yubico

WHITE PAPER

Gemeinsam genutzte Arbeitsplatzgeräte vor Cyberbedrohungen schützen

Phishing-resistente MFA mit außergewöhnlicher UX

Inhalt

Gemeinsam genutzte Arbeitsplatzgeräte sind einfache Ziele für Cyberangriffe

Unternehmen sehen sich heute einer sich ständig weiterentwickelnden Cyberbedrohungslandschaft mit Elementen wie künstlicher Intelligenz und maschinellem Lernen sowie einer Reihe von Bedrohungsvektoren wie Phishing, SIM-Swaps und Man-in-the-Middle (MITM)-Angriffen gegenüber, die immer raffinierter werden. Viele dieser Ansätze sind für die Endnutzer praktisch nicht unterscheidbar, sodass sowohl sie als auch ihre Unternehmen stark gefährdet sind. Kompromittierte Zugangsdaten sind nach wie vor der häufigste Angriffspunkt – 61 % der Datenschutzverletzungen lassen sich auf irgendeine Weise auf Zugangsdaten zurückführen.[2] Unsichere Praktiken in Bezug auf Zugangsdaten, einschließlich der genehmigten und nicht genehmigten Weitergabe von Benutzernamen und Passwörtern, erhöhen das Risiko von Datenschutzverletzungen für Unternehmen sogar noch.

Gemeinsam genutzte Arbeitsplatzgeräte – oft Standard in verschiedenen Branchen wie dem Gesundheitswesen, der Fertigung, dem Einzelhandel, dem Gastgewerbe, der Finanzdienstleistungsbranche, der Energiebranche, der Versorgungsbranche, der Öl- und Gasbranche sowie im Bildungssektor – befinden sich oft in Umgebungen mit hohem Schichtwechsel, saisonalen Mitarbeitern und hoher Fluktuation. Sie bergen potenziell hohe Sicherheitsrisiken, wenn nicht umfangreiche Schutzmaßnahmen getroffen werden. Gemeinsam genutzte Arbeitsplatzgeräte erhöhen die (absichtlichen oder fahrlässigen) Insider-Bedrohungen und stellen zusätzliche Sicherheitsrisiken dar, wenn sie in Bereichen mit vielen potenziellen Benutzern eingesetzt werden. Unsichere Praktiken für gemeinsam genutzte Arbeitsplatzgeräte wie Passwortfreigabe und die Verwendung von Notizzetteln für Passwörter sind in Szenarien mit gemeinsam genutzten Arbeitsplatzgeräten, die von Schichtarbeitern verwendet werden, üblich und weisen auf systemische Probleme mit Authentifizierungsworkflows hin, die grundlegende Aufgaben behindern.

Kosten für Datenschutzverletzungen nach Branche[1]

Gesundheitswesen

9,23 Mio. USD

Finanzdienstleistungen

5,72 Mio. USD

Fertigung

4,99 Mio. USD

Energie

4,65 Mio. USD

Bildung

3,79 Mio. USD

Einzelhandel

3,27 Mio. USD

Gastgewerbe

3,03 Mio. USD

61 %

der Datenschutzverletzungen waren auf **Zugangsdaten zurückzuführen**.[3]

11,45 Mio. USD

durchschnittliche Gesamtkosten von **Insider-Bedrohungen**[4]

46 %

der Mitarbeiter **teilen Passwörter** oder Konten.[5]

82 %

der Einzelpersonen **verwenden dieselben Passwörter** für verschiedene Konten[6]

41 %

verlassen sich bei der Passwortverwaltung auf **Notizzettel**.[7]

Was sind gemeinsam genutzte Arbeitsplatzgeräte?

Gemeinsam genutzte Arbeitsplatzgeräte sind Geräte, die von mehreren Benutzern (manchmal auch als „Roving User“, also umherziehende Benutzer bezeichnet) verwendet werden. Dabei authentifizieren sich mehrere Personen den ganzen Tag über an derselben Workstation, z. B. Callcenter oder Verkaufsstellen-Kiosks, um nur einige zu nennen. Gemeinsam genutzte Arbeitsplatzgeräte werden häufig in Branchen mit Mitarbeitern, die im Schichtbetrieb arbeiten oder im Tagesverlauf rotierende Positionen einnehmen, oder in Branchen mit Stunden-, Zeit- oder Saisonarbeitern verwendet.

Gemeinsam genutzte Arbeitsplatzgeräte und Kiosks sind für den täglichen Betrieb von Unternehmen in einer Vielzahl von Branchen von entscheidender Bedeutung. Diese Systeme verfügen oft über eine direkte Verbindung zu kritischen Systemen und Daten, einschließlich Kundendaten, Zahlungsinformationen, proprietären Informationen, Fertigungs- oder Montagelinien und sogar geschützten Gesundheitsinformationen.

Der Charakter gemeinsam genutzter Arbeitsplatzgeräte macht sie zu einfachen Zielen für Cyber-Kriminelle und Insider-Angriffe:

- **Hat mehrere Benutzer**
- **Wird in stark frequentierten Bereichen verwendet**
- **Zugriff auf kritische Systeme oder Daten**
- **Traditionell anfällig für lückenhafte Sicherheitspraktiken**
- **Keine Garantie, ob es vom Unternehmen selbst verwaltet wird**

Gemeinsam genutzte Arbeitsplatzgeräte verstärken die Risiken im Zusammenhang mit Geräten, Benutzerzugriff, Authentifizierung oder Insider-Bedrohungen, die zum Diebstahl oder Verlust von Zugangsdaten, geschäftskritischen Daten oder geistigem Eigentum führen. Wenn gemeinsam genutzte Arbeitsplatzgeräte aufgrund eines Cyberangriffs nicht verfügbar sind, kann dies zu Geschäftsausfällen und weiteren Konsequenzen in Bezug auf Umsatz und Markenreputation sowie zu Strafen für Verstöße gegen gesetzliche Vorschriften führen.

