Zugangssicherheit-2FA, MFA und FIDO2

Zugangssicherheit: 2FA, MFA und FIDO2

Das Passwort hat eigentlich ausgedient, weil mit FIDO2 ein phishingresistentes Log-in-Verfahren existiert. Wie das funktioniert und warum das eher eine Lösung für übermorgen als für morgen ist.

Von Jürgen Seeger

-tract

- Zwei-Faktor-Authentifizierung (2FA) erhöht die Sicherheit signifikant, ist für Onlinekäufe und Finanztransaktionen sogar vom Gesetzgeber vorgeschrieben.
- Nicht alle 2FA-Verfahren sind sicher, so wurden Accounts, die durch eine per SMS gesendete PIN gesichert waren, Opfer von Phishingangriffen.
- Phishingresistent ist FIDO2, ein Standard, der statt der Übermittlung von Passwörtern ein sicheres Public-Key-Verfahren definiert.

Sicherheit und Zugänglichkeit sind bekanntlich konkurrierende Anforderungen: Je sicherer, desto unbequemer. Logisch also, dass viele – wenn nicht die meisten – Benutzer schlampig mit ihren Passwörtern umgehen. Seien es die berühmt-berüchtigten Zettel unter der Tastatur, Trivial-Passwörter à la „12345678“, immerwährend gleiche Phrasen für verschiedene Zugänge oder der Vorname der Tochter. Daran haben bislang auch erzieherische

Maßnahmen wie der Welt-Passwort-Tag – jedes Jahr am ersten Donnerstag im Mai – wenig geändert.

Wer nationale Gedenktage mag, der kann am Änderere-dein-Passwort-Tag am 1. Februar alljährlich alle, so wirklich die Aufforderung, Passwörter ändern. Dabei ist das BSI von seinem Rat, man möge Passwörter häufig ändern, bereits 2020 abgerückt. Denn das führe nur zu einfachen und somit unsicheren Passwörtern. Hintergrund: Ist ein Bruce-Force-Angriff auf ein zehn Zeichen langes Passwort aus dem Ziffernraum von 0 bis 9 in 10 Sekunden erledigt, dauert dies bei gleicher Rechenleistung bei einem Zeichenraum von 96 (Klein- und Großbuchstaben, Ziffern, Sonderzeichen) über 2000 Jahre. Dabei ist das „Erraten" von Passwörtern mittels automatisierten Ausprobierens oder Wörterbüchern nur eine Variante der Kompromittierung von Zugangsdaten. Sie können auch schlicht abgefangen oder via Social Engineering beziehungsweise Phishing ausspioniert werden. Hinzu kommt die Arbeitsbelastung auf der Serviceseite: Anrufe wegen vergessener Credentials, Mechanismen zum Übermitteln neuer Passwörter und so fort.

Langer Rede kurzer Sinn: Allein die Kombination von Accountnamen und Passwort ist weder sicher noch bequem oder effizient. Ein weiteres Kennwort oder Merkmal zu fordern ist zumindest aus der Sicherheitsperspektive betrachtet eine auf der Hand liegende Idee, also eine Zwei- oder Mehr-Faktor-Authentifizierung (2FA/MFA). Zudem sollte dieser zweite Faktor nicht dauerhaft kompromittierbar sein, weil er nur für ein Log-in oder für einen begrenzten Zeitraum gilt.

Wenn es um Geld geht, ist 2FA vorgeschrieben

Das hat auch der deutsche Gesetzgeber erkannt und für den Zahlungsverkehr 2FA-Verfahren vorgeschrieben. Dabei wurden zum Teil offene Türen eingerannt, denn die Übermittlung einer

