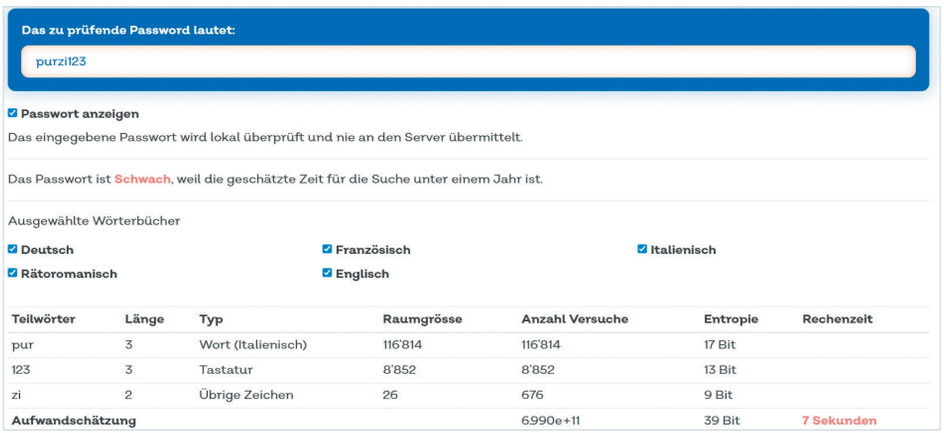
Ist Ihr Passwort sicher?

Nur mit sicheren Passwörtern und den neuesten Technologien sind Ihre Daten und Ihre Konten im Internet effizient geschützt. **Wir haben für Sie die ultimativen Tipps zum Passwort-Check!**

VON MARKUS SELINGER

Jedes Jahr fertigen einige Hersteller von Sicherheits-Software kleine Studien an, welche die am meisten genutzten Passwörter auflisten. So hat vor Kurzem der Anbieter Nordpass seine neue Liste veröffentlicht, die sich nach Ländern sortieren lässt. Weltweit auf Platz 1 steht das Passwort «123456» mit über 21 Millionen gefundenen Quellen. Die Top-3-Passwörter für die Schweiz sind laut Nordpass «dominaria», «admin» und «purzi123». Warum diese Passwörter gewählt wurden oder woher sie stammen, ist nicht bekannt und auch unwichtig. Allerdings haben sie alle eines gemeinsam: Ein herkömmlicher PC könnte etwa «purzi123» in schnellen 1 bis 2 Sekunden errechnen.

Hier ein paar Beispiele, wie schnell bereits normale Computer mit ihrem PC- oder Grafikkartenprozessor per Brute-Force-Attacke ein Passwort erraten. Ein Kennwort mit acht Kleinbuchstaben dauert nur 1 Sekunde. Hat das Passwort einen Grossbuchstaben, geht es vielleicht 2 Sekunden. Auf der Webseite unter passwortcheck.ch, einem Service des Datenschutzbeauftragten des Kantons Zürich, kann man die genannten Beispiele ausprobieren. Keine Angst: Die geprüften Passwörter verlassen dabei den Computer nicht. Die angezeigten Zeiten hängen vom genutzten Rechner und seiner Power ab.



Teilwörter	Länge	Typ	Raumgrösse	Anzahl Versuche	Entropie	Rechenzeit
pur	3	Wort (Italienisch)	116'814	116'814	17 Bit	
123	3	Tastatur	8'852	8'852	13 Bit	
zi	2	Übrige Zeichen	26	676	9 Bit	
Aufwandschätzung				6.990e+11	39 Bit	7 Sekunden

Bild 1: Die Webseite Passwortcheck.ch, ein Service des Datenschutzbeauftragten des Kantons Zürich, prüft die Stärke Ihrer Passwörter

