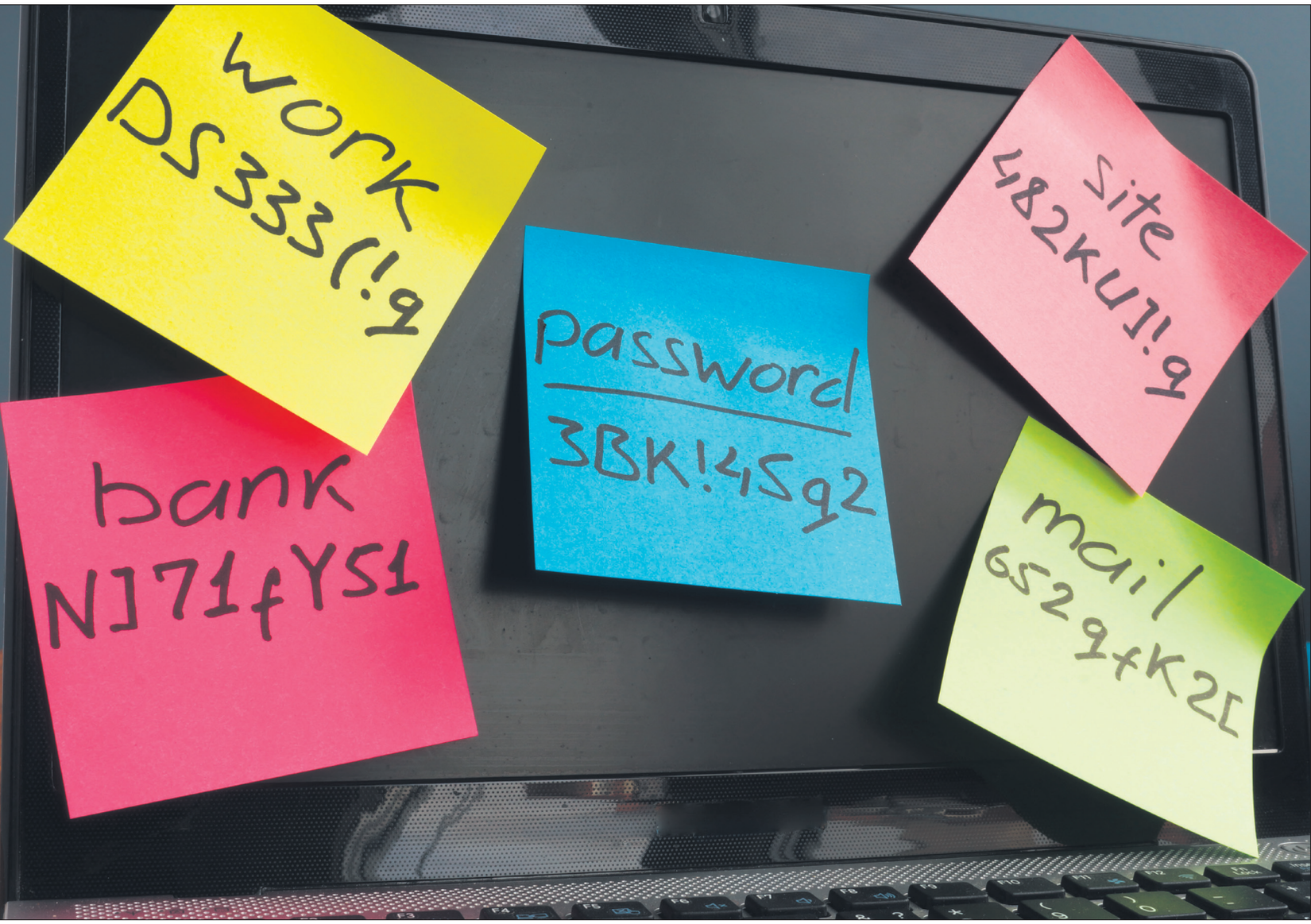

Sicherheit mit Mass

Sichere Kennwörter sind heute zwar ein Muss. Doch die Tipps dazu wirken fast schon grotesk und um die bösen Hacker ranken sich zu viele Mythen. **Deshalb wird es höchste Zeit, das Thema neu zu beurteilen – doch dieses Mal mit Augenmass.** ● VON KLAUS ZELLWEGER

