

LEITFADEN FÜR BEST PRACTICES

Erste Schritte mit der Phishing-resistenten MFA zum Schutz des Finanzdienstleistungssektors

Sechs Best Practices für die Bereitstellung, um die
Einführung in großem Maßstab zu beschleunigen



5,56 Mio. USD



Durchschnittliche Kosten durch
Datenschutzverletzungen bei
Finanzdienstleistungen¹

82 %



aller Cyberbedrohungen gehen auf
gestohlene Zugangsdaten zurück²

Der Fachpublikation (SP) 800-64 des National Institute of Standards and Technology (NIST) zufolge erfüllen derzeit nur zwei Authentifizierungsmethoden die Kriterien für Phishing-resistente MFA: **PIV/Smart Card und der moderne FIDO2/WebAuthn-Authentifizierungsstandard.**

Auswahl des richtigen MFA-Ansatzes für Finanzdienstleistungen

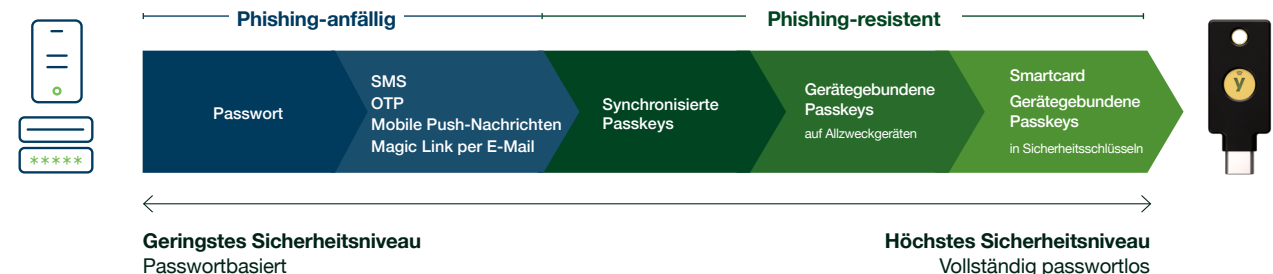
Finanzunternehmen stehen zunehmend unter Druck, ihre Authentifizierung angesichts der Cyberbedrohungen zu verbessern, da diese nicht nur hohe Kosten (im Schnitt 5,56 Mio. USD aufgrund von Datenschutzverletzungen¹) verursachen und das Vertrauen von Verbrauchern schwächen, sondern auch zum größten Teil (82 %) auf gestohlene Zugangsdaten zurückgehen. Es ist daher sinnvoll, dass Finanzunternehmen die Cybersicherheit durch Multi-Faktor-Authentifizierung (MFA) verbessern und Aufsichtsbehörden und Cyber-Versicherer den Einsatz von MFA verlangen.

Die Federal Trade Commission hat 2021 die sogenannte „Safeguards Rule“ (16 CFR 314)³ des Gramm-Leach-Bliley Act (GLBA) aktualisiert, in der MFA für Mitarbeiter, Dritte und Kunden als Sicherheitsmaßnahme vorgeschrieben wird. Mithilfe dieser Regel wurden die US-Finanzvorschriften an die EU-Vorschriften zur Multi-Faktor-Authentifizierung gemäß der Zweiten Zahlungsdiensterichtlinie PSD2 (Payment Services Directive2) der EU und der eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste (Electronic Identification, Authentication and Trust Services) angeglichen.⁴ 2022 erklärte das Consumer Financial Protection Bureau (CFPB) offiziell, dass eine fehlende MFA Haftungsansprüche gemäß CFPB-Vorschriften und dem Dodd-Frank Act bedingen könne, selbst wenn keine Datenschutzverletzung vorliegt.⁵ All dies spricht für die Notwendigkeit einer Multi-Faktor-Authentifizierung und ihre wichtige Rolle bei der Abkehr von unsicheren Passwörtern. Allerdings wird nicht deutlich, welche Form der Multi-Faktor-Authentifizierung die richtige ist.

