Bild: Andreas Martini

Abgedichtet

Angriffe auf den zweiten Faktor – So schützen Sie sich

Benutzerkonten mit einem zusätzlichen Faktor zu schützen ist eine gute Idee, hundertprozentigen Schutz bieten gängige Zwei-Faktor-Methoden allerdings nicht. Wie Sie Ihre Accounts bestmöglich abdichten und wie Sie das Risiko, Opfer eines Angriffs zu werden, minimieren, zeigt dieser Artikel.

Von Kathrin Stoll

Die vorangegangenen Artikel in diesem Schwerpunkt haben gezeigt, wie Hacker die meisten Zwei-Faktor-Verfahren aushebeln können. Man kann es nicht oft genug sagen: Einen zweiten Faktor einzurichten, ist trotzdem unbedingt empfehlenswert, auch wenn er keinen hundertprozentigen Schutz bietet. Hier lesen Sie, welche 2FA-Methoden sicherer als andere sind, und erfahren, wie Sie Ihre Accounts mit verfügbaren Mitteln optimal abdichten können. Ein Patentrezept gegen Cyberschurken haben wir zwar nicht, aber wenn Sie unsere Tipps beachten, haben Sie gute Chancen, Angriffsversuche abzuwehren.

Den ersten Faktor abdichten

Bevor wir uns dem zweiten Faktor widmen, müssen wir allerdings zunächst eine alte Binsenweisheit loswerden: Vergeben Sie starke Passwörter und – ganz wichtig – wählen Sie für jeden Account ein anderes. Damit Sie sich die verschiedenen kryptischen Zeichenfolgen für dutzende Accounts nicht merken müssen, empfehlen wir, einen Passwortmanager zu nutzen. Die meisten können sichere Passwörter generieren. Für welchen Passwortmanager Sie sich entscheiden, ist fast egal, wichtig ist, dass Sie diesen mit einem sicheren Masterpasswort schützen.

Wer vor einer Open-Source-Lösung wie Bitwarden, KeepassXC oder Pass zurückschreckt und kein Geld für ein Abo bei kommerziellen Passwortmanagern wie 1Password ausgeben möchte, kann auf Passwortmanager der Betriebssysteme und Browser zurückgreifen. Wie Sie sich

auch entscheiden, die „Automatisch-Ausfüllen"-Funktion von Browsern und Browsererweiterungen der Passwortmanager sollten Sie deaktivieren. Tracker und Skripte könnten Mailadressen, Passwörter und sonstige sensible Daten stehlen – in vielen Fällen, ohne dass Sie das merken.

Den sichersten zweiten Faktor einrichten

Viele Onlinedienste bieten die Möglichkeit, Nutzerkonten zusätzlich mit einem zweiten Faktor abzusichern. Manche, etwa die Entwicklerplattform GitHub, zwingen ihre Nutzer mittlerweile sogar dazu (siehe c't 10/2023, S. 140). Unbedingt empfehlenswert ist die Einrichtung in jedem Fall. Zweiter Faktor ist dabei aber nicht gleich zweiter Faktor.

Komfortabel und einfach zu nutzen ist beispielsweise SMS. Diese Methode erfordert weder spezielle Hard- noch Software, ein einfaches Mobiltelefon genügt. Trotzdem sollten Sie davon Abstand nehmen, auch wenn SMS dem gänzlichen Verzicht auf einen zweiten Faktor vorzuziehen ist. Der Grund für unsere Abneigung gegenüber SMS: Sie sind nicht an das jeweilige Gerät gekoppelt. Angreifer, die es auf Ihre Onlinekonten abgesehen haben, können einen Kniff namens SIM Swapping nutzen, bei dem Sie in Ihrem Namen eine weitere SIM-Karte für Ihre Telefonnummer beantragen, um die SMS mit den 2FA-Codes abzufangen. Weil der Schutz im Vergleich so gering und für den Dienstanbieter zudem kostenintensiv ist (er muss für die SMS bezahlen), ist die SMS als zweiter Faktor immer seltener im Angebot.