Vermutlich weiss niemand, wann die Empfehlungen für den Umgang mit Kennwörtern aus dem Ruder gelaufen sind. Heute ist in den meisten Artikeln über «sichere Kennwörter» zu lesen, dass nur ein Modell wie *w4w2-q%5?-b22T-3#4** ein gutes Kennwort ist – weil es furchtbar lang und entsetzlich kompliziert ist. Vielleicht werden solche abstrusen Empfehlungen auch deshalb abgegeben, weil kein Ratgeber die Verantwortung übernehmen will, wenn ein schwaches Kennwort zu Problemen führt.

Und doch: Die Gefahr, die von schwachen Kennwörtern ausgeht, wird oft überschätzt. Dazu mischen sich diffuse Ängste über eine mindestens genauso diffuse Bedrohungslage. Diese werden wir ins rechte Licht rücken.

Kenn deinen Feind

Was ist also ein «sicheres Kennwort»? Für eine Antwort muss zuerst die Bedrohungslage analysiert werden. Wenn Sie eine Einkaufsliste mit Ihrer besseren Hälfte über einen Cloud-Dienst teilen, dann ist ein Kennwort wie *1234* so gut wie jedes andere auch. Es gibt keinen Grund, sich das Leben künstlich schwer zu machen, weil niemand – wirklich niemand – auch nur das geringste Interesse an dieser Einkaufsliste zeigen wird. Und falls doch, kann der Eindringling höchstens den Speck von der Liste streichen.

Wenn bei einem Onlinekonto oder Cloud-Dienst hingegen persönliche und finanzielle Daten gespeichert werden, ist ein längeres Kennwort angebracht. Doch beim Online-

Foto: Shutterstock/Vitalii Vodolazskyi

banking müssen Sie das ironischerweise gar nicht so eng sehen; warum das so ist, erklären wir später.

Bei der Wahl des Kennworts sollten Sie auch berücksichtigen, dass Sie es manchmal unter schwierigen Bedingungen eingeben müssen, etwa am Fernseher mit der popeligen Fernbedienung. Wenn Sie bei jedem Einkauf im Microsoft-Store an der Spielkonsole ein 16-stelliges Kennwort mit Sonderzeichen eingeben müssen, weil das so empfohlen wird, dann scheint *1234* plötzlich eine reizvolle Alternative – und das wäre in diesem Fall genauso verkehrt, **Bild 1**.

Tipp: Verwenden Sie einen kurzen Kennsatz, den Sie sich für die Eingabe leicht merken, aber niemand erraten kann, etwa: «1 Saft trinken» oder «12 Zwerge?» oder «Nicht mit mir!». Solche Kennsätze sind nicht zu knacken, aber einfach zu bewirtschaften.

Die Suche nach dem Sinn

Doch warum werden an jeder Ecke sinnlos komplizierte Kennwörter empfohlen, die sich kein Mensch verinnerlicht? Die simple Wahrheit lautet, weil sie einen hervorragenden Schutz bieten – aber nur gegen eine einzige Form der Attacke: Brute Force, zu Deutsch etwa «rohe Gewalt». Bei einer Brute-Force-Attacke wird von einem Computer blindwütig jede Buchstaben- und Zahlenkombination ausprobiert, bis das Kennwort aufgedeckt wird. Eine Brute-Force-Attacke könnte zum Beispiel auf einem modernen PC geritten werden, wobei der Grafikkarte die wichtigste Rolle zukommt; denn selbst eine nicht ganz tauschfrische Nvidia GeForce GTX 1080 schafft ungefähr 30 Millionen Attacken pro Sekunde, **Bild 2**. Die dazugehörige Software gibt es in den Abgründen des Internets.

