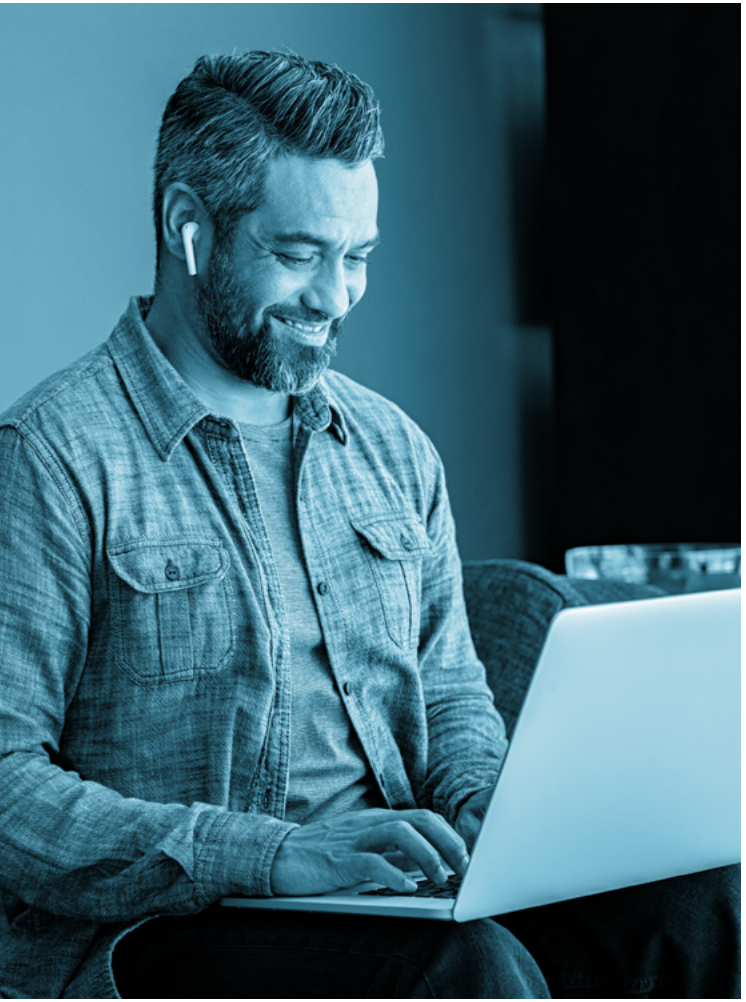
yubico

Ziehen Sie synchronisierte Passkeys für Ihr Unternehmen in Betracht?

Vermeiden Sie die Gefahren, die das Risiko und die Kosten erhöhen



Unterschiedliche Passkey-Implementierungen

Passkeys sind kennwortlose FIDO-Anmeldeinformationen, die in Authentifikatoren verwendet werden, wie etwa in Smartphones, Tablets oder Laptops oder in Authentifikatoren, die speziell für die Sicherheit entwickelt wurden, wie z. B. FIDO-Hardware-Sicherheitsschlüssel.

Passkeys sind sicherer als Passwörter und begünstigen die Umstellung auf eine passwortlose Authentifizierung, die mehr Sicherheit und Effizienz ermöglicht. Für weitere Informationen zu den Grundlagen der Passkeys klicken Sie hier.

Es wird zwischen zwei Arten von Passykeys unterschieden: synchronisierte und hardwaregebundene. Synchronisierte Passkeys sind kopierbare Anmelde-informationen, die über verschiedene Geräte wie etwa Smartphones, Laptops und Tablets mit einem Benutzerkonto übertragen werden können. Dies kann zu einigen abschreckenden Schwachpunkten für das Unternehmen führen.

