gespeichert sind, und der Benutzer ist dafür verantwortlich, den Sicherheitsschlüssel von Gerät zu Gerät zu verschieben. Es ist wichtig zu beachten, dass sich speziell entwickelte Authentifikatoren an spezifische Anwendungsfälle für Unternehmen richten, die Authentifikatoren auf Mobilgeräten einfach nicht abdecken können, wie z. B. die Sicherung von Umgebungen mit Einschränkungen für Mobilgeräte und gemeinsam genutzten Arbeitsplatzgeräten, was für viele Unternehmen von entscheidender Bedeutung ist.

Weitere neue Lösungen auf dem Markt sind Passkey-Drittanbieter. Diese Anwendungen können erstellt werden, um Benutzer bei der Verwaltung von gerätegebundenen oder synchronisierten Passkeys zu unterstützen. Die Einführung von synchronisierten Passkeys im Jahr 2021 wurde durch die Unterstützung der Plattformen für diese verbraucherfreundlichen Passkeys ergänzt. Die verschiedenen Plattformen unterstützen jetzt synchronisierte Passkeys, und einige dieser Plattformen erlauben sogar ausschließlich die Verwendung synchronisierter Passkeys mit ihren Plattform-Authentifikatoren.

iOS und MacOS unterstützen auf ihrer Plattform jetzt nur noch die Erstellung von synchronisierten Passkeys. Google Android unterstützt jetzt ebenfalls nur noch synchronisierte Passkeys. Chrome unterstützt sowohl synchronisierte als auch gerätegebundene Passkeys, sodass die vertrauende Partei bzw. der vertrauende Dienst (z. B. Dropbox) selbst entscheiden kann, welche Art sie erstellen möchten. Zusätzlich zu den Optionen ermöglicht Windows Hello nur die Erstellung von Passkeys, die an das Arbeitsplatzgerät gebunden sind. Und schließlich unterstützen Drittanbieter wie 1Password und Dashlane die Erstellung synchronisierter Passkeys für Benutzer. Es gibt auch Lösungen auf dem Markt, die softwaregestützte, gerätegebundene Passkeys unterstützen, was eine weitere Entwicklung in der entstehenden Passkey-Landschaft darstellt.

Passkey-Terminologiesalat? Hier ist das Wichtigste, das man sich merken sollte... Es geht darum, den privaten Schlüssel zu schützen.

Der Nachweis, wo der private Schlüssel gespeichert ist, ist von grundlegender Bedeutung, um die mit Passkeys verbundenen Risiken zu verstehen. Die vertrauende Partei bzw. der vertrauende Dienst kann die in der Registrierung der Zugangsdaten enthaltene Geräte-Attestierung nutzen, um nachzuweisen, dass der Passkey auf einem für das Unternehmen akzeptablen Gerät gespeichert ist.

Alle Passkeys basieren auf Public-Key-Kryptographie mit einem Schlüsselpaar mit einem privaten Schlüssel, der sicher gespeichert ist, und einem öffentlichen Schlüssel, der freigegeben oder öffentlich gemacht wird. Der private Schlüssel muss privat bleiben. Das ist die Aufgabe der Passkey-Lösung und des zugrunde liegenden Systems, in dem der Passkey gespeichert ist. Synchronisierte Passkeys ermöglichen das Kopieren des privaten Schlüssels auf mehrere Geräte und in ein Cloud-Managementsystem. Dies erschwert es dem Unternehmen, den Schlüssel nachzuverfolgen und ihm zu vertrauen. Gerätegebundene Passkeys bieten eine bessere Verwaltung und die Kontrolle, die ein Unternehmen braucht. Aber nur gerätegebundene Passkeys, die sich in speziell für die Sicherheit entwickelten portablen Hardware-Authentifikatoren befinden, bieten den von Unternehmen benötigten Schutz für private Schlüssel.

Wechsel zu Phishing-resistenten Benutzern

statt nur Phishing-resistenter Authentifizierung

Da Passkeys genutzt werden, um die Einführung der passwortlosen Authentifizierung zu beschleunigen, sollte das neue Ziel für die Unternehmensauthentifizierung darin bestehen, Phishing-resistente Benutzer zu schaffen, anstelle sich lediglich auf eine Phishing-resistente Authentifizierung zu verlassen. Passkeys sollten im Kontext einer echten benutzerzentrierten Authentifizierung und der Arbeitsweise der Benutzer im Unternehmen betrachtet werden. Diese Strategie erfordert, dass jeder Benutzer für jede Authentifizierungsaufgabe eine Phishing-resistente Authentifizierungslösung verwendet. Wenn sich das Ziel von der Phishing-resistenten Authentifizierung auf Phishing-resistente Benutzer verlagert, kann ein Unternehmen die Benutzer in die Lage versetzen, neue Geräte ohne Anrufe beim Helpdesk zu registrieren und ein hohes Maß an Sicherheit aufrechtzuerhalten, sodass die Benutzer sicher aus der Ferne arbeiten können, während gleichzeitig betriebliche Risiken und Sicherheitsrisiken für den Helpdesk beseitigt werden.