Bild 2: Grafikkarten sind das wichtigste Element bei einer Brute-Force-Attacke

Allerdings nimmt der Aufwand für den Angreifer explosionsartig zu, sobald sich Zeichen und Sonderzeichen häufen. Werden nur Ziffern verwendet, stehen zehn Zeichen zur Auswahl (0 bis 9). Ein Möchtegern-Kennwort wie *1234* ist in spätestens 0,3 Millisekunden geknackt (siehe Tabelle unten). Werden hingegen Gross- und Kleinbuchstaben verwendet, stehen 52 Zeichen zur Auswahl. Für eine solche Mischung aus acht Zeichen rechnet derselbe PC bereits 21 Tage, wenn das Kennwort erst im letzten Versuch gefunden wird. Kommen alle verfügbaren Buchstaben, Sonderzeichen und Ziffern zum Einsatz, braucht der PC im dümmsten Fall für acht Zeichen ganze sieben Jahre. Bei 16 Zeichen sind es sogar 47 Billiarden Jahre – und bis dahin sind Ihre Geheimnisse vermutlich nicht mehr relevant.

Nun könnten Sie sich also mit komplexen Kennwörtern erfolgreich gegen Brute-Force-Attacken wappnen. Doch mit an Sicherheit grenzender Wahrscheinlichkeit werden Sie nie das Opfer eines solchen Angriffs. Diese ➜

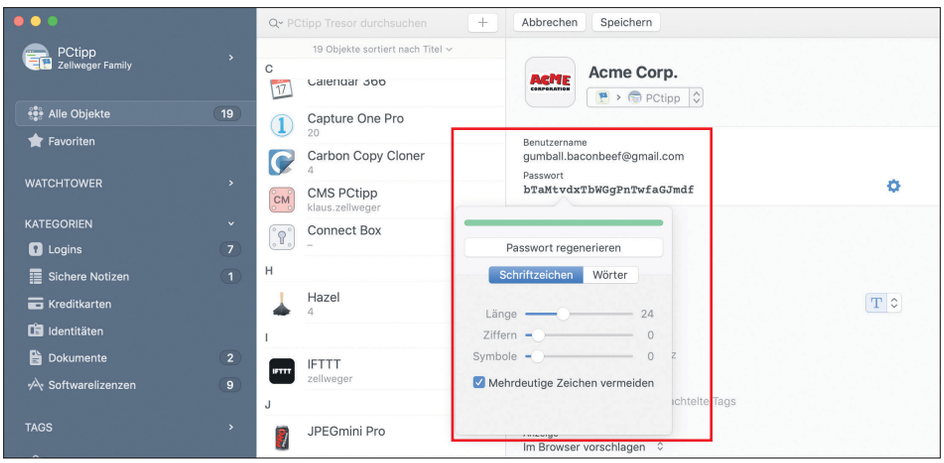

Bild 1: Wenn Kennwortmanager Vorschläge machen, kommt nicht unbedingt Gutes dabei raus

Dauer für Brute-Force-Attacken

		Nur Zahlen	Kleinbuchstaben	Gross- und Kleinbuchstaben	Gross-, Kleinbuchstaben und Zahlen	Alle Symbole auf der Tastatur
Beispiele		1234	ameisen	QrtM	F3P9mN	z&M@P#3
Mögliche Zeichen		10	26	52	62	95
Zeichenzahl	4	0,3 Millisekunden	15 Millisekunden	24 Millisekunden	490 Millisekunden	2,7 Sekunden
Länge des Kennworts	5	3 Millisekunden	400 Millisekunden	13 Sekunden	31 Sekunden	4,3 Minuten
	6	33 Millisekunden	10 Sekunden	11 Minuten	32 Minuten	6,8 Stunden
	7	330 Millisekunden	4,5 Minuten	9,5 Stunden	33 Stunden	27 Tage
	8	3,3 Sekunden	1,9 Stunden	21 Tage	84 Tage	7 Jahre
	9	33 Sekunden	2,1 Tage	2,9 Jahre	14 Jahre	670 Jahre
	10	5,6 Minuten	54 Tage	150 Jahre	890 Jahre	$6{,}3 \times 10^4$ Jahre
	11	56 Minuten	3,9 Jahre	$7{,}9 \times 10^3$ Jahre	$5{,}5 \times 10^4$ Jahre	6×10^6 Jahre
	12	9,3 Stunden	100 Jahre	$4{,}1 \times 10^5$ Jahre	$3{,}4 \times 10^6$ Jahre	$5{,}7 \times 10^8$ Jahre
	13	3,9 Tage	$2{,}6 \times 10^3$ Jahre	$2{,}1 \times 10^7$ Jahre	$2{,}1 \times 10^8$ Jahre	$5{,}4 \times 10^{10}$ Jahre
	14	39 Tage	$6{,}8 \times 10^4$ Jahre	$1{,}1 \times 10^9$ Jahre	$1{,}3 \times 10^{10}$ Jahre	$5{,}1 \times 10^{12}$ Jahre
	15	1,1 Jahre	$1{,}8 \times 10^6$ Jahre	$5{,}8 \times 10^{10}$ Jahre	$8{,}1 \times 10^{11}$ Jahre	$4{,}9 \times 10^{14}$ Jahre
	16	11 Jahre	$4{,}6 \times 10^7$ Jahre	3×10^{12} Jahre	5×10^{13} Jahre	$4{,}7 \times 10^{16}$ Jahre

