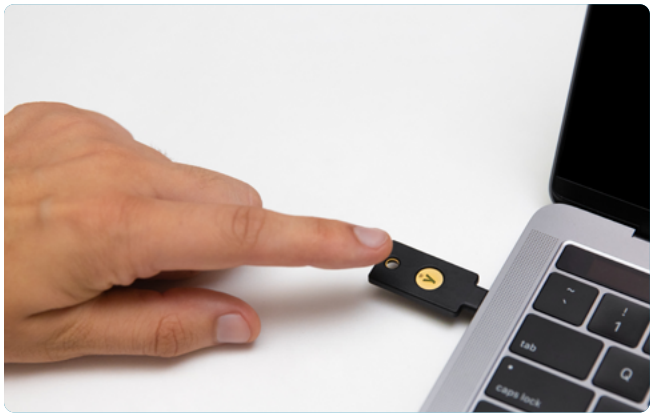
yubico

Phishing-resistente MFA für privilegierte Benutzer

Sichern Sie Daten, Technologie und Menschen mit dem YubiKey



Privilegierte Benutzer und ihre Anmeldedaten sollten bestmöglich gesichert sein. Doch viele Unternehmen schützen diesen Nutzerkreis nur unzureichend und setzen ihn so vermeidbaren Angriffen aus. Forrester schätzt, dass etwa 80 % der Datenschutzverletzungen mit kompromittierten privilegierten Anmeldedaten verbunden sind.[1] Angreifer versuchen mit hochentwickelten Methoden wie Spear-Phishing, Man-in-the-Middle-Angriffen oder Credential Stuffing, Anmeldedaten für privilegierte Accounts zu erbeuten um so Zugriff auf kritische Systeme oder Daten zu erlangen. Im weiteren Verlauf des Angriffs kann es passieren, dass sich Angreifer nach dem initialen Eindringen vertikal und horizontal durch das angegriffene Netzwerk bewegen um die Privilegien noch weiter auszubauen um so Zugriff auf die Kronjuwelen eines Unternehmens zu erlangen.

Was macht privilegierte Benutzer so anziehend für Cyberkriminalität? Und wie sollten Unternehmen sie am besten schützen?

Der erste Schritt zur Sicherung privilegierter Benutzerkonten besteht darin zu verstehen, wer diese Benutzer sind. Der zweite Schritt ist die Analyse der aktuellen Zugangsverwaltung und des Authentifizierungsrahmens. Was sind die Ursachen dafür, dass privilegierte Benutzer ungeschützt sind, und was kann man tun, um die Übernahme von Konten vollständig zu verhindern?

Sie haben vielleicht mehr privilegierte Benutzer, als Ihnen bewusst ist

Traditionell wurden privilegierte Benutzer als Mitarbeiter der IT betrachtet. Aber in der heutigen digitalen Welt können privilegierte Benutzer auch Geschäftsanwender sein – jeder, der auf einer höheren Ebene im Netzwerk, in der Cloud oder in einer Anwendung arbeitet und weitreichenden Zugriff auf anfällige Systeme oder IP wie Kunden-, Personal-, Finanz-, Rechts-, Konstruktions-oder Verkaufsdaten hat.

Dieser Zugang zu kritischen Systemen und sensiblen Daten, macht sowohl privilegierte IT- als auch Geschäftskonten zu einem bevorzugten Ziel für Cyberkriminelle und böswillige Insider.

Immer mehr Nutzer benötigen einen privilegierten Zugang und die digitale Transformation führt dazu, dass immer mehr Daten außerhalb der Kontrolle der IT-Abteilung liegen.Sensible Daten werden in die Cloud und über Microservices gesendet. Arbeit von zu Hause erhöht das Risiko durch ungesicherte Geräte und Heimnetzwerke. Wenn es zu einer Datenverletzung kommt, wird letztlich jeder im Unternehmen plötzlich zu einem privilegierten Benutzer – da Bedrohungsakteure nach Zugangsdaten suchen, die es ihnen ermöglichen, sich im Netzwerk zu bewegen.

Wie IAM- und PAM-Lösungen Sicherheitslücken für privilegierte Benutzer erzeugen

Ein bewährtes Verfahren für Unternehmen zur Stärkung der Sicherheit ist der Einsatz von Identitäts- und Zugriffsmanagement (IAM), privilegiertem Zugriffsmanagement (PAM) und Multifaktor-Authentifizierung (MFA). Viele Unternehmen stellen jedoch fest, dass sie trotz dieser Vorkehrungen anfällig für Phishing, gezielte Angriffe und Kontoübernahmen sind.