Vor diesem Hintergrund verlagert sich die Diskussion von der Wahl des richtigen Authentifikators (Telefon oder Sicherheitsschlüssel usw.) hin zur Sicherstellung, dass jede Authentifizierungsoption (und jeder Passkey), die dem Benutzer zur Verfügung stehen, sicher registriert ist und sowohl den Anforderungen an die Benutzerfreundlichkeit als auch den Sicherheitsanforderungen des Unternehmens entspricht.

Die Abkehr von Passwörtern und alten, nicht phishing-resistenten MFA-Lösungen wie SMS, Einmalpasswörtern und mobiler Authentifizierung bedeutet, dass wir uns in eine Welt begeben, in der Benutzer mehrere Zugangsdaten, Passkeys und Passkey-Anbieter haben werden. Mit dieser Änderung wird der **Lebenszyklus der Anmeldedaten** zum neuen Wendepunkt für Unternehmen, die ihre kritischen Interaktionen mit dem Benutzer verwalten müssen.

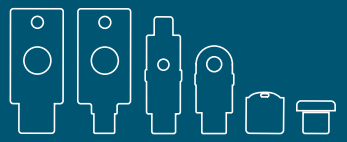
Für jeden Benutzer benötigt ein Unternehmen eine Lösung für die folgenden Ereignisse:

- **Erste Authentifizierung:** Die erste Authentifizierung auf einem neuen Computergerät (Telefon, Laptop oder Desktop), um dieses Gerät sicher im Gerätemanagement-system zu registrieren
- **Registrierung von Zugangsdaten:** Phishing-resistente Registrierung synchronisierter oder gerätegebundener Zugangsdaten auf vertrauenswürdigen/verwalteten oder nicht vertrauenswürdigen/nicht verwalteten Geräten
- **Erste Authentifizierung beim Passkey-Anbieter:** Die erste Authentifizierung beim Passkey-Anbieter auf einem neuen Gerät, um mit der Synchronisierung von Passkeys auf einem vertrauenswürdigen/verwalteten Gerät zu beginnen
- **Web-Authentifizierung beim Passkey-Anbieter:** Authentifizierung bei einem Passkey-Anbieter, um auf Passkeys auf einem nicht vertrauenswürdigen/nicht verwalteten Gerät zuzugreifen
- **Sicheres Self-Service zur Verwaltung von Zugangsdaten:** Ein Self-Service-Tool für den Fall, dass ein Mitarbeiter:
  - Ein verwaltetest Gerät verliert oder außer Betrieb nimmt, wodurch alle darauf gespeicherten Anmeldedaten widerrufen werden.
  - Zugang zu seinem Passkey-Anbieter wiederherstellen muss.
  - Zugang zu seinem Plattformkonto wiederherstellen muss.
  - Bestehende YubiKeys verwalten und verlorene Anmeldedaten widerrufen/als verloren markieren muss, die nicht mehr verwendet werden.
- **Sicheres Self-Service-Authenticator-Management:** Ein Self-Service-Prozess zum Bestellen zusätzlicher gerätegebundener Passkeys (z. B. auf einem YubiKey), falls ein Benutzer einen neuen benötigt, um das Risiko einer Kontosperrung zu vermeiden.
- **Kontosperrung:** Ein sicherer Prozess, um einem Benutzer nach dem Verlust des Zugangs zu allen seinen Authenticatoren/Anmeldedaten neue Anmeldedaten für sein unternehmensverwaltetes Konto auszustellen.

Der Phishing-resistente Benutzer und portable Passkeys

Phishing-Resistenz sollten nicht an ein bestimmtes isoliertes Gerät oder eine bestimmte Plattform gebunden sein, sondern **sich mit dem Benutzer bewegen können,** unabhängig davon, bei welcher App, bei welchem Dienst oder bei welchem System er sich anmeldet sowohl beruflich als auch privat. So entsteht ein durchgängig Phishing-resistentes Unternehmen von Anfang bis Ende. Gerätegebundene Passkeys, wie die in einem YubiKey, kombinieren die sichere Kryptographie von Passkeys auf einer portablen Hardware. Durch die Verwendung von YubiKeys entstehen phishing-resistente Benutzer, bei denen die starke Authentifizierung mit dem Benutzer reist und nicht an eine bestimmte Plattform oder ein mobiles Gerät gebunden ist.

YubiKeys



Gerätegebundene Anmeldedaten mit Attestierung

Unternehmensüberlegungen bei der Auswahl der richtigen Passkeys

Alle Passkeys sind möglicherweise Phishing-resistent, aber nicht alle sind ideal für Unternehmensanforderungen

Viele Lösungen zum Ersetzen von Passwörtern konzentrieren sich darauf, eine Phishing-resistente Authentifizierung auf den Markt zu bringen, und Unternehmen möchten diese Lösungen nutzen, um Passwörter zu ersetzen. Unternehmen müssen jedoch jede Phase des Account-Lebenszyklus und die damit verbundenen unternehmensspezifischen Überlegungen berücksichtigen, um zu bestimmen, ob gerätegebundene Passkeys auf allgemeinen Geräten ausreichen, ob gerätegebundene Passkeys auf speziell für Sicherheit entwickelten Authenticatoren besser geeignet sind oder ob ein hybrider Ansatz die richtige Lösung ist. Die ideale Strategie wird nicht nur wichtige Authentifizierungspunkte Phishing-resistent machen, sondern auch Phishing-resistente Benutzer schaffen, sodass diese während der verschiedenen Authentifizierungsprozesse auf jedem bevorzugten Gerät geschützt sind, wenn sie sich in ihre sensiblen Online-Konten einloggen, sowohl im Berufs- als auch im Privatleben.

