yubico

Mobile MFA lockt Cyberkriminelle

Phishing-resistente MFA, in Form des YubiKeys, kann es richten.

Wir befinden uns an einem kritischen Punkt der Cybersicherheit. Während der COVID-Gesundheitskrise stiegen die Cyberangriffe um 300 %.[1] Im Jahr 2020 forderte Ransomware alle 10 Sekunden ein neues Opfer,[2] und die Zahl der Phishing-Vorfälle verdoppelte sich.[3] Die durchschnittlichen Kosten einer Datenschutzverletzung erreichten 2021 mit 4,24 Mio. US-Dollar ein 17-Jahres-Hoch.[4]

Trotz der zunehmenden Flut und Raffinesse von Cyberangriffen verwenden viele Unternehmen weiterhin herkömmliche Methoden der Multi-Faktor-Authentifizierung (MFA) wie Benutzernamen und Passwörter sowie mobile Authentifikatoren, um den Zugriff auf kritische und sensible Anwendungen und Daten zu sichern. Die Ergebnisse sind bei allen Unternehmen unerwartet: Angriffe, die ihre Abwehr durchdringen, und Mitarbeiter, die frustriert sind.

Warum die mobile Authentifizierung Ihr Unternehmen gefährdet

Zwar bietet jede Form der MFA mehr Sicherheit als die herkömmliche Authentifizierung mit Benutzername und Passwort, doch sind nicht alle Formen der MFA gleich. Tatsächlich sind auf Mobilgeräten basierende MFA-Verfahren wie SMS, OTP und Push-Benachrichtigungen sehr anfällig für Phishing-Angriffe, Man-in-the-Middle-Angriffe (MiTM), Malware, SIM-Swapping und Kontoübernahmen.

Die Bequemlichkeit und Allgegenwärtigkeit von Mobilgeräten macht sie so anfällig für Phishing. Bei der diese Art von MFA gibt es keine Garantie, dass der private Schlüssel auf einem sicheren Speicher auf dem Mobilgerät landet. Mobilgeräte bieten eine große Angriffsfläche für Anwendungen, Kommunikation, Betriebssysteme und Technologien für sichere Elemente. Heutige Hacker kapern zunehmend OTP und Push-Benachrichtigungen durch Abfangen oder Phishing, wobei der Angreifer und die Übernahme des Kontos für den Nutzer nahezu unsichtbar sind.

Untersuchungen von Google, der NYU und der UCSD auf der Grundlage von 350.000 realen Hijacking-Versuchen haben gezeigt, dass SMS- und mobile Authentifizierungssysteme bei der Verhinderung von Kontoübernahmen und gezielten Angriffen nicht sehr effektiv sind.[5] Die Untersuchungen ergaben, dass ein SMS-basiertes Einmalpasswort (OTP) nur 76 % der gezielten Angriffe abwehrte und eine Push-App nur 90 %. Das entspricht einer Penetrationsrate von mindestens 10 %. Bei diesem Ansatz kommt es nicht darauf an, ob Sie angegriffen werden, sondern wann.

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

Abgesehen von der schwächeren Sicherheit bieten mobile Authentifikatoren auch keine einfache Benutzererfahrung. Bei der Authentifizierung mit SMS oder OTP für die Zwei-Faktor-Authentifizierung (2FA)/MFA müssen die Mitarbeiter auf per SMS oder Authentifizierungs-Apps zugestellte Codes warten und diese eingeben. All dies hängt von der Verfügbarkeit einer Mobilfunkverbindung, dem ausreichenden Ladezustand des Telefons und anderen Faktoren ab, die die Benutzererfahrung beeinträchtigen können. Dies erhöht den Zeitaufwand und die Komplexität der Authentifizierung und verringert die Produktivität der Mitarbeiter, während das Unternehmen ungeschützt bleibt.

[1] Rachel England, FBI Sees Cybercrime Reports Increase Fourfold During COVID-19 Outbreak, (April 20, 2020)

[2] Phil Muncaster, One Ransomware Victim Every 10 Seconds in 2020, (February 25, 2021)

[3] Internet Crime Complaint Center, 2020 Internet Crime Report, (March 17, 2021)

[4] IBM Security, Cost of a Data Breach Report, (July 28. 2021)

[5] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019)

Mobile Authentifizierung schafft auch Lücken in Ihrem MFA-Framework

Auch wenn Unternehmen der mobilfunkbasierten MFA Priorität einräumen oder sie sogar vorschreiben, gibt es fast immer Fälle von Mitarbeitern, die die mobile Authentifizierung nicht nutzen können oder wollen. Nicht nur, dass die Mobilfunkabdeckung in bestimmten geografischen Gebieten unzureichend sein kann, es kann auch sein, dass Mitarbeiter ihre privaten Geräte nicht für die Arbeit nutzen oder dem Administrator keinen Zugriff auf ihre Geräte gewähren möchten. Möglicherweise gibt es auch gewerkschaftliche Beschränkungen oder Compliance-Anforderungen, und manche Mitarbeiter sind womöglich nicht einmal in der Lage, ein Smartphone zu benutzen.

Wenn die Ausweichoption Benutzernamen und Passwörter sind, macht dies die Organisation noch anfälliger für Phishing und die Übernahme von Konten.

