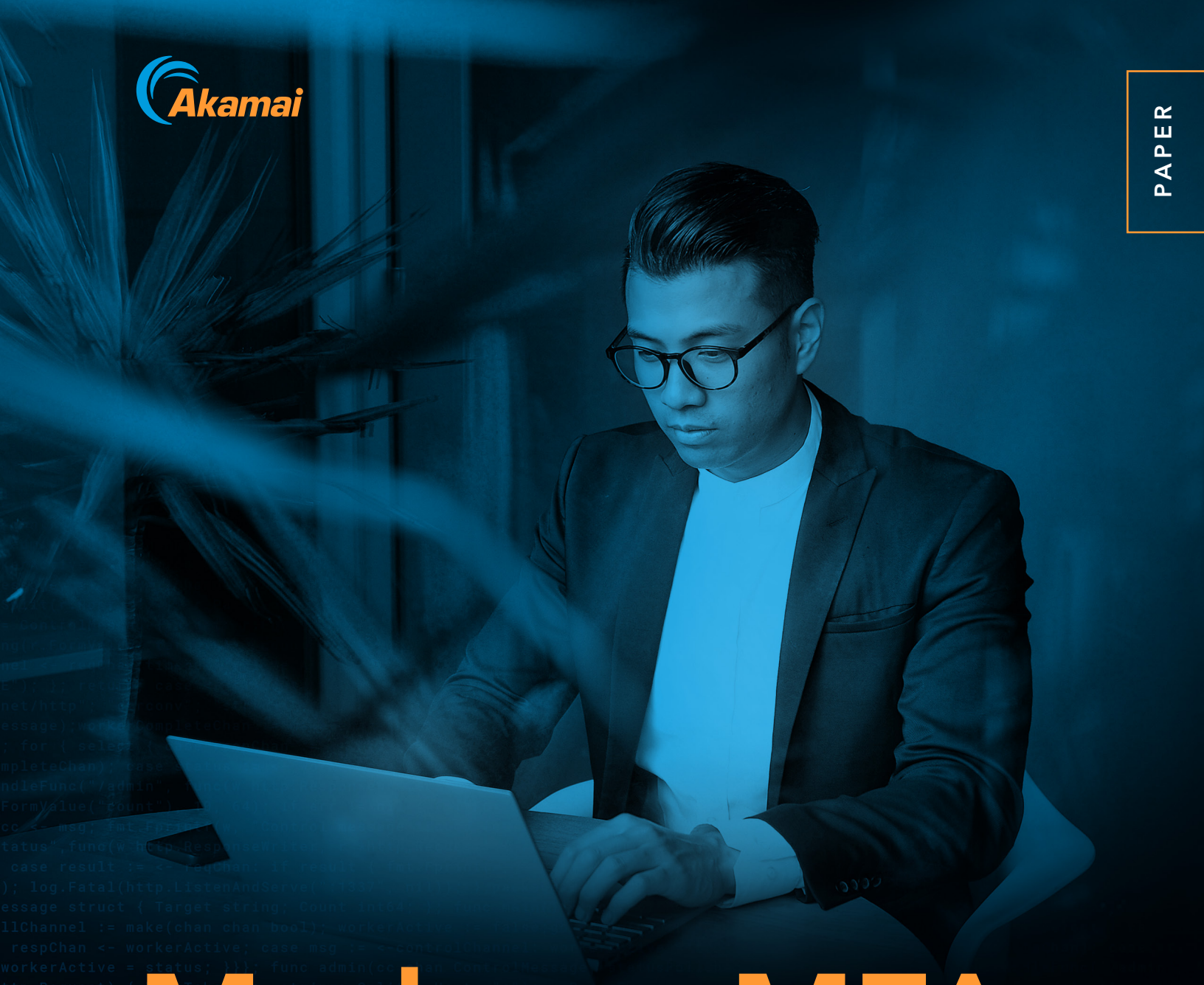
Akamai

PAPER



Moderne MFA – mehr Schein als Sein?

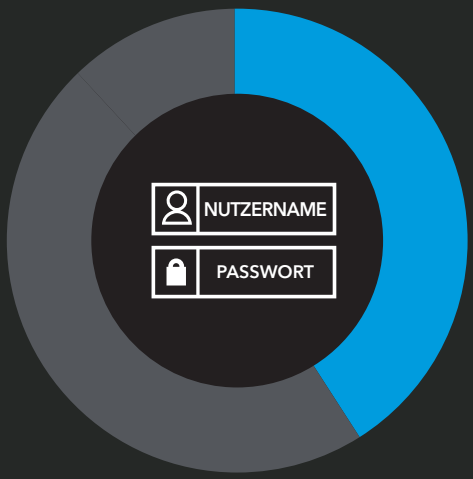
Nutzernamen und Passwörter reichen nicht aus

