okta

Was sind die Kosten von Identitätsdiebstahl?

Unsere persönlichen Daten sind für Cyberkriminelle von hohem Wert. Die Zahl von Account-Takeover-Angriffen, bei denen Hacker echte Anmeldedaten verwenden, um Zugang zu fremden Konten zu erhalten und Informationen zu stehlen, nimmt rasant zu. Der drohende Schaden für den Ruf und den Umsatz betroffener Unternehmen ist enorm. Doch was können Sie tun, um die Risiken zu minimieren und das Vertrauen Ihrer Kunden zu behalten?

Die Zahl der Account-Übernahmen steigt rasant.

Als während der Pandemie immer mehr Menschen anfingen, fast ausschließlich online zu arbeiten und zu shoppen, hat sich die Zahl der Account-Übernahmen verdreifacht.

3x

Anstieg zwischen 2019 und 2021

Quelle: Sift

Unsere Identities sind im Visier der Angreifer

Gestohlene oder missbrauchte Zugangsdaten waren 2021 die häufigste Ursache erfolgreicher Data-Breaches.

61 %

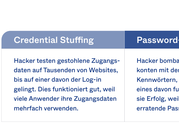
der Data-Breaches im Jahr 2021 gehen auf den Missbrauch von Zugangsdaten zurück

Quelle: Verizon DBIR

> „Hacker brechen nicht ein – sie melden sich an."
>
> Bret Arsenault, Microsoft

Kriminelle kennen viele Wege, um an Zugangsdaten zu gelangen.

Sie nutzen Phishing-Angriffe, um Benutzer zum Teilen ihrer Zugangsdaten zu verleiten, oder kaufen im Dark Web Listen mit häufig genutzten oder gestohlenen Passwörtern.



7 von 10

Unternehmen berichten von einem Anstieg der Phishing-Attacken seit dem Beginn der Pandemie.

Quelle: Sophos

15 Milliarden

Zugangsdaten stehen aktuell im Dark Web zum Verkauf

Quelle: Dark Shadows

Schwache Passwörter verschärfen das Problem

Viele Menschen verwenden Passwörter, die leicht zu erraten sind, oder nutzen dasselbe Passwort auf mehreren Seiten, was sie angreifbarer macht.

123456

Das häufigste Passwort des Jahres 2021

Quelle: NordPass

14

So oft wird ein Passwort im Durchschnitt benutzt

Quelle: LastPass

Wie gelangen Hacker in unsere Systeme?

Credential Stuffing	Password-Spray	Phishing
Hacker testen gestohlene Zugangsdaten auf Tausenden von Websites, bis auf einer davon der Log-in gelingt. Dies funktioniert gut, weil viele Anwender ihre Zugangsdaten mehrfach verwenden.	Hacker bombardieren Benutzerkonten mit den meistgenutzten Kennwörtern, um zu sehen, ob eines davon funktioniert. Oft haben sie Erfolg, weil Menschen leicht zu erratende Passwörter verwenden.	Beim Phishing verleiten Hacker die Benutzer dazu, ihre Anmeldedaten freiwillig zu teilen – z. B. mithilfe einer E-Mail, die sie auffordert, einem Link zu einer Website zu folgen

55 %

der Data-Breaches gehen auf organisierte Gruppen zurück

Quelle: Verizon DBIR

Daten-Breaches sind schlecht für Ihr Geschäft

Viele Cyberkriminelle verwenden automatisierte Online-Tools, um Websites durch Password Spraying zu knacken.

47 %

der Kunden würden sich dauerhaft von einer Marke abkehren, wenn diese erfolgreich angegriffen wird

Quelle: The State of Digital Trust, Okta

4,2 Mio. USD

Durchschnittliche Kosten eines Data-Breaches 2021

Source: IBM Cost of a Data Breach Report

3 Möglichkeiten, um Kunden-Identities zu schützen

1. Schnellere Erkennung von Angriffen

Breach-Detection-Systeme wie Auth0 Credential Guard können Angriffe sofort erkennen und betroffene Passwörter schnell zurücksetzen.

2. Implementierung von Multi-Faktor-Authentisierung

Multi-Faktor-Authentifizierung bietet eine zusätzliche Security-Ebene über das Passwort hinaus, und hilft, Hacker aus Ihrem Netzwerk fernzuhalten.

3. Verzichten Sie auf Passwörter

Immer mehr Unternehmen verzichten inzwischen ganz auf Passwörter und bieten ihren Kunden sichere, benutzerfreundliche Alternativen wie biometrische Verfahren, Einmalpasswörter oder Magic Links.

Verhindern Sie Account-Übernahmen mit Okta

Okta hilft Ihnen, Ihre Kunden, Partner und Mitarbeiter mit starken Authentifizierungslösungen zu schützen, auf die sie sich verlassen können. Setzen Sie strenge Passwortrichtlinien durch, identifizieren Sie frühzeitig betrügerische Anmeldeversuche und stoppen Sie Angreifer mit der automatisierten Threat Detection von Okta.

Was Sie tun können, um Account-Übernahmen zu verhindern, erfahren Sie im Video-Podcast mit Brian Glick, Editor-in-Chief der Computer Weekly, und Ian Lowe von Okta.