Sicheres Onboarding und Wiederherstellung sind ein Muss für Unternehmen

Onboarding/Registrierung

Wiederherstellung der Zugangsdaten

Compliance und Audit

Die MFA, die Unternehmen implementieren, ist nur so sicher wie die Registrierung und Wiederherstellung. Registrierungs- oder Onboarding-Prozesse, die Phishing-anfällige Methoden wie das Senden von Einmalkennwörtern (OTP-Codes) verwenden, führen zu einer anfälligen MFA-Bereitstellung. Wenn jeder Benutzer die FIDO-Zugangsdaten registrieren oder zurücksetzen kann, wird der Zweck einer Phishing-resistenten MFA außer Kraft gesetzt. Unternehmen benötigen eine robuste Onboarding- und Wiederherstellungslösung, um die Registrierung der MFA-Methode durchzuführen.

Schauen wir uns an, wie die verschiedenen gerätegebundenen Passkey-Ansätze im Alltag eines Benutzers in einem Unternehmen funktionieren, wenn er das Onboarding und die Wiederherstellung von Zugangsdaten durchläuft, und welche Auswirkungen die einzelnen Passkey-Ansätze auf die Bereiche Compliance, Audit und Risiken haben.

1. Onboarding/Registrierung

1a. Onboarding mit gerätegebundenen Passkeys auf allgemeinen Geräten

Onboarding **Passkey-Drittanbieter;** gerätegebundene Passkeys auf allgemeinen Geräten

1.

Der Mitarbeiter verwendet eine PIN oder biometrische Daten, um sich am mobilen Gerät anzumelden.

2.

Der Mitarbeiter installiert und konfiguriert die Authentifikator-App als Passkey-Anbieter.

3.

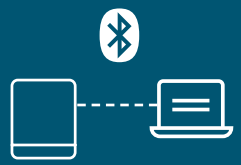
Der Mitarbeiter meldet sich mit seinem Phishing-anfälligen Geheimcode an. Schwachstelle! Phishing-Resistenz unterbrochen

4.

Der Mitarbeiter schließt das Verfahren ab und registriert einen von der App verwalteten Passkey. Der Passkey kann für die Anmeldung bei Apps auf demselben mobilen Gerät verwendet werden.

5.

Um den Passkey an anderen Arbeitsplätzen zu verwenden, muss der Mitarbeiter einen QR-Code mit der Kamera scannen und das Telefon per Bluetooth verbinden, ein Anmeldeverfahren durchführen und das Telefon optional mit dem Arbeitsplatz verknüpfen.*



6.

Der Mitarbeiter kann sich nun mit dem Passkey auf dem Mobilgerät bei jedem seiner anderen Geräte anmelden.

7.

Der Mitarbeiter kann einen gerätegebundenen Passkey zur Optimierung der Anmeldung direkt über den Arbeitsplatz registrieren.*

*sofern dies vom Gerät und Anwendungsfall unterstützt wird

Abbildung 1: Ein Tag im Leben eines neuen Mitarbeiters, dessen Onboarding mithilfe von gerätegebundenen Passkeys erfolgt, die sich in einem Allzweckgerät wie einem Smartphone befinden.

Onboarding/Registrierung

1a. Onboarding mit gerätegebundenen Passkeys auf allgemeinen Geräten

Vorteile

Keine Notwendigkeit, zusätzliche Hardware zu erwerben oder bereitzustellen

Der Vorteil für Unternehmen besteht darin, dass sie den Benutzern keine zusätzliche Hardware zur Verfügung stellen müssen. Das Unternehmen kann sich auf persönliche Endbenutzergeräte verlassen oder ggf. bereits an Benutzer bereitgestellte mobile Geräte nutzen.

Herausforderungen

Niedrige Sicherheitsstufe

Nachdem der Benutzer seine Authentifikator-App installiert und konfiguriert hat, meldet er sich mit dem Phishing-anfälligen Geheimcode bei der App an. Das bedeutet, dass die Passkey-Registrierung mit gerätegebundenen Passkeys auf allgemeinen Geräten von vornherein eine geringe Sicherheit aufweist. Ein böswilliger Angreifer könnte den Benutzer auch dazu verleiten, entweder sein Phishing-anfälliges Geheimnis preiszugeben oder eine gefälschte oder nicht-konforme Passkey-App zu installieren, was dem Angreifer Zugriff auf die Zugangsdaten des Benutzers gewährt und die Kontoübernahme ermöglicht.

Widerstand der Benutzer gegen die Verwendung persönlicher Geräte für die Unternehmenssicherheit

Wie bereits erwähnt, besteht der Hauptvorteil für Unternehmen, die gerätegebundene Passkeys auf allgemeinen Geräten wie Smartphones verwenden, darin, dass sie den Benutzern keine zusätzliche Hardware zur Verfügung stellen müssen und die Sicherheitslücke mit persönlichen mobilen Geräten schließen. Dies könnte jedoch zu Einwänden von Mitarbeitern führen, die Software auf persönlichen Geräten installieren müssen, oder Unternehmen dazu veranlassen, Mitarbeitern die Kosten für die Nutzung ihrer Geräte zu erstatten. Und falls Android 14 und iOS 17 auf einigen Endbenutzergeräten nicht unterstützt werden, sind Unternehmen schnell ratlos, was für diese Mitarbeiter zu tun ist.

