Zweite Abwehrreihe

Logins mit Authenticator zusätzlich absichern

Um Zugänge bei Internetdiensten per Zwei-Faktor-Authentifizierung zu schützen, gibt es kostenlose Authenticator-Apps und erschwingliche Hardware. Mit geringem Aufwand verbessern Sie damit das Sicherheitsniveau ganz erheblich, ohne sich bei Geräteverlust für immer auszusperren.

Von Markus Montz

Auch das beste Passwort hat einen entscheidenden Nachteil: Errät oder erbeutet es ein Mensch mit sinistren Absichten, kann er sensible Daten ausspähen oder seinen Opfern direkt schaden, zum Beispiel finanziell oder sozial. Mit einer Zwei-Faktor-Authentifizierung (2FA) machen Sie Cyberkriminellen solche Einbrüche deutlich schwerer, denn zusätzlich zum Passwort müssen diese Zugang zu einem zweiten Kanal bekommen.

Ein einfacher und preisgünstiger Weg ist ein dynamisch erzeugtes, zeitlich begrenzt gültiges Einmalpasswort – ein sogenanntes TOTP (Time-based One-Time Password). Idealerweise wird dieses auf einem getrennten Kanal generiert, etwa durch eine Software, die auf einem zweiten, vom ersten unabhängigen Gerät arbeitet. Doch selbst wenn beide Kanäle auf dem gleichen Gerät liegen, beispielsweise einem Smartphone, kann ein Angreifer zumindest nicht ohne Zugriff auf dieses Gerät zum Ziel kommen. Das bekannteste Beispiel für diesen Ansatz ist die TAN (Transaktionsnummer) im Onlinebanking: Mithilfe einer Smartphone-App oder eines dedizierten Gerätes, manchmal auch noch in Verbindung mit einer Chipkarte, müssen Sie Überweisungen oder Logins durch die zusätzliche Eingabe eines Zahlencodes absichern.

Nach dem gleichen Prinzip können Sie Mailkonten, Cloudzugänge, soziale Medien, einige Onlinehändler und etliche weitere Dienste besser vor unbefugtem Zugriff schützen. Gerade bei Ihren Mailkonten lohnt sich das: Wer die knackt, kann im schlimmsten Fall Ihre Passwörter bei Onlineshops, Messengern oder sozialen Medien zurücksetzen, Sie aussperren und reichlich Schindluder treiben.

Um eine TOTP-basierte 2FA einzurichten, bieten sich sogenannte Authenticator an. Diese gibt es ebenfalls als App für das Smartphone oder als dedizierte Hardware. Zwar ist auch die mitunter angebotene SMS als TOTP-Kanal besser als gar keine 2FA. Allerdings ist ihr Schutzniveau mangels Verschlüsselung und dem für Kriminelle relativ leichtem Zugang zu Zweit-SIM-Karten (SIM-Swapping) niedriger. Alternativ können Sie auch Krypto-Sticks wie die Yubikeys zum Generieren der TOTP-Codes nutzen [1]. Das hat den Vorteil, dass die genutzten Geheimnisse auf einem geschützten Chip gespeichert werden. Dort sind sie nicht auslesbar und somit auch nicht duplizierbar.

Einrichten und nutzen

Ein softwarebasiertes TOTP wird aus zwei Teilen erzeugt. Bei der Einrichtung der 2FA erhält die App oder Hardware zunächst vom Server des Dienstes ein Geheimnis (Shared Secret Key), das nur diese beiden Parteien kennen. Um daraus das TOTP zu generieren, fließt zusätzlich die aktuelle Unix-Zeit ein, also die seit 1. Januar 1970 um 0 Uhr UTC verstrichene Zeit in Sekunden. Daraus berechnen beide Seiten einen 30 Sekunden lang gültigen kryptografischen Hashwert, aus dem das TOTP destilliert wird. Das ist meist ein sechsstelliger Zahlencode [2].

Es gibt diverse kostenlose Authenticator-Apps, die allesamt diese Aufgabe erfüllen. Welche Sie nehmen, ist eine Frage des persönlichen Geschmacks. Am bekanntesten sind die Apps von Google und Microsoft sowie Authy von Twilio. Es gibt Open-Source Lösungen wie andOTP und Free OTP; KeePass-Nutzer können das darin enthaltene TOTP-Modul verwenden (Links unter ct.de/yd2q). Wichtig ist, dass sich Ihr Smartphone nur durch PIN, Passwort oder biometrisch entsperren lässt, sollte das Gerät einmal in die falschen Hände geraten – auch wenn manche Apps zusätzlich einen eigenen PIN- und Biometrieschutz bieten. Dies gilt insbesondere, wenn es sich um einen Passwort-Manager auf dem Smartphone handelt, der Passwörter *und* die dazu passenden TOTP-Codes ausspuckt.