Zugriffskontrolllösungen wie IAM und PAM spielen eine wichtige Rolle, wenn es darum geht, den richtigen Benutzern den Zugriff auf die benötigten Anwendungen und Daten zu ermöglichen. Sie hinterlassen jedoch immer noch Sicherheitslücken, die von Cyberkriminellen leicht ausgenutzt werden können. Hier sind einige Beispiele:

- Fehlende Unterscheidung zwischen Zugriffs- und Privilegierungsrechten
- Integration von privilegiertem Zugriff mit Single Sign-On (SSO) ohne starke Authentifizierung
- Nicht verwaltete privilegierte Konten: Auftragnehmer, kurzfristige oder gekündigte Mitarbeiter oder sogar Konten, die außerhalb der IT-Kontrolle erstellt wurden (Shadow-IT)
- Gemeinsame Nutzung von Zugangsdaten und unsichere Formen der Authentifizierung für Administratorkonten

Viele dieser Lücken sind darauf zurückzuführen, dass die meisten älteren Zugriffskontrolllösungen nicht ausdrücklich für die Verwaltung von Privilegien konzipiert wurden. Als Best Practice für die Absicherung privilegierter Konten sollten Unternehmen das Prinzip der geringstmöglichen Berechtigungen verfolgen.

Nach diesem Konzept sollten Benutzer verschiedene Stufen von Privilegien haben, je nachdem, was sie in einem System sehen und tun sollen. Mit anderen Worten, es geht darum, den geringstmöglichen Zugriff (wer hat Zugriff worauf) und die geringstmöglichen Privilegien (Aktionen, die jemand ausführen kann), die mit diesem Zugriff verbunden sind, zu gewähren.

Eine PAM-Lösung bietet eine zusätzliche Sicherheitsebene, indem sie die Privilegien von Benutzerkonten und Administratorkonten trennt. Dies begrenzt den Schaden, wenn die Identität eines Benutzers kompromittiert wird. Privilegierte Zugangsdaten sollten sicher verwahrt und vor der Benutzung überprüft werden, aber diese Systeme verlassen sich in der Regel auf das IAM zur Authentifizierung und erfordern oft nicht viel mehr als ein Passwort oder veraltete MFA.

Veraltete MFA setzt privilegierte Benutzer weiterhin der Gefahr von Phishing und Kontoübernahmen aus

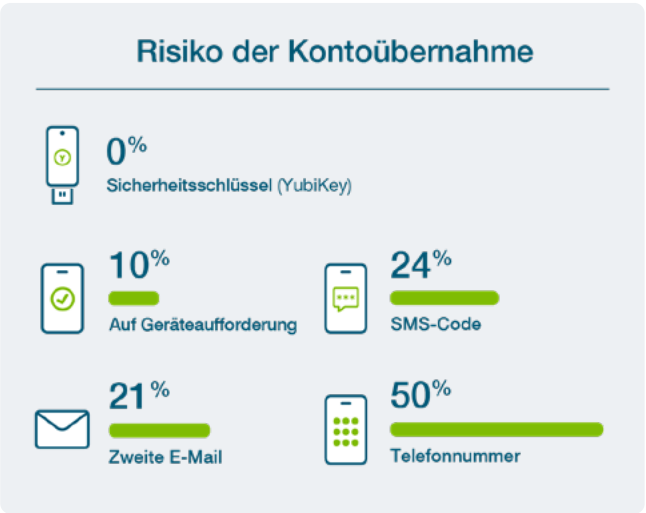
Herkömmliche Authentifizierungsmethoden wie Benutzernamen und Passwörter sowie mobile Authentifizierungsverfahren wie SMS, OTP und Push-Benachrichtigungen sind alle anfällig für Phishing, gezielte Angriffe und Kontoübernahmen.[2] Das liegt daran, dass diese Formen der Authentifizierung auf „gemeinsamen Geheimnissen" beruhen, die durch Phishing-Angriffe, Malware, Man-in-the-Middle-Angriffe, SIM-Swapping und andere Formen der Kontoübernahme verletzt werden können. Heutige Cyberkriminelle können herkömmliche MFA auf eine Art und Weise aushebeln, die für den Endbenutzer fast unerkennbar ist. Wenn diese Angriffe auf privilegierte Konten abzielen, steigt das Risiko Opfer von Sicherheitsverletzungen, Ransomwareattacken oder Cyberspionage zu werden exponentiell an.

