yubico

YubiKey 5 FIPS-Serie: Validierung gemäß FIPS 140-2 sorgt für hohe Sicherheit und Compliance

Die YubiKey 5 FIPS-Serie ist die erste mit FIPS-validierte Multiprotokoll-Support inklusive FIDO2/WebAuthn. 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.

Sicherheitsmaßnahmen, die lediglich auf Benutzernamen und Kennwörtern basieren, setzen Unternehmensdaten Risiken aus.

Nahezu jeden Tag liest man in den Schlagzeilen von neuentdeckten, katastrophalen Datenlecks und Sicherheitsvorfällen. Und das mit gutem Grund: Die Kosten der weltweiten Cyberkriminalität werden sich im Jahr 2021 voraussichtlich auf 6 Billionen US-Dollar belaufen, ein Anstieg von 3 Billionen US-Dollar im Jahr 2015.[1]

Hauptgrund für die meisten Sicherheitsvorfälle: Passwörter. 81 % der Datenlecks entstehen aufgrund von gestohlenen oder schwachen Passwörtern.[2] Daher dürfen sich IT-Organisationen nicht ausschließlich auf Passwörter verlassen, um den Zugriff auf Unternehmensdaten zu schützen. Sie müssen eine stärkere Methode zur Mitarbeiter- und Anbieterauthentifizierung einsetzen oder riskieren, das nächste Angriffsziel zu werden.

Der YubiKey beseitigt Kontoübernahmen

Mit dem YubiKey können Sie ganz einfach sichere und skalierbare Verfahren zur Authentifizierung bereitstellen, die Kontoübernahmen aufgrund von Phishing-Angriffen beseitigen. Der YubiKey ist eine hardwarebasierte Lösung mit den folgenden Funktionen und Eigenschaften:

- Unterstützung mehrerer Authentifizierungs- und Kryptografieprotokolle, darunter FIDO2/WebAuthn, FIDO U2F, PIV-kompatible Smartcards und Yubico One-Time Password (OTP) zum Schutz des Mitarbeiterzugriffs auf Computer, Netzwerke und Onlineservices per Fingertipp.
- Unterstützt passwortlose sichere Anmeldung mit Smartcard und FIDO2/WebAuthn-Authentifizierung.
- Kompatibel mit allen gängigen Betriebssystemen, darunter Microsoft Windows, macOS, Android und Linux, sowie mitdenführenden Browsern.
- In sechs Formfaktoren erhältlich, so dass Benutzer den Schlüssel jederzeit und mit vielen Endgeräten nutzen können.

Google, Facebook und Salesforce verlassen sich seit 2012 auf den YubiKey

Liefert sichere Multifaktor-Authentifizierung: Der YubiKey sorgt dank einer Kombination aus hardwarebasierter Authentifizierung und Public-Key-Kryptografie für sichere Authentifizierung und unterbindet Kontoübernahmen. Zu den Funktionen gehören FIDO2/WebAuthn und FIDO U2F, offene Authentifizierungsstandards, der von der FIDO Alliance unterstützt wird, sowie Smartcard-Funktionalität basierend auf der in NIST SP 800-73 spezifizierten PIV-Schnittstelle.

Senkt IT-Kosten: Bei einer Auswertung von Daten aus einem Deployment von über 50.000 YubiKeys in 70 Ländern stellte Google fest, dass die Benutzerfreundlichkeit und Zuverlässigkeit des Geräts die Supportfälle im Zusammenhang mit Kennwörtern um 92 % reduziert hatte. So spart das Unternehmen jährlich tausende Stunden an Supportkosten.

Liefert einfache, schnelle und zuverlässige Sicherheit für Mitarbeiter: YubiKey-Hardware ist zuverlässig, da sie keine Batterie oder Netzwerkverbindung erfordert. Sie ist also immer einsatzfähig und verfügbar. Die Authentifizierung erfolgt schnell mit einer einfachen Berührung. Somit ist diese Art der Authentifizierung bis zu viermal schneller, als die mobile Zwei-Faktor- und die SMS-Authentifizierung.

Seit der Bereitstellung des YubiKey 2010 erreichte Google:

- Null Kontoübernahmen
- 4-mal schnellere Anmeldung
- 92 % weniger IT-Supportanrufe

[1] Cybersecurity Ventures
[2] 2017 Data Breach Investigations Report 10th Edition, Verizon
[3] Security Keys: Practical Cryptographic Second Factors for the Modern Web, Google Inc.

YubiKeys werden genutzt in:

- **9 der 10 führenden** globalen Technologieunternehmen
- **4 der 10 führenden** Banken in den USA
- **2 der 3 führenden** globalen Einzelhandelsunternehmen

YubiKey: Bewährte, benutzerfreundliche Sicherheit, der weltweit führende Unternehmen vertrauen

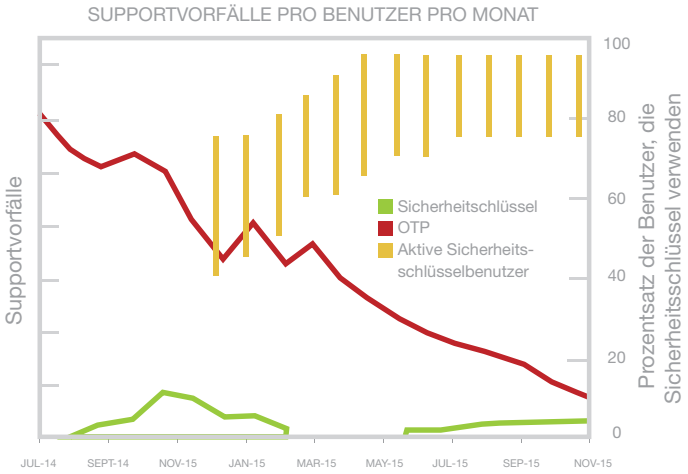
Schutz vor Phishing für die sichere Unternehmensauthentifizierung

Der YubiKey speichert das Authentifizierungs-Secret in einem sicheren Hardwarechip. Dieses Secret wird nie übertragen und kann daher nicht kopiert oder gestohlen werden.