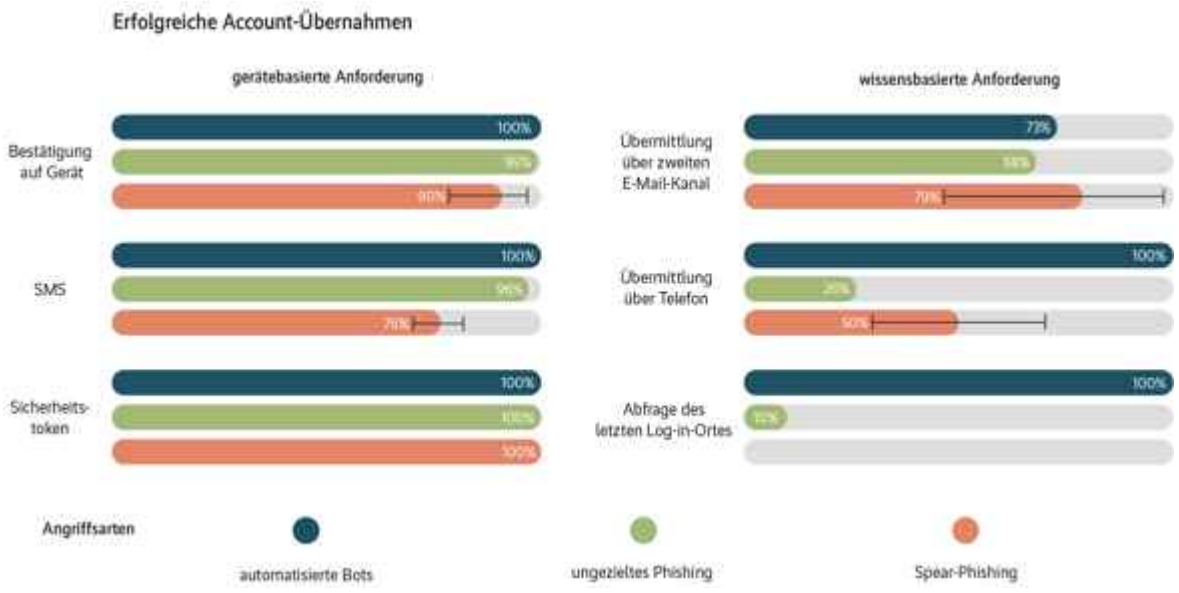
Transaktionsnummer für Zahlungen ist seit Jahren nicht nur gängige Praxis der Kreditinstitute, sondern wurde schon am 14. September 2019 verpflichtend durch die EU-Zahlungsdiensterichtlinie PSD2. Jedenfalls ist seit dem 15. März 2021 2FA für alle Onlinezahlungen, also etwa auch beim Kauf im Webshop, obligatorisch, eine erste Stufe dieser Vorschrift galt schon seit dem 15. Januar 2021. Ob und inwieweit der durch die DSGVO vorgeschriebene Schutz persönlicher Daten durch den Stand der Technik zwingend eine 2FA-Zugangssicherung nach sich ziehen wird, ist derweil noch Zukunftsmusik.

Zur konkreten Ausgestaltung des zweiten Faktors gibt es mehrere Möglichkeiten. Grob unterscheiden lassen sich Besitz eines Gerätes oder Merkmals, das Wissen um ein temporäres Geheimnis sowie Kombinationen davon. Biometrische Merkmale können durch einen Fingerabdruck- oder Iris-Scanner, Gesichts- oder Stimmerkennung verifiziert werden. Die diesen Verfahren inhärenten Risiken für den Anwender (Stichwort: abgeschnittener Finger) werden durch Lebenderkennung zu vermeiden versucht. Beim Faktor Besitz kann es sich um ein dediziertes Gerät handeln, das ein temporäres Passwort generiert. RSA stellte solch ein System unter dem Namen SecurID bereits 1986 vor; mittlerweile existieren zahlreiche Gerätchen, die zeitbasiert oder angestoßen durch zum Beispiel den Scan eines eigens dazu erzeugten QR-Codes ein Einmalpasswort generieren. Inzwischen sind diese Geräte oft durch das Mobiltelefon abgelöst worden, auf dem eine spezielle App läuft. Dass das zweite Merkmal nicht auf demselben Gerät, mit dem man sich einloggen will, erzeugt werden sollte, versteht sich von selbst (und wird auch vom BSI ausdrücklich empfohlen).

Der Vollständigkeit halber sei erwähnt, dass als eine Kombination von Besitz und Wissen auch die Übermittlung des zweiten Passworts über einen separaten Kanal gelten kann, also über eine zweite E-Mail-Adresse oder via SMS. Beides gilt als

nicht sehr sicher, denn diese Nachrichten können abgefangen werden. So hat vor einer Übermittlung durch SMS-Nachrichten das für die Sicherheit von US-Behörden zuständige National Institute for Standards and Technology (NIST) bereits 2016 gewarnt. Die weithin bekannt gewordenen 2FA-Hacks betrafen denn auch SMS als zweiten Faktor: 2018 wurde das Portal Reddit durch Abfangen einer SMS gehackt, 2021 die Kryptobörse Coinbase.