Häufige Szenarien für gemeinsam genutzte Arbeitsplatzgeräte und damit verbundene Schwachstellen

Branchen mit gemeinsam genutzten Kiosks

- Front-of-House im Einzelhandel und Gastgewerbe
- Pflegestationen in Krankenhäusern/Kliniken
- Fertigungs- oder Logistikstation

Gemeinsam genutzte Kiosks

Gemeinsam genutzte Kiosks sind Arbeitsplatzgeräte, die eine Reihe üblicher Anwendungen für viele verschiedene gemeinsame Benutzer in Front-of-House-Szenarien (Restaurants, Hotels, Banken, Postämter, Einzelhandel), auf der Pflegestation im Krankenhaus oder in Fertigungs- und Logistikszenarien bereitstellen. Gemeinsam genutzte Kiosks können stationär oder sogar tragbar sein, wie dies bei mobilen Arbeitsplatzgeräten im Gesundheitswesen der Fall ist.

Gemeinsam genutzte Kiosks unterstützen häufig mehrere Benutzer in einer einzigen Schicht. Dadurch erhöht sich die Häufigkeit unsicherer Praktiken, etwa die gemeinsame Nutzung von Passwörtern zur Reduzierung der Abmelde-/Anmeldezeiten, die für den Zugriff auf gemeinsam genutzte Ressourcen erforderlich sind. Im Gesundheitswesen beispielsweise ist die gemeinsame Nutzung von Passwörtern unter medizinischen Fachkräften nach wie vor verbreitet (73,6 %), wobei die individuellen Zugriffsebenen gleich sind.[8]

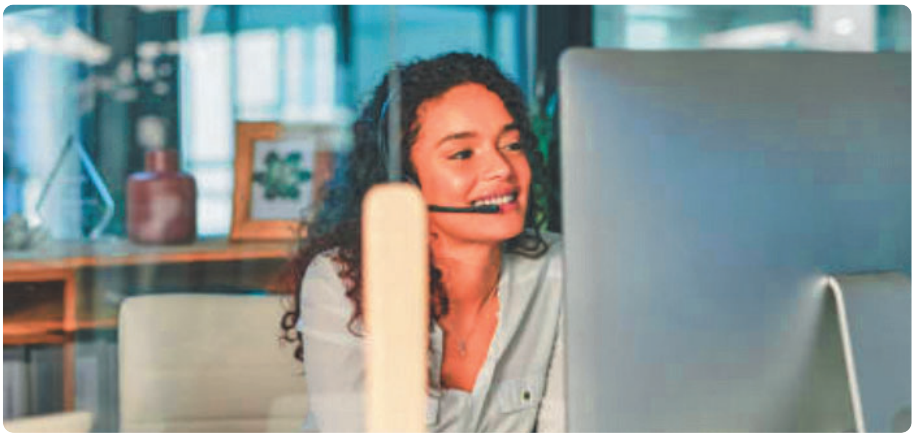
Branchen mit Einschränkungen für Mobilgeräte

- Callcenter
- Reinräume
- Air-Gap-Umgebungen
- Hochsicherheitsstandorte
- Industrie (keine Verbindung, Bohrinseln usw.)

Einschränkungen für Mobilgeräte

Eine Umgebung mit Einschränkungen für Mobilgeräte ist eine Umgebung, in der Mobilgeräte nicht verwendet werden können. Dies kann auf Faktoren zurückzuführen sein, die mit der Umgebung selbst zusammenhängen, wie z. B. Air-Gap-Netzwerke oder isolierte Netzwerke, harte Umgebungen, Offline- oder Offshore-Standorte, Reinräume oder Hochsicherheitsstandorte. Sie können auch auf Einschränkungen durch Vorschriften oder Gewerkschaften zurückzuführen sein oder darauf, dass die Unternehmensrichtlinien einfach vom Einsatz mobiler Geräte abraten. Möglicherweise möchte auch eine Untergruppe von Mitarbeitern innerhalb eines Unternehmens ihre privaten Mobilgeräte nicht für geschäftliche Zwecke verwenden, so dass andere Authentifizierungsmethoden erforderlich sind.

Gemeinsam genutzte Arbeitsplatzgeräte in Umgebungen mit Einschränkungen für Mobilgeräte benötigen zur Förderung der Benutzerakzeptanz eine Authentifizierung, die äußerst sicher, konform mit Branchenvorschriften und einfach zu verwenden ist.



Grab-and-Go-Branchen

- Polizei- und Sicherheitsmitarbeiter
- Gesundheitswesen und häusliche Pflege
- Besuch von Dritten

„Grab-and-Go“

Eine „Grab-and-Go“-Umgebung umfasst in der Regel die Verwendung eines mobilen Wagens mit gemeinsam genutzten Geräten, die vor Ort oder an entfernten Standorten genutzt werden können. Dabei kann es sich um ein modernes Computergerät wie einen Laptop, ein Tablet oder Mobiltelefon handeln oder sogar um ein Gerät, das an ein älteres System gebunden ist. Gemeinsam genutzte „Grab-and-Go“-Geräte sind in Schulen und Bibliotheken, in Strafverfolgungsbehörden und im Gesundheitswesen üblich. In jeder dieser Umgebungen benötigt ein Benutzer das Gerät nur für einen begrenzten Zeitraum.