Methode ist für den Eindringling extrem aufwendig, lässt sich immer nur auf ein Objekt anwenden und der Erfolg ist zweifelhaft – denn vielleicht haben Sie ja eine Mischung aus 16 Zeichen verwendet. Brute Force kommt etwa dann zum Einsatz, wenn das Notebook einer sehr wichtigen Person gestohlen wird und eine kriminelle Organisation an die Daten will. Oder wenn Ermittler den Zugang zu einem Gerät des Täters benötigen. In jedem Fall braucht es viel (kriminelle) Energie und ein gezieltes Vorgehen, vielleicht sogar bis hin zur Gewaltanwendung – und das ist hoffentlich nicht Ihre Bedrohungslage.

Vor allem aber muss die Datei bei einer Brute-Force-Attacke lokal verfügbar sein. Es ist praktisch unmöglich, durch Brute Force in einen Webaccount einzudringen, denn jeder Server ist mit 30 Millionen Versuchen pro Sekunde hoffnungslos überfordert: Wir alle wissen aus Erfahrung, dass ein Login normalerweise zwei Sekunden oder länger dauert. Ausserdem werden wichtige Websites den Zugang sehr viel früher sperren. Ihre Bank wird vielleicht schon nach drei, spätestens aber nach fünf Fehlversuchen den Zugang sperren.

Mit anderen Worten: Wenn Sie sich mit ellenlangen Kennwörtern quälen, dann rüsten Sie sich gegen die einzige Angriffsform, der Sie vermutlich nie begegnen werden. Denn die meisten Internetkriminellen arbeiten mit anderen, sehr viel bequemeren Methoden, indem zum Beispiel 100 Millionen E-Mails in die Welt hinausgetragen werden. Darin werden beispielsweise Probleme mit dem Konto angekündigt, die behoben werden müssen. Falsche Absender, Bild 3 A, oder Links, die auf die gefälschte Seite zeigen B, sind die Klassiker. Nur: Gegen dieses «Phishing» bietet auch das komplizierteste Kennwort keinen Schutz.

Ebenfalls sehr lukrative Angriffsziele sind die Datenbanken grosser Websites, in denen die Kundendaten gespeichert werden. Sie sind für Kriminelle besonders attraktiv, weil sich auf einen Schlag Tausende oder sogar Abermillionen Zugänge erbeuten lassen. Wenn eine solche Datenbank in kriminelle Hände fällt, wird ein einfaches Kennwort wie *Halligalli* genauso gestohlen wie das vermeintlich sichere *w4f$3Ppfu*aaBj*. Darum sollten Sie Ihre Kennwörter nicht komplizierter, sondern sicherer machen.