Google hat 2019 auf einer Webkonferenz die Ergebnisse einer Langzeitstudie zum Thema Sicherheit von 2FA-Verfahren veröffentlicht. Diese unterschied zwischen automatisierten Bot-Attacken, ungezieltem und gezieltem Phishing sowie zwei Arten von 2FA: geräte- und wissensbasiert. Das Ergebnis der Studie ist eindeutig: Bot-Attacken wurden durch fast alle 2FA-Verfahren vollständig abgewehrt (siehe Abbildung 1). Am schlechtesten schnitt die Übermittlung des zweiten Kennworts via E-Mail ab, aber auch die half schon gegen drei Viertel der Bot-Angriffe. Gegen ungezieltes Phishing lag die Abwehrrate der gerätebasierten Verfahren nahe bei 100 Prozent. Sogar gegen Spear-Phishing, gezielte Angriffe auf einzelne Accounts, erwiesen sich die gerätebasierten Verfahren als signifikant erfolgreicher, mit Abstand am besten schnitten Security-Token ab (siehe dazu auch den Test von vier ausgewählten Token im Artikel „Vier FIDO2-Token für den USB-Port“ ab Seite 50).



Klarer Sieger im Abwehrspiel: Security-Token konnten alle Arten von Angriffen abwehren (Abb. 1). *Google*

HOTP und TOTP

Zur Generierung von Einmalpasswörtern existieren zwei Verfahren, bezeichnet als HMAC-based One-time Password (HOTP) und Time-based One-time Password (TOTP). HOTP ist ereignisgesteuert, aus einem Server und Client bekannten gemeinsamen Geheimnis und einem bei der Registrierung synchronisierten Zähler wird auf beiden Seiten durch den Keyed-Hash Message Authentication Code ein Schlüssel erzeugt, der übereinstimmen muss. Der Zähler wird bei jeder Authentifizierung hochgezählt.

Durch HOTP generierte Passwörter haben kein inhärentes Verfallsdatum. Der Client kann den Zähler bei einem fehlgeschlagenen Log-in hochsetzen. Um sich weiterhin mit dem Server abgleichen zu können, geht dieser nicht von einem fixen Zählerstand aus, sondern von einem Bereich, dem Validierungsfenster. Ist dieses zu groß, gibt das Angreifern die Gelegenheit zum Erraten des OTP. Ist es zu klein, müssen Client und Server erneut synchronisiert werden.

