Weg vom Passwort

Viele Onlineservices verabschieden sich vom Passwort und drängen Nutzer zum Anlegen von sogenannten Passkeys. Aber ist das sicherer? **Wir erklären Ihnen Funktionsweise und Nutzung der Passkeys von A bis Z.** ● **VON MARKUS SELINGER**

Über Jahrzehnte war das Passwort der Standardschutz für digitale Konten. Es sollte leicht genug sein, damit Menschen es sich merken können, und gleichzeitig stark genug, um Angriffe abzuwehren. In der Praxis ist das schon immer gescheitert: Passwörter werden zu oft wiederverwendet, zu schwach gewählt, per Phishing abgegriffen oder durch Datenlecks kompromittiert. Deshalb kamen mit der Zeit zusätzliche Schutzmechanismen hinzu – vor allem die 2-Faktor-Authentifizierung (kurz 2FA) und allgemein die Mehr-Faktor-Authentifizierung (kurz MFA). Sie machen zwar Passwörter sicherer, schaffen sie aber nicht ab.

Passkeys gelten heute als der nächste grosse Schritt, denn damit benötigt es keine Passwörter mehr. Die Keys sollen viele Schwächen klassischer Passwörter beseitigen und gleichzeitig die Anmeldung einfacher machen. Statt ein schwieriges Kennwort einzugeben, das ein Mensch sich merken muss, nutzt ein Passkey Kryptografie. Das Ziel ist klar: weniger Angriffsfläche, mehr Komfort und ein Log-in, das im Alltag sicherer ist als ein Passwort.

2FA vs. Passkeys

2FA – also die Bestätigung eines Log-ins nach der Passworteingabe mit einem zweiten Faktor, etwa einem Code per SMS, per E-Mail oder einer Ja/Nein-Abfrage am Smartphone ist schon sehr sicher. Aber: das Passwort ist immer noch ein Teil des Log-ins.

Genau hier setzen Passkeys an. Sie entfernen das Passwort als zentrale Schwachstelle und ersetzen es durch ein kryptografisches Verfahren. Die Nutzerinnen und Nutzer bestätigen die Anmeldung lokal über einen Fingerabdruck, via Gesichtserkennung oder über eine Geräte-PIN, aber der eigentlich generierte Schlüssel wird nicht eingegeben und nicht übertragen. Dadurch sind Passkeys deutlich besser gegen Phishing und Datenlecks geschützt.

Bild: Shutterstock/NMStudio789

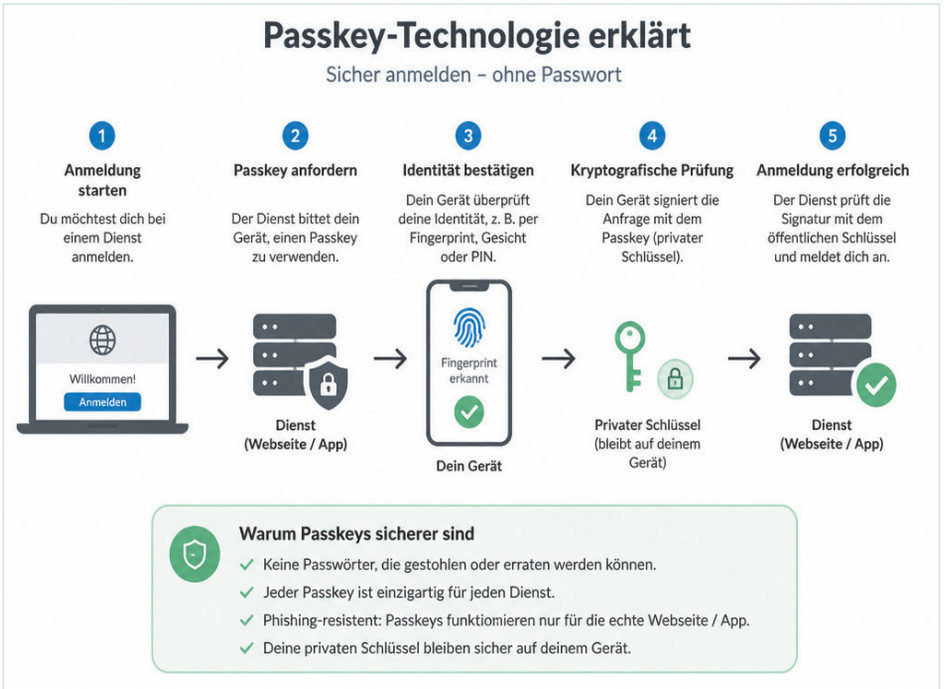

Bild 1: Ganz ohne Eingabe eines Passworts: So funktioniert die Technik mit den neuen Passkeys bei der Anmeldung an einem Account