Statt offene, dokumentierte 2FA-Standards zu nutzen, integrieren manche Webdienste ihre mobile App in den Anmeldeprozess. Sie kennen das Prinzip möglicherweise von Google, PayPal, Microsoft, Apple oder Steam. In der Regel erhalten Sie dabei eine Push-Benachrichtigung der App auf Ihrem Smartphone oder Tablet. Entweder müssen Sie die Anmeldung anschließend über eine Schaltfläche bestätigen oder eine Zahlenfolge oder ein Symbol abgleichen. Diese Methode zu wählen, hat gegenüber etablierten 2FA-Standards Nachteile. So kann man in der Regel nicht nachvollziehen, wie die Funktion implementiert ist und ob das Ihren persönlichen Sicherheitsanforderungen genügt. Hinzu kommt, dass man sich als Nutzer schnell daran gewöhnt, Login-Anfragen zu bestätigen, gerade wenn dazu nur der Klick auf eine Schaltfläche notwendig ist. Die Gefahr, dass ein Fremdzugriff durchrutscht, ist hoch. Seien Sie wachsam und bestätigen Sie Login-Anfragen nie leichtfertig. Erhalten Sie ohne Anlass eine solche Anfrage, kann es sein, dass sich gerade jemand mit Ihren Zugangsdaten einloggen will. Ändern Sie dann Ihr Passwort, um auf Nummer sicher zu gehen.

Etwas sicherer sind zeitlich begrenzt gültige Einmalpasswörter als zweiter Faktor, sogenannte Time-based One-Time Passwords (kurz TOTP). Ist TOTP aktiv, müssen Sie beim Einloggen zusätzlich zu Ihrem festen Passwort einen Zahlencode eingeben, den Sie mit einer App wie dem Google- oder Microsoft-Authenticator, Authy, OTP oder FreeOTP generieren können. Einige Passwortmanager, darunter 1Password und der iCloud-Schlüsselbund in iOS können das auch. Wer es noch sicherer haben will, nutzt dafür einen TOTP-Stick, zum Beispiel einen YubiKey oder einen Hardware-TOTP-Generator wie den Reiner SCT Authenticator. So sind die kryptografischen Geheimnisse zum Erzeugen der Codes vor Trojanern geschützt, da sie auf einer gesicherten separaten Hardware gespeichert werden.

Die sicherste Wahl

Wo Apps und Websites es anbieten, sollten Sie auf das FIDO2-Verfahren setzen. FIDO2 nutzt ein kryptografisches Public-Private-Key-Verfahren. Der private Schlüssel wird sicher auf der Hardware des Benutzers gespeichert, der öffentliche Schlüssel wird auf dem Server des jeweiligen Anbieters einer Website oder App abgelegt. Beide Bestandteile des Schlüsselpaars in Kombination sind nötig, um sich in einem sogenannten Challenge-Response-Verfahren zu authentifizieren. Bei FIDO2 fließt automatisch die Domain des Dienstes in die Authentifizierung ein. Das macht das Verfahren resistent gegen klassisches Phishing, bei dem Angreifer versuchen, Sie dazu zu bringen, Ihre Zugangsdaten auf einer Phishing-Website einzugeben (siehe S. 16).

Um einen Account per FIDO2 abzusichern, brauchten Sie bis vor einiger Zeit einen externen Sicherheitsschlüssel.

Um einen Account per FIDO2 abzusichern, brauchten Sie bis vor einiger Zeit einen externen Sicherheitsschlüssel, der als Authenticator dient. Mittlerweile können Sie stattdessen auch den in modernere Rechner, Smartphones und Tablets eingebauten Sicherheitschip (je nach Anbieter auch unter TPM, Trusted Plattform Module oder Secure Element bekannt) einsetzen. Details und offene Fragen zum FIDO2-Standard haben wir in einer FAQ beleuchtet (siehe c't 9/2022, S. 32). Je nach Implementierung kommt FIDO2 auch ohne Passwort aus. Das ist der Königsweg, denn wo es kein Passwort gibt, kann es auch nicht geklaut werden.