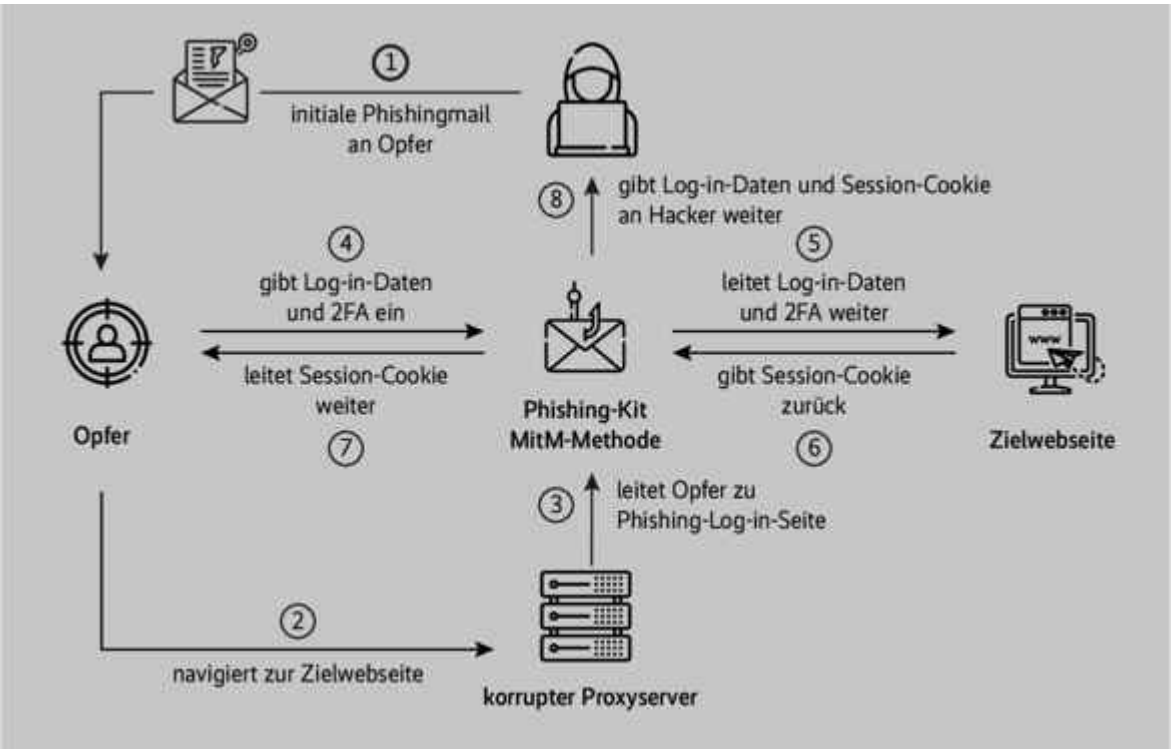
Beim neueren TOTP wird statt eines Zählers die Uhrzeit benutzt, die Gültigkeitsdauer des generierten Passworts ist implementierungsabhängig. Auch hier stehen sich Bequemlichkeit, also ein langer Zeitraum, und Sicherheit, eine kurze Gültigkeitsdauer, gegenüber. Laufen die Uhren auf Client und Server auseinander, steht eine neue Synchronisierung an.

Das generierte Einmalpasswort kann im Klartext angezeigt, via Telefon oder Mail übermittelt oder als QR-Code präsentiert werden.

MFA hilft, ist aber kein Allheilmittel

2FA beziehungsweise MFA hilft also auf jeden Fall. Aber leider ist es kein Allheilmittel. Denn im ständigen Wettlauf zwischen

Sicherheitsimplementierungen und Angreifern ist eine Schwachstelle im 2FA-Konzept aufgefallen: Was passiert eigentlich, wenn die den zweiten Faktor anfordernde Stelle nicht die ist, für die sie sich ausgibt? Es geht um eine Variante des Man-in-the-Middle-Angriffs (MITM), bei der eine zwischengeschaltete Stelle die Informationen abfängt, zwischen Client und Server hin- und herleitet und zwischenspeichert (siehe Abbildung 2). Es gibt dafür seit ein paar Jahren fertige MITM-Pakete wie Evilginx, Muraena oder Modlishka. Eine Suche nach „2fa bypass“ bei GitHub ergab beim Schreiben dieser Zeilen über 40 Treffer, in einer Veröffentlichung der Sicherheitsfirma Malwarebytes Labs ist von 1200 Toolkits zum Umgehen von 2FA-Verfahren die Rede.



Kommunikation abgefangen: Das MITM-Tool leitet auch den zweiten Faktor hin und her (Abb. 2).

Man kann zwar den Erfolg von Phishingangriffen durch Schulungen und Aufmerksamkeitskampagnen unwahrscheinlicher machen. Also klarstellen, dass vor einem Mausklick das Ziel genau geprüft werden soll et cetera. Die grundsätzlichere Lösung besteht aber im Errichten einer Verbindung zwischen Client und Server, bei der sich beide Seiten ausweisen. Und genau das macht FIDO, aufgelöst Fast Identity Online, aktuell

gilt FIDO Version 2 (FIDO2). Das „Fast“ hängt damit zusammen, dass man bei FIDO2 überhaupt kein Passwort mehr eingeben muss, sich also schnell einloggt und sich alle Debatten um sichere Passwörter erledigt haben. Damit hat sich das eingangs erwähnte Dilemma „je sicherer, desto unbequemer“ weitgehend in Wohlgefallen aufgelöst, FIDO ist sowohl sicher als auch bequem.

