yubico

Phishing-resistente MFA für Ihre hybriden und dezentralen Arbeitskräfte

Fünf Schritte zur Verbesserung der Sicherheit und Erhöhung der Produktivität mit dem YubiKey

Hybride und dezentrale Arbeitsformen werden sich durchsetzen. Das kann jedoch Herausforderungen für die IT-Sicherheit mit sich bringen, was die Notwendigkeit erhöht, agil zu sein und die digitale Transformation voranzutreiben. Bei Remote-Mitarbeitern reichen die übliche Perimetersicherheit und die herkömmlichen Formen der Authentifizierung – wie Benutzernamen und Passwörter und mobile Authentifizierung – nicht mehr aus, um unbefugten Zugriff auf Netzwerke, Anwendungen und Daten vorzubeugen. Benutzernamen und Passwörter können leicht missbraucht werden, und mobile Authentifizierungssysteme sind anfällig für Phishing, Malware, SIM-swapping und Man-in-the-Middle-Angriffe (MiTM), wodurch Ihr Unternehmen dem Risiko einer Datenschutzverletzung ausgesetzt ist.

Schützen Sie Ihre hybriden Remote-Mitarbeiter vor modernen Cyber-Bedrohungen mit dem YubiKey – einem Multi-Protokoll-Hardware-Sicherheitsschlüssel von Yubico, der Phishing-resistente Zwei-Faktor-Authentifizierung (2FA), Multi-Faktor-Authentifizierung (MFA) und passwortlose Authentifizierung bietet. Der YubiKey ist in verschiedenen Formfaktoren erhältlich und bietet eine portable und einfache Benutzererfahrung auf Desktops, Laptops, mobilen Geräten und Tablets. Der YubiKey ermöglicht auch das Zurücksetzen von Passwörtern im Self-Service, was die IT-Supportkosten erheblich reduziert. Unternehmen auf der ganzen Welt stellen ihren Mitarbeitern YubiKeys zur Verfügung, um einen sicheren Zugang zu Unternehmensnetzwerken, Daten und Anwendungen zu gewährleisten und die Betriebskosten zu senken.

Mit den folgenden fünf Schritten können Sie Ihre Mitarbeiter, Ihr Netzwerk und Ihre Geräte mit dem YubiKey schützen:

1 MFA-Zugang für Identitäts- und Zugriffsmanagement Systeme (IAM) und Identitätsanbieter (IdP) ermöglichen

Die meisten führenden Hybrid- und Cloud-Umgebungen nutzen IAM-Lösungen, damit die Mitarbeiter für verschiedene Unternehmensanwendungen und -dienste ohne die Mühe mehrerer Benutzernamen und Passwörter arbeiten können. Die Aktivierung von MFA auf Ihrer IAM-Plattform wird Ihre Sicherheitslage verbessern.

Erhöhen Sie die Sicherheit in Ihrem gesamten Unternehmen, indem Sie MFA mit dem YubiKey aktivieren. Führende IAM-Plattformen wie Microsoft Azure Active Directory, Duo, Google Cloud, Okta Workforce Identity, OneLogin, Axiad, Ping Identity platform und RSA SecurID® Suite unterstützen die YubiKeys standardmäßig und können für Single Sign-on (SSO) für Messaging- und Videokonferenz-Apps wie Microsoft Teams, Google Hangouts und Zoom verwendet werden.

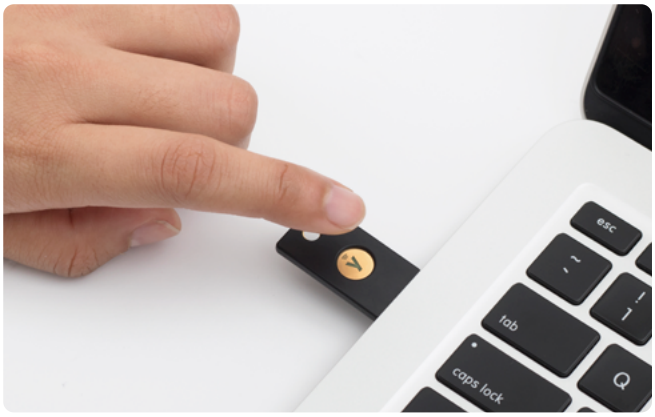
2 Schützen Sie sich vor der Übernahme Ihrer Konten durch Verzicht auf weniger starke Authentifizierung mit Smartphones

Zweistufige Authentifizierungsmethoden wie Einmal-Passcodes und geräteinterne Aufforderungen sind an mobile Geräte gebunden, die durch Malware, SIM-Swapping und MiTM-Angriffe gefährdet werden können. Untersuchungen von Google, NYU und UCSD auf der Grundlage von 350.000 realen Hijacking-Versuchen haben gezeigt, dass SMS- und mobile Authentifizierungssysteme nicht sehr effektiv sind, um die Übernahme von Konten und gezielte Angriffe zu verhindern.[1]

YubiKey-Integrationen schützen Ihre Arbeitskräfte überall

DUO · FORGEROCK · idaptive · intercede · Microsoft · okta · ONE IDENTITY · onelogin · Onion ID · PingIdentity · secure W2

[1] Google Security Blog: New research: How effective is basic account hygiene at preventing hijacking



Schützen Sie Ihre Mitarbeiter vor Kontoübernahmen, indem Sie die alten mobilfunkbasierten Authentifikatoren durch den YubiKey ersetzen. Durch die Nutzung moderner offener FIDO2- und WebAuthn-Authentifizierungsstandards können Sie Ihren Mitarbeitern ein Höchstmaß an Sicherheit bieten, um sie vor Phishing- und Man-in-the-Middle-Angriffen zu schützen.

