2FA sperrt Hacker aus!

Schützen Sie Ihre wertvollen Log-ins von Amazon, Dropbox, Google oder Microsoft mit einer sicheren 2-Faktor-Authentifizierung – das geht bei fast allen Diensten. **Diese erhöht den Schutz gegen Eindringlinge massiv.** ● **VON MARKUS SELINGER**

Zugegeben, der Begriff 2-Faktor-Authentifizierung – kurz 2FA – erschliesst sich nicht sofort jedem Nutzer. Hinter der sperrigen Bezeichnung steckt aber eine tolle Technologie, mit der Sie fast alle Ihre Zugänge zu Onlinediensten perfekt absichern können und sich dabei nur leichte Passwörter oder gar keine merken müssen. Der Begriff 2FA oder auch MFA (Multi-Faktor-Authentifizierung) ist ein Oberbegriff für eine Schutztechnik, mit der Sie bestimmt schon unbewusst eine Berührung hatten. Denn hinter dem Begriff versteckt sich Folgendes: Bei jedem Log-in in ein Konto verwendet ein Anwender zum Beispiel nebst einem Passwort als weitere Bestätigung einen SMS-Code, der an ein zuvor definiertes Smartphone geschickt wird. Aber das ist nur

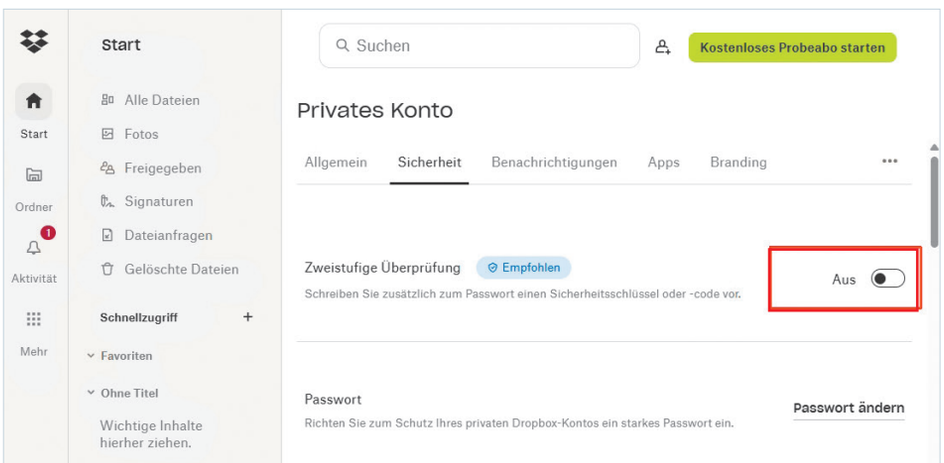

Bild 1: In Dropbox ist die 2FA schnell eingestellt und der Account gesichert

Bild: Shutterstock/David Gyung

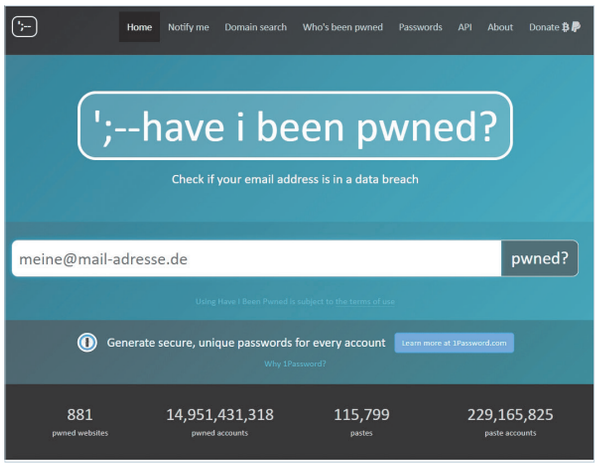

Bild 2: Prüfen Sie bei «';--have i been pwned?», ob Ihre E-Mail-Adresse und Passwörter aus Hacks bekannt sind

