CLOUDFLARE

KURZDARSTELLUNG DER LÖSUNG

Wie starke Authentifizierung Phishing-Angriffe stoppen kann

Security-Key und ein Zero-Trust-Ansatz können Phishing-Angreifern das Handwerk legen

Welche Gefahren von Phishing ausgehen

Verlorene Daten, kompromittierte Netzwerke, gestohlene Konten

Gezielte Phishing-Angriffe sind eine der gefährlichsten Bedrohungen, denen Unternehmen heute ausgesetzt sind. Phishing- und Social-Engineering-Angriffe zielen darauf ab, Menschen so zu manipulieren, dass sie vertrauliche Informationen oder Zugang preisgeben. Anmeldedaten sind ein beliebtes Ziel.

Erfolgreiche Angriffe dieser Art können Folgen haben wie:

- Kontoübernahme
- Ein Link in einem größeren Supply Chain-Angriff
- Exfiltration von Daten wie PII und IP
- Malware-Angriffe wie Ransomware

Glücklicherweise gibt es hochwirksame Lösungen, um das Risiko von Phishing zu verringern. Eine der wichtigsten ist die Multi-Faktor-Authentifizierung (MFA).

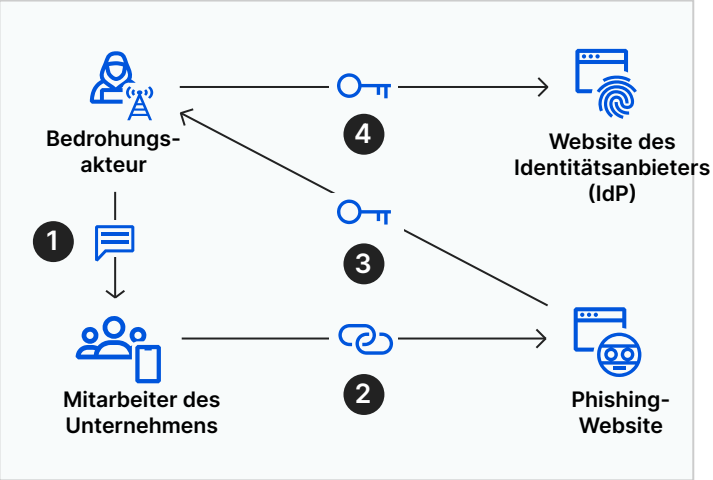


Abbildung 1: Anatomie eines SMS-Phishing-Angriffs. 1. Legitim aussehende SMS wird gesendet. 2. Verknüpfung mit einer legitim aussehenden Website. 3. In Echtzeit werden die Anmeldedaten des Opfers und ein zeitbasierter Einmal-Passcode übermittelt. 4. Meldet sich bei der echten IdP-Website des Unternehmens an.

Wie die Multi-Faktor-Authentifizierung (MFA) Phishing verhindert

MFA neutralisiert Passwortdiebstahl

MFA verlangt von Nutzern, dass sie bei der Anmeldung zusätzlich zu ihrem Benutzernamen und Passwort einen Key angeben. Ohne diesen Key können sie nicht auf ihre Konten zugreifen, und ein Angreifer kann das auch nicht.

MFA mit Softkeys

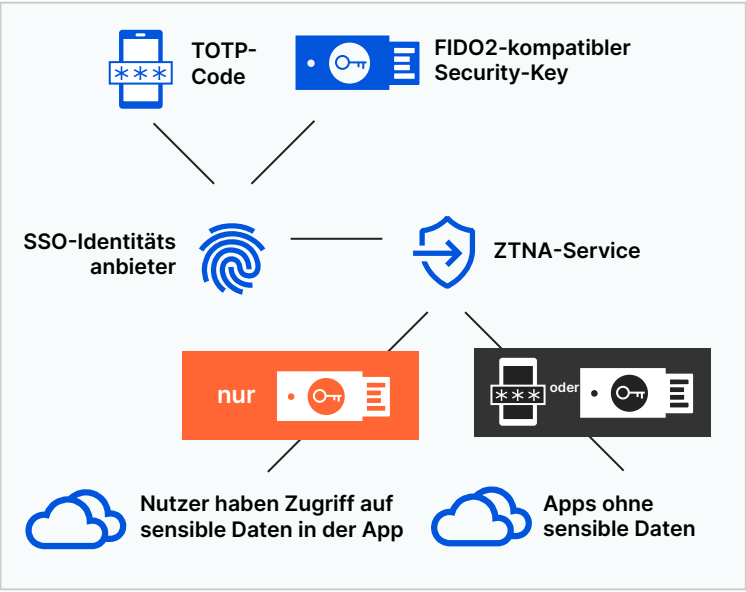
Eine gängige Implementierung von MFA ist die Verwendung von Softkeys wie z.B. zeitbasierte Einmal-Passcodes (Time-based one-time passcodes, TOTPs). TOTPs werden oft per SMS, E-Mail oder App ausgestellt. Softkeys sind zwar sicherer als die Ein-Faktor-Authentifizierung, können aber von Angreifern abgefangen werden.