Darüber hinaus haben viele Branchen nach der Pandemie auf die Realitäten der hybriden Arbeit reagiert, indem sie mehr „Grab-and-Go“-Gelegenheiten bieten, um Mitarbeiter zu unterstützen, die sich möglicherweise für eine feste Heimkonfiguration entschieden haben. Seit der Pandemie betrachten Mitarbeiter „Grab-and-Go“-Geräte und „Hoteling“ eines Arbeitsplatzes im Büro als flexible und attraktive Arbeitsoption.[9]

Da ein Gerät nicht mit einem Benutzer verknüpft ist, müssen Kontrollen vorhanden sein, die Zugriff nur auf die Anwendungen und Dienste gewähren, die mit den spezifischen Benutzeranmeldeinformationen verknüpft sind. Außerdem muss die Authentifizierung schnell und zuverlässig erfolgen, um die Produktivität zu unterstützen.

Point-of-Sale-Branchen

- Einzelhandel
- Lebensmittel
- Großhandel

Point-of-Sale (POS)

Diese speziellen Workstations, die für Finanztransaktionen mit Kunden im Einzelhandel, im Lebensmittelhandel, in der Fast-Food- und Gastronomiebranche oder im Großhandel verwendet werden, können von Mitarbeitern oder sogar von Kunden (Self-Service-Kiosks) genutzt werden. Um die Kundenerfahrung zu optimieren, muss besonders auf eine schnelle und einfache Authentifizierung geachtet werden, um mögliche Konto-sperrungen zu vermeiden und vor allem die Sicherheit von Kunden- und Zahlungs-informationen zu gewährleisten.

Aufgrund des hohen Risikos für Finanzdaten am Point-of-Sale sind diese Workstations gemäß dem PCI DSS (Payment Card Industry Data Security Standard) streng reguliert. Karten-Skimming ist das häufigste Risiko bei POS-Terminals. Dabei werden Daten von der Zahlungsinfrastruktur, Overlays, Malware oder kompromittierter Software erfasst oder drahtlos bzw. über NFC abgefangen. Die hohe Fluktuationsrate der Mitarbeiter und die Natur der saisonalen Arbeit schaffen häufig zusätzliche Druckpunkte beim Onboarding und Offboarding des Mitarbeiterzugriffs auf POS-Systeme.

Ein wachsender Problembereich im POS-Bereich ist die Verwendung von Smartphones, Tablets oder anderen drahtlosen Geräten anstelle eines standardmäßigen POS-Terminals. Bis 2023 wird Schätzungen zufolge 1 von 4 POS-Transaktionen über mPOS (Mobile Point of Sale) abgewickelt. Dieser Prozess erhöht das Risiko von Man-in-the-Middle (MITM)-Angriffen und bringt andere mobile Schwachstellen mit sich.[10]

> MFA ist von entscheidender Bedeutung, aber nicht alle MFA-Methoden sind gleich. Twitter verwendete die anwendungsbasierte MFA, die eine Authentifizierungsanforderung an das Smartphone eines Mitarbeiters sendete. Dies ist eine gängige Form der MFA, die aber umgangen werden kann. Während des Twitter-Hacks haben die Hacker die MFA überwunden, indem sie die Twitter-Mitarbeiter davon überzeugten, die anwendungsbasierte MFA während der Anmeldung zu authentifizieren. Die sicherste Form der MFA ist ein physischer Sicherheitsschlüssel oder eine Hardware-MFA, bei der ein USB-Stick zur Authentifizierung von Benutzern an einen Computer angeschlossen wird. Diese Art von Hardware-MFA hätte die Hacker gestoppt und Twitter implementiert sie jetzt anstelle der anwendungsbasierten MFA."
>
> New York Department of Financial Services, Twitter Investigation Report, Oktober 2020

Vier wichtige Authentifizierungsanforderungen für gemeinsam genutzte Arbeitsplatzgeräte

Sicherheit | Effizienz | Zuverlässigkeit | Kosten

Neben der Effektivität der Lösung beim Schutz vor externen Cyberangriffen und Insider-Bedrohungen sollten Unternehmen auch die Auswirkungen der Lösung auf die Benutzerproduktivität (Kontosperrungen, Anmeldezeiten), die Zuverlässigkeit der Lösung über verschiedene Umgebungen und Anwendungsfälle hinweg, die externen Variablen, die sich negativ auf die Leistung auswirken können (z. B. Mobilfunksignale und Akkus), und die langfristigen Gesamtbetriebskosten berücksichtigen.

Im Folgenden finden Sie vier wichtige Authentifizierungsanforderungen, die Unternehmen für jede Umgebung mit gemeinsam genutzten Arbeitsgeräten berücksichtigen sollten:

Sicherheit

Wie stellen Sie sicher, dass der Benutzer, der sich am Gerät anmeldet, die legitime Person ist?

Wie sichern Sie gemeinsam genutzte Geräte und interne Ressourcen mit mehreren rotierenden Benutzern, um sicherzustellen, dass die Benutzerkonten sicher sind und die Benutzer nur Zugriff auf die Anwendungen, Services und Daten erhalten, auf die sie Zugriff haben sollten?

Admin-Konten oder gemeinsam genutzte Arbeitsplatzgeräte mit Zugriff auf vertrauliche Informationen sollten mit einem Authentifizierungsmechanismus geschützt werden, der gegen Identitätswechsel geschützt ist.

Gemeinsam genutzte Arbeitsplatzgeräte sollten sich in hohem Maße auf Benutzerberechtigungen und Zugriffskontrollen verlassen (keine gemeinsamen, Gast- oder anonymen Anmeldungen) und über Einschränkungen verfügen, die das Speichern von Passwörtern verhindern. Administrator-Konten sollten auch individuell und nicht gemeinsam genutzt werden, um die persönliche oder Remote-Fehlerbehebung zu unterstützen.