Seit 2022 wird das passwortlose FIDO2-Verfahren auch unter dem Namen Passkeys gehandelt (siehe c't 26/2022, S. 126). Dabei handelt es sich im Wesentlichen um eine benutzerfreundlichere Version des FIDO2-Standards. Passkeys sind über die Herstellerclouds von Apple und Google zwischen Geräten aus demselben Produktuniversum synchronisierbar und lassen sich aufgrund der Cloudspeicherung auch bei Verlust aller Ihrer Geräte wiederherstellen. Microsoft soll dieses Jahr nachziehen. Eine nahtlose Synchronisation zwischen Geräten aus unterschiedlichen Produktuniversen soll noch in diesem Jahr über die Passwortmanager 1Password und Dashlane möglich werden. Auch die Open-Source-Software Bulwark Passkey erlaubt es, Passkeys über ver-

c't kompakt

- 2FA ist eine wertvolle zweite Verteidigungslinie gegen Angreifer. Die verfügbaren Verfahren sind allerdings nicht alle gleich sicher.
- Selbst das derzeit sicherste verfügbare Verfahren schützt nicht vor Session-Cookie-Diebstahl.
- Schützen können Sie sich, indem Sie wachsam gegenüber Social-Engineering-Techniken bleiben.

Per QR-Code koppeln Sie das Smartphone mit dem Rechner.

schiedene Gerätetypen hinweg zu synchronisieren. Bisher unterstützt Bulwark Linux- und Windows, Support für macOS, Android und iOS soll folgen. Die Software emuliert einen USB-Sicherheitsschlüssel, um die Passkeys unabhängig vom Browser und Client nutzbar zu machen. Anders als bei Apple, Google und Microsoft werden die Passkeys dabei nicht in einem Hardwaresicherheitschip abgelegt, sondern mit dem Verschlüsselungsstandard AES-256 mithilfe des Masterpassworts verschlüsselt, bevor sie wahlweise lokal auf Ihrem Gerät oder in der Cloud gespeichert werden. Gegenüber der Speicherung auf einem Hardwaresicherungschip ist das weniger sicher, mehr Sicherheit als die bis zu dieser Stelle vorgestellten 2FA-Verfahren bietet es aber trotzdem.

So gehts

Die Einrichtung von Passkeys ist einfach. Beim Registrieren eines neuen Benutzerkontos bei einem Dienst geben Sie wie gewohnt einen Benutzernamen ein und bestätigen, dass Sie einen Passkey auf dem Gerät sichern wollen. Voraussetzung ist lediglich, dass Sie unter macOS, iOS und iPadOS den iCloud-Schlüsselbund aktiviert haben. Eine Liste von Diensten, die die Authentifizierung per Passkey bereits anbieten, finden Sie unter der Webadresse passkeys.directory.

Nutzen Sie Google Chrome oder Safari auf einem Rechner, können Sie Ihr Smartphone oder Tablet (Android und iOS) als externen Passkey-Authenticator einrichten. Ihr Smartphone fungiert in diesem Szenario als physischer Sicherheitsschlüssel, den Sie jedes Mal benötigen, wenn Sie sich gegenüber einem Dienst per Passkey authentifizieren wollen. Beim Anlegen eines Passkeys für eine Website zeigt diese Ihnen einen QR-Code. Den QR-Code scannen Sie mit der Kamera Ihres Smartphones oder Tablets. Anschließend bestätigen Sie auf dem Mobiltelefon oder Tablet, dass Sie es per QR-Code mit dem Rechner koppeln wollen. Bei Android-Geräten können Sie das Häkchen „Diesen Computer merken“ setzen, wodurch das Gerät dauerhaft mit Ihrem Rechner verknüpft wird. Steht die Verbindung, bietet Ihnen Ihr Mobilgerät an, den Passkey für die Website zu speichern.