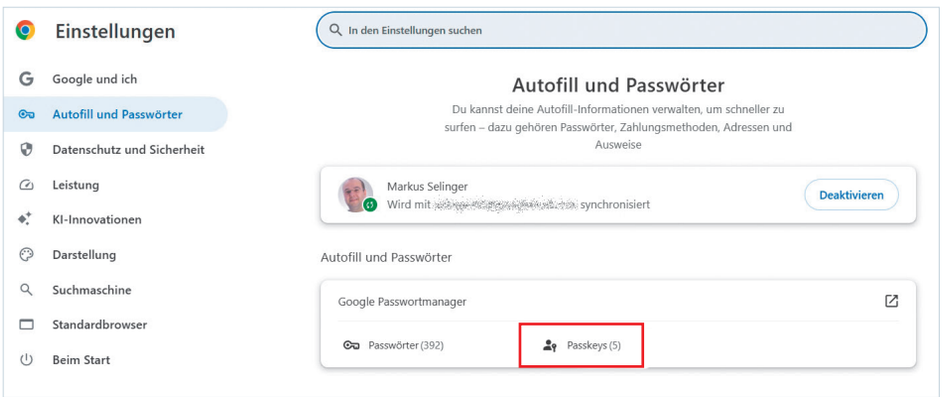

Bild 2: Google verwaltet via Chrome auch Passkeys und speichert sie im Cloud-Konto

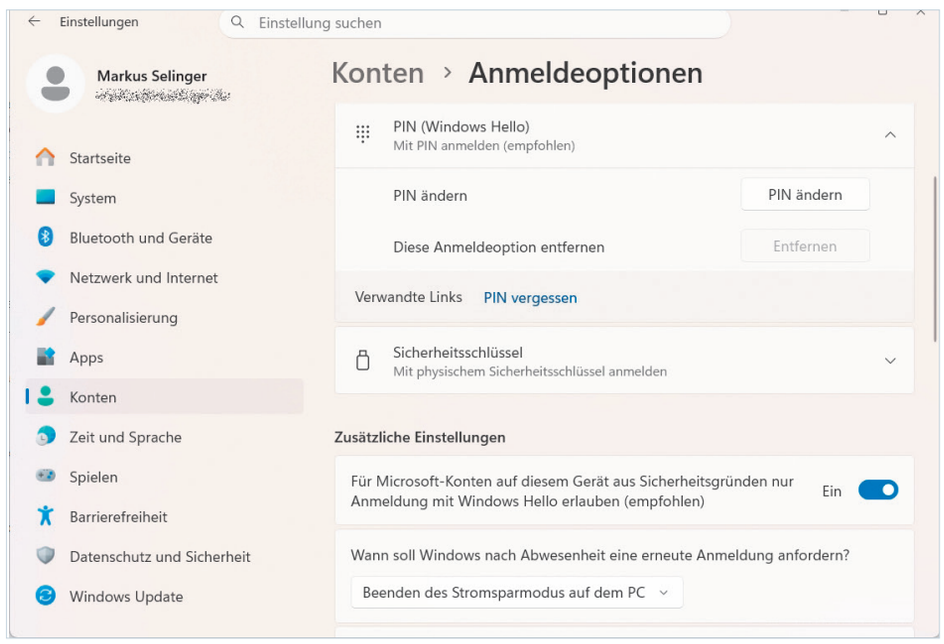

Bild 3: Unter Windows meldet sich immer wieder Windows Hello mit der PIN-Abfrage zum erweiterten Schutz bei der Eingabe oder Anlage eines Passkeys

So funktionieren Passkeys

Ein Passkey ist im Expertenjargon eine Anmeldemethode auf Basis asymmetrischer Kryptografie, Bild 1. Vereinfacht gesagt, gibt es dabei ein Schlüsselpaar: einen privaten Schlüssel und einen öffentlichen Schlüssel. Der private Schlüssel bleibt sicher auf Ihrem Gerät oder in einem geschützten, synchronisierten Speicher – selbstverständlich hoch verschlüsselt. Der öffentliche Schlüssel wird beim Onlinedienst hinterlegt. Bei einem Log-in wird somit nicht mehr ein Passwort abgefragt, sondern eine kryptografische Prüfung bzw. ein Vergleich dieser Schlüssel durchgeführt.