Bild: Erstellt mit Google Gemini

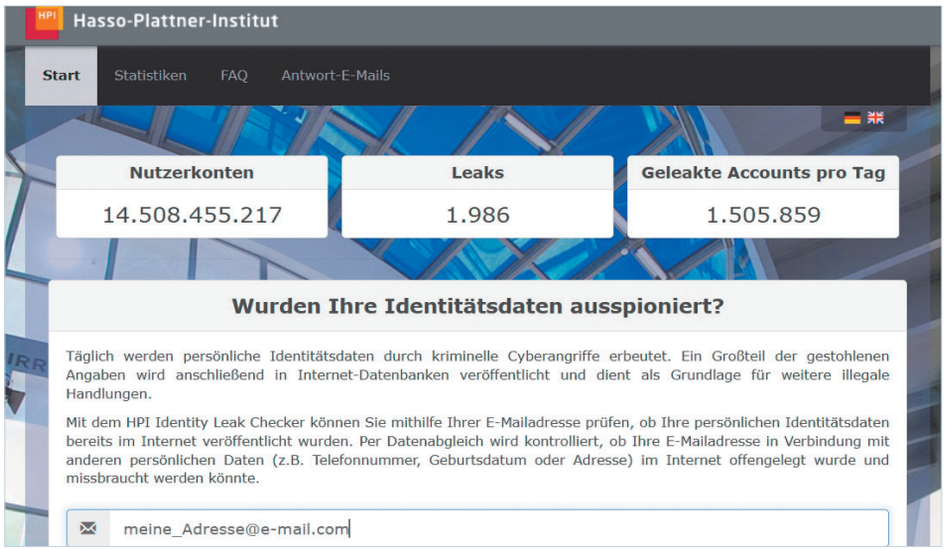


Bild 2: Das Hasso Plattner Institut sammelt E-Mail-Adressen und Passwörter aus Datenpannen – prüfen Sie die Datenbank mit Ihrer eigenen E-Mail-Adresse

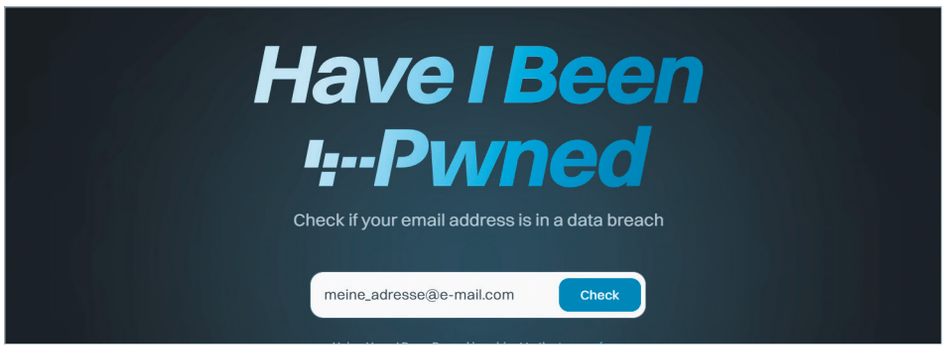


Bild 3: Der Sammelservice für E-Mail-Adressen und Passwörter aus Datenpannen «Have I Been Pawned» kennt inzwischen über 2 Milliarden Passwörter

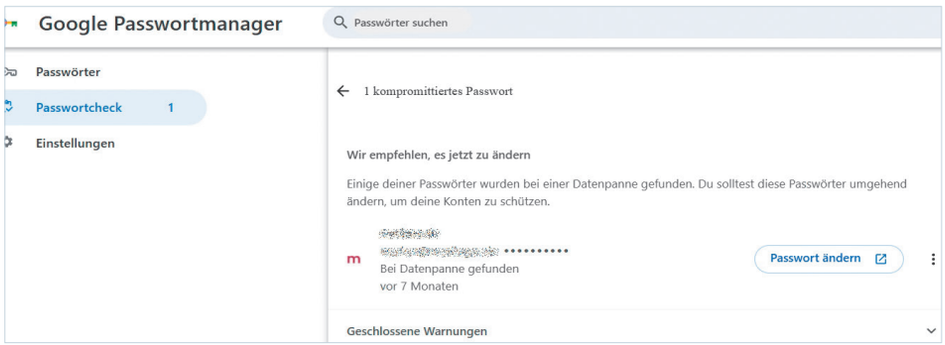


Bild 4: Der Passwortmanager von Chrome prüft auf Wunsch alle vorhandenen E-Mail-Adressen und Passwörter, ob sie in Datenpannen auftauchen

Bild 5: Kasperskys «Passwort Checker» zeigt die Stärke eines Passworts und sagt, ob es bereits im Netz unterwegs ist

Wir nutzen im Schnelltest einen flotten i7-Intel-Prozessor, was sich in sehr kurzen Errechnungszeiten bemerkbar macht. Der Service nutzt zum «Ausprobieren» einfache Wörterbücher. Je mehr Wörterbücher dabei verwendet werden, umso schneller geht es, Bild 1.