Um privilegierte Benutzer- und Administratorkonten zu schützen, sollten alle Unternehmen den Einsatz einer Phishing-resistenten MFA unter Verwendung von Hardware-Sicherheitsschlüsseln wie dem YubiKey in Betracht ziehen.

Im Gegensatz zu Benutzernamen- und Passwort-basierter Authentifizierung und älteren Formen von MFA, wie z. B. mobilen Authentifikatoren, bietet der YubiKey eine Phishing-resistente und kosteneffiziente bedarfsgerechte Authentifizierung.

YubiKeys bieten einen Rundum-Schutz für privilegierte Benutzer

Yubico bietet mit dem YubiKey eine moderne und hochsichere MFA-Lösung an, die speziell auf die Bedürfnisse von Unternehmen zum Schutz privilegierter Benutzer zugeschnitten ist. Private Schlüssel werden im sicheren Element auf dem YubiKey gespeichert und können nicht exfiltriert werden, wodurch sichergestellt wird, dass privilegierte Benutzer und Daten immer geschützt sind. Es ist die einzige Lösung, die nachweislich 100 % aller Kontoübernahmen, einschließlich massenhafter und gezielter Phishing-Angriffe, verhindert.[3]



Forschung von Google, NYU und UCSD auf der Grundlage von 350.000 realen Hijacking-Versuchen. Die angezeigten Ergebnisse beziehen sich auf gezielte Angriffe.

	Veraltete Authentifizierung	YubiKey
Sicherheit	Gefahr von Kontoübernahmen	Phishing-resistente starke Authentifizierung
Kosten	Kosten im Zusammenhang mit Geräten und Diensten, mobilem Management, zurücksetzen von Passwörtern sowie potenzielle Kosten für Datenverletzungen	Schlüsselfertige Lieferung, Self-Provisioning
Benutzer-erfahrung	Passwort + 2. Faktor verringert die Produktivität und führt zu Frustration, funktioniert nicht in allen Situationen	Einfaches Antippen oder Berühren zur Authentifizierung, keine Netzwerk- oder Batterieanforderungen
Protokoll Unterstützung	Einfach	Unterstützung mehrerer Protokolle
Integrationen	Ein Berechtigungs-nachweis pro Anwendung, teuer zu verwalten	Ein einziger, vollständig kompatibler Berechtigungsnachweis, der auf einem sicheren Schlüssel gespeichert ist
Portabilität	2FA kann ein mobiles Gerät oder Leser erfordern	Tragbare Root of Trust (RoT)

Der YubiKey unterstützt moderne Authentifizierungsprotokolle wie FIDO U2F und FIDO, sowie OTP, SmartCard und OpenPGP, wodurch sichergestellt wird, dass ein einziger Schlüssel in älteren und modernen Infrastrukturen und Anwendungen funktioniert. YubiKeys bieten auch eine außergewöhnliche Benutzererfahrung (User Experience), die die Benutzerakzeptanz erleichtert. Benutzer können sich durch einfaches Antippen oder Berühren des YubiKeys anmelden.

YubiKeys arbeiten sofort mit führenden IAM- und PAM-Lösungen zusammen und lassen sich mit Dutzenden von Drittanbietersystemen integrieren, einschließlich Axiad, Duo, Google Cloud, Microsoft Azure Active Directory, Okta Workforce Identity, PingID, RSA SecurID Suite und CyberArk.

Yubico bietet flexible und kosteneffiziente Unternehmenstarife an, die Organisationen mit 500 oder mehr Nutzern dabei helfen, sich von der veralteten und nicht funktionierenden MFA zu lösen und den Übergang zu einer Phishing-resistenten Authentifizierung im großen Maßstab zu beschleunigen. Mit dem YubiEnterprise-Abonnement können Unternehmen von vorhersehbaren Betriebskosten profitieren und sind außerdem fähig, zusätzliche Dienstleistungen und Produktangebote zu erwerben.

Privilegierte Benutzeraccounts sind die Schlüssel zu jedem Unternehmen – Schlüssel, für die Cyber-Kriminelle vor nichts zurückschrecken werden. Setzen Sie eine Phishing-resistente Authentifizierung ein, um privilegierte Benutzer und Ihr Unternehmen vor modernen Cyber-Bedrohungen zu schützen.

[1] Andras Cser, et. al., The Forrester Wave: Privileged Identity Management, Q4 2018

[2] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking

[3] Ibid

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
2nd floor
SE-111 35 Stockholm
Schweden

Yubico Inc.
5201 Great America Pkwy
Suite 301
Santa Clara, CA 95054
USA