Der grosse Vorteil ist, dass der private Schlüssel das Gerät nicht verlässt. Ein Beispiel: Ein Angreifer baut eine gefälschte Log-in-Seite, auf die ein Anwender vielleicht sogar hereinfällt. Ein zuvor generierter Passkey funktioniert allerdings nur mit der echten Internetadresse (Domain), da ja das kryptografische Schlüsselpaar verglichen wird. Das macht Passkeys besonders phishing-resistent. Denn auf diese Weise gibt es kein Passwort, das in falsche Hände geraten oder in mehreren Diensten wiederverwendet werden könnte.

Wichtig: Passkeys sind nicht immer automatisch der vollständige Ersatz für alle bisherigen Log-in-Methoden. Viele Dienste unterstützen sie zunächst zusätzlich zum Passwort oder neben anderen Wiederherstellungsoptionen. Der Übergang läuft also oft schrittweise und nicht einfach durch ein sofortiges Abschalten aller alten Verfahren.

Umstieg auf Passkeys

Der Begriff «Passkey» ist nicht gerade selbsterklärend. Daher zögern viele Anwender, die neue Sicherheit zu nutzen. Deshalb sollten Sie wissen, wo und wie in Zukunft Ihre Zugänge gespeichert sind: Ein Passkey gehört immer zu einem konkreten Onlinekonto, etwa Amazon, Discord, eBay, Dropbox, GitHub, Nintendo, PayPal oder TikTok – um nur einige zu nennen. Natürlich bieten auch die grossen Dienstleister wie Apple, Google oder Microsoft den Schutz per Passkeys. Insbesondere Microsoft will so die stark attackierten Windows-Konten besser schützen.

Nun müssen Sie zuerst wissen, wo denn Ihre Passkeys in Zukunft gesichert werden sollen, denn darauf haben Sie Einfluss.

Die Standardmethode: Apple, Google und Microsoft bieten Ihnen an, alle erstellten Passkeys in einem Speicher- bzw. Synchronisationskonto abzulegen, Bild 2. Microsoft kombiniert speziell den Zugang mit Windows Hello und speichert so den Zugriff in Ihrem Konto. Andere Passkeys nimmt es eigentlich nicht auf, dient aber unter Windows immer als Bestätigungshilfe, Bild 3.

Die meisten Nutzer speichern ihre Keys in einem Apple- oder Google-Account. Das hat den Vorteil, dass diese an das Konto gebunden sind, sich so sehr einfach im Alltag ➜

verwenden lassen und bei einem Gerätewechsel leicht mitzunehmen sind. Diese Hauptkonten sind besonders geschützt durch Passwort, Passkey, Biometrie und 2FA.

Der Nachteil: Alle abgelegten Passkeys sind an diese Konten gebunden. Legen Sie ein neues Konto an, lassen sich aus Sicherheitsgründen die Keys nicht einfach übertragen. Es gibt keine Export- oder Import-Funktion. Es gibt nur einen sehr komplizierten Weg über Passwortmanager. Sie sollten sich am besten gleich zu Beginn entscheiden, wo sie die Keys speichern möchten.

Der Haken: Wenn Sie sich nun etwa für Google entscheiden, werden die Passkeys im Chrome-Passwortmanager abgelegt und in Ihrem Konto gespeichert. Wenn Sie jetzt aber Firefox oder Opera als Webbrowser nutzen, haben Sie keinen direkten Zugriff auf Ihre Passkeys! Sie müssen sich wieder per Passwort einloggen (das geht noch) oder ihr Smartphone per Bluetooth mit Windows koppeln und danach den fremden Log-in über Firefox und Passkey bestätigen. Das ist aber extrem zeitaufwendig.