Wenn Sie sich künftig mit dem Passkey beim Webdienst am Rechner anmelden wollen, scannen Sie den QR-Code erneut und bestätigen anschließend, dass Sie den Passkey verwenden möchten. Das Scannen entfällt, wenn Sie Rechner und Android-Smartphone durch Setzen des Hakens dauerhaft verknüpft haben. Während der Anmeldung am Rechner erscheint dann eine Benachrichtigung auf dem Smartphone, über die Sie den Passkey freigeben.

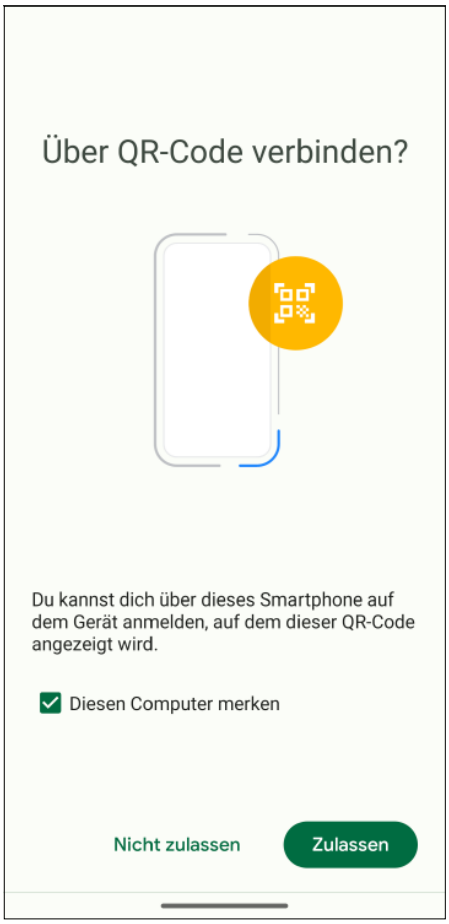
Die Gefahr, Anmeldedaten versehentlich auf einer Phishing-Website einzugeben, wird mit Passkeys erfolgreich eliminiert. Auch durch die auf Seite 17 beschriebene MFA-Fatique-Masche können Hacker Ihre Accounts nicht übernehmen, schließlich gibt es weder Passwörter zu stehlen noch Möglichkeiten, Sie dazu zu bewegen, Ihren zweiten Faktor durch ständige Pushbenachrichtigungen oder wiederholte nächtliche Anrufe preiszugeben. Wo es angeboten wird, sollten Sie FIDO2 entweder als zweiten Faktor oder besser noch in der passwortlosen Variante unbedingt einrichten.

Nicht ganz wasserdicht

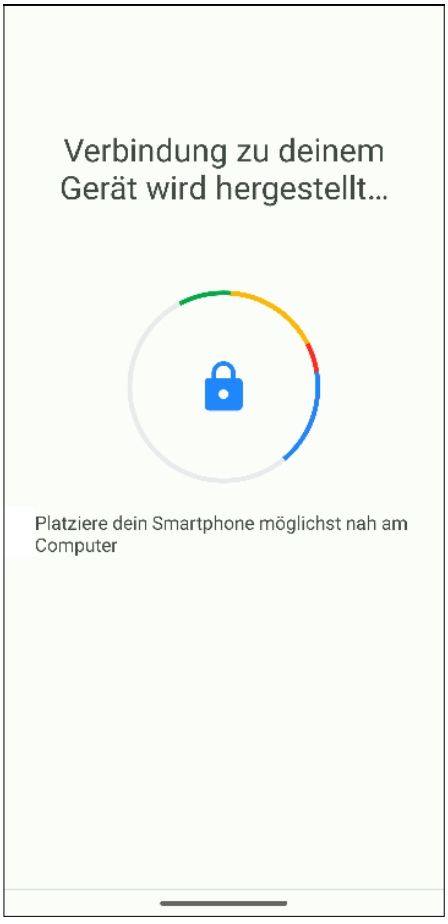
Hundertprozentige Sicherheit bietet allerdings auch FIDO2 nicht. Selbst Nutzerkonten, die Sie mit dieser derzeit sichersten aller gängigen Authentifizierungsmethoden absichern konnten, sind nicht vor Session-Cookie-Diebstählen geschützt. Session Cookies sind kleine Datenpakete, die beim Einloggen auf Websites in ihrem Browser hinterlegt werden. Durch die Cookies werden Sie als Nutzer identifizierbar. Sie stellen sicher, dass Sie sich nicht bei jedem Seitenwechsel erneut anmelden müssen und erleichtern die Interaktion mit einer Webanwendung erheblich.