Eine nicht intuitive User Experience

Das Onboarding von Benutzern ist nicht auf allen Plattformen und Geräten standardisiert, was zu Verwirrung und Produktivitätseinbußen bei den Benutzern führt. Dies bedeutet, dass Unternehmen in detaillierte Benutzerschulungen investieren müssen, um die Akzeptanz von gerätegebundenen Passkeys auf allgemeinen Geräten erfolgreich zu gestalten. Die Benutzer werden oft mit der Installation und Konfiguration von Apps konfrontiert, was zu einem zusätzlichen Aufwand und einer schlechten User Experience führt, insbesondere für Unternehmen mit BYOD-Programmen.

Mehrere Geräte/Registrierungen erforderlich

Um die Wiederherstellung und ein optimales Benutzererlebnis zu unterstützen, ist eine Registrierung auf allen Geräten erforderlich, auf denen Zugriff auf Systeme benötigt wird. Außerdem bräuchte der Benutzer ein zweites mobiles Gerät oder einen Desktop, auf dem ein separater Passkey für die Wiederherstellung des Kontos registriert werden kann. Dies kann für das Unternehmen und/oder den Benutzer frustrierend und kostspielig sein.

Begrenzte Abdeckung von Anwendungsfällen in Unternehmen

Da sich diese Passkeys auf alltäglichen Geräten wie Mobiltelefonen befinden, gibt es Einschränkungen bezüglich der Verwendung des Authentifikators. In Szenarien mit gemeinsam genutzten Arbeitsplatzgeräten oder Desktops, BYOD, hochsicherheitsrelevanten, mobileingeschränkten und einigen Offline-Szenarien, darunter auch mit älteren Geräten und Plattformen, können diese Arten von gerätegebundenen Passkeys nicht alle betrieblichen Anwendungsfälle abdecken.

1. Onboarding/Registrierung

1b. Onboarding mit gerätegebundenen Passkeys auf speziell für Sicherheit entwickelten Authenticatoren

Es gibt drei Möglichkeiten für das Onboarding von Benutzern mit hardwaregebundenen Passkeys.

- Der Manager oder Administrator registriert einen FIDO2-Sicherheitsschlüssel im Namen des Endbenutzers.
- Der Mitarbeiter erhält einen werkseitig bereitgestellten vorregistrierten Sicherheitsschlüssel direkt an sein Postfach.
- Der Endbenutzer verwendet ein vom Unternehmen bereitgestelltes Passwort oder einen Phishing-anfälligen Code, um sich für den Self-Service anzumelden.

Hier sehen wir uns die ersten beiden Optionen an, die ein sicheres und nahtloses Benutzer-Onboarding für Phishing-resistente MFA und passwortlose Nutzung von gerätegebundenen Passkeys, die in Sicherheitsschlüsseln (z.B. YubiKeys) gespeichert sind, ermöglichen.

Onboarding **Sicherheitsschlüssel;** gerätegebundene Passkeys auf Authentifikatoren, speziell für die Sicherheit entwickelten Authenticatoren

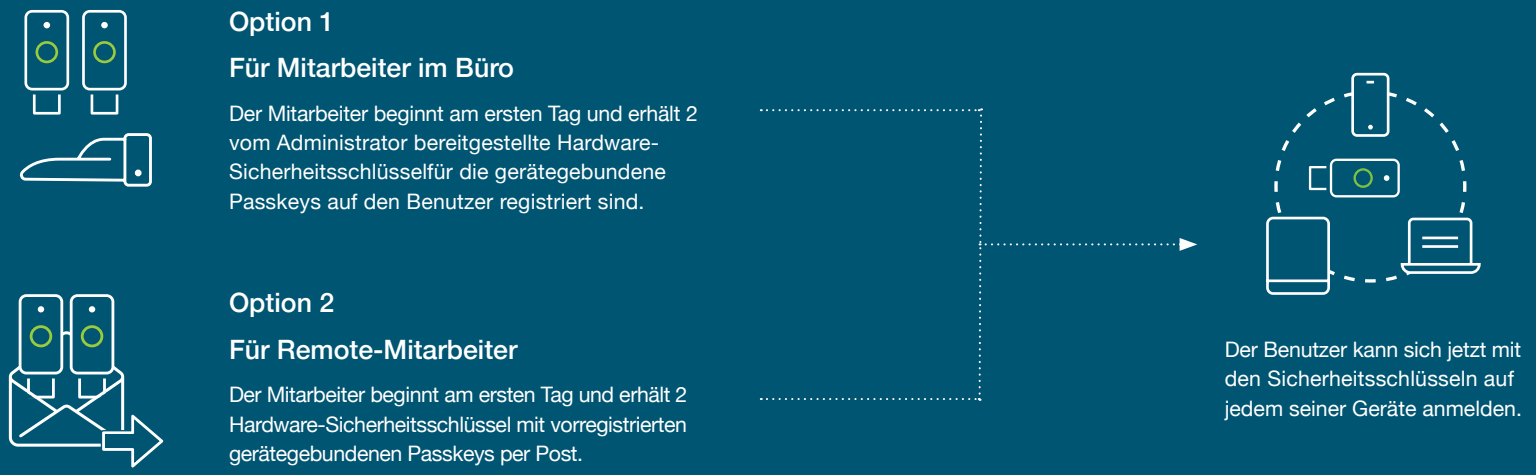


Abbildung 2: Ein Tag im Leben eines neuen Mitarbeiters, dessen Onboarding mit YubiKeys erfolgt