Heute beginnt das Regulierungsumfeld zu erkennen, dass **nicht alle Formen der Multi-Faktor-Authentifizierung (MFA) gleichwertig sind.** Die meisten grundlegenden Authentifizierungsmethoden wie SMS, Authentifizierung per Mobilgerät und Einmalpasswörter sind anfällig für Kontoübernahmen durch Phishing, Social Engineering und MITM-Angriffe (Man in the middle). Deswegen wurde mit der überarbeiteten Version des Payment Card Industry Data Security Standard (PCI DSS v4.0) der Finanzstandard eingeführt, der für sämtliche Zugriffe auf die Karteninhaberdatenumgebung eine **Phishing-resistente MFA** vorsieht.⁶

Was ist Phishing-resistente MFA?

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



Der YubiKey gewährleistet die Sicherheit von 8 der 10 weltweit größten Banken



YubiKey bietet eine Phishing-resistente MFA

Der YubiKey enthält die Passkeys mit höchster Sicherheitsstufe und ermöglicht eine Phishing-resistente Multi-Faktor- und passwortlose Authentifizierung. Diese Passkeys sind im Vergleich zu anderen Passkeys immun gegen Angriffe, ermöglichen eine äußerst mobile und benutzerfreundliche Authentifizierung, werden sicher generiert und sind in einem Hardware-Formfaktor gespeichert. YubiKeys unterstützen mehrere Protokolle auf einem einzigen Schlüssel, lassen sich sowohl nahtlos in verwaltete als auch moderne Umgebungen integrieren und erleichtern Finanzunternehmen den **Übergang in eine passwortlose Zukunft**. YubiKeys sind mit [Hundertern von Produkten, Diensten und Anwendungen](#) kompatibel, darunter führende Plattformen für Identitäts- und Zugriffsverwaltung (IAM), Lösungen für die privilegierte Zugriffsverwaltung (PAM) sowie Hunderte von Cloud-Diensten.

Hardware-Sicherheitsschlüssel wie der YubiKey sind eine ideale Lösung für eine starke, Phishing-resistente MFA, da sie weder eine externe Stromversorgung noch Batterien oder eine Netzwerkverbindung benötigen – ein Benutzer kann mit einem einzigen Schlüssel Hunderte von Anwendungen und Diensten sichern, wobei die Zugangsdaten niemals zwischen den Diensten weitergegeben werden. Der YubiKey reduziert erwiesenermaßen [das Risiko um 99,9 %](#) und bietet gleichzeitig ein großartiges Benutzererlebnis, bei dem sich Benutzer mit nur einem Tastendruck oder einer Berührung sicher anmelden können:



Höchste Sicherheit

Risikominderung
um 99,9 %



Hohe Rendite

Erreichen eines
ROI von 203 %



Mehr Wert

Reduzierung der Support-
Tickets um 75 %



Schneller

Verringern der
Authentifizierungszeit um
mehr als das Vierfache

Wie sieht es mit Passkeys aus?

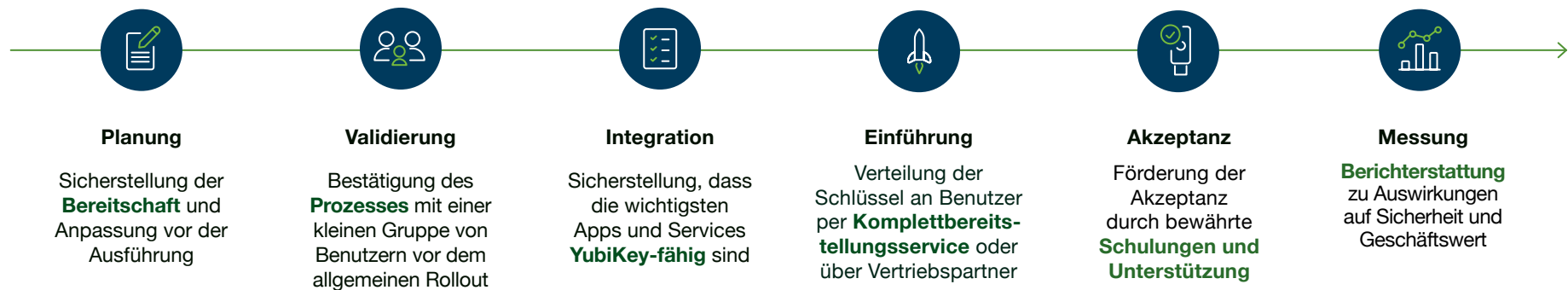
Passkeys sind ein neuer Begriff in der Branche, aber das Konzept ist nicht neu. Bei Passkeys handelt es sich einfach um FIDO-Zugangsdaten ohne Passwort, die die Abkehr von Passwörtern ermöglichen und Schutz vor Phishing bieten. Es gibt verschiedene Passkey-Implementierungen:

- **Synchronisierte Passkeys** werden auf einem Smartphone, Tablet oder Laptop gespeichert und können zwischen den Geräten kopiert werden. Während synchronisierte Passkeys die Kontowiederherstellung im Falle eines verlorenen oder gestohlenen Telefons oder Laptops erleichtern, sind FIDO-Zugangsdaten schwieriger nachzuverfolgen und eignen sich daher für Szenarien mit geringerer Sicherheitsgewährleistung.
- **Hardware-gebundene Passkeys** existieren ausschließlich auf einem speziell für Sicherheitszwecke entwickelten Hardware-Schlüssel, z. B. einem YubiKey, der für höchste Anforderungen an die Authentifizierungssicherheit und die Einhaltung von Vorschriften geeignet ist.

Angesichts der aktuellen Bedrohungslage wird die Notwendigkeit einer modernen, gegen Phishing resistenten MFA von Tag zu Tag deutlicher. **Aber wie beginnen Sie den Weg?**

Sechs wichtige Best Practices zur beschleunigten Einführung einer Phishing-resistenten MFA

Der Einstieg ist ganz einfach. Aufgrund der Erfahrungen, die Yubico bei der Unterstützung von Hunderten von Kunden – darunter 4 der 10 führenden US-Banken – bei der Einführung Phishing-resistenter MFA gesammelt hat, haben wir einen sechsstufigen Bereitstellungsprozess entwickelt, um die Einführung Phishing-resistenter MFA in großem Maßstab zu planen und zu beschleunigen.



01. Planung

Klärung der Anwendungsfälle und Gewährleisten der Bereitschaft

Ein stufenweiser Ansatz ist die beste Möglichkeit, eine reibungslose Bereitstellung zu gewährleisten. Setzen Sie Ihre **wertvollsten Benutzer und Daten an erste Stelle** und arbeiten Sie sich dann weiter vor. Ordnen Sie Anwendungsfälle und Benutzergruppen nach Risiko, Standort der Belegschaft, geschäftlichen Auswirkungen und einfacher technischer Integration.



Anwendungsfälle ermitteln

Es gibt viele Anwendungsfälle für Finanzdienstleistungen, bei denen eine Phishing-resistente MFA unerlässlich ist. Priorisieren Sie zunächst Anwendungsfälle und Benutzerpopulationen jeweils nach Risiko und geschäftlicher Auswirkung, bevor Sie weitere Anwendungsfälle und Gruppen abarbeiten. Einige Unternehmen führen Phishing-resistente MFA wegen Sicherheitsbedenken oder Compliance-Vorschriften zuerst für Benutzergruppen ein, andere Unternehmen wiederum entscheiden sich für die Bereitstellung einer Phishing-resistenten MFA an Endkunden-Gruppen (gewerbliche und/oder Privatkunden) über Online- und Mobile-Banking.

Hauptszenarien für eine moderne, Phishing-resistente Authentifizierung



Privilegierter Zugriff

Schützen Sie vertrauliche Daten und ausgewählte Mitarbeiter, die erhöhte Zugriffsrechte auf Systeme oder Daten haben.



Gemeinsam genutzte Arbeitsplatzgeräte

Ermöglichen Sie sicheren und effizienten Zugriff auf gemeinsam genutzte Computer in Banken und Callcentern, einschließlich Bereichen mit Einschränkungen für Mobilgeräte.



Remote-Arbeit

Fügen Sie eine zusätzliche Schutzebene hinzu, die sicheren Zugriff auf VPN-, IAP-, IAM- und IdP-Plattformen ermöglicht.



Transaktionen mit hohem Risiko

Ermöglichen Sie eine zusätzliche Authentifizierungsstufe, um Benutzer bei risikoreichen Services oder Transaktionen mit hohem Wert erneut zu verifizieren.



Software-Lieferkette

Schützen Sie den Zugriff auf Code und implementieren Sie vertrauenswürdige Code-Signaturen.