> Überlegen Sie, wie viel Zeit für die Authentifizierung angemessen ist und wie oft ein Benutzer sich im Verlauf einer Schicht oder eines Tages authentifizieren muss."

Effizienz

Wie stellen Sie sicher, dass sich der Benutzer schnell und nahtlos authentifizieren kann?

Jeder für gemeinsam genutzte Arbeitsplatzgeräte verwendete Authentifizierungsmechanismus sollte eine schnelle und einfache Authentifizierung für die Mitarbeiter gewährleisten, um Unterbrechungen des Arbeitsablaufs und nicht genehmigte Problemumgehungen zu vermeiden. Derzeit glauben 54 % der Mitarbeiter, dass zweistufige Authentifizierungslösungen wie OTP und Push-Codes ihren täglichen Arbeitsablauf stören.[11] Außerdem kam es bei 34 % der Mitarbeiter schon vor, dass sie nicht auf wichtige arbeitsbezogene Informationen zugreifen konnten, da sie keinen Zugriff auf ein Smartphone oder eine Authentifizierungs-App hatten.[12]

Wie bereits erwähnt, bieten nicht alle Formen der Multi-Faktor-Authentifizierung (MFA) ein optimales Gleichgewicht zwischen starker Sicherheit und einer schnellen und einfachen Benutzererfahrung, die eine hohe Produktivität ermöglicht. Einige mobile Authentifikatoren können die Anzahl der Schritte im Authentifizierungsprozess erhöhen. Dadurch müssen Benutzer auf OTP- oder Push-App-Codes warten oder – im Falle von Pharma-, Gesundheits- und Chemieunternehmen – für den Authentifizierungsprozess ihre persönliche Schutzausrüstung (PSA) ablegen. Überlegen Sie unabhängig vom Szenario, wie viel Zeit für die Authentifizierung angemessen ist und wie oft ein Benutzer sich im Verlauf einer Schicht oder eines Tages authentifizieren muss. Wenn hohe Effizienzanforderungen bestehen, sollten Sie eine passwortlose Authentifizierung in Betracht ziehen.

Zuverlässigkeit

Wie stellen Sie eine konsistente Authentifizierung sicher, die immer funktioniert, selbst in schwierigen Umgebungen mit variierender Verbindungsstärke?

Authentifizierung ist ein unternehmenskritischer Service. Wenn Mitarbeiter nicht in der Lage sind, sich bei den von ihnen verwendeten Apps oder Portalen anzumelden, können sie ihre Arbeit nicht erledigen. Jede Authentifizierungslösung muss für jeden Benutzer zuverlässig funktionieren und nicht von üblichen Fehlerpunkten bei Konnektivität, Geräte-Akku, Mobilfunkempfang oder Hardtoken-Akku abhängen. Authentifizierungslösungen sollten auch Funktionen wie NFC aufweisen, die für Umgebungen wie Labore, industrielle Fertigung, Reinräume und andere Umgebungen ohne Funkenbildung geeignet sind.

Denken Sie daran, dass jede Authentifizierungslösung, die auf „etwas, das man kennt" (z. B. auf einem Passwort) basiert, menschlichem Versagen unterliegt – verloren gegangene, vergessene oder falsch eingegebene Angaben, die die Authentifizierungserfahrung beeinträchtigen. Dadurch werden Benutzer möglicherweise aus ihren Konten ausgeschlossen. In Umgebungen mit gemeinsam genutzten Arbeitsgeräten, in denen die Mobilfunkabdeckung an Orten wie Offshore-Anlagen, Umgebungen für Betriebstechnologie (OT) und abgelegenen geografischen Gebieten lückenhaft oder nicht vorhanden ist oder in denen Benutzer sich bei einer mobilen Authentifizierung auf den Geräteakku verlassen müssen, funktionieren mobile Authentifizierungslösungen nicht immer zuverlässig.

> Das durchschnittliche Unternehmen verliert jährlich aufgrund von Kontosperrungen 5,2 Mio. USD an Produktivität”
>
> Ponemon Institute, Bericht zu Passwort- und Authentifizierungs-sicherheitsverhalten, 2019

Kosten

Wie können Sie die Anzahl der authentifizierungsbezogenen Support-Tickets reduzieren?

Jede Form der Legacy-Authentifizierung, beispielsweise Benutzernamen und Passwörter sowie die mobile Authentifizierung, die massengerecht angewendet und durchgesetzt wird, erfordert eine kontinuierliche Durchsetzung von Richtlinien, Benutzerschulungen und IT-Support. Alle Formen der mobilen Authentifizierung, darunter SMS, OTP und Push-Benachrichtigungen, können eine enorme Belastung für den Support verursachen, wenn Codes verzögert werden, Benutzer aus ihren Konten ausgesperrt sind oder Benutzer neue Geräte registrieren müssen.

Immer wenn ein Benutzer Probleme mit der mobilen Authentifizierung hat, ist er nicht produktiv. Je schneller ein Benutzer sich authentifizieren und seine Aufgaben sicher ausführen oder bei Bedarf sogar sein Passwort selbst zurücksetzen kann, desto höher ist die Rentabilität.