Bei 80 Prozent der Sicherheitsvorfälle kommen gestohlene Anmeldedaten zum Einsatz.[1] Zwar spielt hierbei meist die fehlende Kennwortsicherheit der Nutzer eine wichtige Rolle, doch auch Passwörter, die von Algorithmen generiert werden, können ein Problem darstellen.[2] Eine kürzlich im Dark Web durchgeführte Studie ergab, dass sich dort 15 Milliarden gestohlene Anmeldedaten aus 100.000 Angriffen im Umlauf befinden.[3]

Durch die Kombination aus digitaler Konnektivität, dem Einsatz von Cloudservices, der Verbreitung hybrider Umgebungen und der anhaltenden Nutzung von Passwörtern sind Nutzer für verschiedenste Angriffsvektoren anfällig:

- **Credential Stuffing**
- **Password Spraying und andere Brute-Force-Methoden**
- **Direktes Abgreifen von Anmeldedaten vor Ort und durch Insider**
- **Phishing und Social Engineering**
- **Keylogging**
- **Schädliche Proxy- und Antwortkampagnen**

Die globale Pandemie hat das Problem noch weiter verschärft und uns gezeigt, dass wir einen geräte- und standortunabhängigen Sicherheitsansatz benötigen. 100 Prozent der Sicherheitsvorfälle, die Anmeldedaten betreffen, treten auf, nachdem ein Nutzer authentifiziert wurde. Diese Tatsache beweist, dass Passwörter der Aufgabe sicherer Authentifizierung einfach nicht gewachsen sind.



Obwohl sie die Schwächen kennen, gehen 41 Prozent der Unternehmen weiterhin davon aus, dass Nutzernamen und Passwörter eine der effektivsten Methoden für Zugriffsmanagement sind.[4]

---

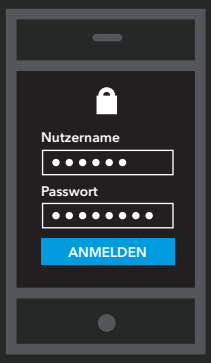
500 %

Studien von Akamai haben ergeben, dass Angriffe über Phishing, Social Engineering, Credential Stuffing und Brute Force zunehmen. Zwischen März und Mai 2020 haben wir einen Malware-Anstieg von 500 Prozent verzeichnet.

Die Vorteile von Multi-Faktor-Authentifizierung

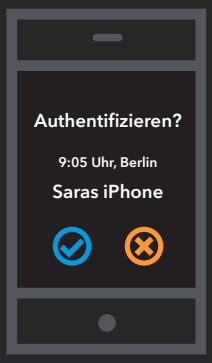
Angesichts der Situation ist es kaum überraschend, dass MFA-Technologie (Multi-Faktor-Authentifizierung) stetig an Beliebtheit gewonnen hat. Einfach ausgedrückt: MFA schützt Ihr Unternehmen, indem zur Bestätigung der Nutzeridentität mehr als eine Authentifizierungsquelle verwendet wird. Erst wenn beide validiert wurden, erhält der Nutzer Zugriff.

MFA erfordert eine erfolgreiche Kombination aus mindestens zwei der folgenden drei Authentifizierungsfaktoren:



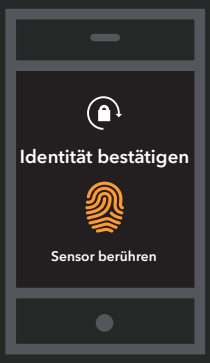
Etwas, das Sie wissen

Dieser Authentifizierungsfaktor ist informationsbasiert. Hierbei kann es sich um ein Passwort, eine PIN, die Antwort auf eine Sicherheitsfrage oder auch ein Piktogramm handeln.



Etwas, das Sie haben

Dieser Authentifizierungsfaktor basiert auf Token (Hard- oder Software). Hierbei kann es sich um eine Chipkarte oder einen Digitalschlüssel, ein einmaliges Passwort, eine Push-Benachrichtigung oder einen SMS-Code auf einem Mobilgerät handeln.



Etwas, das Sie ausmacht

Dieser Authentifizierungsfaktor ist kontext- oder biometriebasiert. Hierbei kann es sich um Verhaltens- oder Standortsignale, den Zeitpunkt, einen Fingerabdruck, Gesichts-, Stimm- oder Spracherkennung oder eine Unterschrift handeln.