Benutzergruppen



Büroangestellte

Ausgeklügelte Angriffe und laterale Eskalationswege machen aus jedem Benutzer einen privilegierten Benutzer.



Callcenter

Verifizieren Sie die Identität von Callcenter-Mitarbeitern, bevor Sie Zugriff auf zentrale Systeme und gemeinsam genutzte Arbeitsplatzgeräte in Umgebungen mit Einschränkungen für Mobilgeräte gewähren.



Privatkunden- Finanzdienstleistungen (Retail Finance)

Unterstützen Sie die nahtlose Authentifizierung zwischen Arbeitsplatzgeräten, um Kunden zu bedienen oder Transaktionen zu autorisieren.



Drittanbieter

Ermöglichen Sie eine zusätzliche Authentifizierungsstufe, um Benutzer bei risikoreichen Services oder Transaktionen mit hohem Wert erneut zu verifizieren.



Endkunden

Schützen Sie Kundenkonten vor Betrug und stärken Sie die Treue und das Vertrauen Ihrer Kunden durch die Bereitstellung in wichtigen Kundensegmenten.

Zusammenführung wichtiger Stakeholder

Zwar kann die Anzahl der für das Projekt erforderlichen Ressourcen je nach Umfang und Reichweite der YubiKey-Bereitstellung variieren, doch können wichtige Entscheidungsträger in den folgenden Abteilungen die unternehmensweite Bereitstellung einer Phishing-resistenten MFA positiv beeinflussen. Für eine reibungslose Einführung ist es wichtig, dass alle Teams mitziehen:



Ggf. Einbeziehung der Experten von Yubico

Yubico unterstützt bereits seit Jahren einige der sicherheitsbewusstesten Unternehmen weltweit und nutzt diese Erfahrung, um flexibel und kostengünstig Sicherheitsprodukte und -services bereitzustellen, die für mehr Sicherheit und Produktivität in Unternehmen sorgen.

Unternehmen können in hohem Maße von einem „YubiKeys as a Service“-Modell profitieren, und unser Professional-Services-Team bietet erstklassige technische und operative Unterstützung bei der Implementierung und beim Rollout Ihrer YubiKey-Lösung.



YubiKey as a Service*		Yubico Professional Services	
 Enrollment services	 Delivery services	 Deployment 360	 Bereitstellungsplanung
Vereinfacht die Beschaffung, Aktualisierung und Unterstützung von YubiKeys durch Unternehmen	Globale Verteilung an Remote- und Bürostandorte	Schlüsselfertige Planung, technische Integration und Bereitstellungsunterstützung	Schneller Einstieg in die Einführung mit Workshops und Projekten , um Anwendungsfälle zu prüfen und eine maßgeschneiderte Strategie zu entwickeln

* YubiKey as a Service ist für Unternehmen mit 500 oder mehr Benutzern verfügbar.



02. Validierung

Bestätigung des Prozesses mit einer kleinen Gruppe von Benutzern

Validieren Sie den Prozess mit einer kleinen Gruppe von Benutzern anhand eines prioritären Anwendungsfalls, um Bestätigung und Feedback zu erhalten, und nutzen Sie dabei die Best-Practice-Leitfäden, Videos und Inhalte von Yubico. **Üben, lernen und fahren Sie dann mit der Erweiterung fort.**



Arbeiten mit YubiKey

YubiKeys sind branchenweit die Nr. 1 und funktionieren bei Hunderten von Produkten, Services und Anwendungen. Informationen zur YubiKey-Kompatibilität finden Sie yubi.co/wwwyk.



03. Integration

Sicherstellen, dass Ihre Umgebung YubiKey-fähig ist

YubiKeys eignen sich für beliebig viele professionelle und Privatdienstleistungen ohne gemeinsame Geheimnisse zwischen den Dienstleistungen und ermöglicht so hohe Sicherheit und Datenschutz in großem Umfang. Ein einziger Schlüssel kann für über 1000 Anwendungen und Services verwendet werden, um die Arbeit und das persönliche digitale Leben Ihrer Benutzer zu schützen. Um sicherzustellen, dass die YubiKeys nahtlos in die wichtigsten Anwendungen und Services integriert werden, die Sie sichern möchten, sollten Sie im Folgenden **einige wichtige Fragen** beantworten. Als bewährte Best Practice sollten Sie zunächst diese Fragen für Ihr Pilotprogramm beantworten und sie dann für jede erweiterte Umsetzung wiederholen.