Public/Private Keys statt Passwörtern

Statt auf die Übermittlung von Passwörtern setzt FIDO2 auf ein Public-Private-Key-Verfahren. Dazu bedarf es eines Authenticator, Software mit Zugriff auf einen dedizierten Chip (Token), auf einem Mobiltelefon oder einem PC mit TPM-Baustein, derzeit unter Android und iOS beziehungsweise macOS und Windows 10/11. Dieser Authenticator identifiziert sich durch ein nicht extrahierbares Geheimnis, etwa eine Zahlenfolge, und ist gebunden an das Gerät. Aus einer Kombination dieser Zahlenfolge und der Internetadresse der Gegenstelle, des Servers, generiert er ein asymmetrisches Schlüsselpaar, bestehend aus privatem und öffentlichem Schlüssel.

Bei der Registrierung speichert der Server des Dienstes den öffentlichen Schlüssel, nicht mehr wie bisher Accountname und Passwort. Der Server verwahrt also auch keine Geheimnisse mehr, die missbraucht werden können. Der private Key verlässt nicht den Authenticator und muss dort nicht einmal gespeichert sein, wahlweise kann das Schlüsselpaar bei jedem Kontakt zum Server neu erzeugt werden.

Bei einem Log-in-Wunsch schickt der Server eine sogenannte Challenge, eine sich bei jedem Log-in ändernde Zeichenfolge, die der Authenticator mit dem privaten Schlüssel signiert und zurückschickt. Der Server überprüft mittels des bei der Registrierung hinterlegten öffentlichen Schlüssels die Gültigkeit der Signatur und gibt im positiven Fall dem Log-in-Wunsch statt. Dieser Vorgang wird bei jedem Log-in-Wunsch

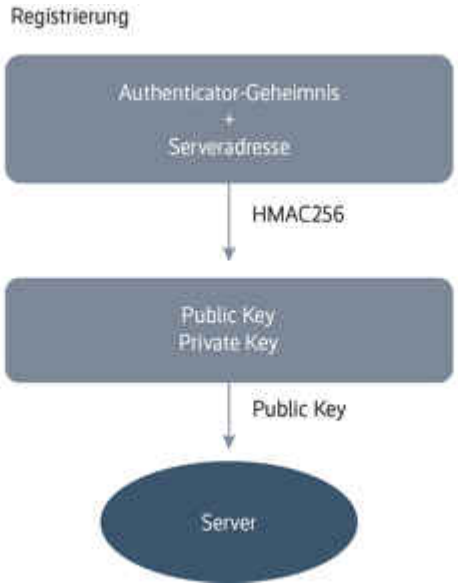
wiederholt, es wird für jeden Server ein jeweils eigenes Public-Private-Paar generiert. Da die Serveradresse in die Schlüsselerzeugung eingeht, ist eine Umleitung auf einen anderen Server nicht möglich. Damit ist der übliche Weg für Phishingattacken versperrt.

Das Übersenden der signierten Challenge muss vom Benutzer bestätigt werden, durch einen biometrischen Abgleich oder eine PIN. Nichts davon geht über die Leitung, diese Daten verwendet nur der Authenticator als Sendegenehmigung. Worin diese besteht, wird beim Registrierungsprozess festgelegt. Bliebe die Möglichkeit, dass ein Trojaner den Authenticator steuert. Das ist bei einem dedizierten Token, das etwa einen Fingerabdruck zum Senden der signierten Challenge fordert, allerdings schwer vorstellbar. FIDO2 kann als alleiniges, passwortfreies Authentifizierungsverfahren eingesetzt werden oder zusätzlich zum vorhandenen Log-in-Prozedere, im letzteren Fall ist die Abfrage einer Sendegenehmigung optional.

Zur Generierung des Schlüsselpaars kommt wie bei HOTP und TOTP Keyed-Hash Message Authentication Code (HMAC-SHA256) zum Einsatz, für das Signieren der Challenge das auf elliptischen Kurven beruhende ECDSA P-256. Dass optional auch das veraltete RSA weiterhin mitspielen darf, wird in Sicherheitskreisen kritisiert.