Durch Implementierung einer MFA-Lösung können Sie das Risiko eines unautorisierten Zugriffs oder einer Kompromittierung Ihrer Systeme erheblich reduzieren. So sind erfolgreiche Angriffe bei Unternehmen, die MFA nutzen, um 99,9 Prozent weniger wahrscheinlich als bei Unternehmen, die darauf verzichten.[5] MFA ermöglicht und optimiert den sicheren Zugriff auf alle Umgebungen: Cloud, On-Premises, webbasiert, SaaS und IaaS. Eine MFA-Lösung stellt auch eine wichtige Komponente für die Migration der Unternehmenssicherheit zu Frameworks wie Zero Trust und SASE dar.

Durch Erweiterung der Authentifizierung über Nutzernamen und Passwörter hinaus, durch Vereinheitlichung des Anmeldevorgangs und durch Integration in andere cloudnative Sicherheitstools können MFA-Technologien die Nutzerproduktivität und -freundlichkeit steigern. Darüber hinaus werden durch die zentral verwaltete Authentifizierung viele Compliance-Anforderungen erfüllt.

Doch herkömmliche MFA ist nicht so sicher, wie Sie denken

Ein MFA-Service, der auf standardmäßigen Push-Benachrichtigungen basiert, kann von Hackern leicht manipuliert werden, um ein Konto zu übernehmen. Sofern der Service nicht durch zusätzliche Sicherheit ergänzt wird, sind Sie auch mit aktuellen MFA-Technologien Risiken ausgesetzt.

MFA ist eine Art der Netzwerksicherheit. Doch mit der Cloud und dem modernen Arbeitsstil lässt sich dieses Netzwerk nur schwer abstecken. MFA ist nicht darauf ausgelegt, Angriffe aufzuhalten, die nichts mit Logins zu tun haben. Die Technologie schützt nur die Anmeldung im Netzwerk, also den Vorgang, bei dem ein Nutzer Systemzugriff anfordert. Und Cyberkriminelle haben relativ einfache, aber äußerst effektive Methoden des Social Engineering und Phishing entwickelt, um diesen Schutz zu umgehen.

Stellen Sie sich folgendes Szenario vor:

1. **Ein Mitarbeiter wird durch Social Engineering dazu verleitet, seinen Nutzernamen und sein Passwort auf einer gefälschten Site einzugeben, die der Angreifer zwecks Phishing eingerichtet hat.**
2. **Nachdem er diese Anmeldedaten erhalten hat, kann der Angreifer sie im echten Loginportal eingeben.**
3. **Hierdurch wird eine Push-Benachrichtigung an das Handy des Mitarbeiters gesendet.**
4. **Der Mitarbeiter sieht die Push-Benachrichtigung als normalen Anmeldungsschritt und reagiert darauf.**
5. **Der Angreifer hat jetzt zwei Authentifizierungsfaktoren bestätigt und erhält Zugriff.**

Das ist die größte Schwachstelle standardmäßiger Push-Benachrichtigungen: Jeder Angreifer mit gestohlenen Anmeldedaten kann Benachrichtigungen generieren und an das Gerät des Mitarbeiters senden. In diesem Fall lässt sich der bevorstehende Sicherheitsvorfall nur verhindern, wenn der Mitarbeiter eine legitime Benachrichtigung von einem Betrugsversuch unterscheiden kann. Und selbst wenn diese Betrugsversuche 999 Mal erkannt werden – dem Angreifer reicht schon ein einziger erfolgreicher Versuch, um sich Zugriff zu verschaffen.

Phishing-sichere MFA

Eine wirklich sichere MFA-Lösung nutzt FIDO2-Standards. Das bedeutet unter anderem, dass die Sicherheit durch Technologie bereitgestellt wird und nicht länger von Nutzerentscheidungen abhängig ist.

Wie wird das erreicht? Die FIDO2-Standards umfassen eine Reihe von Methoden, um Phishing zu verhindern:

Zunächst einmal wird die Authentifizierungsanfrage (die MFA-Abfrage) immer an die Workstation gesendet, die die Zugriffsanfrage generiert hat. Der Browser auf dieser Workstation leitet die Authentifizierungsanfrage dann an lokal angeschlossene physische Sicherheitsschlüssel weiter. Für unser oben beschriebenes Szenario bedeutet das Folgendes: Der Angreifer kann den MFA-Service nicht mehr dazu bringen, eine Push-Benachrichtigung an das Handy des Mitarbeiters zu senden. Stattdessen wird die MFA-Abfrage direkt an die Workstation des Angreifers gesendet. Da der Angreifer nicht über den Sicherheitsschlüssel des Mitarbeiters verfügt, kann dieser auch nicht auf die Abfrage antworten. Die Kontoübernahme wird somit verhindert.

Definition: Authentifizierungsstandards und -spezifikationen

FIDO Alliance (Fast IDentity Online)

Die Gesellschaft, die für die Entwicklung und Nutzung von bzw. die Compliance mit den entsprechenden Authentifizierungsstandards verantwortlich ist.