Wer

Wer benötigt Zugriff?

Mitarbeiter,
Auftragnehmer,
Dritte, Lieferkette



Was

Welchen Authentifizierungsansatz werden Sie wählen?

MFA (Passwort und starke zweite Authentifizierungsstufe), passwortlos



Wo

Wo in Ihrer Umgebung benötigen Sie eine starke Authentifizierung?

Wichtige Infrastrukturelemente, Netzwerk, Anwendungen, Entwicklertools.

Wie verwalten Sie den Zugriff?

IAM, IdP, PAM, SSO, VPN



Wie

Wie wirkt sich der Standort auf die Bereitstellung aus?

Remote, Hybrid, On-Premise, mehrere Standorte

Welche Gerätetypen müssen unterstützt werden?

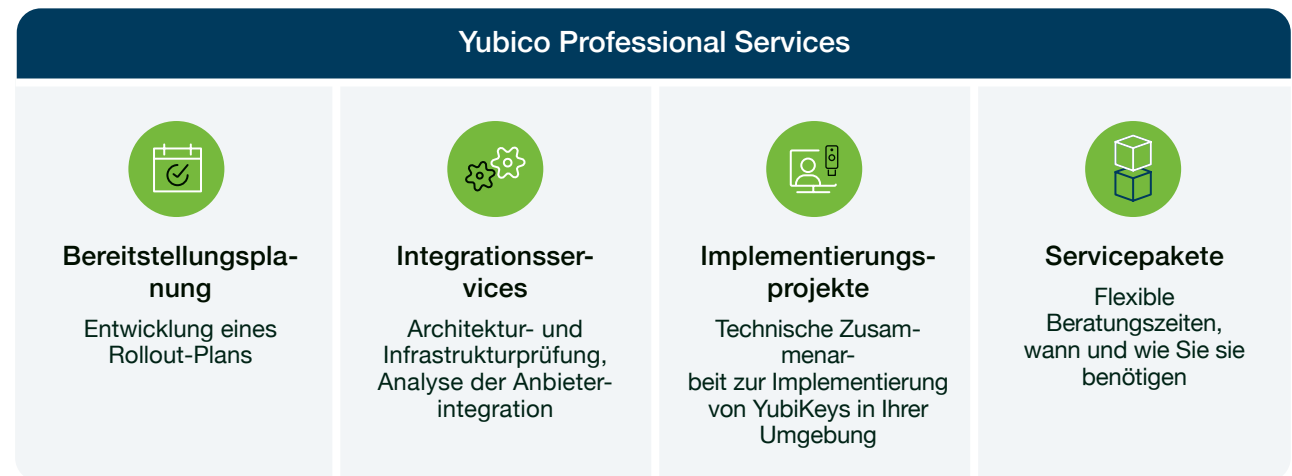
Unternehmenseigene Geräte, private Geräte (BYOD), Desktop, Laptop, Smartphone

“ Da jeder Benutzer einen YubiKey besitzt, muss ich mich nicht um die Gefahr der Weitergabe von Zugangsdaten kümmern. Das ist als CISO eine sehr, sehr gute Ausgangslage.“

Mike Schwermin | CISO | Afni

Vorbereitung auf die Bereitstellung

Nachdem Sie sichergestellt haben, dass Ihre Umgebung YubiKey-fähig ist, ist es an der Zeit, einen Plan für die Bereitstellung von YubiKeys im gesamten Unternehmen zu erstellen. Die Optimierung der Bereitstellung erfordert organisatorisches Änderungsmanagement durch effektive Kommunikation, Schulung und Unterstützung. Yubico bietet eine Vielzahl von Professional Services an, die Sie bei einer schnellen Bereitstellung unterstützen:



Was?

Sensibilisierung

Bauen Sie Materialien für Benutzerschulungen und Support auf.



Warum?

Stärkere Interaktion

Zeigen Sie den Mehrwert für das Unternehmen und die Benutzer.