Ein Beispiel: Das Berechnen des Passworts «TanteMargot12345» dauert mit dem deutschen Wörterbuch 49 Jahre. Nimmt man die Wörterbücher Französisch, Italienisch, Rätoromanisch und Englisch dazu, sinkt die Zeit auf lediglich 7 Stunden.

Tipp: Nutzen Sie eine einfache Strategie bei Ihren Passwörtern: Immer, wenn Sie Ihre persönlichen Daten angeben und vielleicht sogar Kontodaten oder Bezahlinformationen hinterlegen, sollten Sie ein neues, noch nie verwendetes Passwort verwenden. Dazu sollten Sie eine 2-Faktor-Authentifizierung oder Passkeys nutzen (dazu später noch mehr). Wie einfach Sie das umsetzen und wie schnell Sie eigene Passwörter prüfen, zeigen Ihnen die folgenden Tipps.

Passwort-Checker nutzen

Im Internet finden Sie kostenlose Datenbanken, mit denen Sie prüfen können, ob Ihre E-Mail-Adresse und Ihre Passwörter bereits im Internet bekannt sind. Die grössten und vertrauenswürdigsten Datenbanken sind «Have I Been Pwned» (haveibeenpwned.com) und «HPI Identity Leak Checker» (sec.hpi.de/ilc), Bild 2. Auf diesen Serviceseiten prüfen Sie per E-Mail-Angabe, ob Ihre Adresse und Ihre Passwörter in grossen Datenpannen auftauchen. Der Service von «Have I Been Pawned» hat aktuell über 2 Milliarden Passwörter in seiner Datenbank, Bild 3.

Nutzen Sie den Chrome-Webbrowser, haben Sie einen eingebauten Passwort-Checker. Allerdings nur die Passwörter, die per Google und Chrome erfasst sind. Probieren Sie es aus: In Chrome klicken Sie unter dem *Drei-Punkte*-Symbol oben rechts auf *Passwörter und Autofill/Google Passwortmanager/Passwortcheck*. Google prüft jetzt in grossen Datenbanken, ob das Passwort bei einer Datenpanne gefunden wurde und somit kompromittiert ist, Bild 4.

Achtung: Nutzen Sie nicht einfach alle möglichen Passwort-Checker die Sie im Internet finden. Unter Umständen verteilen Sie so Ihre Passwörter auf unseriösen Seiten! Wenn Sie ein Passwort prüfen möchten, sollten Sie es zum Test verändern, aber die Struktur behalten. Wäre das Passwort etwa «TanteErna123!» könnten Sie «OnkelPaul456!» prüfen lassen.

Eine gute Anlaufstelle dazu ist etwa der «Kaspersky Password Checker» unter der Internetadresse password.kaspersky.com/de. Dort wird unser Beispiel-Passwort als zu schwach bewertet, da es eigentlich zu kurz ist. Wenn Sie auf der Seite auch echte Passwörter testen, gibt Ihnen Kaspersky gleich an, ob das Passwort in einer Datenpanne gefunden wurde. Ein Check mit dem Passwort «123456» gibt an, dass es bereits über 42 Millionen Mal in geleakten Passwort-Datenbanken aufgetaucht ist, Bild 5.

Wenn Sie Chrome oder Firefox als Browser nutzen und darin mit Ihrem Google-Konto angemeldet sind, können Sie sich bei der Anmeldung an einem neuen Account automatisch ein starkes Passwort generieren lassen. Der Generator meldet sich selbstständig und unterstützt Sie, sobald Sie auf einer Seite ➜

zum Festlegen eines Passworts aufgefordert werden. Danach speichert Google das Passwort auch auf Ihren Wunsch hin in seinem internen Passwortmanager und synchronisiert die Daten mit Ihrem Google-Konto. Somit stehen die Passwörter ebenfalls auf anderen Geräten bereit, etwa dem Windows-PC oder dem Smartphone, Bild 6.

Es existieren zwar vertrauenswürdige Webseiten wie die erwähnte von Kaspersky, aber es gibt einen viel sichereren Weg, um Passwörter auf ihre Stärke bzw. Sicherheit zu prüfen: kostenlose Passwortmanager! Hier haben Sie die Auswahl zwischen:

- Cloud-Passwortmanagern wie 1Password, LastPass oder Bitwarden mit integrierten Passwortgeneratoren und Sicherheitsscans.
- Browsererweiterungen, die direkt beim Erstellen und Speichern von Passwörtern Sicherheitshinweise geben.
- Windows-Passwortmanagern mit lokal gespeicherter Datenbank und eingebautem Passwort-Checker sowie -Generator.