Onboarding/Registrierung

1b. Onboarding mit gerätegebundenen Passkeys auf Authentifikatoren, die speziell für die Sicherheit entwickelt wurden

Vorteile

Phishing-resistentes Onboarding

Der Benutzer oder Prozess darf niemals mit Phishing-anfälligen Geheimnissen hantieren, um den Passkey zu registrieren.

Konsistente User Experience

Der Vorteil für Unternehmen mit gerätegebundenen Passkeys, die in YubiKeys gespeichert sind, besteht darin, dass sie eine konsistente User Experience über alle Geräte und Plattformen hinweg bieten. Die höchste Sicherheit begleitet den Benutzer in einer tragbaren Form der starken Authentifizierung, wodurch der Benutzer phishing resistent wird, während er sich durch seinen Tagesverlauf bewegt.

Höchste Sicherheitsstufe (AAL3)

YubiKeys erfüllen die höheren Sicherheitsanforderungen des Authenticator Assurance Level 3 (AAL3) der NIST-Empfehlungen und damit die strengsten Compliance-Anforderungen. Dies bietet Unternehmen eine hohe Sicherheit und Beschleunigung der Geschäftsabläufe ohne Kopfzerbrechen.

Herausforderungen

Erwerb und Bereitstellung eines separaten Geräts

Die größte Herausforderung für Unternehmen besteht darin, ein separates Gerät zu erwerben, bereitzustellen und an Benutzer zu senden. Dies erscheint komplex, da das Unternehmen Logistik und Vertrieb berücksichtigen muss. Yubico bietet Enterprise-Delivery-Services zur Unterstützung von Logistik- und Vertriebsanforderungen. Alternativ können Unternehmen auch mit lokalen Vertriebspartnern zusammenarbeiten.

2. Wiederherstellung von Zugangsdaten/Konten

2a. Wiederherstellung von Zugangsdaten mit gerätegebundenen Passkeys auf allgemeinen Geräten

Wiederherstellung von Zugangsdaten Passkey-Drittanbieter; gerätegebundene Passkeys auf allgemeinen Geräten

1.

Ein Frontline-Mitarbeiter verliert sein mobiles Gerät mit dem registrierten Passkey.

2.

Er geht persönlich beim Helpdesk vorbei oder ruft dort an, um den Verlust/Diebstahl des mobilen Geräts zu melden.

3.

Die Identitätsprüfung beginnt persönlich oder aus der Ferne.

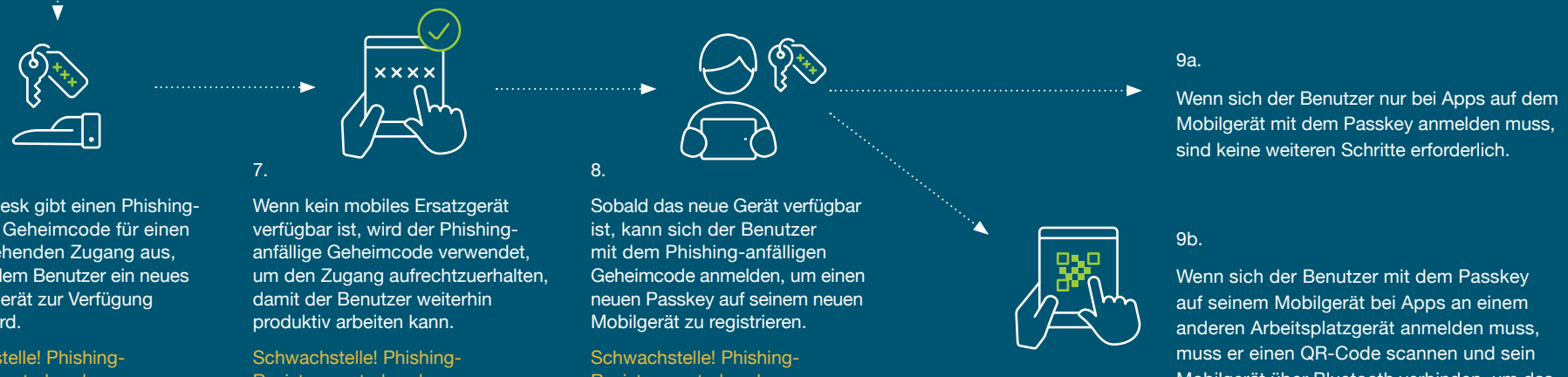
Schwachstelle! Spoofing des Benutzers oder von Benutzerzugangsdaten

4.

Die Identitätsüberprüfung wurde erfolgreich abgeschlossen.

5.