Sie können auch alle Passkeys in Ihrem Microsoft-Account ablegen, aber dann haben Sie diese nicht auf einem Smartphone mit Android. Diese Welt ist voneinander getrennt. Nutzer eines Mac und iPhone haben dagegen eine geschlossene Welt. Passkeys speichert Apple in seinem iCloud-Schlüsselbund und stellt sie im System bereit. Dabei ist es egal, ob Sie als Webbrowser Safari nutzen oder einen anderen Surfboliden, Bild 4.

DIE PASSWORTMANAGER-METHODE

Alle Passkeys lassen sich – ähnlich wie bei Passwörtern – auch in einem Manager verwalten. Dieser managed alle Keys und synchronisiert sie verschlüsselt via Cloud mit anderen installierten Versionen. Ein Beispiel dafür ist das kostenlose Tool Bitwarden (bitwarden.com), das es für alle Plattformen gibt: iOS, Android, Windows, macOS. Zusätzlich steht

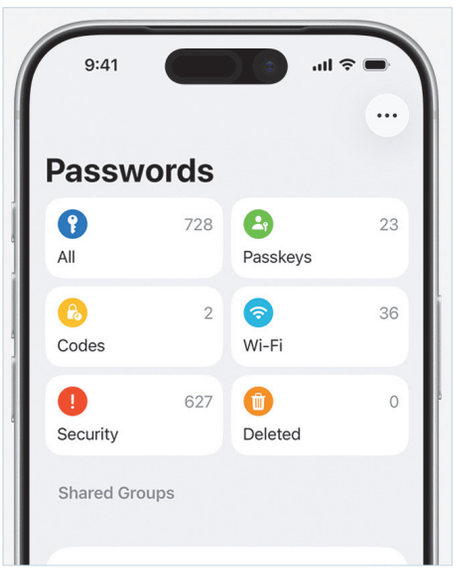

Bild 4: macOS und iOS verwalten neben den Passwörtern auch Passkeys

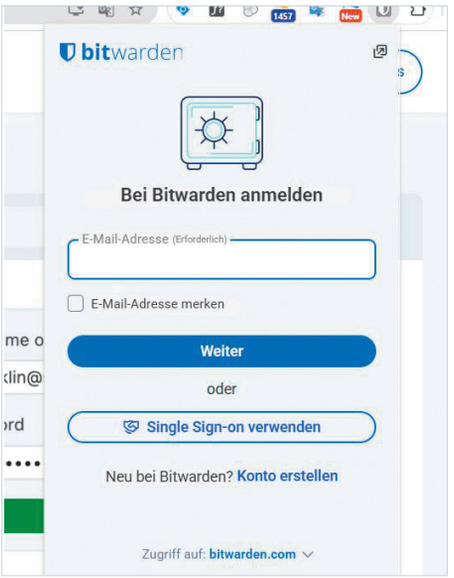

Bild 5: Der Passwortmanager Bitwarden ist flexibel und auf vielen Plattformen verfügbar

der Manager als Browsererweiterung für neun Webbrowser zur Verfügung. In der Praxis funktioniert das so: Wenn Sie auf einer Website oder in einer App einen Passkey erstellen, erscheint automatisch der Dialog Ihres Passwortmanagers. Der legt den Key für Sie ab, was Sie per Fingerabdruck, Gesichtserkennung oder PIN bestätigen.

Unser Tipp: Wenn Sie alles auf Passkeys umstellen möchten, ist ein Passwortmanager die flexibelste Lösung, da sie auf allen Geräten mit allen Browsern funktioniert und nicht an Google, Windows oder Mac gebunden ist.

Umgekehrt meldet sich der Manager natürlich bei einem Log-in automatisch, Bild 5. Das ist zwar alles bequem, aber die Daten liegen bei einem Passwortmanager in der Cloud. Allerdings wurde Bitwarden noch nie durch einem Hack oder Datenverlust belastet, wie bereits andere Cloud-Passwortmanager.