04. Einführung

Erhalt der Schlüssel und Planung von Go-Live-Events

Wir möchten, dass Ihre Bereitstellung für alle Teams und Benutzer so reibungslos wie möglich verläuft. Dies umfasst die Vereinfachung von Bereitstellungsplänen, die Ihnen bei der Beantwortung wichtiger Fragen zur Verteilung von Schlüsseln an Benutzer und zur Verwaltung des YubiKey-Lebenszyklus helfen:



“ Wir nehmen den gleichen Weg wie die weltweit führenden Organisationen. Und wir führen gerade alle YubiKeys ein.“

Mike Schwermin | CISO | Afni

Best Practices für den YubiKey-Rollout

Sobald Ihre Benutzer über ihre YubiKeys verfügen, müssen Sie im nächsten Schritt die Schlüssel bei den Anwendungen und Geräten registrieren, die sie verwenden werden. Es wird empfohlen, jedem Benutzer einen zweiten YubiKey als Backup bereitzustellen. Wenn Benutzer ihren YubiKey nicht finden können, wird das Entziehen und Ersetzen von Schlüsseln als nächster Schritt empfohlen. Wenn ein Benutzer das Unternehmen verlässt, fordern einige Organisationen YubiKeys vor dem Ausscheiden zurück, während andere es vorziehen, den ausscheidenden Benutzern zu erlauben, ihre YubiKeys zu behalten und sie weiterhin für ihre eigenen persönlichen Konten zu verwenden.



Flexibilität und Auswahl im YubiKey-Formfaktor



Zwei YubiKeys pro Person als Backup



Zukunftssicher mit **zusätzlichen Schlüsseln** als Ersatz für verlorene/ gestohlene Schlüssel



Fördern Sie die **Sicherheit** durch Richtlinien zur persönlichen Nutzung.



Planen Sie ein Event, um die Zukunft der Sicherheit Ihres Unternehmens spannend zu gestalten.

Go-Live-events

Unterstützen Sie die Einführung mit einer Reihe von Kick-off-Mitteilungen, die Benutzern den YubiKey vorstellen – kommunizieren Sie frühzeitig und häufig. Die ideale Go-Live-Kommunikation sorgt dafür, dass Benutzer von den modernen Funktionen des YubiKey begeistert sind.



Wie?

Schulung der Benutzer

Formulieren Sie klare Handlungsaufforderungen für den Einstieg und den Erhalt von Hilfe.



05. Akzeptanz

Unterstützung der Akzeptanz und Steigerung der Interaktion

Wir bei Yubico glauben, dass der Erfolg nicht daran gemessen werden sollte, wie viele YubiKeys Sie haben, sondern daran, wie viele Schlüssel verwendet werden.

Während durch die Go-Live-Kommunikation die Benutzer erfahren, **was YubiKeys sind** und **warum sie wichtig sind**, müssen die Support-Teams darauf vorbereitet sein, das **Wie** zu erklären und FAQs zur Verfügung stellen, die bei allen Fragen rund um das Onboarding und die Fehlerbehebung helfen (z. B. was im Falle eines verlorenen Schlüssels zu tun ist).

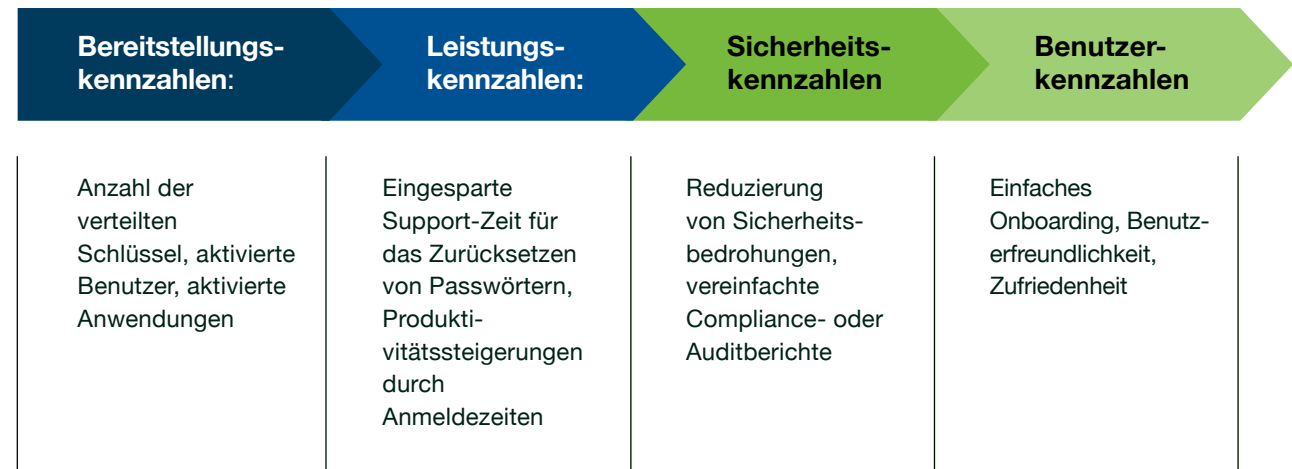
In dieser Phase ist eine effektive Aufklärung und Sensibilisierung wichtig, um Ihrer Benutzer-Community zu zeigen, warum das Unternehmen in den YubiKey investiert hat und welche direkten Vorteile sich dadurch für die Benutzer ergeben. Die einfache Bedienung des YubiKey erfordert nur minimale Schulung und laufende Unterstützung für die Benutzer.