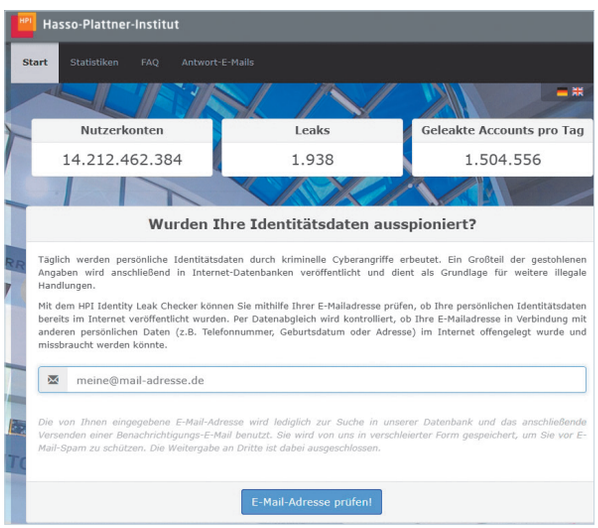

Bild 3: Auch das Hasso-Plattner-Institut hat eine Datendank mit gesammelten Daten aus Hacks

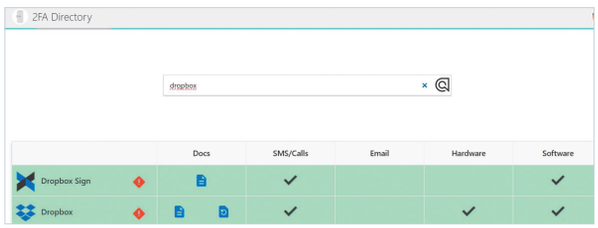

Bild 4: Auf der Webseite 2FA.Directory finden Sie eine Liste aller Onlineservices, die 2FA unterstützen

ein «zweiter Faktor», der möglich ist. Zum Passwort lassen sich meist folgende Faktoren nutzen, die es nach der Eingabe des Kennworts zusätzlich zur Freigabe braucht:

- ein SMS-Code
- ein Code per E-Mail
- eine spezielle Handy-App
- Biometrie (Webcam am Rechner, Daumenabdruck oder Gesicht am Handy)
- eine Authentifizierungs-App wie Googles Authenticator
- ein Telefonanruf (nur für Aktivierungen)
- ein Hardware-Token wie der YubiKey

Die genannten 2FAs sind für viele Onlinedienste nutzbar, etwa für Amazon, OneDrive oder auch Dropbox, Bild 1.

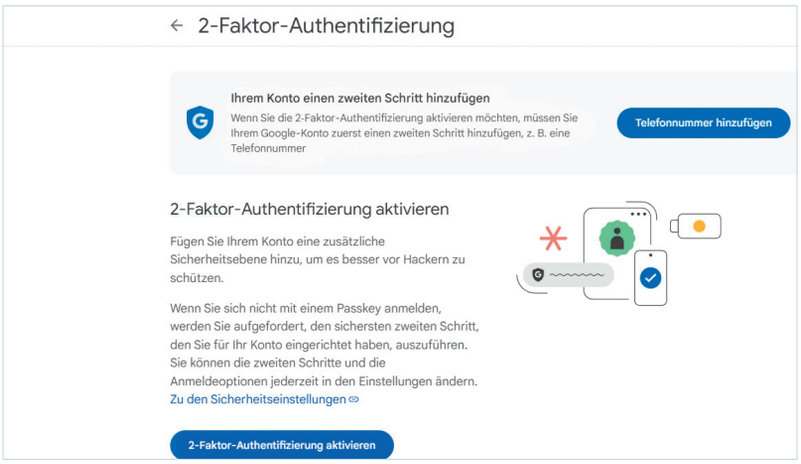

Bild 5: Sichern Sie unbedingt Ihr wichtiges Google-Konto mit 2FA, da dort auch Passwörter hinterlegt sind

Hinweis: In diesem Artikel sprechen wir nicht über den Zugangsschutz zu Banken oder anderen Zahlungssystemen, da diese in der Regel mit anderen Verfahren arbeiten, etwa mit speziellen SecureGo-Apps oder ChipTAN-Lösungen.

Schützt 2FA?