Senkt IT-Kosten

Der YubiKey trägt zu einer wesentlichen Reduzierung der IT-Supportkosten bei. Diese sind größtenteils auf Kennwort-rücksetzungen zurückzuführen, die z. B. Microsoft mehr als 12 Millionen US-Dollar monatlich kosten.[4]

Durch den Wechsel von mobilen Einmalkennwörtern zu YubiKeys konnte Google die Supportfälle im Zusammenhang mit Kennwörtern um 92 % reduzieren, da YubiKeys zuverlässig, schnell und benutzerfreundlich sind.



Dieses Diagramm veranschaulicht, wie schnell Google Supportvorfälle im Zusammenhang mit Kennwörtern nach dem Wechsel von Einmalkennwörtern zu YubiKey reduzieren konnte.[5]

Benutzerfreundlich, schnell und zuverlässig

Benutzer müssen nichts installieren. Kunden oder Mitarbeiter registrieren ihren YubiKey einfach, geben ihren Benutzernamen und ihr Kennwort ein, setzen den YubiKey ein und tippen darauf, wenn sie dazu aufgefordert werden.

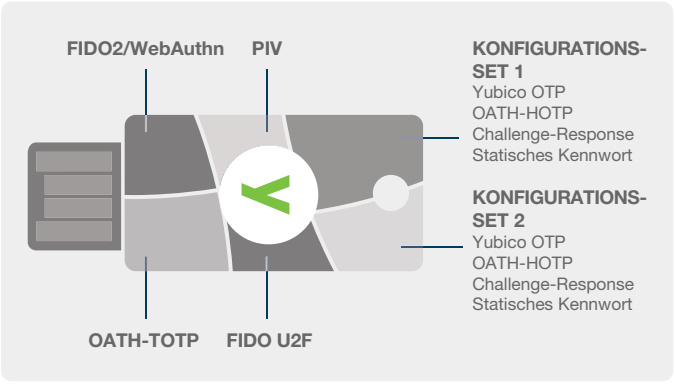
YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS und YubiKey 5C FIPS lassen sich ganz einfach an einem Schlüsselbund befestigen, während YubiKey 5 Nano FIPS und YubiKey 5C Nano FIPS im USB-Anschluss verbleiben können. So ist jeder YubiKey stets zugänglich und bietet die gleiche digitale Sicherheit. Der YubiKey 5 NFC FIPS/5 Nano FIPS ist dabei sehr robust und wasserfest.

[4] „Saying Goodbye to Passwords", Alex Simons, Manini Roy, Microsoft Ignite 2017

[5] Security Keys: Practical Cryptographic Second Factors for the Modern Web, Google Inc.

Einfach bereitzustellen

Die IT-Abteilung kann YubiKeys innerhalb von Tagen anstatt Monaten bereitstellen. Sie können so mit einem einzelnen Key auf die unterschiedlichsten, egal ob modern und älter, Systeme zugreifen, ohne dass separate Hardware oder zusätzlicher Integrationsaufwand erforderlich ist.



YubiKey-Funktionen: Diese Funktionen sind in den Sicherheitsschlüsseln YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS und YubiKey 5C Nano FIPS enthalten. Technische Daten finden Sie auf yubico.com.

Vertrauenswürdiger führender Authentifizierungsanbieter

Yubico ist der Hauptentwickler des Authentifizierungsstandards U2F, der von der FIDO Alliance übernommen wurde, und das erste Unternehmen, das den U2F-Sicherheitsschlüssel hergestellt hat.

YubiKeys werden in neun der zehn führenden globalen Technologieunternehmen, vier der zehn führenden Banken in den USA und zwei der drei führenden globalen Einzelhandels-unternehmen eingesetzt.

YubiKeys werden in unseren Niederlassungen in den USA und Schweden hergestellt, unter Einhaltung strenger Sicherheits- und Qualitätskontrollen während des gesamten Fertigungsprozesses.

FIPS 140-2-geprüft

Schützen Sie Ihr Unternehmen mit der nach FIPS 140-2 geprüften Version (Gesamtstufe 1 und 2, Physische Sicherheitsstufe 3) der branchenführenden YubiKey-Lösung für Multifaktor-Authentifizierung. Mit der YubiKey FIPS-Serie können Regierungsbehörden und regulierte Branchen die Anforderungen der höchsten Sicherheitsstufe für Authentifikatoren (Authenticator Assurance Level 3, AAL3) aus den neuen NIST SP800-63B-Empfehlungen erfüllen.

Über Yubico Yubico setzt neue weltweite Maßstäbe für den einfachen und sicheren Zugriff auf Computer, Server und Onlinekonten. Yubico ist ein 2007 gegründetes Privatunternehmen und unterhält Geschäftsstellen in Australien, Deutschland, Singapur, Schweden, dem Vereinigten Königreich und in den USA. Erfahren Sie, warum neun der Top-10-Internetmarken und Millionen Benutzer in über 160 Ländern unsere Technologie nutzen: www.yubico.com.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Schweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (gebührenfrei)
650-285-0088