Einige übliche Szenarien, in denen Ihre synchronisierten Passkeys bei der Arbeit Anfälligkeiten mit sich bringen könnten:

1. **Risiken bei der Remote-Arbeit** – Sicherheitsrisiken treten auf, wenn Mit-arbeitende von zu Hause aus arbeiten und das Gerät eines Angreifers für Anmeldeinformationen von Mitarbeitenden verwendet wird, da die Informationen mithilfe der synchronisierten Passkeys einfach kopiert werden können.
2. **Schwachstellen in der Lieferkette** – Insider-Bedrohungen treten auf und die Integrität der Lieferkette wird beeinträchtigt, wenn Mitarbeitende synchronisierte Passkey-Anmeldedaten über Konten und Geräte hinweg teilen.
3. **Komplexität bei Compliance- und Support** – Die Ausbreitung des Passkey-Ökosystems bietet Unternehmen die Möglichkeit, mehrere Passkey-Anbieter zu nutzen, wodurch es schwierig wird, die für die Compliance erforderlichen Anmeldedaten zu verfolgen und ihnen zu trauen. Des Weiteren erhöhen sich Aufwand und Kosten für den IT-Helpdesk.

Lesen Sie die folgenden Szenarien, um zu erfahren, wie synchronisierte Passkeys die Risiken und Kosten für das Unternehmen erhöhen können.

Synchronisierte vs hardwaregebundene Passkeys

Synchronisierte Passkeys

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

Hardwaregebundene Passkeys

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

Szenario 1

Risiken bei der Remote-Arbeit

Ein Passkey synchronisiert alle Geräte eines einzigen iCloud-Kontos. Dies stellt sich in der folgenden Geschichte für Jim als gefährlich heraus, der als Remote-Mitarbeiter in Vollzeit für ein Technologieunternehmen tätig ist. Jim arbeitet von zu Hause aus, wo seine ganze Familie dasselbe iCloud-Konto mit sechs verschiedenen Geräten nutzt. Sehen wir uns an, wie ein Angreifer synchronisierte Passkeys für seine Zwecke verwenden kann.

1. Jim meldet sich mit einem Passkey auf seinem Telefon bei seinem geschäftlichen Konto an. Er hat sein Telefon zu seinem persönlichen iCloud-Konto hinzugefügt, das auch mit anderen Geräten geteilt wird, die von seiner Familie verwendet werden.

2. Jims Sohn Ben erhält eine E-Mail mit einem coolen Link zu einem App-basierten Spiel, das er gerne spielt. Er klickt auf den Link.

3. Ben wird dazu überlistet, seinen iCloud-Benutzernamen und sein Passwort anzugeben, die vom Angreifer abgefangen werden. Ben akzeptiert die Aufforderung, ein neues Gerät hinzuzufügen, womit der Angreifer sein eigenes Gerät beim iCloud-Konto der Familie registrieren kann.

4. Da Jims geschäftliches Telefon bereits mit der Cloud synchronisiert ist, wird auch sein geschäftlicher Passkey automatisch mit allen Geräten im iCloud-Konto synchronisiert. Dazu gehört auch das Gerät des Angreifers!

5. Sobald der Angreifer in Besitz von Jims geschäftlichen Anmeldedaten ist, kann er sich als Jim auf den Arbeitsseiten anmelden und dann nach anderen Anmeldedaten mit höheren Berechtigungen suchen.

WUSSTEN SIE SCHON?

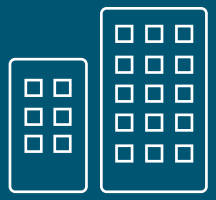
89 % der Unternehmen wurden im letzten Jahr Opfer eines Phishing-Angriffs.

HYPR, 2022 State of Passwordless Security Report

Szenario 2

Schwachstellen in der Lieferkette

Ein synchronisierter Passkey kann über die AirDrop-Funktion auf dem iPhone ganz einfach außerhalb der direkten Kontrolle eines Benutzers mit einem anderen Gerät geteilt werden. Und auch wenn die gemeinsame Nutzung eines Passkey in einigen Situationen praktisch ist, kann es zu erheblichen Sicherheitslücken wie etwa Insider-Bedrohungen führen, wenn Mitarbeitende ihre Anmeldedaten fahrlässig teilen. Dies führt zu einem erhöhten Risiko sowie einem Vertrauensverlust innerhalb der gesamten Lieferkette. Kiras Geschichte



1. Ein großer Einzelhändler mit einer komplexen Lieferkette ermöglicht es seinem HVAC-Systemmonitor (einem externen Anbieter), sich bei wichtigen Systemen anzumelden, um die Echtzeitbedingungen zu überwachen.