06. Messung

Berichterstattung zu Auswirkungen auf Sicherheit und Geschäft

Wir wissen: **die Wahrheit liegt in den Zahlen.** Validieren Sie das Pilotprojekt anhand dieser Kennzahlen, weiten Sie es dann auf andere Benutzer aus, um die Gesamtwirkung auf das Geschäft zu erhöhen.





Professional Services Deployment 360 Program

Introducing Yubico's Deployment 360 program which packages up all of the essential elements needed in getting your organization jump started on deploying YubiKeys. The Deployment 360 program is a turnkey, start-to-finish consulting package designed to ensure your successful YubiKey deployment. Using the expertise of Yubico Professional Services to assist with both the operational and technical pieces of your deployment, it will help ensure that you start and complete your deployment quickly and on time.

Yubico is leading the charge toward a more secure and frictionless authentication future. Our Professional Services team is composed of trained and accredited security professionals with experience gained from hundreds of customer implementations across a wide range of industries and the government sector.



Plan
Our Professional Services experts will guide you through workshops and projects to ensure your technical, logistical and operational deployment readiness.



Distribute
Let our Deployment Advisors help you create the optimal YubiKey distribution plan for your users, and prepare for the lifecycle management of your YubiKeys.

Laden Sie die Lösungsbeschreibung für Professional Services herunter:
yubi.co/ps

“ Cloud-Abonnements sind für mich nichts Neues und YubiKey as a Service bietet einige hilfreiche Vorteile, die für unsere Anforderungen einfach genau richtig sind.“

Mike Schwermin | CISO | Afni

Bereit für Skalierung

Yubico bietet fachkundige Beratungsservices an, darunter betriebliche und technische Workshops, Implementierungsprojekte, On-Demand-Ressourcen und kundenspezifische Interaktionen, um Ihre YubiKey-Bereitstellung in großem Maßstab zu beschleunigen.

YubiKey as a Service*		Yubico Professional Services		
YubiKey as a Service	Delivery services	Einführungsplanung	Schulung und Support	Analysen und Berichterstellung
Kostengünstiger und flexibler Erwerb von YubiKeys	Globale Verteilung an Remote- und Bürostandorte	Erstellen Sie einen Marketing- und Kommunikationsplan , der auf Ihre Benutzer zugeschnitten ist	Best Practices für Schulungs- und Unterstützungsmaterialien und -prozesse	Individuelle Kennzahlen und Dashboard-Design

* YubiKey as a Service ist für Unternehmen mit 500 oder mehr Benutzern verfügbar.



YubiKey as a Service

Profitieren Sie von führender, Phishing-resistenter Authentifizierungssicherheit für weniger als den Preis einer Tasse Kaffee pro Benutzer und Monat. YubiKeys as a Service ist ein abonnierbarer Dienst, der in einer unsicheren Welt für Zuversicht sorgt.

MEHR DAZU HIER →



Delivery

YubiEnterprise Delivery bietet Ihren IT-Teams leistungsstarke administrative Funktionen zur Bereitstellung von Hardware-Sicherheitsschlüsseln für Nutzer weltweit und beschleunigt die Einführung einer starken Authentifizierung.