Der Helpdesk entfernt das verlorene/gestohlene Gerät aus dem Benutzerkonto.



6.

Der Helpdesk gibt einen Phishing-anfälligen Geheimcode für einen vorübergehenden Zugang aus, während dem Benutzer ein neues mobiles Gerät zur Verfügung gestellt wird.

Schwachstelle! Phishing-Resistenz unterbrochen

7.

Wenn kein mobiles Ersatzgerät verfügbar ist, wird der Phishing-anfällige Geheimcode verwendet, um den Zugang aufrechtzuerhalten, damit der Benutzer weiterhin produktiv arbeiten kann.

Schwachstelle! Phishing-Resistenz unterbrochen

8.

Sobald das neue Gerät verfügbar ist, kann sich der Benutzer mit dem Phishing-anfälligen Geheimcode anmelden, um einen neuen Passkey auf seinem neuen Mobilgerät zu registrieren.

Schwachstelle! Phishing-Resistenz unterbrochen

9a.

Wenn sich der Benutzer nur bei Apps auf dem Mobilgerät mit dem Passkey anmelden muss, sind keine weiteren Schritte erforderlich.

9b.

Wenn sich der Benutzer mit dem Passkey auf seinem Mobilgerät bei Apps an einem anderen Arbeitsplatzgerät anmelden muss, muss er einen QR-Code scannen und sein Mobilgerät über Bluetooth verbinden, um das Gerät zu verbinden.*

Abbildung 3: Ein Tag im Leben eines Frontline-Mitarbeiters, der versucht, nach dem Verlust eines mobilen Geräts sein Konto wiederherzustellen

Wiederherstellung von Zugangsdaten/Konten

2a. Wiederherstellung von Zugangsdaten mit gerätegebundenen Passkeys auf allgemeinen Geräten

Vorteile

Weniger Geräte für den Benutzer – „eine Sache weniger zu tragen“

Benutzer, die bereits über Telefone verfügen, können dasselbe Gerät für Produktivität und Authentifizierung verwenden.

Keine zusätzlichen Kosten für Hardware-Sicherheitsschlüssel

Unternehmen können möglicherweise die zusätzlichen Kosten für den Erwerb von Hardware-Sicherheitsschlüsseln mit höchster Sicherheit vermeiden.

Herausforderungen

Erfordert mehrere Geräte

Wenn ein Benutzer nur über ein Gerät verfügt, das Passkeys unterstützt, kann eine Benutzersperre/ Kontowiederherstellung kostspielig und riskant sein und eine schlechte User Experience bieten. Um diesen Fallstrick zu vermeiden, müssen mehrere Geräte mit Passkeys registriert werden.

Schlechte User Experience

Wenn ein Mobilgerät verloren geht oder gestohlen wird, müssen alle Arbeitsplatzgeräte, auf die mit diesem Passkey zugegriffen wurde, erneut verbunden werden, indem der QR-Code gescannt und das Mobilgerät über Bluetooth mit dem Arbeitsplatzgerät verbunden wird. Die Wiederherstellung des geräteübergreifenden Zugriffs nach der Wiederherstellung kann mehrere Geräte und Schritte umfassen.

Zusätzliche Kosten für Überwachung und Verwaltung

Gerätegebundene Passkeys auf allgemeinen Geräten umfassen in der Regel zusätzliche Software und Administratoren zur Verwaltung und Überwachung der Sicherheitslage des Mobilgeräts, und die Kosten können sich summieren.

Hohe Wiederherstellungsrate

Wenn Geräte an belebten öffentlichen Orten benutzt werden, steigt die Wahrscheinlichkeit, dass ein Mobiltelefon gestohlen wird, verlegt wird, ausfällt oder kaputt geht. Bei gerätegebundenen Passkeys, wie z. B. einem YubiKey, ist dies weit weniger wahrscheinlich. Außerdem ist es wichtig zu bedenken, dass ein gerätegebundener Passkey, der sich in einem allgemeinen Gerät wie einem Smartphone befindet, versehentlich gelöscht werden kann, während ein Passkey auf einem YubiKey nicht versehentlich gelöscht werden kann. Und schließlich ist es wichtig, die Aktualisierungszyklen von Geräten zu berücksichtigen. Während dieser Zeit werden Authentifizierungs-Apps mit Passkeys möglicherweise nicht ordnungsgemäß auf die aktualisierten Geräte der Benutzer übertragen. Darüber hinaus können Betriebssystem-Updates, Firmware-Updates und App-Updates die Passkey-Abläufe unterbrechen und nicht wie geplant funktionieren. Außerdem treten regelmäßig potenzielle Schwachstellen auf, die Unternehmen dazu zwingen, ihre Geräte sorgfältig zu verwalten und zu patchen.