Interessanterweise bieten grosse und mittlere Anbieter seit vielen Jahren eine 2-Faktor-Authentifizierung an. Zu Beginn wurde der Service allerdings nicht weiter beworben, da der stärker geschützte Zugang auch ein höheres Support-Aufkommen bei Problemen bedeutet. Aber dies kann inzwischen kein Argument mehr sein, da weltweit tausende Accounts im Sekundentakt gehackt werden. Das liegt manchmal gar nicht an den Nutzern, sondern an Sicherheitslücken bei den Anbietern, wodurch Hacker gleich an zigtausende Nutzerdaten kommen. Wer das als Übertreibung empfindet, sollte Webportale wie «';--have i been pwned?» (haveibeenpwned.com) oder HPI Identity Leak Checker (sec.hpi.de/ilc) besuchen, Bild 2. Dort finden sich jeweils 14 bis 15 Milliarden Zugangsdaten, die im Darknet veröffentlicht oder verkauft wurden, Bild 3. Das sind in etwa 1,5 Millionen Accounts am Tag!

Falls Sie Ihre E-Mail-Adresse in diesen Datenbanken finden, ist das nicht tragisch, aber Sie müssen trotzdem konsequent handeln und die 2-Faktor-Authentifizierung nutzen. Die gute Nachricht: Sie müssen nicht mal Ihr Passwort ändern – das Aktivieren von 2FA reicht meistens aus.

Tipp: Wenn Sie im Chrome-Webbrowser, in Firefox oder in Edge ein Konto verwenden, um Passwörter sowie E-Mail-Adressen bei Log-ins automatisch einzufügen, prüft der Webbrowser, ob Ihre E-Mail-Adresse in einem Hack auftaucht und informiert Sie.

Wer unterstützt 2FA?

Ohne Übertreibung kann man sagen, dass eigentlich alle Services im Internet, die ein Konto-Log-in nutzen, auch eine 2FA anbieten. Sie müssen diese nur aktivieren.

Grosse Shopping-Portale wie Amazon, eBay oder auch Coop und Migros bieten den Schutz der Log-ins mit 2FA. Aber auch Anbieter von Cloud-Speichern kennen die Schutzfunktion, beispielsweise Dropbox oder OneDrive. Der einzige Unterschied bei den Anbietern ist, welchen Faktor sie unterstützen. Ein Codeversand per SMS ist am weitesten verbreitet. Einmal angefordert und eingegeben, wird das genutzte Gerät (Browser oder Handy) meist als vertrauenswürdig registriert und erfordert 30 bis 90 Tage keine weiteren Zusatzcodes.

Eine gute, aber vielleicht nicht vollständige Übersicht zum Thema 2FA bei Onlinediensten zeigt die Webseite 2FA.Directory unter 2fa.directory/de. Dort können Sie zuerst nachsehen – eventuell schon vor einer Anmeldung –, ob bestimmte Services auch 2FA anbieten, Bild 4. Sie werden sehen, dass das fast immer der Fall ist. Bei einem Eintrag auf der Webseite sehen Sie gleich, welche 2FA-Faktoren unterstützt werden. Der Punkt *Docs* bei einem Eintrag führt Sie per Link auf die technische 2FA-Seite des Anbieters.

Wenn Sie die 2FA-Sicherheitsfunktion suchen, finden Sie diese fast immer bei den Kontoeinstellungen unter dem Punkt *Sicherheit*. Einer der wichtigsten Services: Ihr Google-Konto! Lassen Sie den Zugang schützen, indem Sie sich in Ihr Google-Konto einloggen und zu *Sicherheit* wechseln. Dort finden Sie den Punkt *So melden Sie sich in Google an* und *2-Faktor-Authentifizierung*, Bild 5.

Sobald Sie den Punkt auswählen, müssen Sie zuerst noch einmal Ihr Passwort eingeben. Danach reicht eine Telefonnummer als zweiter Faktor und Sie bekommen Log-in-Codes per SMS. Sie können aber auch ein bei ➜

Google angemeldetes Smartphone verwenden, Bild 6. Dann bekommen Sie eine Sicherheitsabfrage am Smartphone-Display, ob Sie es sind, der sich einloggen will und müssen dies mit *Ja* bestätigen, Bild 7. Das geht auch für mehrere Geräte. Einmal eingerichtet, ist der Schutz aktiv.