Bild 3: der Klassiker – Phishing über eine E-Mail mit gefälschtem Absender

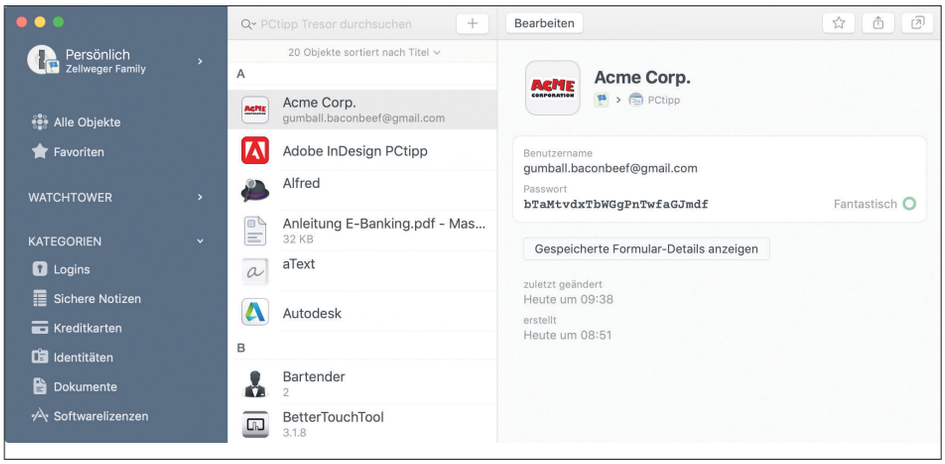

Bild 4: 1Password deckt weit mehr ab als nur die sichere Verwaltung der Kennwörter

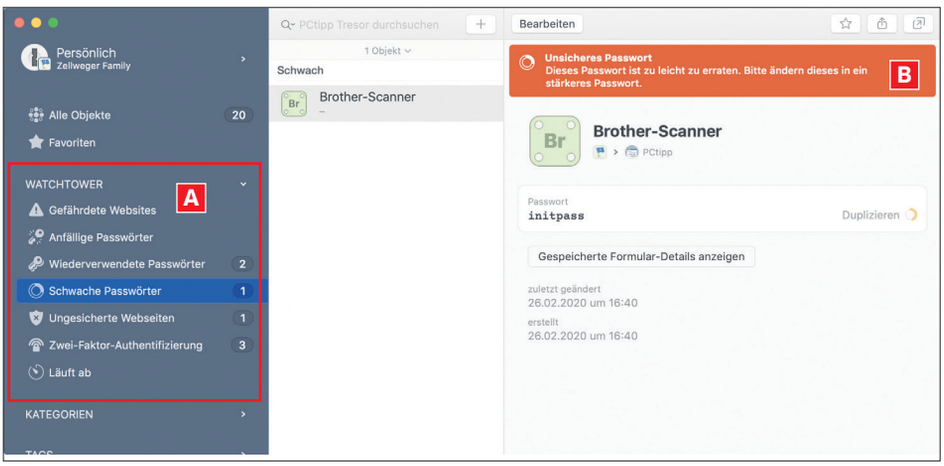

Bild 5: Der «Watchtower» kümmert sich um die typischen Einfallstore und Schwachstellen

Der Kennwortmanager

Wenn Sie Ihre Kennwörter sicher verwahren und aktuell halten möchten, dann führt kein Weg an einem guten Kennwortmanager vorbei. Diese Programme leisten weit mehr als nur die verschlüsselte Speicherung Ihrer Kennwörter. Sie füllen auch die Anmeldedaten auf einer Website automatisch aus, sodass der Umgang mit diesem sperrigen Thema sehr viel komfortabler wird. Und schliesslich synchronisieren sie die Daten zwischen allen Rechnern und Mobilgeräten, mit denen Sie arbeiten. Nicht alle Produkte bieten alle Möglichkeiten. Im Folgenden zeigen wir den Kennwortmanager 1Password, der mit gutem Gewissen als Zierde seiner Art bezeichnet werden kann, Bild 4 (mehr dazu auf 1password.com/de). Das Jahres-Abo kostet für einzelne Personen etwa 33 Franken, für Familien mit bis zu fünf Personen etwa 55 Franken – und dieses Geld ist sehr gut angelegt! Es existieren noch weitere Produkte mit ähnlichen Funktionen.

UNTERSCHIEDLICHE KENNWÖRTER

Der erste Tipp lautet: Verwenden Sie für jeden Dienst ein eigenes Kennwort. Das Kennwort zu Ihrer Apple-ID sollte aus naheliegenden Gründen nicht dasselbe sein wie jenes zu Ihrem Microsoft-Konto. Bereits hier stösst das menschliche Gehirn an seine Grenzen, denn nur die wenigsten können sich 200 verschiedene Login-Daten merken. Allein damit ist die Anschaffung eines Kennwortmanagers gerechtfertigt. Doch 1Password geht noch einen Schritt weiter: Unter dem Sammelbegriff «Watchtower» (Wachturm) werden verschiedene Sicherheitsmassnahmen zusammengefasst, Bild 5 A. Dazu gehört auch, dass die Software vor mehrfach eingesetzten Kennwörtern oder schwachen Kennwörtern B warnt. So wissen Sie genau, an welcher Stelle Sie den Hebel ansetzen müssen, um Ihre Kennwortsammlung sicherer zu machen.

