yubico

Sicherung von Finanzdienstleistungen mit moderner, Phishing-resistenter MFA

Die Finanzdienstleistungsbranche ist immer wieder Cyberangriffen ausgesetzt

Die Finanzdienstleistungsbranche ist ein beliebtes Ziel für Cyberkriminelle, wobei sich die Kosten einer Datenschutzverletzung im Bereich Finanzdienstleistungen auf durchschnittlich 5,9 Millionen US-Dollar belaufen.[1] Finanzdienstleistungsunternehmen sehen sich an zwei Fronten mit den Herausforderungen der Cybersicherheit konfrontiert: Auf Seite der Belegschaft müssen sie sich vor Identitätsdiebstahl von Mitarbeitern schützen, während Geschäfts- und Privatkunden dem Risiko von Kontoübernahmen in Verbindung mit Online- und Mobile-Banking ausgesetzt sind.

Nicht alle Arten der MFA sind gleich

Die Finanzdienstleistungsbranche hat schon frühzeitig mobile Authentifizierungsmethoden wie SMS, OTP und Push-Benachrichtigungen eingeführt. Jede Form der Multi-Faktor-Authentifizierung (MFA) ist besser als ein Passwort allein, doch nicht alle Arten der MFA sind gleich wirksam. Passwörter können leicht gehackt werden, und MFA in Form von Sicherheitsfragen, SMS-Codes, OTP und Push-Benachrichtigungen sind anfällig für Phishing-Angriffe, SIM-Swaps und Man-in-the-Middle-Angriffe. Auf Mobilgeräten basierende Authentifikatoren bieten darüber hinaus nicht die beste Benutzererfahrung.

Phishing-resistente MFA kann eine leistungsstarke erste Verteidigungslinie für Finanzdienstleistungsunternehmen sein – zum Schutz von Unternehmens- und Kundenressourcen.

Was ist Phishing-resistente MFA?

Phishing-resistente MFA-Prozesse basieren auf einer kryptografischen Überprüfung zwischen Geräten oder zwischen dem Gerät und einer Domäne, wodurch sie ideal gegen Versuche geschützt sind, den Authentifizierungsprozess zu gefährden oder zu untergraben. Der Fachpublikation (SP) 800-63 des National Institute of Standards and Technology (NIST) zufolge erfüllen derzeit nur zwei Authentifizierungsmethoden die Kriterien für Phishing-resistente MFA: PIV/Smart Card und der moderne FIDO2/WebAuthn-Authentifizierungsstandard.

Moderne, Phishing-resistente, passwortlose Multi-Faktor-Authentifizierung mit dem YubiKey

Um unternehmensweiten Identitätsdiebstahl und die Übernahme von Kundenkonten einzuschränken, stellt Yubico den YubiKey für eine starke, einfache und passwortlose Multi-Faktor-Authentifizierung bereit.

Unabhängige Forschungen zeigen, dass YubiKeys nachweislich den höchsten Schutz gegen Kontoübernahmen bieten, gezielte Angriffe verhindern und dabei auch noch einen ROI von 203 % einfahren.[2]

Risiko der Kontoübernahme

Studien von Google, NYU und UCSD basierend auf 350.000 echten Hijacking-Versuchen. Die angezeigten Ergebnisse beziehen sich auf gezielte Angriffe.

YubiKeys eignen sich hervorragend für Remote- und Hybridarbeitsplätze, Büroarbeitsplätze, Bereiche miteingeschränkter Mobilität, gemeinsam genutzte Arbeitsplätze und Geräte, digitale Dienste auf Kundenseite sowie für Benutzer, die mobile Authentifizierung nicht nutzen können oder wollen. Die Implementierung und Anwendung ist kinderleicht: Ein einzelner YubiKey kann für ältere und moderne Anwendungen, Services und Geräte verwendet werden, unterstützt mehrere Protokolle für Smart Card, OTP, OpenPGP, FIDO U2F und FIDO2/WebAuthn auf einem einzigen Schlüssel und bildet so eine Brücke zu moderner passwortloser Authentifizierung.

Außerdem erfüllen YubiKeys nach FIPS 140-2 die Sicherheitsstufe 3 der NIST-Empfehlungen zur Authentifizierung (AAL3) SP 800-63B und stellen Compliance mit SOX, PCI DSS 4.0, PSD2, DSGVO und CFP-Rundschreibens 2022-04 sicher.

Häufige Anwendungsfälle des YubiKeys im Finanzsektor

1. Sicherheit für Remote- und Hybridarbeitsplätze

Phishing-resistente MFA sollte eine der wichtigsten Anforderungen an Remote- und Hybridarbeitsplätze sein. YubiKeys bieten höchste MFA-Sicherheit und lassen sich einfach in bestehende Systeme und Infrastrukturen integrieren, einschließlich Identitäts- und Zugriffsverwaltungssystemen wie Microsoft, Okta, Duo, Ping und Hypr. Mithilfe des YubiKeys können Finanzdienstleistungsunternehmen an Remote- und Hybridarbeitsplätzen den sicheren Zugriff auf Computer, VPN und Passwortmanager sicherstellen – und das standortunabhängig. YubiKeys können sogar für die sichere Erstellung zeitbasierter Einmalpasswörter verwendet werden.

2. Sicherheit für Transaktionen mit hohem Risiko und hohem Wert

Mitarbeiter, die täglich Transaktionen mit hohem Risiko und hohem Wert durchführen, sind oft das Ziel von Cyberkriminellen. Der Zugang zu risikoreichen Systemen kann durch die Anwendung einer starken und modernen MFA mit YubiKeys verstärkt werden, sodass nur autorisierte Kontozugriffe und autorisierte Transaktionen mit hohem Wert durchgeführt werden können.