Nachteile der alten MFA

Geringe Sicherheit und Zuverlässigkeit, hohe Kosten und Reibung

Zugangsdaten gehören weiterhin zu den Top-Zielen für Cyberangreifer und sind mit 61 % aller Datenschutzverletzungen verbunden.[13] Der durchschnittliche Mitarbeiter muss 191 Passwörter verwenden und sich diese merken, was zur Komplexität und zur Frustration der Benutzer beiträgt.[14] Für das durchschnittliche Unternehmen hängen derzeit 60 % der IT-Service-Desk-Interaktionen mit dem Zurücksetzen von Passwörtern zusammen.[15] Neben den IT-Kosten verliert das durchschnittliche Unternehmen aufgrund von Kontosperrungen jährlich 5,2 Mio. USD an Produktivität.[16]

Was ist die wahrscheinlichste Folge einer anhaltenden Frustration bei der Authentifizierung? Unsichere Sicherheitsumgehungen – selbst von Benutzern mit dem höchsten Wissensstand. Tatsächlich geben 49 % der IT-Sicherheitsexperten zu, dass sie ihre Passwörter mit anderen teilen.[17] Wir wissen, dass gemeinsam genutzte Arbeitsplatzgeräte mit höheren Raten der Passwortfreigabe, einer Passwortwiederverwendung für verschiedene Konten oder Passwortspeicherungen im Browser oder in der Anwendung einhergehen – diese Praktiken sind niemals sicher, in einem Szenario mit gemeinsam genutzten Arbeitsplatzgeräten verstärken sie die Risiken jedoch erheblich.

Es ist jedoch wichtig zu beachten, dass jede Form der Zwei-Faktor-Authentifizierung (2FA) oder MFA mehr Sicherheit bietet als Passwörter allein, dass beide aber dennoch auf Passwörtern als erstem Faktor basieren. Darüber hinaus ist bei der herkömmlichen MFA, wie beispielsweise der mobilen MFA, der zweite Faktor an das mobile Gerät gebunden. Dies ist ein Warnsignal, das auf drei Aspekte zurückzuführen ist: Es gibt keine echte Garantie dafür, dass der private Schlüssel auf einem sicheren Element auf dem mobilen Gerät landet; der OTP-Code oder private Schlüssel kann auf bestimmte Weise abgefangen werden, und es ist unmöglich, den Besitznachweis zu gewährleisten – oder in den Worten des NIST (National Institute of Standards and Technology): Es ist unmöglich nachzuweisen, dass es gegen Identitätsdiebstahl resistent ist.

> “FIDO2 Hardware-Sicherheitsschlüssel bieten Multi-Faktor- und passwortlose Authentifizierung mit hoher Sicherheit und einer außergewöhnlichen User Experience. Sie bieten außerdem eine tragbare Vertrauensbasis, die sich für gemeinsam genutzte Arbeitsplatzgerätumgebungen hervorragend eignet.”

Die herkömmliche mobile Authentifizierung ist anfällig für moderne Cyberangriffe wie Phishing, Brute-Force-Angriffe, Man-in-the-Middle (MITM)-Angriffe, Malware und SIM-Swapping. Neben diesen Sicherheitsaspekten bringt die herkömmliche mobile Authentifizierung viele versteckte Kosten mit sich, die mit Produktivitätseinbußen, Gerätekosten, erhöhtem IT-Support und Reibung bei der User Experience zusammenhängen. Tatsächlich geben 43 % der Unternehmen an, dass die Benutzererfahrung das größte Hindernis bei der Nutzung der MFA darstellt.[19] Weitere Informationen finden Sie in unserem Whitepaper: The Top 5 Mobile Authentication Misconceptions: Demystifying the myth versus reality of legacy MFA (Die fünf größten Missverständnisse in Bezug auf mobile Authentifizierung: Aufklärung der Mythen hinsichtlich herkömmlicher MFA).

Der erste Schritt bei der Verbesserung der Sicherheitspraktiken ist das Ersetzen der herkömmlichen Single-Factor-Authentifizierung (Benutzername und Passwort) durch eine Phishing-resistente MFA.

Da letztendlich die Aktionen des Benutzers die größte Schwachstelle bei der herkömmlichen Authentifizierung darstellen und die mehrstufige Authentifizierung einen großen Beitrag zur Unzufriedenheit des Benutzers darstellt, entwickelt sich die globale beste Praxis hin zu einer passwortlosen Authentifizierung – d. h. einer Authentifizierung, bei der der Benutzer bei der Anmeldung kein Passwort eingeben muss.

Der Übergang von der herkömmlichen MFA zur Phishing-resistenten MFA ist ein wichtiger Schritt in Richtung einer Sicherung gemeinsam genutzter Arbeitsplatzgerätumgebungen. Und der nächste Schritt für die moderne MFA ist die Einführung der passwortlosen Authentifizierung. Ein OTP per SMS ist eine Form der passwortlosen Authentifizierung, die aber aus Sicherheitsgründen als schwach betrachtet wird. Herkömmliche Smartcards sind eine weitere Form der passwortlosen Authentifizierung, die eine hohe Sicherheit bieten, aber in der Regel hohe Investitionsausgaben für SmartcardLeser, Karten und Backend-Verwaltungsplattformen erfordern. Sie bieten auf modernen Geräten wie Smartphones und Tablets nicht die beste User Experience. Aus diesem Grund geht die Branche über zu einem modernen, passwortlosen Anmeldefluss, der FIDO2/WebAuthn nutzt.

FIDO (Fast Identity Online) ist ein moderner Authentifizierungsstandard, der herkömmliche Benutzernamen und Passwörter durch eine starke Zwei-Faktor-, Multi-Faktor- und passwortlose Authentifizierung ersetzt. Der FIDO-Standard wurde von der FIDO Alliance entwickelt, einem offenen Industrieverband mit dem Ziel, die Abhängigkeit von Passwörtern zu verringern. FIDO2/WebAuthn ist der neueste FIDO-Standard und verwendet Public-Key-Kryptographie für hohe Sicherheit, wobei die privaten Schlüssel niemals den Authentifikator verlassen. FIDO2 Hardware-Sicherheitsschlüssel bieten Multi-Faktor- und passwortlose Authentifizierung mit hoher Sicherheit und einer außergewöhnlichen User Experience. Sie bieten außerdem eine tragbare Vertrauensbasis, die sich für gemeinsam genutzte Arbeitsplatzgerätumgebungen hervorragend eignet.