GESTOHLENE KENNWÖRTER

Oft wird auch empfohlen, dass Kennwörter regelmässig gewechselt werden – doch das ist unsinnig, wenn es dazu keinen Anlass gibt.

Denn erstens ist das bereits bei zwei Dutzend Kennwörtern eine mühselige Angelegenheit. Zweitens kann eine Datenbank ja auch gestohlen werden, nachdem Sie vor zwei Minuten das Kennwort geändert haben. Sogar Firmen distanzieren sich unterdessen von solchen Praktiken: Denn wenn man die Leute dazu zwingt, regelmässig neue und komplexe Kennwörter zu generieren, steigt die Wahrscheinlichkeit, dass sie auf einem Zettel unter der Schreibunterlage stehen.

Stattdessen wacht 1Password darüber, ob Ihr Zugang bei einem Datenleck kompromittiert wurde. Dabei wird die Datenbank von 1Password im Hintergrund mit dem Dienst «Have I Been Pwned?» abgeglichen. Es ginge zu weit, die Herkunft dieses Slangs an dieser Stelle zu erläutern, aber frei übersetzt heisst das etwa «Wurde ich erwischt?».

Der Dienst sammelt im Internet alle gestohlenen Kennwörter, die er finden kann, wobei vor allem die Datenbanken einverleibt werden, die in den schmuddeligen Ecken des Webs angeboten werden. Sie können unter der Adresse **haveibeenpwned.com** Ihre E-Mail-Adresse eingeben, **Bild 6 A**, und prüfen, ob diese Adresse Teil eines Datenlecks war **B**. 1Password automatisiert diese Abfragen und warnt, wenn eine Adresse in der Datenbank gefunden wurde, **Bild 7**.

Das Wichtigste: 2FA

Die wichtigste Schutzmassnahme überhaupt ist jedoch die 2FA, die Zwei-Faktor-Authentisierung. Wenn sie aktiviert ist, reichen Benutzername und Kennwort nicht mehr aus, um sich bei einem Dienst anzumelden. Stattdessen benötigen Sie einen zweiten Faktor. Das kann eine SMS sein, eine Push-Benachrichtigung oder das berühmt-berüchtigte «gelbe Kästchen» der PostFinance: Sie müssen sich bei PostFinance zwar mit Name und Kennwort anmelden. Doch selbst wenn diese Hürde genommen ist, müssen Sie sich jetzt mit der Zugangskarte und dem Kästchen autorisieren, **Bild 8**. Das ist in diesem Fall der zweite Faktor.

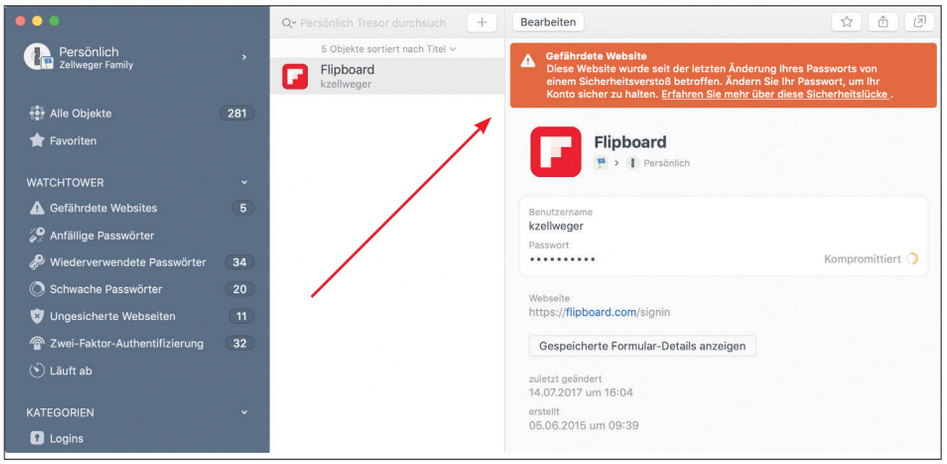

Bild 7: 1Password warnt, wenn Webseiten in der Vergangenheit Opfer von Hackern wurden