Bei anderen Anbietern wie PayPal funktioniert das ähnlich. Im Kontobereich besuchen Sie den Punkt *Einstellungen/Sicherheit* und wählen neben *Einrichten* die *Zweistufige Verifizierung*. Danach haben Sie die Wahl, ob Sie eine Telefonnummer angeben, um SMS-Freigabecodes zu bekommen, Bild 8. Oder Sie nutzen den QR-Code für eine Authenticator-App (dazu gleich mehr).

Authenticator-Apps

Viele Anbieter lassen die Anwenderinnen und Anwender auch eine Authenticator-App nutzen. Dabei handelt es sich um eine App, die in Echtzeit sechsstellige Zahlencodes generiert, die aber immer nur für 30 Sekunden gültig sind. Danach generiert die App neue Codes. Dabei muss zuerst das Log-in-Konto an die Authenticator-App gekoppelt werden, damit die beiden immer den gleichen Code generieren und die Richtigkeit nach der Eingabe geprüft werden kann. Dazu tauschen sie bei der Einrichtung einen per Algorithmus errechneten Schlüssel aus. Klingt kompliziert, ist es aber nicht. Sie laden sich einfach über den Google Play Store oder über den Apple App Store eine Authenticator-App und verknüpfen diese mit einem Konto. Wenn Sie nun einen Dienst in die Liste aufnehmen möchten, reicht es, einen QR-Code per Kamera aufzunehmen.

Am oberen Beispiel von PayPal nehmen Sie den QR-Code einfach auf. Danach wird in der App ein Eintrag *PayPal* erstellt, der die Codes produziert. Bei PayPal müssen Sie nur noch die Nutzung bestätigen – fertig. In der Praxis loggen Sie sich per Passwort bei Ihrem Anbieter ein, danach wird der Zahlencode verlangt, genauso wie bei PayPal, Bild 9.

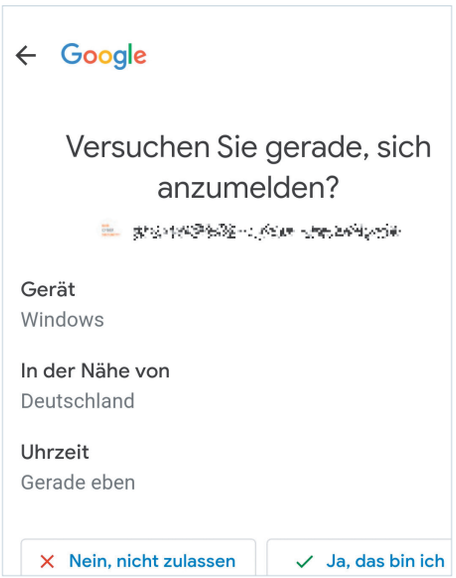

Bild 7: Wurde ein mobiles Gerät angegeben, erscheint beim Log-in eine Abfrage

Bild 8: Nutzen Sie PayPal? Lassen Sie sich SMS-Codes für mehr Sicherheit schicken

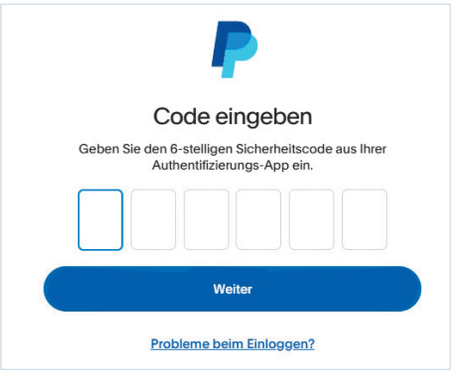

Bild 9: Ohne die Eingabe eines zusätzlichen sechsstelligen Codes geht bei PayPal nichts

Als Authenticator-App empfehlen wir, die Apps von Google oder von Microsoft zu nutzen. Beide gibt es als Android- und iOS-Version. Beide speichern die erfassten Onlinedienste verschlüsselt in Ihrem Konto. Unser Favorit ist Googles Authenticator-App, da diese auch mit den Sicherheitsfunktionen des Chrome-Webbrowsers zusammenarbeitet und alles in einem einzigen Konto verschlüsselt gesichert ist.