Sicherung gemeinsam genutzter Arbeitsplatzgeräte mit Phishing-resistenter MFA

Der YubiKey bietet starken Phishing-Schutz, Portabilität und eine außergewöhnliche UX

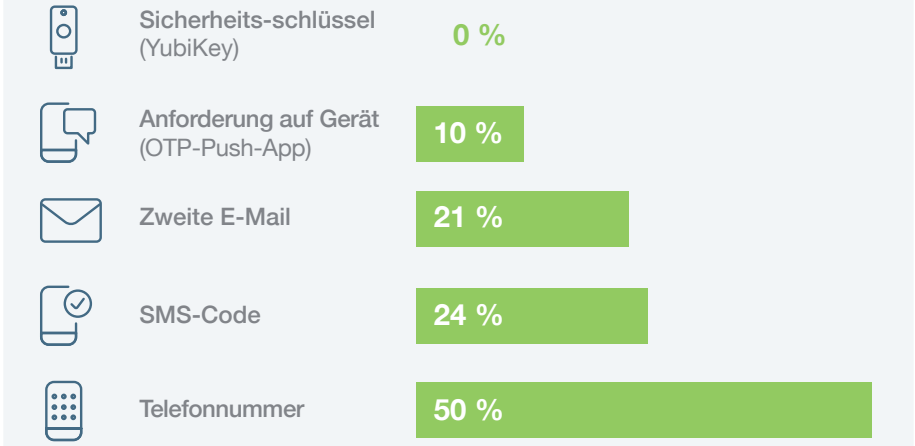
Google: Wie effektiv ist die grundlegende Kontohygiene beim Schutz vor Hijacking

Die YubiKey 5 Serie
Von links nach rechts: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano und YubiKey 5C Nano

Die YubiKey 5 FIPS Serie
Von links nach rechts: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS und YubiKey 5C Nano FIPS

YubiKey Bio Serie – FIDO Edition
Von links nach rechts: YubiKey Bio - FIDO Edition, YubiKey C Bio - FIDO Edition

Prozentuale Wahrscheinlichkeit einer Verhinderung von Kontoübernahmen[18]



Yubico hat den YubiKey entwickelt, einen Hardware-Sicherheitsschlüssel, der Phishing-resistente Sicherheit und eine außergewöhnliche User Experience in einem tragbaren USB- und Nano-Formfaktor bietet. Mit dem YubiKey können sich Benutzer sicher und einfach bei mehr als 700 Anwendungen und Diensten auf einer Vielzahl von Geräten authentifizieren – durch einfaches Antippen oder Berühren.

Der YubiKey bietet eine starke, Phishing-resistente Zwei-Faktor-, Multi-Faktor- und passwortlose Authentifizierung in großem Umfang. Dabei schützt der Hardware-Authentifikator vertrauliche Daten auf einem sicheren Element, das nicht leicht exfiltriert werden kann. Der YubiKey ist die einzige Lösung, die nach unabhängigen Untersuchungen nachweislich 100 % der Kontoübernahmen verhindert.[20]

Der YubiKey verwendet moderne Authentifizierungsprotokolle wie FIDO U2F und offene FIDO2-Authentifizierungsstandards, um Phishing-Angriffe auf Zugangsdaten zu verhindern. YubiKeys unterstützen auch SmartCard-, OTP- und OpenPGP-Protokolle und ermöglichen so die Verwendung eines einzelnen Sicherheitsschlüssels in einer Vielzahl moderner und älterer Systeme. Der vielseitige YubiKey erfordert keine Softwareinstallation, keine Batterie und keine Mobilfunkverbindung. Daher eignet er sich ideal für Umgebungen mit gemeinsam genutzten Arbeitsplatzgeräten und Einschränkungen für Mobilgeräte, einschließlich isolierter Bereiche. Benutzer können von einem reibungslosen Authentifizierungs-Workflow profitieren. Der Benutzer schließt den YubiKey an einen USB-Anschluss an und berührt eine Taste zur Authentifizierung, oder er tippt den YubiKey einfach mit NFC gegen ein Gerät (sehr gut geeignet für Umgebungen ohne Funkenbildung).

YubiKeys bieten auch eine Brücke zur passwortlosen Authentifizierung mit Unterstützung mehrerer Authentifizierungsprotokolle. Um das Benutzererlebnis und die Authentifizierungsgeschwindigkeit weiter zu verbessern, bietet Yubico auch die YubiKey Bio Series – FIDO Edition an. Sie unterstützt FIDO U2F und FIDO2 und bietet die gewohnte Sicherheit aller YubiKeys mit einer neuen biometrischen, passwortlosen Erfahrung.

Anwendungsfälle in der Industrie

Schutz von vertraulichen personenbezogenen und finanziellen Informationen in Callcentern für Privatkunden-Banking

Im Jahr 2019 befragte die Aite Group 25 Führungskräfte bei 18 der 40 größten US-amerikanischen Finanzinstitute und stellte fest, dass 61 % der Betrugsfälle auf das Contact Center zurückgeführt werden können.[21] Bei einer hohen Mitarbeiterfluktuation, saisonalen Spitzen und anderen schwierigen Geschäftsdynamiken benötigen Callcenter-Umgebungen mit gemeinsam genutzten Arbeitsplatzgeräten einen sicheren, aber einfachen Ansatz, um die Identität von Mitarbeitern zu überprüfen, bevor sie Zugriff auf kritische Systeme und personenbezogene Daten erhalten.