MEHR DAZU HIER →

Yubico Professional Services



Deployment 360

Servicezeiten-Pakete



Workshops

Implementierungsprojekte



Sind Sie bereit?

Es besteht kein Zweifel daran, dass Phishing-resistente MFA die Lösung ist, um Finanzdienstleister vor modernen Cyberbedrohungen zu schützen. Auch wenn der Weg hin zu einer Phishing-resistenten MFA und einer passwortlosen Zukunft abschreckend erscheinen mag, muss er dies nicht sein.

Sie wissen nicht, wo Sie anfangen sollen? Die gute Nachricht ist, dass Sie nicht im Voraus schon wissen müssen, wie viele und welche Art von Schlüsseln Sie kaufen müssen, wie Sie diese in Ihre Umgebungen integrieren und wie Sie diese an die Endbenutzer verteilen.

Moderne Unternehmen haben erkannt, dass Security as a Service das Rätselraten um den Erfolg überflüssig machen kann. Wenn Sie sich für YubiKeys as a Service entscheiden, können Sie Entscheidungen nach und nach treffen und dabei auf unsere Einblicke und Hilfe zurückgreifen. So vereinfachen Sie den Prozess der Skalierung von YubiKeys auf größere Benutzerkreise, wenn Ihre geschäftlichen Anforderungen wachsen. Wir bieten Ihnen Erfolgsleitfäden und vorrangige Unterstützung, damit Sie so schnell wie möglich erfolgreich sind.

Wenn Sie eine engere Partnerschaft bei einem der sechs Schritte dieses Plans wünschen, steht Ihnen das [Professional Services Team von Yubico](#) gerne zur Verfügung.



Kontaktieren Sie uns
yubi.co/contact



Erfahren Sie mehr
yubi.co/ps

Quellen

¹ IBM Cost of a Data Breach Report 2025, <https://www.ibm.com/reports/data-breach>

² Shalanda D. Young, Office of Management and Budget, M-22-09, (January 26, 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>

³ National Security Memorandum/NSM-8, <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/>

⁴ NIST, FIPS 201-3, (January 2022), <https://csrc.nist.gov/publications/detail/fips/201/3/final>

⁵ CFPB, [Consumer Financial Protection Circular 2022-04](#), (August 11, 2022)

⁶ PCI SSC, [PCI DSS v4.0](#), (March 2022)



Über Yubico

Yubico (Nasdaq Stockholm: YUBICO) ist ein modernes Cybersicherheitsunternehmen mit dem Ziel, das Internet für alle sicherer zu machen. Als Erfinder des YubiKey setzen wir den Goldstandard für moderne, Phishing-resistente, hardwaregestützte Authentifizierung, verhindern Kontoübernahmen und machen sicheres Einloggen einfach.

Bereits seit 2007 gestalten wir aktiv globale Authentifizierungsstandards mit, haben an der Entwicklung von FIDO2, WebAuthn und FIDO U2F mitgewirkt und sind Wegbereiter des originalen Passkeys. Heute schützt unsere Passkey-Technologie Menschen und Unternehmen in über 160 Ländern und verändert grundlegend, wie die digitale Identität geschützt wird – vom Onboarding bis hin zur Kontowiederherstellung.

Weltweit vertrauen führende Marken, Regierungsbehörden und Institutionen mit höchsten Sicherheitsanforderungen auf unsere Lösungen. YubiKeys sind sofort einsatzbereit, funktionieren standardmäßig mit Hunderten von Apps und Diensten und bieten einen schnellen, passwortlosen Zugang ganz ohne Reibungsverluste oder Kompromisse bei der Sicherheit.

Wir glauben, dass jeder von starker Sicherheit profitieren können sollte. Im Rahmen unserer philanthropischen Initiative „Secure it Forward“ spenden wir YubiKeys an gemeinnützige Organisationen, die gefährdete Gemeinschaften unterstützen.

Unser Unternehmen mit Hauptsitzen in Stockholm, Schweden, und Santa Clara, Kalifornien, ist stolz darauf, von TIME als eines der 100 einflussreichsten Unternehmen und von Fast Company als eines der innovativsten Unternehmen ausgezeichnet worden zu sein. Weitere Informationen finden Sie unter www.yubico.com.