3 Sichere Fernzugriffstechnologien mit MFA

Virtual-Private-Networks (VPN) oder Identity-Aware-Proxies (IAP) werden in vielen Unternehmen für den Zugriff zu Unternehmensnetzen, geschützten Ressourcen oder bestimmten Anwendungen genutzt. Eine Verbindung über VPN oder IAP bietet Sicherheit, nachdem die Verbindung hergestellt wurde. Eine Verbindung über ein ungesichertes privates oder öffentliches WLAN kann jedoch immer noch riskant sein, wenn VPNs oder IAPs mit herkömmlichen Formen der Authentifizierung gesichert sind.

Der YubiKey sichert den Fernzugriff, indem er Phishing-resistente 2FA oder MFA für führende VPN-Anwendungen ermöglicht, wie Pulse Secure und Cisco AnyConnect sowie Fernzugriffsanwendungen mit Smartcard (PIV), One-Time-Password (OTP), FIDO U2F oder FIDO2-Funktionen.

4 Computer-Login mit MFA schützen

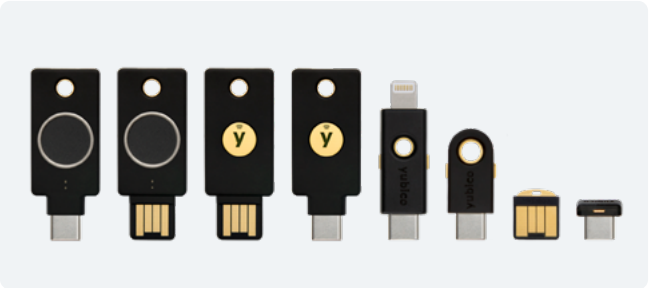
Wenn die Laptops der Mitarbeiter nicht ordnungsgemäß gesichert sind, können sie Einfallstore für externe Bedrohungen sein, die zu einem Sicherheitsverstoß führen, der finanzielle, rechtliche und rufschädigende Folgen für Ihr Unternehmen haben kann.

YubiKeys sichern Computeranmeldungen und schützen Anwendungen auf dem Gerät sowie wichtige Geschäftsdaten. Mehrere Anmeldeoptionen umfassen die Authentifizierung für Macs und Windows Computer einschließlich derer, die über Azure Active Directory, Active Directory und Microsoft-Konten verbunden sind. Eine der wirksamsten Methoden zur Sicherung des Computerzugangs ist die Nutzung der YubiKey-Smartcardfunktion, die einen YubiKey und eine PIN erfordert.

5 Aktivieren Sie die Step-up-Authentifizierung für Passwortmanager.

Viele Unternehmensmitarbeiter verlassen sich auf Passwortmanager. Wenn Ihr Passwortmanager jedoch nicht durch Phishing-resistente MFA geschützt wird, ist er anfällig für Angriffe und erlaubt Angreifern Zugang zu Passwörtern für Ihre gesamten Unternehmensanwendungen und -daten.

Der YubiKey lässt sich mit verschiedenen Unternehmens-Passwortmanagern integrieren, darunter 1Password, Dashlane, Keeper Security, LastPass und andere, um zu verhindern, dass nachlässige Richtlinien für Passwortverwaltung zu einem Sicherheitsverstoß führen.



Fangen Sie heute noch an und stellen Sie YubiKeys nahtlos für Ihre Hybrid- und Remote-Mitarbeiter bereit

Yubico bietet flexible und kosteneffiziente Unternehmenstarife an, die Organisationen mit 500 oder mehr Nutzern dabei helfen, von veralteten und fehlerhaften MFA-Lösungen wegzukommen und den Übergang zu einer Phishing-resistenten Authentifizierung im großen Maßstab zu beschleunigen.

Mit YubiEnterprise Subscription profitieren Unternehmen von einem vorhersehbaren OPEX-Modell, der Flexibilität, Benutzerpräferenzen mit der Wahl eines beliebigen YubiKeys zu erfüllen, Upgrades auf die neuesten YubiKeys und schnellere Rollouts mit einfachem Zugang zu Deployment Services und Priority Support. Abonnement-Kunden sind auch berechtigt, zusätzliche Dienstleistungen und Produktangebote zu erwerben.

Kontaktieren Sie das Vertriebsteam von Yubico hier.

YubiKeys werden genutzt in:

9 der 10 führenden Technologieunternehmen weltweit

4 der 10 führenden US-Banken

5 der 10 führenden globalen Handelsunternehmen

Über Yubico Als Erfinder des YubiKey macht Yubico sicheres Login mit Phishing-resistenter MFA-Technologie sehr einfach. Yubico setzt globale Standards für den plattformübergreifenden sicheren Zugang zu Anwendungen und Endgeräten und ist einer der Hauptentwickler und Mitgestalter von offenen Authentifizierungsstandards wie FIDO2 (WebAuthn) und FIDO U2F. Weitere Informationen finden Sie hier: www.yubico.com.

Yubico AB
Kungsgatan 44
2. Stock
SE-111 35 Stockholm
Schweden

Yubico Inc.
5201 Great America Pkwy
Suite 122
Santa Clara, CA 95054
USA