Notfallcodes und mehr

Wenn Sie die 2FA-Funktion in Onlineservices aktivieren, erhalten Sie in der Regel immer den Hinweis, dass Sie entweder ein zweites 2FA-Verfahren festlegen sollen oder man bietet Ihnen Notfallcodes an.

Ein zweites 2FA-Verfahren, am Beispiel von Google, ist ein Code per E-Mail oder eine SMS. Wenn Sie beim Log-in Probleme haben, können Sie auswählen, dass Sie dieses Mal einen anderen zweiten Faktor nutzen möchten. Alternativ bietet man Ihnen Notfallcodes an, die sich einmal nutzen lassen. Diese müssen Sie sicher aufbewahren.

Wohin damit? Wenn Sie einen Passworttresor wie das unabhängige Windows-Programm KeePass (Download-Link: keepass.info/download.html) nutzen, können Sie dort die Codes direkt zu den normalen Log-in-Daten hinterlegen, Bild 10. Das Tool gibt es auch für Android-Geräte.

Unser Tipp: Wenn Sie KeePass als Passworttresor nutzen, können Sie die hochverschlüsselte Datenbank (KDBX-Datei) in Ihrem eigenen Cloud-Speicher ablegen, teilen und sie so mit dem PC und anderen mobilen Geräten nutzen. Sie haben damit eine «eigene» hochsichere Cloud-Lösung für Ihre Passwörter.

Richten Sie unbedingt einen weiteren 2FA-Faktor ein oder speichern Sie die Notfallcodes. Nur so können Sie auch immer die Einstellungen für 2FA zurücksetzen.

Windows Hello und 2FA

Mit Windows 11 und teilweise mit den letzten Updates von Windows 10, verwenden Sie zwangsweise einen zweiten Faktor bei der Windows-Anmeldung. Ausser dem Passwort

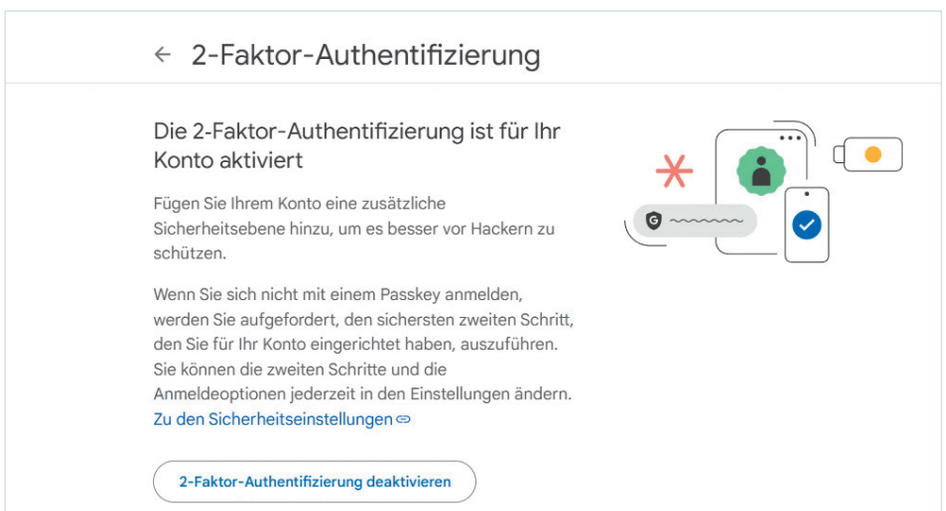

Bild 6: Der Google-Konto-Schutz bietet viele 2FA-Optionen: entweder per Telefonnummer, per QR-Code für die Authenticator-App oder per Angabe eines mobilen Geräts