Das ist allerdings nur die eine Seite der Medaille. Die Kehrseite ist, dass Angreifer diese Cookies stehlen und so Ihre aktiven Onlinesitzungen übernehmen können, auch ohne Ihre Zugangsdaten zu kennen. Eine Methode des Cookie-Raubs, die bei einem per FIDO2 abgesicherten Account nicht funktioniert hätte, weil eine Phishing-Website involviert war, haben Sie bereits auf Seite 22 kennengelernt. Es gibt jedoch auch Session-Cookie-Diebstahl-Varianten, gegen die FIDO2 nicht schützt:

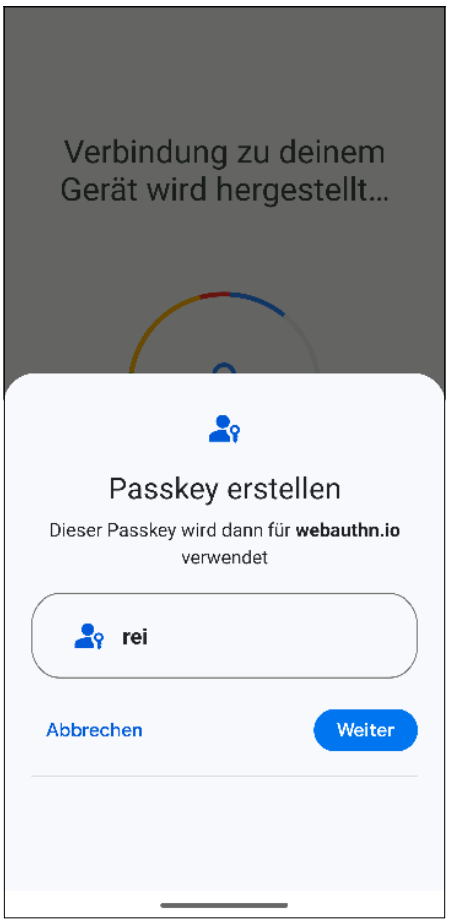
Der Angreifer jubelt Ihnen dabei zum Beispiel einen verseuchten Mailanhang unter, der die Cookies aus Ihrem Browserprofil abgreift. Importiert er die Cookies anschließend in seinen Browser, ist er bei allen Accounts eingeloggt, bei denen Sie sich nicht aktiv ausgeloggt haben. Ihre Zugangsdaten oder den zweiten Faktor benötigt er für diesen Angriff nicht. Dagegen schützen können Sie sich, indem Sie bei wichtigen Diensten nicht dauerhaft eingeloggt bleiben – etwa, indem Sie sich grundsätzlich nach jeder Nutzung ausloggen. Dadurch schließt der Dienst die aktive Sitzung und das Session-Cookie wird für den Angreifer wertlos. Beachten Sie außerdem grundlegende Security-Tipps für Ihre Geräte, die wir im Rahmen unserer Security-Checklisten (etwa in c’t 20/2021, S. 14) zusammengefasst haben. Achten Sie besonders unter Windows darauf, dass ein Antivirenprogramm mit aktuellen Virensignaturen aktiv ist, damit eine derartige Malware es nicht auf Ihr System schafft. Der vorinstallierte Windows Defender macht einen guten Job. Standard sollte auch sein, dass Sie unabhängig vom Betriebssystem stets alle verfügbaren Sicherheitsupdates installieren. Bietet der Her-



Smartphone als Passkey-Authenticator: Android-Geräte können Sie dauerhaft mit einem Rechner koppeln.