FIDO2

Der allgemeine Begriff für die neuesten Authentifizierungsspezifikationen der FIDO Alliance; in der Sammlung sind die Standards CTAP1, CTAP2 und WebAuthn enthalten. Mit FIDO2 können Nutzer normale Geräte verwenden, um sich einfach bei Onlineservices zu authentifizieren – sowohl in mobilen als auch in Desktopumgebungen.

WebAuthn

Dieser Webstandard wird vom World Wide Web Consortium (W3C) entwickelt und stellt eine Kernkomponente von FIDO2 dar. Ziel des Projekts ist es, die Schnittstelle zur Authentifizierung von Nutzern bei Webanwendungen und -services über Public-Key-Verschlüsselung zu standardisieren.

Client to Authenticator Protocol (CTAP)

Diese Spezifikation wird von der FIDO Alliance entwickelt und ermöglicht die sichere Kommunikation zwischen einem mobilen Authentifikator (wie z. B. ein Smartphone) und einem internen Authentifikator (Client oder Plattform).

Die zweite Methode besteht darin, dass der Browser mit der Authentifizierungsanfrage Daten an den Sicherheitsschlüssel sendet. Diese Daten umfassen den Domainnamen des Ursprungs, der die Authentifizierungsanfrage laut Browserdaten gesendet hat. Wenn der Angreifer die empfangene Authentifizierungsanfrage einfach an die Mitarbeiter-Workstation weitergeleitet hat, enthalten diese Daten die Domain der Phishing-Site. Der Sicherheitsschlüssel würde erkennen, dass es sich bei der Domain, die den Zugriff anfordert, nicht um die ursprünglich registrierte Domain handelt, und würde die Antwort verweigern. Auch in diesem Fall wird der Angriff also abgewehrt.

Wenn phishing-sichere MFA möglich ist, warum wird sie dann nicht überall genutzt? Weil man hierfür physische Sicherheitsschlüssel benötigt, die kostspielig sind und einiges an Aufwand verursachen. Zumindest bisher.

Die nächste Generation der MFA an der Edge

Die IT muss bislang bei der Auswahl und Implementierung von MFA-Technologien Kompromisse eingehen. Um die bestmögliche Sicherheit zu erhalten, muss viel Geld in den Rollout von Hardware investiert werden, da jeder Mitarbeiter einen physischen Sicherheitsschlüssel benötigt. Zudem verursachen auch die Verteilung und Verwaltung der vielen Schlüssel einiges an Kosten. Und die IT-Abteilung muss jeden Nutzer von dem wenig ansprechenden Authentifizierungserlebnis überzeugen, das die Schlüssel bieten – schließlich stellen sie für viele nur lästige Hardware dar, auf die sie aufpassen müssen.

Die Alternative wäre eine geringere Sicherheit in Form komfortabler Push-Benachrichtigungen auf Mitarbeiter-Smartphones. Diese Methode verursacht keine zusätzlichen Kosten. Der geringe Aufwand dieser Alternative ist der Grund dafür, dass sie auch heute noch so häufig zum Einsatz kommt – und dafür, dass so viele Unternehmen anfällig für Angriffe sind.

Doch dieser Kompromiss zwischen Sicherheit und Kosten bzw. einfacher Nutzung gehört jetzt der Vergangenheit an.

Denn der Service Akamai MFA führt einen neuen Authentifizierungsfaktor ein und digitalisiert so die Sicherheit von FIDO2 nur mit einem Smartphone und einem Webbrowser. Darüber hinaus bietet der Service ein einfaches und vertrautes Erlebnis mit Push-Benachrichtigungen, mit dem jede Plattform als mobiler Authentifikator verwendet werden kann. Physische Sicherheitsschlüssel sind nicht erforderlich. Die Lösung stellt die sichersten Funktionen der FIDO2-Standards zu geringen Kosten bereit – mit einfacher Installation und Verwendung sowie Interoperabilität mit beliebten Identity Providern.

Schützen Sie Ihr Unternehmen mit Akamai MFA vor Phishing, Credential Stuffing und Kontoübernahmen. Erfahren Sie mehr über die einzigartige MFA-Technologie von Akamai und bereiten Sie sich auf eine sichere Zukunft ohne Passwörter vor.

Weitere Informationen erhalten Sie unter akamai.com/mfa.

Quellen:

1. https://enterprise.verizon.com/resources/reports/dbir/
2. https://www.infosecurity-magazine.com/opinions/problem-password-everything-1/
3. https://www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/?sh=27fa6368180f
4. https://www.businesswire.com/news/home/20200616005047/en/Weakest-Link-Prevails-Overreliance-Passwords-Continues-Compromise
5. https://www.hipaajournal.com/multi-factor-authentication-blocks-99-9-of-automated-cyberattacks/