2. Kira ist eine neue Mitarbeiterin des Anbieters. Sie hat die Einrichtung ihres Kontos beim Händler noch nicht abgeschlossen, muss aber in der nächsten Schicht arbeiten. Daher hat ein Kollege seinen Passkey mit AirDrop via Bluetooth mit ihr geteilt.

3. Ein paar Monate später kündigt Kira, hat allerdings noch den Passkey ihres Kollegen, da es keine automatisierte Möglichkeit gibt, den geteilten Passkey des Kollegen auf Kiras Gerät zu sperren.

   Das Unternehmen kann das Löschen der Passkeys auf Kiras Gerät nicht erzwingen.

4. Eine falsche Einstellung des HVAC-Systems verursacht plötzlich einen erheblichen Ausfall.

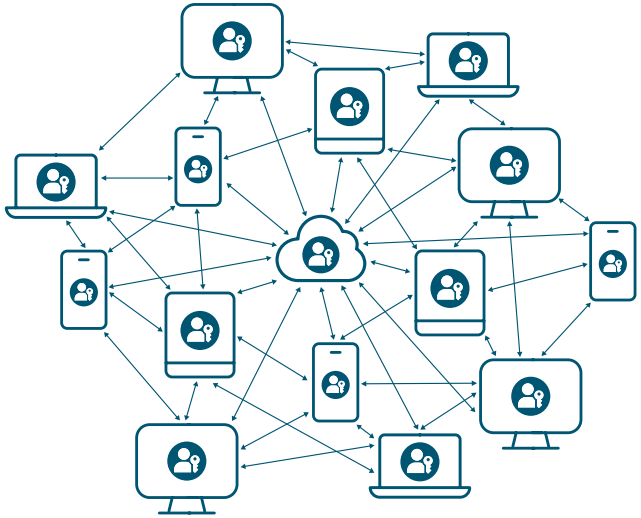
   Der Passkey ist an mindestens zwei Speicherorten vorhanden: Die Auditprotokolle zeigen die verwendeten Passkey-Anmeldedaten an, aber die Protokolle können nicht bestimmen, ob die Anmeldung durch Kira oder ihren Kollegen erfolgt ist.

5. Die Risiken aufgrund gesetzlicher Vorschriften nehmen zu, da Auditprotokolle weniger zuverlässig sind und der Anbieter die Kontrolle darüber verliert, wo die Passkey-Anmeldedaten gespeichert und verwaltet werden.

Szenario 3

Komplexität bei Compliance und Support

Passkeys werden über eine Vielzahl von Anbietern und Produkten hinweg implementiert. Benutzer müssen nicht nur einen davon verwenden. Das bedeutet, dass ein Unternehmen mit dem Risiko konfrontiert ist, dass Benutzer viele Passkeys über verschiedene Plattformen und Passwortmanager hinweg besitzen. Wie verfolgt das Unternehmen, welcher Passkey wo gespeichert wird, und wie hilft es Benutzern, die auf Probleme mit dem Passkey-Support stoßen, wenn das Unternehmen keinen Durchblick hat?



1. Frank wird von der IT-Abteilung gebeten, Passkeys zu registrieren, um die Sicherheit seiner geschäftlichen Login-Daten zu verbessern.

2. Frank beschließt aus Gründen der Zweckmäßigkeit, drei verschiedene Passkey-Dienstanbieter (Apple, Google, Passwortmanager) zu verwenden, damit sich Frank mit einem seiner synchronisierten Passkeys beim Unternehmenssystem anmelden kann.