Cloud-Passwortmanager

In den vergangenen Jahren haben sich immer mehr Passwortmanager im Internet etabliert. Der Vorteil: Man kann sich auf jedem PC in seinem Passwortdienst anmelden und seine Log-in-Daten abrufen. Das funktioniert auch auf mobilen Geräten, wie Tablets und Smartphones. Leider sind die meisten Anbieter nicht mehr komplett kostenfrei oder haben nur kurze Testphasen. Definitiv kostenlos ist der Service von Bitwarden, Bild 7.

Sie finden den Anbieter im Internet unter bitwarden.com. Der Service ist natürlich auch in deutscher Sprache verfügbar. Die Nutzung als Privatperson ist kostenlos. Eine Mini-Premium-Version kostet 8 Franken pro Jahr. Es lässt sich auch ein Familienpaket buchen für etwas über 30 Franken im Jahr und so die Datenbanken teilen. Der Service lässt sich direkt online nutzen, per installierter App auf mobilen Geräten oder per Browsererweiterung für Chrome, Firefox, Edge, Safari und sogar Opera. Wenn Sie zum Beispiel von der Google-Passwortverwaltung in Chrome umsteigen möchten, hilft Ihnen Bitwarden mit einem Export-Import-Prozess.

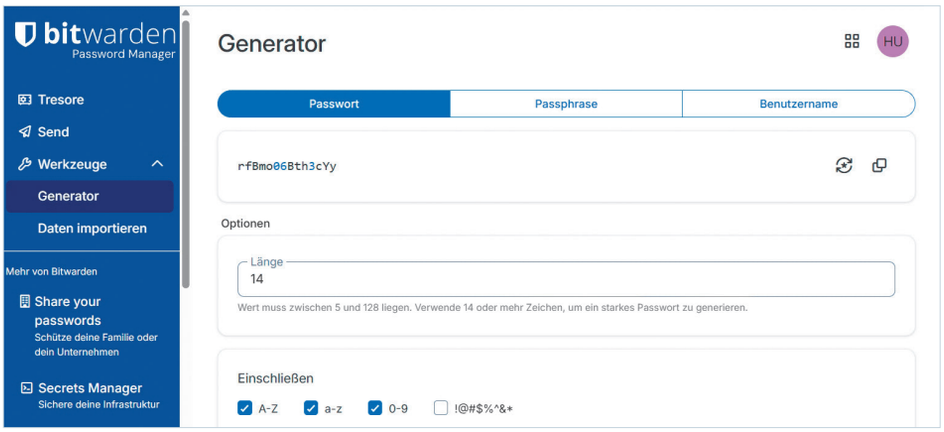


Bild 8: Bitwarden bietet einen Passwortgenerator, der genau einstellen lässt, wie stark ein Passwort sein soll oder welche Länge es haben muss

Im Tool finden Sie neben der Passwortverwaltung auch noch einen sehr umfangreichen Passwortgenerator, Bild 8. Dieser zeigt Ihnen auch an, wie sicher ein Passwort ist – oder auch nicht. Vorhandene Passwörter lassen sich zwar auf ihre Stärke überprüfen, aber nur ausserhalb des Tools auf der Webseite. Sie werden sehen, dass die meisten zu schwach sind.

Lokale Passwort-Tools

Wenn Sie Cloud-Angeboten nicht vertrauen möchten, können Sie lokale Passwortmanager nutzen. Dabei haben Sie eine grosse Auswahl. Nutzen Sie eine Security-Software in einer Premium-Version, haben Sie meist einen guten Passwortmanager mit im Gepäck. Schauen Sie nach: Sie finden einen zum Beispiel in den Premium-Versionen bei Avira, Bitdefender, Eset, Kaspersky, McAfee oder Norton, Bild 9.

Mit diesen Passwort-Tools haben Sie nicht nur ein Check-Tool für vorhandene Passwörter zur Hand. Sie können Passwörter damit verwalten und neu generieren. Wenn Sie ein Paket mit mehreren Lizenzen haben, dann synchronisiert sich der Manager auch über mehrere Geräte.