Callcenter von Finanzdienstleistern können YubiKeys implementieren, um eine höhere Sicherheit zu gewährleisten, die die Identität von Callcenter-Mitarbeitern sicher überprüfen kann, bevor sie Zugriff auf personenbezogene Daten und andere sensible Daten erhalten oder Änderungen an einem Kundenkonto vornehmen, z. B. eine Erhöhung des Kreditrahmens. In der Praxis hat der YubiKey niedrige Gesamtbetriebskosten in Callcenter-Umgebungen umgesetzt, sodass keine häufigen Passwortaktualisierungen mehr erforderlich sind, Kontosperrungen und kostspieliger IT-Support vermieden werden und die Mitarbeiterproduktivität optimiert wird. Weitere Informationen finden Sie im Whitepaper: Essentials for enabling strong authentication in financial services call centers (Grundlagen für eine starke Authentifizierung in Callcentern von Finanzdienstleistern).

> “Anstatt YubiKey als dringend empfohlene Lösung für unsere Kunden darzustellen, sind wir auf dem Weg, den YubiKey zu einer Pflichtlösung zu machen. Wir bauen die Lösung in unsere Hosting-Suite und in unsere Benutzergebühren ein.”
>
> **Kontrollsysteme für den Einzelhandel**

Sichere Arbeitsplatzgeräte für Pflegepersonal und Tap-and-Go-Geräte in Krankenhäusern

Unternehmen im Gesundheitswesen sind weiterhin das wichtigste Ziel für Datendiebstahl. Dies erschwert die Sicherung des Point-of-Care-Zugriffs auf gemeinsam genutzte Arbeitsplatzgeräte und Tap-and-Go-Geräte, die für Rundgänge verwendet werden.

Die meisten Krankenhäuser verfügen über Ausweiskartenlösungen für den Zugriff auf gemeinsam genutzte Arbeitsplatzgeräte. Allerdings setzen diese Systeme in Fällen, in denen ein erhöhter Zugriff erforderlich ist (für den Administratorzugriff oder für die elektronische Rezeptausstellung für kontrollierte Substanzen), weiterhin auf eine zweistufige Authentifizierung mit Passwörtern, mobiler Authentifizierung oder biometrischen Daten. In diesen Szenarien können YubiKeys mit einem FIDO2-basierten kennwortlosen Erlebnis eine Step-up-Authentifizierung mit Antippen/Berührung und einer PIN bereitstellen, die lokal auf dem Schlüssel gespeichert und verifiziert wird, ohne dass zusätzliche Hardwaretreiber erforderlich wären, wie sie mit Smartcards benötigt würden.

Weitere Informationen zur Verwendung des YubiKeys für die Phishing-resistente MFA im Gesundheitswesen finden Sie im Whitepaper: Best Practices für eine starke Authentifizierung im Gesundheitswesen mit dem YubiKey.

Sicherheit von POS im Einzelhandel

Retail Control Systems (RCS) vermarkten und unterstützen Geschäftsmanagement- und POS-Systeme (Point-of-Sale) für Einzelhändler und Gaststätten. Unter den zunehmend strengeren PCI-Compliance-Anforderungen (Payment Card Industry) suchte RCS nach einer Lösung, die intern von RCS verwendet werden konnte, um den Remote-Admin-Zugriff auf Systeme zu sichern, aber auch extern, um den Zugriff auf sensible Daten zu schützen.

RCS authentifiziert heute in einem typischen 48-Stunden-Zeitraum mehr als 11.000 Benutzer-Anmeldungen mit YubiKeys. Dies hilft beim Schutz von Geräten sowie bestimmten Benutzern und gemeinsam genutzten Benutzerprofilen.

Zusammenfassung

Der YubiKey ist eine äußerst robuste und zuverlässige Lösung (IP68-zertifiziert) mit hoher Sicherheit und außergewöhnlicher UX, die zeitaufwändige und unsichere Zweitfaktoren durch ein konsistentes Tap-and-Go-Erlebnis ersetzt, das nicht nur die Benutzererfahrung unterstützt, sondern auch die IT-Supportkosten senkt.

Um eine hohe Sicherheit für Ihre gemeinsam genutzten Arbeitsplatzgeräte zu gewährleisten, wurde der YubiKey speziell für die Anforderungen von Unternehmen und Benutzern entwickelt und bietet eine hohe Phishing-Resistenz. Er bietet moderne MFA-Funktionen und hilft Ihnen sogar dabei, Passwörter komplett abzuschaffen – so erreichen sie ein besseres Benutzererlebnis und eine höhere Gesamteffizienz. Bleiben Sie der sich ständig weiterentwickelnden Bedrohungslandschaft einen Schritt voraus – mit erstklassiger Sicherheit, die Sie nicht nur jetzt, sondern auch in Zukunft auf Erfolgskurs bringt.

Der YubiKey bietet eine moderne, Phishing-resistente MFA und ermöglicht den Übergang zu passwortloser MFA für ein besseres Benutzererlebnis und eine höhere Gesamteffizienz.