Passkeys im Alltag

Bevor Sie jetzt jeden einzelnen Service, den Sie nutzen, im Support-Teil nach der Passkey-Aktivierung durchforsten, sollten Sie das *Passkeys.directory* des Anbieter 1Password unter dem Link passkeys.directory nutzen, Bild 6. Dort finden Sie eine aktuelle Liste aller Ser-

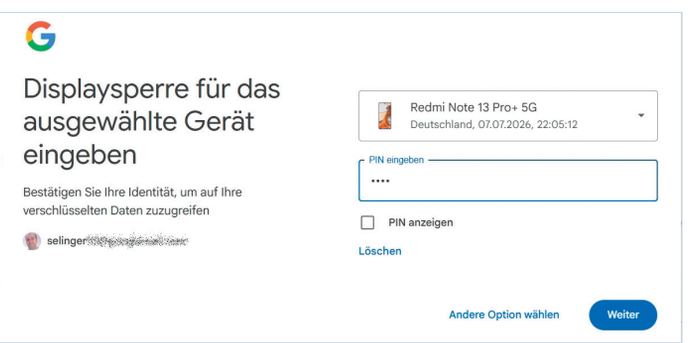

Bild 7: Wenn Sie in Dropbox zu einem Passkey wechseln, werden Sie aufgefordert, Ihr Smartphone per Google-Account zu registrieren

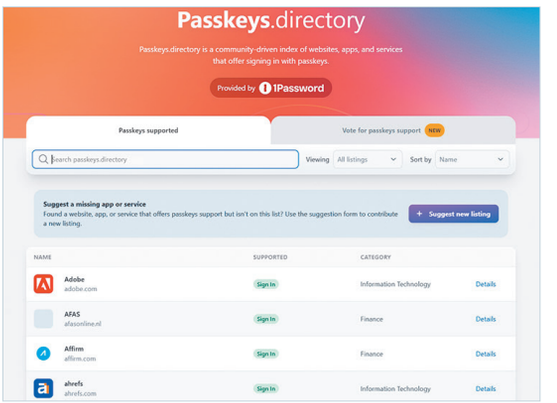

Bild 6: Im *Passkeys.directory* können Sie nachsehen, ob Ihr Serviceanbieter Passkeys unterstützt

vices, bei denen Sie einen Passkey als Log-in verwenden können. Zusätzlich entdecken Sie dort den Hinweis auf eine Alternative, etwa 2FA sowie passende Links zum Support- oder Doku-Teil mit der richtigen Information.

Kleiner Hinweis: Der Anbieter markiert die Möglichkeit eines Passkeys mit dem grün unterlegten Zusatz *Sign In*.

Suchen Sie dort den Dienst, bei dem Sie den Zugang ändern möchten, etwa Dropbox. Loggen Sie sich bei Dropbox wie gewohnt mit Ihrem Passwort und der eventuell nötigen 2FA ein. In den Einstellungen und unter *Sicherheit* finden Sie den Punkt *Hauptschlüssel*. Damit ist der Passkey gemeint. Sobald Sie damit starten, meldet sich ein Google-Dialog, der Sie auffordert Ihr mobiles Gerät auszuwählen und die PIN der Displaysperre einzugeben, Bild 7.

Danach vergeben Sie noch einen Kurznamen (nur intern für Dropbox) und speichern das Ganze. Chrome informiert Sie dabei, dass der Passkey bei den Passwörtern abgelegt wurde. Wenn Sie dort hineinschauen, finden Sie statt einem Passwort in Sternchenform nur den Hinweis, dass es sich um einen Passkey handelt, Bild 8.

Noch ein Tipp: Verwenden Sie immer zusätzlich einen Passwortmanager. Wir haben Ihnen viele zuverlässige in der PCtipp-Ausgabe 2/2026 vorgestellt. PCtipp-Abonnenten finden den Artikel digital unter dem Link archiv.pctipp.ch. Warum ein Passwortmanager? Dort können Sie Ihre Passwörter sicher ablegen und vor dem Vergessen bewahren. Zusätzlich ist dort der perfekte Platz für die Ablage von Notfallcodes in Textform. Denn die bietet Ihnen zum Beispiel auch Dropbox unter dem Punkt *Sicherheit/Einmalige Zugangscodes* an, damit sie auch bei Problemen ins Konto gelangen, Bild 9.