3. Sicherheit für privilegierte Nutzer

Privilegierte Nutzer zählen zu den Hauptzielen von Cyberkriminellen, da solche Nutzer leichteren Zugriff auf vertrauliche Unternehmens- und Kundendaten haben. Finanzdienstleistungsunternehmen können die Verwaltung privilegierter Zugriffe optimieren und gezielte Angriffe abwehren, indem sie sicherstellen, dass die Best Practices in Sachen Authentifizierungssicherheit eingehalten werden. Dabei sollten privilegierte Nutzer dazu aufgefordert werden, sich mit Phishing-resistenten Hardware-Sicherheitsschlüsseln wie dem YubiKey zu authentifizieren.

4. Sicherheit für Callcenter-Mitarbeiter

Bei einer hohen Mitarbeiterfluktuation, saisonalen Höchstständen und anderen schwierigen Geschäftsdynamiken benötigen Callcenter-Umgebungen einen sicheren, aber einfachen Ansatz, um die Identität von Mitarbeitern zu überprüfen, bevor sie Zugriff auf kritische Systeme und Daten erhalten. YubiKeys gewährleisten eine höhere Sicherheit, die die Identität von Callcenter-Mitarbeitern sicher bestätigen kann, bevor diese Zugriff auf personenbezogene und andere sensible Daten erhalten oder Änderungen an einem Kundenkonto vornehmen, z. B. eine Erhöhung des Kreditrahmens initiieren. Und im Gegensatz zu Mobiltelefonen, die Bilder von Kunden- und Finanzdaten erfassen können, bieten YubiKeys eine sichere und konforme Authentifizierungslösung.

5. Sicherheit für gemeinsam genutzte Arbeitsplätze/Terminals

In Banken und Callcentern ist es üblich, dass Mitarbeiter an gemeinsam genutzten Arbeitsplätzen und Geräten arbeiten. Mitarbeiter wechseln von einem Arbeitsplatz zum nächsten, und Vorgesetzte autorisieren an verschiedenen Arbeitsplätzen Transaktionen. Nutzer in diesen Umgebungen sind häufig Teilzeitmitarbeiter mit höherer Fluktuationsrate und zeigen möglicherweise nur minimale Leistungsbereitschaft für das Unternehmen, wodurch sie zu Insider-Bedrohungen werden. Der YubiKey gewährleistet eine starke Authentifizierung über gemeinsam genutzte Terminals, Arbeitsplätze und Geräte hinweg, um unbefugten Zugriff auf Systeme und Ressourcen von hohem Wert zu verhindern.

6. Sicherheit für vermögende Kunden

Im Vergleich zu Benutzernamen und Passwörtern, SMS und OTP-Codes bieten YubiKeys höchste Sicherheit, um Bankkunden sowie Online- und Mobile-Banking-Konten vermögender Kunden vor Kontoübernahmen zu schützen. Indem Finanzdienstleistungsunternehmen Kunden eine einfach zu verwendende, starke Authentifizierung bereitstellen, können sie leichter neue Kunden akquirieren und die Kundenbindung festigen. Die YubiKey-Unterstützung lässt sich einfach in Online- und Mobile-Banking integrieren. Finanzdienstleistungsunternehmen wie Vanguard, Morgan Stanley und KeyBank bieten kundenorientierte, starke Authentifizierungslösungen, die FIDO-Hardware-Sicherheitsschlüssel unterstützen.

Einfache Beschaffung und Bereitstellung skalierbarer YubiKey-Authentifizierungslösungen

Yubico bietet flexible und kostengünstige Pakete, die Unternehmen mit 500 oder mehr Benutzern eine Umstellung von veralteter und defekter MFA auf skalierbare Phishing-resistente Authentifizierung ermöglicht.

Mit der YubiEnterprise Subscription profitieren Unternehmen von einem vorhersehbaren OPEX-Modell, von Flexibilität in den gewünschten Benutzereinstellungen bei jedem beliebigen YubiKey, von Upgrades auf die neuesten YubiKeys und schnelleren Rollouts mit einfachem Zugriff auf den Bereitstellungsdienst sowie Priority Support.

Abonnementkunden haben außerdem, durch den Kauf, Anspruch auf zusätzliche Services wie eine weltweite Lieferung durch vertrauenswürdige Partner.

Bewährter und führender Authentifizierungsanbieter

Yubico ist der Haupterfinder der WebAuthn-/FIDO2- und U2F-Authentifizierungsstandards, die von der FIDO Alliance übernommen wurden. Es ist das erste Unternehmen, das den U2F-Sicherheitsschlüssel und einen FIDO2 Authentifikator mit mehreren Protokollen produziert hat.

Die YubiKeys werden in den USA und in Schweden produziert, um die Sicherheit und Qualitätskontrolle über den gesamten Produktionsprozess zu gewährleisten.

Die YubiKey 5 Serie

Von links nach rechts: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano und YubiKey 5C Nano

Kontaktieren Sie uns
yubi.co/kontakt

Erfahren Sie mehr
yubi.co/yk5-de

[1] IBM Cost of a Data Breach Report 2023

[2] Forrester, The Total Economic Impact of Yubico YubiKeys

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) ist Erfinder des YubiKey, dem Goldstandard für eine Phishing-resistente Multi-Faktor-Authentifizierung (MFA), und hat wesentlich zur Entwicklung der offenen FIDO-Authentifizierungsstandards beigetragen. Das Unternehmen ist ein Pionier bei der Bereitstellung einer hardwarebasierten Passkey-Authentifizierung für Kunden in über 160 Ländern. Für weitere Informationen besuchen Sie uns bitte unter yubico.com