	Benutzername und Passwort	Auf Mobilgeräten basierende Authentifikatoren	YubiKey
Sicherheit	Niedrig, leicht zu hacken	Mittel, 10-15 % Kontoüber-nahmeraten[22]	Hoch, 0 % Kontoüber-nahmerate[23]
Effizienz	Passwortermüdung, Kontosperrungen	Benutzer, die die mobile MFA nicht nutzen können oder wollen	Einfach antippen und los geht‘s. 4-mal schnellere Anmeldung als OTPP[24]
Zuver-lässigkeit	Anfällig für menschliches Versagen	Von der Geräte-batterie und dem Mobilfunknetz abhängig. Nicht geeignet für Umgebungen mit Einschränkungen für Mobilgeräte	Robuste Ausführung, erfordert keine Mobilfunk-verbindung
Kosten	Keine Investitionskosten. Hohe IT-Supportkosten Hohes potenzielles Risiko	1.840 USD sind die wahren Kosten für Enterprise Mobility pro eigenem Gerät[25]	Niedrige Kosten im Vergleich zur mobilen MFA und 92 %-ige Reduzierung der Support-Tickets[26]

Quellen

[1] IBM, 2021 Cost of Data Breach Report (Bericht zu den Kosten von Datenverstößen, 2021) (aufgerufen am 14. September 2021),

[2] IBM, 2021 Cost of Data Breach Report (Bericht zu den Kosten von Datenverstößen 2021) (aufgerufen am 14. September 2021), https://www.ibm.com/security/data-breach; Verizon, 2021 Data Breach Investigations Report (Bericht zu Untersuchungen von Datenverstößen 2021) (aufgerufen am 18. Mai 2021)

[3] Verizon, 2021 Data Breach Investigations Report (Bericht zu Untersuchungen von Datenverstößen 2021) (aufgerufen am 18. Mai 2021),

[4] IBM, Cost of Insider Threats: Global Report 2020 (Kosten von Insider-Bedrohungen, Globaler Bericht 2020), (aufgerufen am 12. November 2021)

[5] Keeper, 4 Rules for Safe Password Sharing in the Workplace (4 Regeln zum sicheren Teilen von Passwörtern am Arbeitsplatz) (April 2021)

[6] IBM, 2021 Cost of Data Breach Report (Bericht zu den Kosten von Datenverstößen 2021) (aufgerufen am 14. September 2021)

[7] Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report (Bericht zur Situation in Bezug auf Passwort- und Authentifizierungssicherheitsverhalten 2020) (Februar 2020)

[8] Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report (Bericht zur Situation in Bezug auf Passwort- und Authentifizierungssicherheitsverhalten, 2020) (Februar 2020), Ayal Hassidim, MD et. al., Prevalence of Sharing Access Credentials in Electronic Medical Records (Häufigkeitsrate des Teilens von Zugangsdaten in elektronischen medizinischen Aufzeichnungen), Healthcare Informatics Research, (Juli 2017)

[9] Simon Constable, How Hot Desking Will Kill Your Company (Wie Hot Desking Ihr Unternehmen umbringt) (20. Juni 2019); Jessica Dickler, Post-pandemic, the office will now have a whole new look (Nach der Pandemie wird das Büro ganz anders aussehen) (12. Juli 2021)

[10] Juniper Research, POS & mPOS Terminals: Market Summary & Key Takeaways (POS & mPOS Terminals: Marktübersicht & Wichtigste Schlussfolgerungen) (aufgerufen am 10. November 2021); Charlie Osborne, PayPal, Square vulnerabilities impact mobile point-of-sale machines (Schwachstellen bei PayPal und Square beeinflussen mobile Point-of-Sale-Geräte) (10. August 2018)

[11] Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report (Bericht zur Situation in Bezug auf Passwort- und Authentifizierungssicherheitsverhalten, 2020) (Februar 2020), Ayal Hassidim, MD et. al., Prevalence of Sharing Access Credentials in Electronic Medical Records (Häufigkeitsrate des Teilens von Zugangsdaten in elektronischen medizinischen Aufzeichnungen), Healthcare Informatics Research, (Juli 2017)

[12] Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report (Bericht zur Situation in Bezug auf Passwort- und Authentifizierungssicherheitsverhalten, 2020) (Februar 2020), Ayal Hassidim, MD et. al., Prevalence of Sharing Access Credentials in Electronic Medical Records (Häufigkeitsrate des Teilens von Zugangsdaten in elektronischen medizinischen Aufzeichnungen), Healthcare Informatics Research, (Juli 2017)

[13] Verizon, 2021 Data Breach Investigations Report (Bericht zu Untersuchungen von Datenverstößen 2021) (aufgerufen am 18. Mai 2021)

[14] Amber Steel, LastPass Reveals 8 Truths about Passwords in the New Password Exposé (LastPass deckt in neuem Passwort-Exposé 8 Wahrheiten zu Passwörtern auf) (1. November 2017)

[15] Gartner, 3 Simple Ways IT Service Desks Should Handle Incidents and Requests (Auf diese 3 Weisen sollten IT-Service-Desks mit Vorfällen und Anfragen umgehen) (Aug. 2019)

[16] Ponemon Institute, 2019 State of Password and Authentication Security Behaviors Report (Bericht zur Situation in Bezug auf Passwort- und Authentifizierungssicherheitsverhalten, 2019) (aufgerufen am 14. September 2021)

[17] Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report (Bericht zur Situation in Bezug auf Passwort- und Authentifizierungssicherheitsverhalten, 2020) (Februar 2020), Ayal Hassidim, MD et. al., Prevalence of Sharing Access Credentials in Electronic Medical Records (Häufigkeitsrate des Teilens von Zugangsdaten in elektronischen medizinischen Aufzeichnungen), Healthcare Informatics Research, (Juli 2017)

[18] 451 Research, 2021 Yubico und 451 Research Study (April 2021)

[19] Kurt Thomas und Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking (Neue Studie: wie effektiv ist die grundlegende Kontohygiene beim Schutz vor Hijacking) (17. Mai 2019)

[20] Aite Group für PinDrop, 61% of Fraud Traced Back to the Contact Center (61 % der Betrugsfälle gehen auf das Contact Center zurück) (aufgerufen am 15. November 2021)

[21] https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[22] Ibid.

[23] Ibid.

[24] Wander: Uncovering the true costs of enterprise mobility (Die wahren Kosten der Enterprise Mobility)

[25] https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

yubico

Über Yubico

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

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

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