MEINUNG: Besser keine Biometrie nutzen

Als Autor mit über 30 Jahren Erfahrung in der IT-Welt habe ich eine persönliche Abneigung gegen biometrische Verfahren wie Fingerabdruckscanner, Gesichts-ID oder Iris-Scan. Warum? Ich denke, wir Nutzer haben diese Merkmale nur jeweils ein Mal und falls diese ins Internet gelangen, lassen Sie sich nicht mehr ändern. 2018 gab es einen Diebstahl von Teilen einer staatlichen indischen Datenbank mit über einer Million biometrischer Daten. Aktuelle Geräte wie Smartphones grosser Hersteller oder Anbieter wie Google sichern ihre biometrischen Daten bestimmt besser. Aber so lange es Alternativen wie 2FA per SMS, Authenticator-Apps oder Freischalt-Apps gibt, verwende ich diese. Ich nutze die Google Authenticator-App und Notfallcodes, falls ich das Gerät verliere. Auch der Zugriff auf die Authenticator-App auf dem Smartphone ist durch die Privatsphärenfunktion geschützt, mit der ich das Handy entsperre.

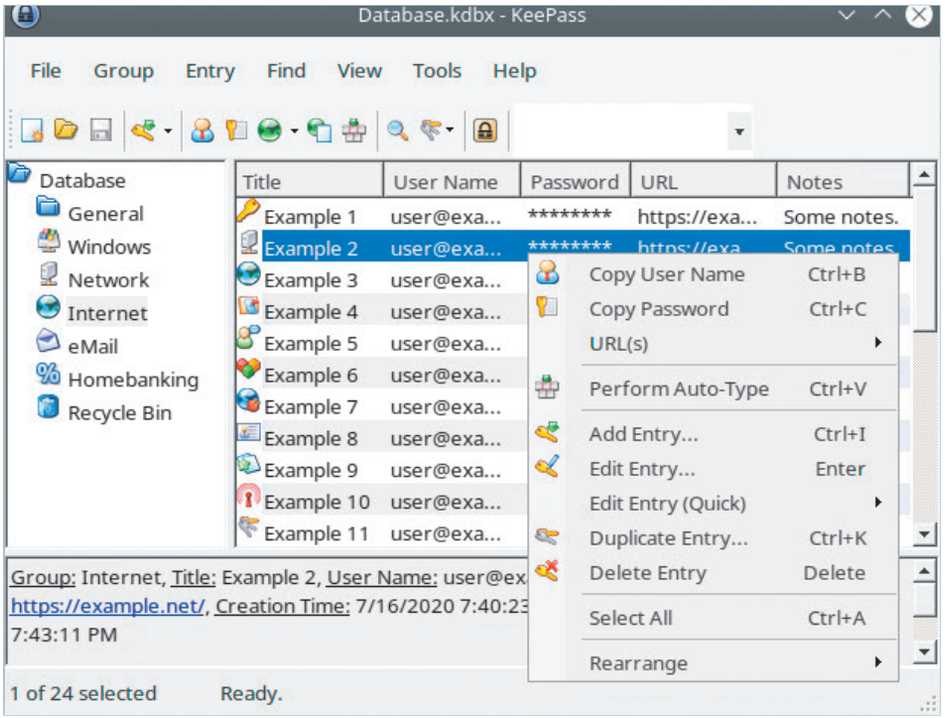

Bild 10: Legen Sie Ihre Passwörter und Notfallcodes geschützt im kostenlosen, hochsicheren Passworttresor KeePass ab