Da sich Unternehmen auf eine neue Arbeitsweise zubewegen, bei der Remote- und Hybridarbeit die Norm ist, ist es nicht mehr effektiv, sich alleine auf die Perimetersicherheit zu verlassen. Unternehmen, die heute mobilfunkbasierte Authentifikatoren verwenden, sollten in jedem Fal ihre langfristige MFA-Strategie überdenken und den Wechsel zu modernen, phishing-resistenten MFA-Lösungen in Betracht ziehen.

In diesen Szenarien bietet ein Hardware-Sicherheitsschlüssel Unternehmen eine breite Abdeckung von Geschäftsszenarien und Benutzergruppen und gewährleistet gleichzeitig die beste Sicherheit und Benutzerfreundlichkeit.

Aufbau einer sicheren, langfristigen MFA-Strategie

Um Ihr Unternehmen in hohem Maße phishing-resistent zu machen, sollten Benutzerkonten mit starker 2FA oder MFA gesichert werden, die speziell entwickelte Hardware-Sicherheitsschlüssel verwenden, um den Benutzerzugang mit dem stärksten Phishing-Schutz zu sichern und gleichzeitig die beste Benutzererfahrung zu bieten. Mit Hardware-Sicherheitsschlüsseln, die moderne Authentifizierungsprotokolle unterstützen, können Benutzer einen einzigen Sicherheitsschlüssel für Hunderte von Diensten registrieren, wobei für jeden Dienst ein eindeutiges öffentliches/privates Schlüsselpaar erzeugt wird. Die Geheimnisse werden niemals zwischen den Diensten ausgetauscht, und der private Schlüssel wird im sicheren Element auf dem Hardwareschlüssel gespeichert und kann nicht ex filtriert werden. Außerdem erfordern Hardware-Sicherheitsschlüssel, dass der Benutzer zur Authentifizierung eine Taste antippt oder berührt, um seine Anwesenheit nachzuweisen. Auf diese Weise verhindern Hardware-Sicherheitsschlüssel Fern-, MiTM- und Phishing-Angriffe. Anders als bei der Authentifizierung per SMS oder einer mobilen App darf nur der registrierte Dienst die Authentifizierungsanfrage initiieren.

[6] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019)

Unternehmen müssen auch die neuen und aktualisierten Vorschriften berücksichtigen, die in den nächsten Jahren erwartet werden, insbesondere infolge von COVID-19. Auch wenn die mobile Authentifizierung heute als „gut genug“ erachtet wird, erfüllt sie möglicherweise nicht die zukünftigen MFA-Compliance-Standards. Eine wirklich zukunftssichere Sicherheitsinvestition sollte ein Unternehmen für sichere und moderne Anmeldevorgänge, z. B. ohne Passwort, sowie für die langfristige Compliance rüsten.

YubiKeys bieten moderne phishing-resistente Authentifizierung im großen Maßstab und schlagen eine Brücke zur passwortlosen Anmeldung

Der YubiKey von Yubico ist ein Hardware-Sicherheitsschlüssel, der speziell für hohe Sicherheit entwickelt wurde, um Phishing und andere Formen der Kontoübernahme im Keim zu ersticken und eine starke Authentifizierung in großem Umfang zu ermöglichen.

Es ist die einzige Lösung, die nachweislich 100 % der Kontoübernahmen, einschließlich massenhafter und gezielter Phishing-Angriffe, verhindert.[6]

YubiKeys bieten eine moderne, starke MFA-Lösung, die den Anforderungen von Unternehmen für Büroangestellte, privilegierte Benutzer, Standortferne oder hybride Belegschaften, mobile eingeschränkte Umgebungen, gemeinsam genutzte Arbeitsplätze, Drittanbieter/Lieferkette und sogar Endkunden gerecht wird. Ein einzelner YubiKey funktioniert nahtlos in älteren und modernen Systemen und Anwendungen, mit Multiprotokoll-Unterstützung für Smartcard (PIV), OTP, OpenPGP, FIDO U2F und FIDO2/WebAuthn. Und für Unternehmen, die ihre Reise in die passwortlose Welt beginnen möchten, schlägt der YubiKey eine Brücke von der heutigen Situation zu einer modernen passwortlosen Zukunft, ohne dass ein Rip and Replace erforderlich ist.

Rüsten Sie Ihr Unternehmen mit einer zukunftssicheren Sicherheitsinvestition aus, die nicht nur eine hohe Sicherheit bietet, sondern Ihnen auch dabei hilft, die sich verändernde Compliance-Landschaft zu meistern. Die sicherheitsbewusstesten und risikoreichsten Organisationen der Welt vertrauen dem YubiKey für eine starke phishing-resistente Zwei-Faktor-, Multi-Faktor- und passwortlose Authentifizierung.

	Mobile Authentifizierung	YubiKey
Phishing-resistent	–	✓
Immer sicher	–	✓
Kostengünstig	–	✓
Benutzerfreundlich	–	✓
Rundum abgedeckt	–	✓
Zukunftssicher	–	✓

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.
530 Lytton Avenue,
Suite 301
Palo Alto, CA 94301
USA