2. Wiederherstellung von Zugangsdaten/Konten

2b. Wiederherstellung von Zugangsdaten mit gerätegebundenen Passkeys auf Authentifikatoren, die speziell für die Sicherheit entwickelt wurden

Wiederherstellung von Zugangsdaten **Sicherheitsschlüssel;** gerätegebundene Passkeys auf Authentifikatoren, die für Sicherheit entwickelt wurden

1. Verlust oder Diebstahl des Sicherheitsschlüssels. Der Benutzer kann dieses Problem mithilfe des Self-Service lösen.
2. Der Benutzer ruft seinen Backup-Sicherheitsschlüssel ab.
3. Der Benutzer meldet sich bei seinem Sicherheits-registrierungsportal an und entfernt den verlorenen Sicherheitsschlüssel aus seinem Konto.
4. Der Benutzer hat weiterhin Zugriff und bleibt dank der Phishing-resistenten Authentifizierung mit seinem Backup-Schlüssel produktiv, während er auf einen Ersatzschlüssel wartet.
5. Sobald der Ersatzschlüssel dem Konto hinzugefügt wurde, ist kein besonderer Prozess für alle Geräte erforderlich, bei denen sich der Benutzer anmelden muss.

Abbildung 4: Ein Tag im Leben eines Mitarbeiters, der versucht, den Zugriff auf sein Konto mithilfe von YubiKeys wiederherzustellen

Wiederherstellung von Zugangsdaten/Konten

2b. Wiederherstellung von Zugangsdaten mit gerätegebundenen Passkeys auf Authentifikatoren, die speziell für die Sicherheit entwickelt wurden

Vorteile

Nicht kostspielig

Im Vergleich zu zwei mobilen Geräten sind die Kosten für einen Backup-Sicherheitsschlüssel, wie z. B. einen YubiKey, viel geringer. Außerdem ermöglicht ein Backup-YubiKey eine viel schnellere und einfachere Wiederherstellung per Self-Service.

Ständig aktiver Schutz vor Phishing

Der Verlust eines Sicherheitsschlüssels (der gerätegebundene Passkeys enthält) unterbricht den normalen Arbeitsablauf nicht und verringert auch nicht die Authentifizierungsstärke.

Herausforderungen

Backup-Schlüssel erforderlich

Wenn ein Benutzer seinen Sicherheitsschlüssel verliert, sind einige Schritte erforderlich, um den Zugriff auf das Konto wiederherzustellen. Daher wird jedem Benutzer ein zweiter Sicherheitsschlüssel als Backup empfohlen, um den Kontozugriff zu erhalten und eine Phishing-resistente Methode zum Hinzufügen einer neuen Sicherungsmethode bereitzustellen.

YubiKeys machen andere gerätegebundene Passkeys sicherer.

Es muss nicht entweder das eine oder das andere sein: Ein hybrider Ansatz könnte in bestimmten Szenarien am besten für ein Unternehmen geeignet sein, z. B. bei der Verwendung von Passkey-Drittanbietern für Apps/Nutzer mit geringem Risiko oder für den vorübergehenden Gebrauch während der Wiederherstellung. Bedenken Sie auch, dass die Verwendung eines vorregistrierten YubiKeys, der dem Endbenutzer zur Verfügung gestellt wird, die starke Bindung schafft, die erforderlich ist, um die Einrichtung eines anderen Typs gerätegebundener Passkeys bei einem Drittanbieter zu unterstützen. Damit wird die Messlatte für Sicherheit und Benutzerfreundlichkeit deutlich höher gelegt und eine robuste Strategie für den Lebenszyklus von Zugangsdaten geschaffen, auf der ein Unternehmen aufbauen kann.

Zusätzliche Überlegungen für Unternehmen

Compliance, Audit und Risiken

Compliance und Audit mit gerätegebundenen Passkeys auf allgemeinen Geräten

Herausforderungen

Beschränkte Attestierungsmöglichkeiten; schwer festzustellen, welche Geräte/Hardware die Passkeys schützen

Gerätegebundene Passkeys auf allgemeinen Geräten wie Smartphones, Laptops oder Tablets erfüllen nur AAL2

Erfüllt nicht die strengsten Compliance- und Zertifizierungsanforderungen

Compliance und Audit mit gerätegebundenen Passkeys auf Authentifikatoren, die speziell für die Sicherheit entwickelt wurden

Vorteile

Die Attestierung der Hardware-Authentifizierung bietet die größte Sicherheit, dass die Passkeys sicher auf bekannter, vertrauenswürdiger Hardware mit bekannten Eigenschaften gespeichert sind

Gerätegebundene Passkeys auf YubiKeys sind die einzigen Schlüssel, die AAL3 erfüllen

Erfüllt strengste Compliance- und Zertifizierungsanforderungen

YubiKeys erfüllen die Bundesvorschriften für höchste Sicherheit

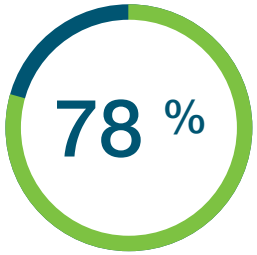
- YubiKeys sind in gesicherten Bereichen erlaubt, in denen mobile Geräte verboten sind.
- YubiKeys können helfen, wenn Unternehmen über ältere oder speziell angefertigte Systeme verfügen, die mit gerätegebundenen Passkeys auf Allzweckgeräten nicht kompatibel sind.