Wenn Sie sich nun bei Ihrer Dropbox im Internet einloggen möchten, klicken Sie zuerst bei *E-Mail* in

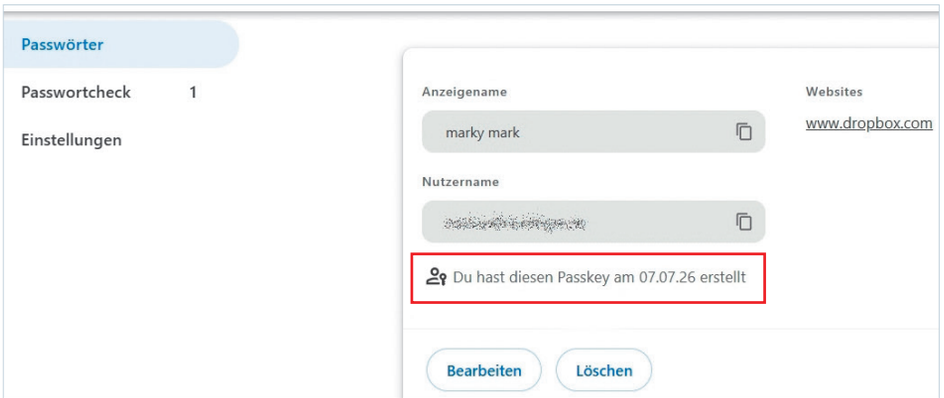

Bild 8: Der neue Passkey für Dropbox wurde im Chrome-Passwortmanager abgelegt und wird per Google-Account synchronisiert – sofern gewünscht

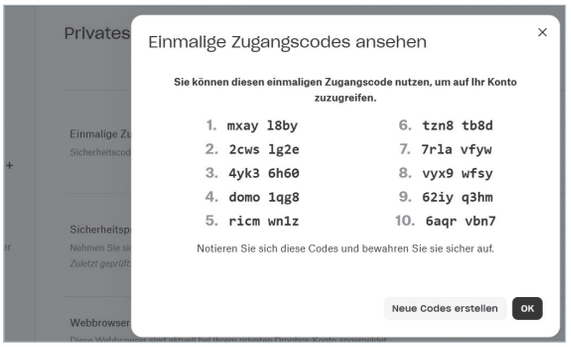

Bild 9: Wie Dropbox bieten Ihnen viele Serviceanbieter Notfallcodes für einen Log-in – verwahren Sie diese gut

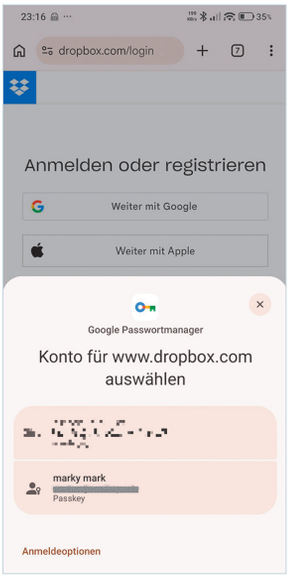

Bild 10: Bei der passwortlosen Anmeldung am Smartphone steht unter Chrome der generierte Passkey für Dropbox bereit

Bild 11: Beim Log-in mit einem Passkey in Android muss der Zugang ohne Passwort via Bildschirmsperre bestätigt werden – mittels PIN oder Biometrie

das Anmeldefenster und wählen im Dialogmenü den passenden Eintrag mit dem Passkey aus, Bild 10. In Windows 11 ist das Ganze noch durch Hello geschützt und Sie müssen Ihre PIN eingeben. Danach sind Sie eingeloggt. Findet das Log-in auf einem mobilen Gerät statt, würde die Bildschirmsperre abgefragt, also eine PIN oder ein biometrisches Merkmal, Bild 11.

Viele Services fordern Sie aktiv auf, für den Zugang einen Passkey anzulegen. Aber der ist nicht immer praktisch und wie weiter oben genannt auch an Accounts oder Systeme gebunden. Sie müssen selbst entscheiden: Wo liegen wichtige Daten, wo liegen sensible Zahlungsinformationen? Für diese Webseiten oder Services ist ein Passkey ein echter Sicherheitsvorsprung. Aber das Ganze ist nicht so flexibel wie ein Passwort und ein zweiter Faktor. Sie sollten daher die Risiken beim Zugang zu Ihren Services abwägen und die Techniken am besten mischen.