Haben Sie kein Passwort-Tool in Ihrer Schutz-Software, gibt es eine kostenlose Alternative, die dazu auch noch hochsicher ist: KeePass für Windows (keepass.info), Bild 10. Das Tool ist zwar nur für einen Arbeitsplatz gedacht, aber mit einem Trick lässt es sich auch zum privaten Cloud-Tool verwandeln. Wie das geht, erklärt der Artikel «Ein Safe für Passwörter» in PCtipp 10/2025 ab S. 14. Abonnenten finden den Artikel als PDF unter dem Link pctipp.ch/epaper.

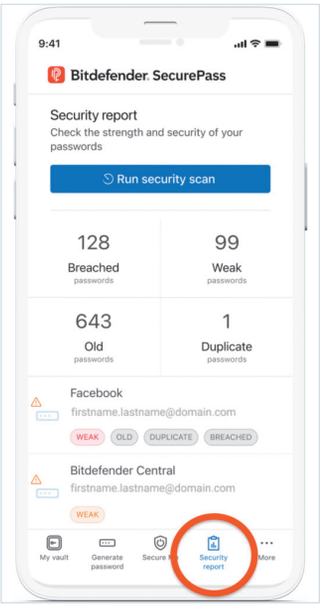


Bild 9: Die Security-Tools als Premium-Version haben oft Passwortmanager dabei

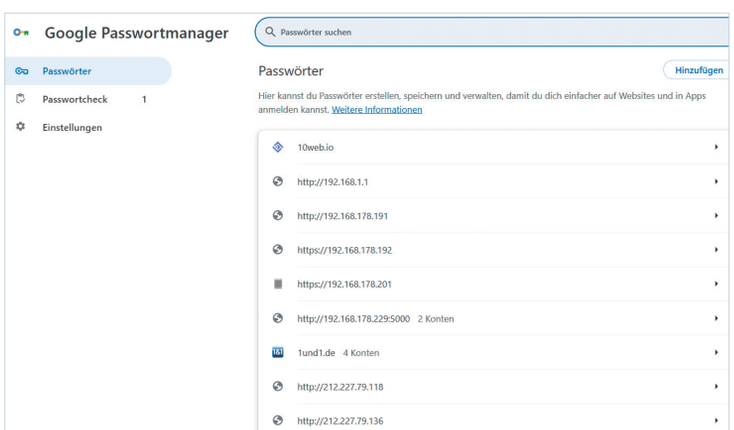


Bild 6: Die im Google-Konto gesicherten Passwörter stehen an anderen Geräten für ein Log-in bereit – egal ob auf dem PC oder auf dem Handy

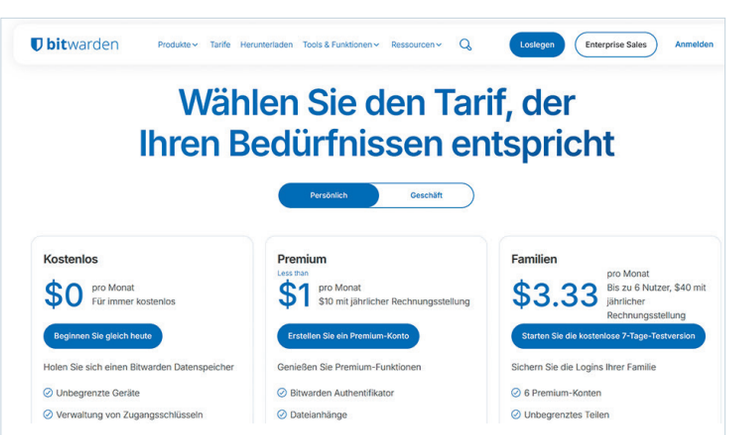


Bild 7: Bei privater Nutzung ist der Bitwarden-Passwortmanager samt Check-Tool kostenlos und bietet jede Menge