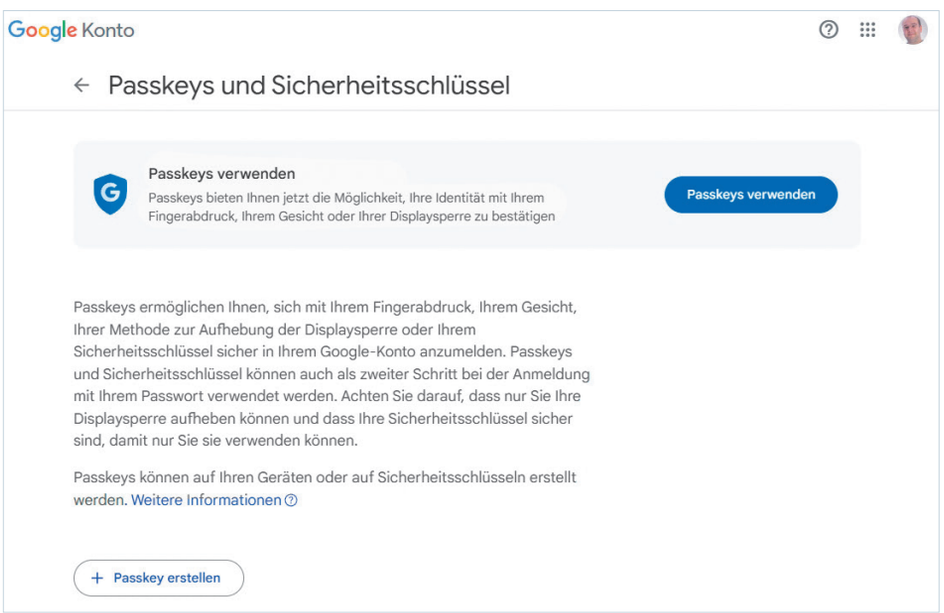

Bild 12: In Ihrem Google-Konto aktivieren Sie die Nutzung von Passkeys, dann reicht eine PIN für den Log-in oder ein biometrischer Faktor

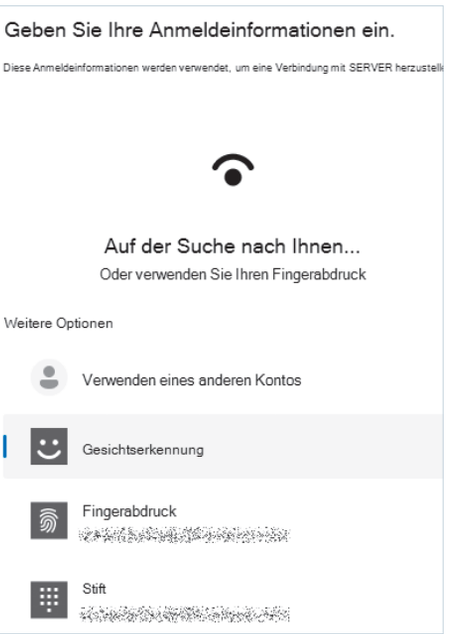

Bild 11: Sie können den Windows-Zugriff bei Windows Hello mit einer Face-ID absichern

für Ihr Windows-Konto «zwingt» Windows Sie zur Nutzung eines weiteren Faktors. Meistens ist das eine vierstellige PIN beim Log-in auf der Oberfläche. Bei Windows Hello können Sie aber auch den weiteren Faktor wechseln, Bild 11. Dabei können Sie etwa Ihre Webcam für eine Face-ID/Gesichtserkennung nutzen oder Sie verwenden einen Fingerabdruckscanner. Den müssen Sie aber extern anschliessen. Einige Notebooks haben diesen eingebaut. Als oberste Sicherheit lässt sich auch ein Hardware-Token verwenden, etwa ein spezieller USB-Stick zur Freigabe.

Passkeys = 2FA?

Sie wurden bestimmt schon öfter aufgefordert, Passkeys für ein Konto anzulegen. Das ist aber keine 2FA, da Passkeys in Zukunft die Passwörter ersetzen sollen und 2FA nur ein Sicherheitszusatz für Passwörter ist. Bei Passkeys wird nach der Anmeldung ein Schlüsselpaar (privater und öffentlicher Schlüssel) zur Authentifizierung generiert. Es wird keine Eingabe mehr verlangt, da der Schlüssel auf dem Gerät des Nutzers liegt. Passkeys gelten als sicherer als Passwörter, da sie nicht anfällig für Phishing oder Passwortlecks sind. Unter Windows beispielsweise werden Passkeys im Zusammenhang mit Windows Hello gespeichert, mit dem sich Nutzer auch beim Start von Windows anmelden, etwa mit einer PIN oder einem biometrischen Verfahren. Um allerdings die Schlüssel auch auf anderen Geräten nutzen zu können, muss man über ein Google-Konto verfügen. Ist das vorhanden, werden alle Passkeys automatisch mit Google synchronisiert und dort verschlüsselt abgelegt. Sollen die Passkeys auf andere Geräte übertragen werden, muss zuvor im Konto zum Beispiel eine Sicherheits-PIN zur Transferfreigabe erstellt werden, Bild 12.