Damit verliert die Komplexität des Kennworts nahezu jede Bedeutung. Selbst wenn Sie bei einem Dienst ein schwaches Passwort wählen und dieser Dienst einem Datendiebstahl zum Opfer fällt, sind Ihre Daten sicher. Denn ohne den zweiten Faktor bleibt dem Datendieb der Zugang verwehrt. Es kommt nicht von ungefähr, dass alle grossen Dienste immer vehementer dazu drängen, die 2FA zu aktivieren – und sie haben recht.

Andere Dienstleister, allen voran die Banken, machen die 2FA seit jeher zur Pflicht: früher mit Streichlisten, dann mit Zugangskarten und Kartenleser. Heute bietet sich vor allem das Smartphone dafür an, die Rolle des zweiten Faktors zu übernehmen. Und so paradox es klingt: Sie können für das heilige Onlinebanking ein so unanständig schwaches Kennwort verwenden, wie die Bank es nur zulässt. Nach drei bis fünf fehlgeschlagenen Versuchen ist sowieso Schluss. Doch selbst wenn der Eindringling diese Hürde nimmt, scheitert er am zweiten Faktor.

Zur «Watchtower»-Funktion von 1Password gehört auch die Prüfung, ob ein Dienst eine 2FA anbietet und Sie diese nicht nutzen. Bereinigen Sie Ihre Logins und aktivieren Sie die 2FA überall dort, wo es für Sie wichtig ist. Das Kennwort *123* mit aktivierter 2FA ist unendlich viel sicherer als ein Rattenschwanz aus 20 gemischten Zeichen, der nicht durch die 2FA zusätzlich abgesichert ist.

DIE SCHWACHSTELLE DER 2FA

Die einzige Schwachstelle ist der Mensch. Achten Sie darauf, wo und wie Sie eine Website aufrufen, die mit 2FA abgesichert ist. Wenn Sie sich an einem öffentlichen PC anmelden, prüfen Sie die Optionen. Manchmal sehen Sie Markierungsfelder wie *Diesem Computer vertrauen* – und die sollten Sie natürlich ignorieren. Die Funktion dient dazu, dass Sie an Ihrem eigenen Gerät nicht jedes Mal die 2FA durchlaufen müssen – aber sie wird eine Schwachstelle, wenn Sie einen fremden Rechner als vertrauenswürdig markieren.

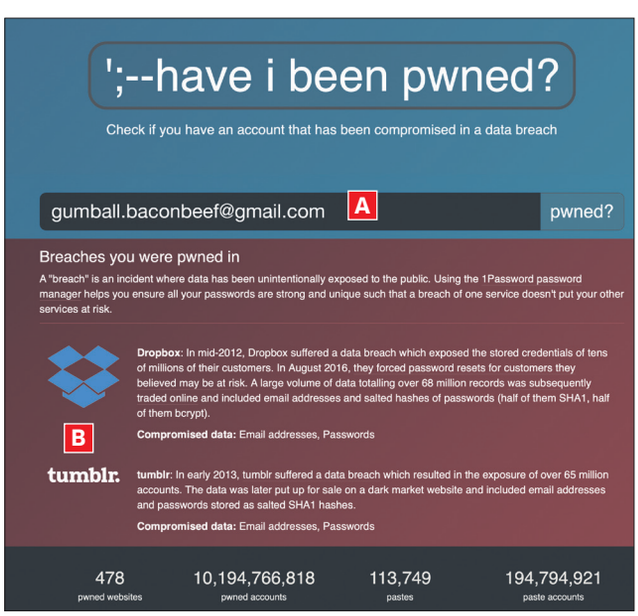

Bild 6: Die hilfreiche Website haveibeenpwned.com kennt viele gestohlene Zugangsdaten

Bild 8: Das gelbe Kästchen der PostFinance als zweiter Faktor gilt als Klassiker