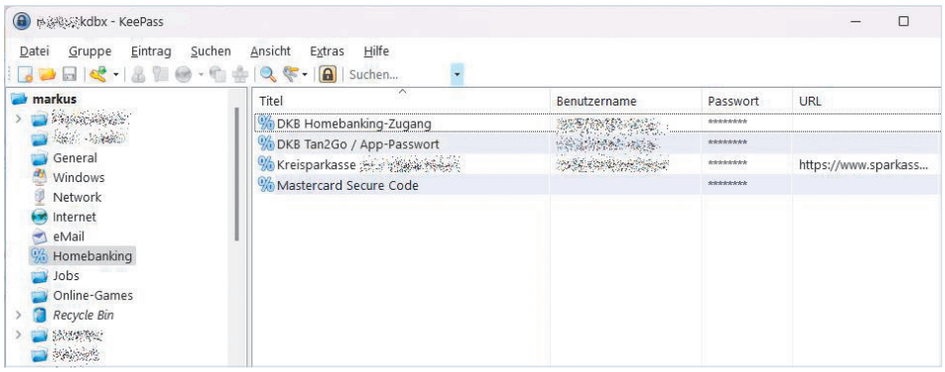


Bild 10: Das kostenlose Passwort-Tool KeePass gilt als eines der besten. Er lässt sich in vielen Sprachen nutzen und hat ein Dateiformat, das auch andere Tools unterstützen

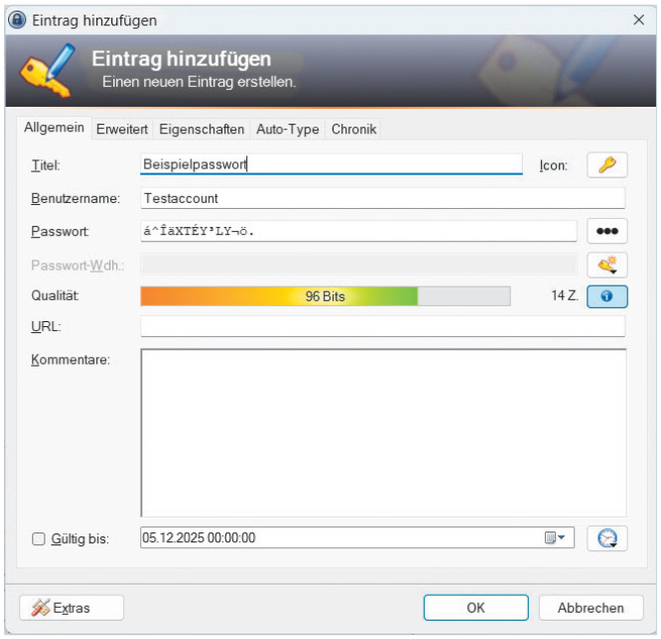


Bild 11: KeePass ist von Passwortexperten entwickelt, die sogar das Passwort «á^ÎäXTÉY³LY¬ö.» nicht besonders sicher finden

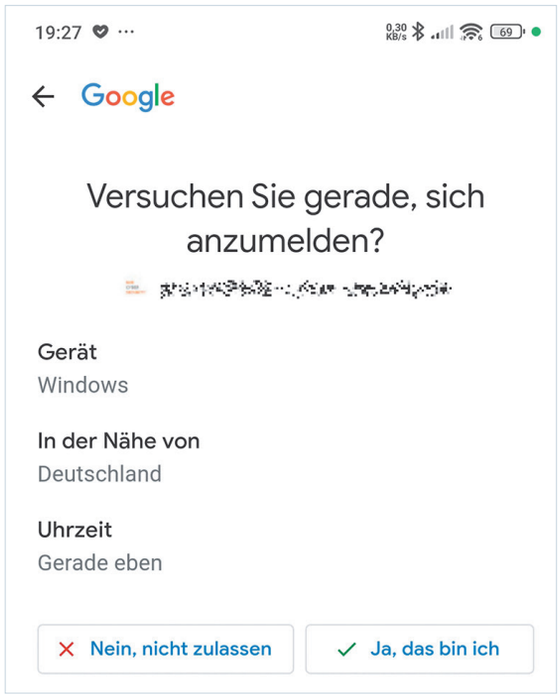


Bild 12: Nutzen Sie die 2-Faktor-Authentifizierung von Google, das erhöht die Sicherheit massiv

Das Tool verwaltet ihre Zugangsdaten gut gesichert und ist nur per starkem Masterpasswort zugänglich. Im Programm legen Sie Ihre Passwörter ab oder nutzen den internen Generator. Dieser lässt sich ganz spezifisch einstellen. Das heisst, dass Sie sogar festlegen können, aus welchen Buchstaben, Zeichenlängen, Sonderzeichen oder Zahlen ein Passwort bestehen soll. Die Sicherheit für ein Passwort wird in KeePass in Form von «Entropiebits» von 0 bis 256 dargestellt. Alles von 80 Bits bis 112 Bits gilt als «mässig» sicher. Das Passwort «á^ÎäXTÉY³LY¬ö.» hat zwar nur 96 Bits, aber die anfangs erwähnte Website Passwortcheck.ch stuft es als sehr sicher ein. KeePass ist da strenger, **Bild 11**. An dieser Stelle kommt die alte Expertendiskussion auf: Wird ein Passwort extrem sicher, ist es kaum noch anwendbar. Ohne einen Passwortmanager, liesse sich dieses Passwort nirgendwo verwenden. Daher muss eine andere, praktikablere Lösung her und die wurde bereits gefunden.