Wenn alles funktioniert, stellen sich gleich weitere Fragen nach der Sicherheit. Da wäre etwa: Was passiert, wenn jemand mein Google-Account knackt? Wenn mein Handy gestohlen wird oder wenn es beim Wandern am Berg verloren geht? Was ist, wenn ich meine Passkeys verliere oder lösche? Das sind alles gute Fragen, auf die es aber auch klare Antworten gibt.

SICHERHEIT BEIM GOOGLE-ACCOUNT

Jedes Konto ist irgendwie knackbar – aber eigentlich nur mit viel Aufwand und wenn Sie Ihren Account nicht mit einem zweiten Faktor geschützt haben. Diesen sollten Sie unbedingt bei Ihrem Account nutzen, Bild 12. Ist das der Fall, und ein Hacker schafft es trotzdem online in Ihren Account, kann er mit den Passkeys nichts anfangen. Die arbeiten nur mit der Bestätigung per Windows oder Android am Gerät. Das hat der Angreifer nicht. Allerdings kann er vorhandene Passwörter auslesen – noch ein Argument für einen externen Passwortmanager.

MEIN HANDY IST GESTOHLEN/VERLOREN

In diesem Fall sollten Sie das Gerät aus der Ferne löschen lassen. Damit sind zwar alle Daten weg und auch der Google-Account gelöscht, aber da alle Geräte in der Regel synchronisiert sind, wurden sämtliche Daten im Account gesichert. Sobald Sie ein neues Gerät einrichten und mit Ihrem Google-Account verbinden, sind auch alle Passkeys wieder da.

ICH HABE MEINE PASSKEYS GELÖSCHT

Wenn Sie die Passkeys gelöscht haben, dann sind sie weg. Aber die Serviceanbieter haben eigentlich immer eine Nottür. Wie am Beispiel von Dropbox gibt es Notfallcodes, die Sie in einem Passwortmanager aufbewahren sollten. Ausserdem ist bei den meisten Konten noch das Passwort vorhanden, mit dem Sie sich ebenfalls zur Not einloggen können. Wenn Sie wieder drin sind, legen Sie einfach neue Keys an.

Wichtig zu wissen: Einige Services bieten Ihnen an, ein vorhandenes Passwort zu löschen. Das passiert aber nur, wenn genügend andere sichere Anmeldemethoden vorhanden sind. Das heisst: Sie haben einen Passkey, können sich biometrisch ausweisen, haben noch einen E-Mail-Kontakt für Codes und eine hinterlegte Telefonnummer. Wenn Sie das machen, sollten Sie unbedingt die bereits erwähnten Notfallcodes in einem Passwortmanager speichern, auch wenn das vielleicht schon etwas nach Paranoia klingt. Aber so gelangen Sie im schlimmsten Fall noch in Ihr Konto.

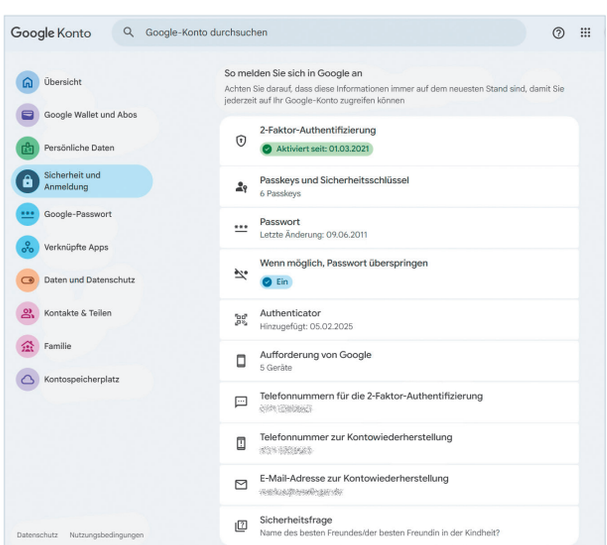

Bild 12: Prüfen Sie die Sicherheit Ihres Google-Accounts – die 2-Faktor-Authentifizierung sollte unbedingt aktiviert sein