Risiken und Kostenbelastung

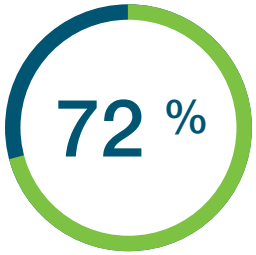
Im Allgemeinen besteht ein höheres Risiko, dass mobile Geräte verloren gehen, gestohlen oder kompromittiert werden, da die Benutzer diese Geräte für eine Vielzahl von Aktivitäten nutzen. Passkeys, die sich auf mobilen allgemeinen Geräten befinden, sind einem größeren Risiko ausgesetzt, kompromittiert zu werden, verglichen mit Passkeys, die sich auf speziell für die Sicherheit entwickelten Authentifikatoren befinden, wie z. B. Hardware-Sicherheitsschlüssel. Der Austausch eines Smartphones ist viel teurer als der Austausch eines Sicherheitsschlüssels.

Allgemeine Geräte für die Sicherheit

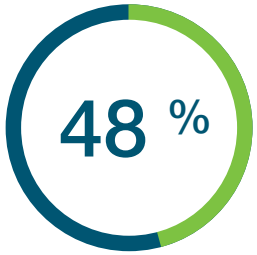
Riskante Benutzer



der Benutzer nutzen ihr Arbeitsgerät für persönliche Aktivitäten.



nutzen private Geräte für die Arbeit.



lassen Freunde oder Familienmitglieder das Gerät benutzen.

Quelle: Bericht „2024 State of the Phish“ von Proofpoint

Der YubiKey – Legen Sie die Messlatte für die Sicherheit aller anderen Passkey-Anbieter höher

Unternehmen, die Passwörter aus dem Alltag ihrer Benutzer entfernen möchten, können mit dem YubiKey eine einfache, sichere und tragbare Möglichkeit bieten, die Sicherheit zu erhöhen. Benutzer können den YubiKey verwenden, um sich bei ihren Arbeitsplatzgeräten zu authentifizieren anschließend ihre Passkey-Anbieter (sowohl plattformgebundene als auch Drittanbieter) zu entsperren um somit die Sicherheitsstandards für ihre Passkey-Anwendungen zu erhöhen.

Gerätegebundene Passkeys in YubiKeys bieten die **höchste Sicherheit** in Bezug auf die Verwaltung des privaten Schlüssels auf Grundlage des integrierten FIDO-Attestierungsstandards. Der YubiKey stellt sicher, dass der private Schlüssel in einem speziell entwickelten Hardware-Sicherheits-modul gespeichert und geschützt wird. Andere Arten von gerätegebundenen Passkeys müssen sich auf weniger zuverlässige Ansätze verlassen, um Informationen über die Sicherheit und Kontrolle des privaten Schlüssels bereitzustellen. Dies kann dazu führen, dass Unternehmen nicht in der Lage sind, Compliance-Vorschriften oder notwendige Sicherheitsstandards zu erfüllen.

Zusammenfassung

Wichtige Passkey-Erkenntnisse für Ihr Unternehmen

Passkeys bieten eine FIDO-fähige Welt, aber für Unternehmen, die strenge Kontrolle über die Benutzeridentität erfordern, senken gerätegebundene Passkeys auf allgemeinen Geräten wie Smartphones, Laptops und Tablets möglicherweise nicht das Risiko für Ihr Unternehmen. Gerätgebundene Passkeys, die auf Sicherheitsschlüsseln gespeichert sind, bieten die höchste Sicherheitsgarantie und ermöglichen Unternehmen das vertrauenswürdige Management des Lebenszyklus von Anmeldeinformationen sowie die erforderlichen Attestierungsfähigkeiten, um die stärkste Sicherheit, das einfachste Benutzer-Onboarding und die Verwaltung von Anmeldeinformationen und Kontowiederherstellung über verschiedene Geräte und Plattformen hinweg sicherzustellen und gleichzeitig die strengsten Anforderungen branchenübergreifend zu erfüllen.

- Achten Sie auf Phishing-resistente Authentifizierungsmethoden, die alle Bereiche der Authentifizierung und Zugangsdatenverwaltung unterstützen, um Phishing-resistente Benutzer zu schaffen. Onboarding- und Wiederherstellungsabläufe sind häufige Bereiche, in denen die Phishing-Resistenz einbricht, was sie zu einem attraktiven Angriffsvektor macht.
- Für eine Vielzahl unterschiedlicher Geräte kann nur eine teilweise oder gar keine Attestierung vorliegen. Der Dienst/die vertrauenswürdige Partei bzw. das Unternehmen kann nicht wissen, welche Art von Gerät verwendet wurde oder wie vertrauenswürdig der Authetifikator ist und wie der Passkey gespeichert wird. Es ist entscheidend, dass Unternehmen den von ihren Benutzern verwendeten Passkeys vertrauen können.
- Passkey Anmeldeinformationen, wie sie in modernen FIDO-Sicherheitsschlüsseln gespeichert sind, bieten ein höheres Maß an Sicherheit als Passkeys auf einem Smartphone. Während diese Passkeys mit niedrigerer Sicherheit eine AAL2-Zertifizierung bieten, können Passkeys in Sicherheitsschlüsseln eine AAL3-Zertifizierung der NIST bieten – die höchste Authenticator Assurance Level 3 – die für die Einhaltung von Compliance Vorschriften von entscheidender Bedeutung ist.

Kontaktieren Sie uns
yubi.co/kontakt

Weitere Informationen:
yubi.co/passkey

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. Weitere Informationen finden Sie unter: www.yubico.com.