Alternativ gibt es Hardware wie den Reiner SCT Authenticator (ab 32 Euro) [3]. Auch hier ist die Auswahl nicht auf einen Hersteller beschränkt. Der Vorteil der autarken Hardware ist, dass sie anders als ein Smartphone nicht aus dem Internet erreichbar und somit nicht angreifbar ist. Achten Sie darauf, das Gerät mit einer PIN zu schützen.

Eine 2FA per TOTP können Sie beispielsweise bei Google, Samsung und Microsoft, Maildiensten wie Posteo und GMX, sozialen Netzwerken wie Twitter und Facebook, Bezahldiensten und Shops wie PayPal und Amazon, diversen Webhostern sowie vielen Kryptobörsen einrichten.

Alternativ zu einer Smartphone-App können Sie auch einen Hardware-Authenticator nutzen. Das Angebot an solchen Gadgets ist bisher aber überschaubar.

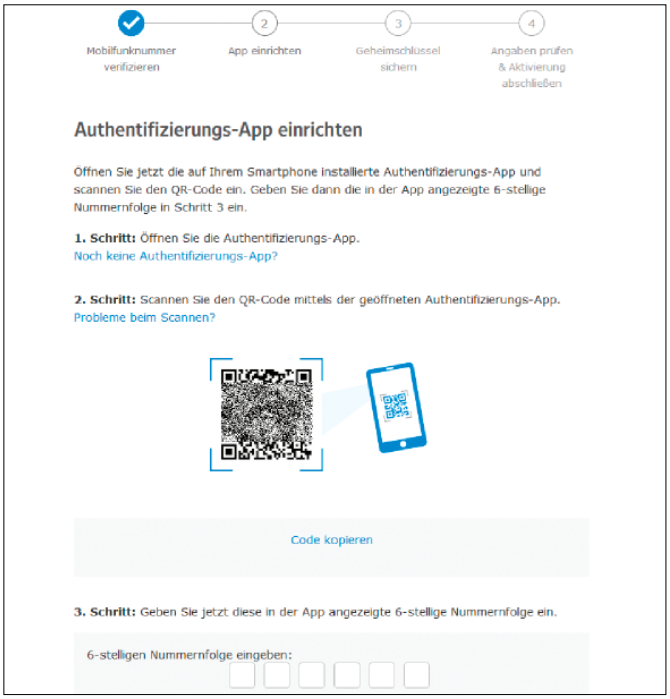
Einen gut sortierten Überblick finden Sie auf der englischsprachigen Seite 2FA Directory (siehe ct.de/yd2q); ein Haken bei „Software Token“ steht dort für Authenticator-Unterstützung. Die Einrichtung der 2FA bei den verschiedenen Diensten ist simpel und läuft relativ ähnlich ab. Oft finden Sie diese in den Einstellungen unter „Sicherheit“, „Login“ oder „Passwort“. Im Aktivierungsprozess zeigt Ihnen der Dienst dann einen QR-Code oder eine Zeichenkette für den Schlüsseltausch. In der App oder auf dem Gerät klicken Sie auf „Hinzufügen“ und können den QR-Code nun einscannen oder die Zeichenkette eintippen. Anschließend geben Sie zur Kontrolle erstmals das TOTP ein – fertig.

Fortan wird Ihnen das TOTP als sechsstelliger Zahlencode in der Liste der App oder des Gadgets angezeigt. Dieser wechselt alle 30 Sekunden, wobei er meist noch einige Sekunden länger gültig ist. Wollen Sie sich nun in den jeweiligen Dienst einloggen, müssen Sie ab sofort zusätzlich zum Passwort den gerade gültigen Code eingeben.

Wiederherstellung

Normalerweise können Sie nur ein Gerät pro Dienst für das TOTP nutzen. Ist dies ein Smartphone, sind Sie auf eine App beschränkt. Das bedeutet auch: Wird das Gerät gestohlen, geht verloren oder lässt sich die App nicht mehr starten, ist der zweite Faktor weg und Sie können Ihren Zugang oft nur noch mühselig wiederherstellen. Wie das geht, erklärt der Dienst meistens während des 2FA-Aktivierungsprozesses; schreiben Sie am besten mit und bringen Sie hinterlegte Daten wie Telefonnummern, Post- und Mailadressen zur Reaktivierung auf den aktuellen Stand.