FIDO2 wurde 2019 veröffentlicht und fasst die Standards FIDO und U2F (Universal Second Factor) zusammen. Definiert sind zwei APIs, WebAuthn auf Client- und Serverseite sowie CTAP, das Client-to-Authenticator Protocol zur Verbindung des Authenticators mit einem Webbrowser oder einem anderen Client. Für beide Standards ist der Code offengelegt und auf GitHub in verschiedenen Implementierungen und Programmiersprachen verfügbar, derzeit für Android, iOS, macOS und Windows 10/11 sowie die Browser Chrome, Edge, Firefox und Safari. Der Standard wird vom W3C und einer breiten Allianz von Behörden und Firmen unterstützt, von Apple und Amazon über Intel und Microsoft bis Visa und Yahoo. Auch das deutsche BSI und das

US-Pendant NIST sind bereits seit 2015 Mitglied.



Mit FIDO2 gehen weder bei der Registrierung noch … (Abb. 3a) *ss*

… beim Log-in geheime Daten über die Leitung (Abb. 3b).

Genügend Gründe für einen baldigen Erfolg eigentlich. Wären da nicht die Beharrlichkeit von Benutzern und die notorische Sparsamkeit der Geschäftsführungen. Denn ein Log-in mit Benutzername und Passwort ist seit Jahren eingeübt und auch nicht langsamer als das passwortlose FIDO2-Verfahren, zumindest wenn man einen Passwortmanager nutzt. So ist bei einem Log-in via Webbrowser, der die Zugangsdaten gespeichert hat, häufig nicht einmal der Griff zur Tastatur nötig – zwei bestätigende Mausklicks reichen. Hinzu kommt die Angst vor Schlüsselverlust. Diese war in einer Untersuchung der Universität Bochum zur Akzeptanz von FIDO2-Token der von den Testpersonen meistgenannte Grund für ein Beharren auf den gewohnten Log-in-Verfahren. Hier kommt auch die Kostenfrage ins Spiel. Denn das Budgetargument ist nicht mit dem Verweis

auf die relativ günstigen USB- oder NFC-Token vom Tisch, und auch nicht mit dem Hinweis auf die ohnehin vorhandenen Smartphones oder PCs mit Authenticator-Funktionalität. Die eigentlichen Belastungen entstehen im Ausrollen von FIDO2 nebst Verfahren zum Ersatz verlorener Token, und eine firmen- oder behördeninterne Akzeptanzkampagne dürfte dazukommen.

Passkeys – alles wird noch einfacher?

Mit FIDO2 muss man jeden Dienst auf einem Gerät mit Authenticator-Funktionalität registrieren, oder ein entsprechendes Token dabei haben, ein sogenanntes Roaming-Device. Hier kommt die im Mai 2022 von Apple, Google und Microsoft vorgestellte FIDO2-Erweiterung Passkeys ins Spiel (siehe Artikel „Das Passwort ist tot – es leben die Passkeys“ ab Seite 46, Demo-Site: Passkeys.io). Bei diesem Verfahren wird das bei der Registrierung erzeugte Schlüsselpaar in der Hersteller-Cloud hinterlegt, der private Schlüssel verlässt also den Authenticator-Client. So kann man dann einfach einen weiteren Dienst integrieren oder ein verlorenes Token ersetzen. Vorausgesetzt, man kennt noch die Credentials für die Hersteller-Cloud. Also Benutzername, Passwort und irgendeinen zweiten Faktor. Den FIDO-Segen erhielt das Verfahren durch die Erweiterung Multi-Device FIDO Credentials.

So verlassen natürlich die privaten Schlüssel entgegen der ursprünglichen FIDO-Intention den Client, es liegen doch wieder sensible Daten in der Cloud. Immerhin haben sich kurze Zeit nach der Vorstellung von Passkey Apple und Google darauf verpflichtet, die privaten Schlüssel der Benutzer so zu speichern, dass die Konzerne darauf keinen Zugriff haben. Ende 2022 ist auch Microsoft mit diesem Versprechen nachgezogen.

Für den Zugang zum Firmennetz ist Passkeys (noch?) keine Option. Hier wird man mit dem Ausrollen von FIDO2-Mechanismen zum Umgang mit verlorenen oder zerstörten Schlüsseln aufsetzen müssen. (js@ix.de)

1. Quellen
2. Verweise auf die Dokumente der FIDO-Allianz, den Code bei GitHub, den Usenix-Talk zur 2FA-Akzeptanz und die Google-Studie zur Wirksamkeit von 2FA-Maßnahmen sind unter ix.de/zy24 zu finden.