Das Koppeln funktioniert aus Sicherheitsgründen nur, wenn sich die Geräte in der Nähe befinden.



Im letzten Schritt bestätigen Sie am Smartphone, dass Sie einen Passkey für den Dienst erstellen wollen.

steller Ihres Geräts keine Updates mehr an, ist ein Wechsel anzuraten. Auch Programme wie den Webbrowser, den Mailclient und das Office-Paket sollten Sie stets auf dem aktuellen Stand halten.

Hören Sie trotz vorbildlich mit der jeweils besten verfügbaren Methode geschützter Accounts auf keinen Fall damit auf, E-Mails von unbekannten Absendern grundsätzlich mit Skepsis zu begegnen. In Zeiten von dedizierten Phishing-Kits, wie wir sie ab Seite 16 vorgestellt haben, und KI-Modellen wie ChatGPT (siehe c't 8/2023, S. 108) sind Phishing-Mails oft schwer zu erkennen. Die alten Hinweisgeber, etwa eine völlig abwegige Senderadresse, hanebüchene Rechtschreibung und Grammatik oder ein allzu schlecht kopiertes Corporate Design großer Firmen haben sich überlebt.

Verzichten Sie weiterhin darauf, leichtfertig auf Links in E-Mails von unbekannten Absendern zu klicken. Die Vertrauenswürdigkeit von E-Mailadressen und URLs können Sie schnell und unkompliziert von einem geeigneten Dienst einschätzen lassen. Dabei helfen kann Ihnen zum Beispiel die Browserextension Mitaka (siehe c't 14/2022, S. 86). Sie bietet eine große Auswahl an Tools, die Ihnen binnen Sekunden verraten können, ob die URL login.m1crosoftonline.tld oder die Emailadresse support@microsoft-online.tld wohl wirklich zu Microsoft gehören. Wenn einschlägige Tools wie Email.io keine eindeutige Einschätzung liefern und Sie unsicher sind, ob eine Mail nicht doch vom angegebenen Absender stammt, fragen Sie besser direkt bei der betreffenden Person nach. Am besten nutzen Sie einen bereits zuvor genutzten Kontaktweg, etwa das Telefon.

Bei Mailanhängen ist besondere Vorsicht geboten (siehe c't 19/2022, S. 18). Der häufigste Verbreitungsweg für Schädlinge sind verseuchte Dateianhänge. Grundsätzlich gilt: Öffnen Sie Anhänge nur, wenn sie von einem vertrauenswürdigen Absender stammen. Meiden Sie ausführbare Dateiformate wie EXE und SCR, Office-Dateien mit Makros sowie Dateiarchive wie ZIP und ISO.

Fazit

2FA macht Ihre Accounts sicherer, jedoch leider nicht so sicher, dass Sie sich darauf ausruhen können, bei allen Ihren Accounts einen – oder sogar den jeweils sichersten – zweiten Faktor eingerichtet zu haben. Lobenswert und sinnvoll ist es trotzdem. Schützen können Sie sich nur, indem Sie sich unabhängig vom jeweiligen Schutzlevel Ihrer Onlinekonten weiterhin umsichtig verhalten. Eine einzelne technische Maßnahme, die Ihre Accounts komplett abdichtet, sodass Sie sich gänzlich entspannt zurücklehnen können, wird es möglicherweise niemals geben. Denn selbst falls doch in Kürze eine Authentifizierungsmethode auf dem Plan treten sollte, gegen die alle bisherigen Angriffsszenarien wirkungslos sind, würde es vermutlich nicht lange dauern, bis Cyberschurken einen Weg gefunden haben, sie zu umgehen. *(kst@ct.de)* c't