Sie können sich allerdings viel Zeit und Mühe ersparen, wenn Sie bei der Einrichtung den QR-Code gleich mit mehreren Geräten scannen oder den Startwert sichern, den sogenannten Seed. Das ist das Geheimnis, das sich Authenticator und Server des Dienstes teilen. Der Seed steckt im QR-Code für die 2FA-Einrichtung. Viele (aber nicht alle) Dienste zeigen ihn aber auch als „Backup-Code“, „Secret“ und dergleichen genannte Zeichenkette an. Den Seed sollten Sie sich ganz altmodisch abschreiben oder ausdrucken und sicher verwahren. Wir raten davon ab, ihn auf dem Rechner oder in der Cloud zu speichern, weil dort im Fall der Fälle auch ein Hacker darauf zugreifen kann.



Um die Zwei-Faktor-Authentifizierung eines Dienstes im Authenticator zu aktivieren, müssen Sie meist einen QR-Code einscannen und anschließend zur Bestätigung das erste Einmalpasswort eingeben.

Komfort-Kompromisse

Wenn Sie bereit sind, zwischen maximaler Sicherheit und etwas mehr Komfort abzuwägen, können Sie sich das Leben erleichtern – und haben immer noch ein höheres Schutzniveau als mit einem Passwort allein. Die meisten Apps bieten Funktionen, um den Authenticator samt Seeds der hinterlegten Dienste auf ein neues Gerät umzuziehen oder auf ein weiteres Gerät zu übertragen. Authy enthält eigens zu diesem Zweck eine Synchronisationsfunktion, der Google Authenticator erzeugt zur Weitergabe einen QR-Code, den Sie mit der gleichen App auf einem anderen Gerät abscannen können. Nutzen Sie diese Funktionen aber mit Bedacht. Je mehr Geräte Sie für die 2FA aktivieren, desto mehr potenzielle Ziele haben auch Angreifer.

Auch bei der Eingabe des TOTP können Sie oftmals den Komfort erhöhen: Nach einmaliger 2FA lassen sich dort das beim Login verwendete Gerät und darauf befindliche Apps und Browser von der 2FA ausnehmen. Dazu wird ein vertrauenswürdiges Token hinterlegt. Meist können Sie diese Option in der Login-Maske auswählen. Trotz Ihres Komfortgewinns muss ein Angreifer, der über ein fremdes Gerät auf eines Ihrer Nutzerkonten zugreifen will, weiterhin eine 2FA durchführen. Geräte, auf denen Sie solch eine Komfortfunktion aktivieren, sollten Sie aber gut vor unbefugtem Zugriff schützen. Am besten aktivieren Sie auch etwaige Alarmfunktionen für Zugriffsversuche von unbekannten Geräten. Dann bekommen Sie beispielsweise eine Warnmail auf Ihr Zweit-Mailkonto bei einem anderen Dienst. Das geht unter anderem bei Google und GMX.

Sie können Ihre Nutzerkonten außerdem einfach auf zwei oder mehr Authenticator aufteilen. So lassen sich beispielsweise beruflich und privat genutzte Konten trennen oder besonders sensible Zugänge kompromisslos schützen, während Sie bei anderen gewisse Zugeständnisse an den Komfort machen.

Fazit

Wie stark Ihre Passwörter auch sind: Jede 2FA bietet prinzipbedingt mehr Schutz als ein Passwort allein. App-basierte Authenticator-Lösungen sind sogar kostenlos und einfach für viele Onlinedienste umzusetzen. Auch der Komfort muss darunter nicht signifikant leiden, wenn Sie kleinere Kompromisse in Sachen Sicherheit eingehen können und gut auf die beteiligten Geräte aufpassen. *(mon@ct.de)* c't

Literatur

[1] Jan Mahn, Zweifach abgesichert, FIDO2-Hardware einrichten und ausreizen, c't 25/2019, S. 74
[2] Jürgen Schmidt, Doppelt genäht, Zwei-Faktor-Authentifizierung schmerzfrei einsetzen, c't 24/2018, S. 178
[3] Ronald Eikenberg, Reiner Schutz, 2FA-Generator Reiner SCT Authenticator, c't 8/2021, S. 82

Apps und Liste von Diensten mit 2FA-Option: **ct.de/yd2q**