3. Monate später kommt eine Datenpanne ans Licht, die deutlich macht, dass bei einem von Franks Passkey-Dienstleistern ein Sicherheitsvorfall im Passkey-Managementsystem vorlag.

4. Aufgrund der zu hohen Gefährdung des Ökosystems ist Franks Identität anfällig für Angreifer. Frank muss jetzt alle synchronisierten Passkeys von den drei verschiedenen Anbietern entfernen und die Passkeys für seine Unternehmensanmeldung neu registrieren.

5. Für den Helpdesk des Unternehmens wird die Unterstützung von Mitarbeitenden wie Frank bei der Lösung von Zugriffsproblemen schwer, da Kenntnisse über die verschiedenen Passkey-Dienstanbieter fehlen. Unternehmen müssen die Supportkosten für die Aktivierung synchronisierter Passkeys berücksichtigen.

Welche Passkeys eignen sich für Ihr Unternehmen?

Die fünf wichtigsten Punkte

Passkeys sind besser als Passwörter, da sie auf modernen FIDO-Protokollen basieren und einen stärkeren Schutz vor Phishing bieten.

Dies sind die fünf wichtigsten Punkte, die Sie über synchronisierte Passkeys wissen sollten. Darüber hinaus legen wir dar, warum hardwaregebundene Passkeys eine sicherere und konforme Option für Unternehmensanforderungen bieten! Nicht alle Passkeys sind gleich, und Unternehmen sollten die Fallstricke synchronisierter Passkeys meiden.

- Passkeys ermöglichen eine FIDO-fähige Welt. Für Unternehmen, die eine strenge Kontrolle über die Benutzeridentität voraussetzen, können synchronisierte Passkeys jedoch ein erhöhtes Risiko bergen.
- Synchronisierte Passkeys können mitgeführt werden, womit sie eher einen Anmeldemechanismus als einen tatsächlichen zweiten Faktor darstellen.
- Synchronisierte Passkeys können dazu führen, dass Unternehmen Dritten vertrauen, die keine fachlichen Sicherheitsanbieter sind.
- Synchronisierte Passkeys bieten Benutzern einfachere Wege zum Teilen von Anmeldedaten, und Benutzer können diese standardmäßig verwenden, wenn sie aktiviert sind.
- Hardwaregebundene Passkeys, wie solche, die sich in modernen, tragbaren FIDO-Sicherheitsschlüsseln befinden, bieten einen höheren Schutz und erfüllen die Compliance-Anforderungen des Unternehmens besser.

Kontaktieren Sie uns
yubi.co/kontakt

Erfahren Sie mehr
yubi.co/passkey

So wählen Sie Ihre richtige Passkey-Lösung

DIENSTLEISTER

Verbraucher

Die meisten Verbraucher können synchronisierte Passkeys auf ihren Geräten verwenden, da diese die bessere Alternative zu Passwörtern sind.

Gefährdete Verbraucher

Hochrisikobenutzer wie z. B. Journalisten, können von sichereren Passkeys profitieren, wozu etwa diejenigen zählen, die in Hardware-Sicherheitsschlüsseln vorhanden sind.

UNTERNEHMEN

Mitarbeitende im Einsatz

Viele dieser Mitarbeitenden können keine privaten Telefone oder Laptops am Arbeitsplatz verwenden und benötigen daher eine Passkey-Lösung, die nicht von solchen Geräten abhängig ist.

Büroangestellte

Diese Mitarbeitende benötigen Sicherheitsschlüssel mit Hardwarebescheinigung, um sicherzustellen, dass die Zugangsdaten des Passkeys nicht kopiert werden können.

Privilegierte Benutzer

Benutzer, die die Ziele mit dem höchsten Risiko sind, benötigen Sicherheitsschlüssel mit Hardwarebescheinigung, um den Speicherort der Passkey-Anmeldedaten zu kennen.

yubico

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

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

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