MFA mit Security-Keys

FIDO2-konforme Security-Keys können, sobald sie ausgestellt wurden, von einem Angreifer nicht mehr abgefangen werden und sind ohne physischen Zugang nahezu unmöglich zu stehlen. Eine Studie von Google ergab, dass die Verwendung von FIDO2-/U2F-konformen Security-Keys 100 % der Versuche einer Kontoübernahme verhindert.[1]

Selektiv starke Authentifizierung durchsetzen

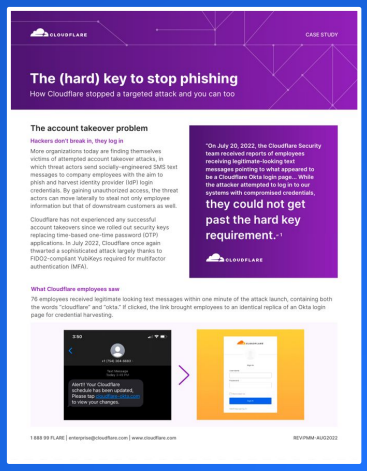
Einige IAM-Lösungen unterstützen zwar eine starke Authentifizierung, erlauben es den Administratoren jedoch nicht, diese wirklich erforderlich zu machen. Mit ZTNA können Sie sicherstellen, dass die FIDO2-Authentifizierung insbesondere für Apps mit sensiblen Daten erforderlich ist. Cloudflare verlangt für jede Authentifizierung einen Security-Key (MFA). Dies hat unser Sicherheitsniveau stark erhöht.



„Am 20. Juli 2022 erhielt das Cloudflare-Sicherheitsteam Berichte über Mitarbeiter, die legitim aussehende SMS erhielten, die auf eine scheinbare Cloudflare-Okta-Login-Seite verwiesen... Der Angreifer versuchte zwar, sich mit kompromittierten Anmeldedaten in unsere Systeme einzuloggen,

konnte aber die Hardkey-Anforderung nicht umgehen.“ [2]

CLOUDFLARE



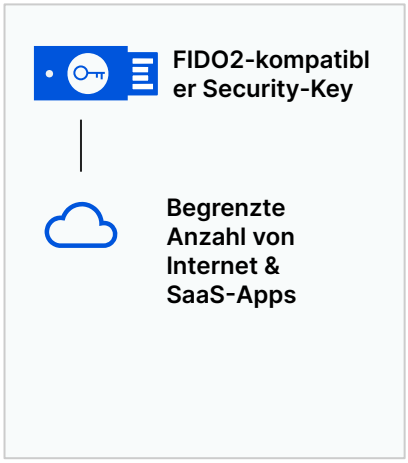
Führen Sie überall starke Authentifizierung ein

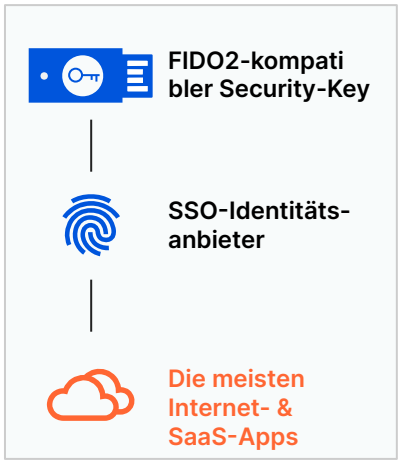
FIDO2-konforme MFA für alle Ihre Apps

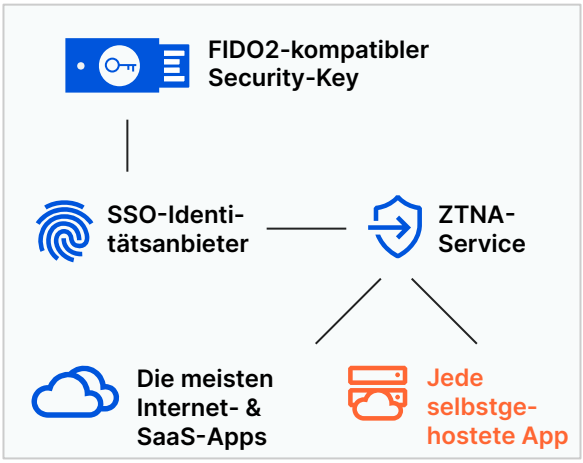
Die Durchsetzung von MFA für Cloud-Dienste ist auf verschiedene herkömmliche Arten möglich, insbesondere wenn ein Single Sign-On (SSO)-Dienst verwendet wird. Dies kann jedoch bei älteren oder nicht webbasierten Anwendungen schwierig sein, von denen viele diese Art der Authentifizierung nicht nativ unterstützen.

Vereinfachen Sie den Rollout mit ZTNA

Zero Trust Network Access (ZTNA) fungiert als Aggregationsschicht um all Ihre Ressourcen und ermöglicht strenge Authentifizierungsrichtlinien für jede dieser Ressourcen. SaaS-, selbst gehostete und nicht webbasierte Anwendungen können gleichermaßen hinter ZTNA stehen, was die Durchsetzung einer starken Authentifizierung über alle Anwendungen hinweg erleichtert.







Wichtigste Erkenntnisse für Unternehmen, die eine starke Authentifizierung implementieren

1

Zentralisieren Sie Ihr IAM

Zentralisieren Sie das Identitäts- und Zugriffsmanagement (IAM), so dass MFA für alle Anwendungen einfacher zu implementieren ist.

2

MFA selektiv durchsetzen

Richten Sie die selektive Durchsetzung von MFA-Optionen - TOTP und FIDO2 oder nur FIDO2 - je nach Identität und Kontext ein.

3

Unterstützung für mobile Geräte

Stellen Sie FIDO2-Lösungen für Laptops, Desktop-Computer und Server sowie für mobile Geräte aus.

Beschleunigen Sie Ihre Roadmap zur Zero-Trust-Implementierung

Architektur-Workshop anfordern

Noch nicht bereit für Ihre Analyse?

Kostenlose Testversion anfordern.

1. krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/
2. Cloudflare Blog-Beitrag, 9. August 2022, „The mechanics of a sophisticated phishing scam and how we stopped it“, blog.cloudflare.com/2022-07-sms-phishing-attacks/