Gute Alternativen

Eine bereits alte Alternative ist das Verwenden sogenannter Passphrasen. Dabei merkt sich der Anwender einen ganzen Satz, aber verwendet nur die Anfangsbuchstaben für das Passwort. So wäre etwa «Unser Hund der kleine Max springt über 276 Zäune!» das recht starke Passwort «UHdkMsü276Z!». Allerdings lässt sich dieser Trick nicht auf die zahlreichen benötigten Passwörter im Internet anwenden und viele Nutzer setzen daher auf nur drei oder vier gleiche Passwörter. Das ist den meisten nicht auszutreiben, da es für viele alternativlos ist. Daher sagen Experten: «Bleiben Sie dabei, sofern Sie zusätzlich eine 2-Faktor-Authentifizierung oder Passkeys nutzen».

Der Einsatz einer 2-Faktor-Authentifizierung oder von Passkeys macht Ihnen in Sachen Passwörter das Leben leichter. Das Ganze funktioniert so:

- **2-Faktor-Authentifizierung (2FA):** Für ein Log-in gibt es ein Passwort und als sogenannten zweiten Faktor eine weitere Bestätigung. Diese erfolgt etwa durch die Angabe eines Codes per SMS oder E-Mail. Möglich ist auch die Eingabe einer Nummernfolge, die eine Authenticator-App vorgibt, etwa der Google Authenticator. Es gibt aber auch diverse Hardware-Token. Das sind USB-, NFC- oder Bluetooth-Sticks – manche Sticks zeigen auch auf einem Mini-Display einen Code an, der jede Minute wechselt.

Wer zum Beispiel einen Google-Account verwendet, kann noch eine andere 2FA-Technik nutzen. Dabei wird auf einem Smartphone ein Hinweis angezeigt, dass sich jemand am Google-Konto einloggen will, und man muss *Ja* oder *Nein* antippen, **Bild 12**.

- **Neue Passkeys:** Die Technik der Passkeys ist relativ neu und stellt eine Weiterentwicklung der 2-Faktor-Authentifizierung dar. Dabei loggt sich der Nutzer mit oder auch ohne Passwort ein und bestätigt den Zugang meist an einem mobilen Gerät und einer biometrischen Erkennung. Das ist mehrheitlich ein Fingerabdruck oder ein Gesichtsscan.

Viele Nutzer kennen diese Art des Log-ins auch bei Windows. So sind etwa die Log-in-Daten bei Windows im System mit Namen und Passwort hinterlegt. Wird unter Windows eine Kontobestätigung benötigt, muss der Anwender den zuvor festgelegten Windows-Hello-PIN angeben oder den Account per Webcam und einem Gesichtsscan freigeben.

Der Einsatz der beiden Technologien hat für den Anwender viele Vorteile: Verliert etwa ein Anbieter durch einen Hack oder eine Datenpanne die Zugangsdaten eines Nutzers, so kann niemand etwas damit anfangen, da der zweite Faktor zur Freigabe fehlt.

Allerdings gibt es beim Thema Passkeys etwas zu bedenken. Nutzen Sie diese mit einem biometrischen Faktor wie einem Fingerabdruck oder dem Gesichtsscanner ist der Zugang zu einem Account ganz persönlich an Sie gebunden. In einem Notfall, wenn eine andere Person sich in Ihrem Sinne einloggen soll, kann sie das nicht ohne ihre persönliche Anwesenheit. Daher ist die Freigabe per PIN oder durch ein Freigabemuster auf einer 9-Punkte-Matrix zu empfehlen. Diese Informationen können Sie gefahrlos weitergeben und bei bedarf auch wieder ändern.

So muss der Angehörige keine Accountdaten haben und der PIN ist nur zu nutzen, wenn er das Gerät hat. Hacker haben das Smartphone auf keinen Fall zur Hand. ●