

Sichere Passwörter ganz einfach merken

Mit diesen Tipps vergessen
Sie nie wieder Zugangsdaten!

Plus: Neue Techniken machen
das Passwort überflüssig

Sichere Passwörter

Doppelt hält besser

Zwei-Faktor-Authentifizierung macht Passwörter nahezu unknackbar und ist leicht einzurichten
aus CHIP 01/2015

Unknackbare Passwörter

Standardkennwörter entschlüsseln Hacker im Handumdrehen. CHIP zeigt, wie Sie schnell sichere Passwörter finden und optimal mit ihnen umgehen
aus CHIP 08/2014

Gehackt? So testen Sie's

Passwort-Diebstähle bei Internet-Riesen wie Adobe und eBay verbreiten Unsicherheit. Wurden auch Ihre Daten schon geklaut?
aus CHIP 09/2014

Der Trick mit dem Stick

Wenn Hacker auf Passwortjagd gehen, ist niemand sicher. Es sei denn, Sie legen Ihre Kennwörter verschlüsselt auf einem sicheren Stick ab
aus CHIP 03/2014

In diesem E-Paper finden Sie sorgfältig ausgewählte Artikel aus dem Archiv der CHIP-Redaktion. In den Texten genannte DVDs können Sie unter chip-kiosk.de nachbestellen

Doppelt hält besser

Zwei-Faktor-Authentifizierung macht Passwörter nahezu unknackbar und ist leicht einzurichten


Von Niels Held

Als im August bekannt wurde, dass zahlreiche intime Fotos von Prominenten aus Apples iCloud entwendet worden waren, reagierte das Unternehmen schnell: Apple führte nur drei Wochen später die Zwei-Faktor-Authentifizierung für iCloud-Backups ein. Hacker, die eine Passwort-Kombination zu einem so geschützten iCloud-Account erbeuten, können damit nun ohne Zugriff auf das iPhone des Account-Inhabers nichts mehr anfangen.

Anders als die typische E-Mail-Passwort-Kombination, die jeder Eingeweihte eingeben kann, erfordert die Zweifaktor-Authentifizierung den gemeinsamen Einsatz zweier unabhängiger Faktoren zur zweifelsfreien Identifikation einer Person. Der erste Faktor ist in der Regel ein Kennwort oder eine PIN. Der zweite Faktor kann ein Token wie ein spezieller USB-Stick, eine auf dem Handy generierte PIN, eine Smartcard oder ein Fingerabdruck sein – etwas, das nur dem Account-Inhaber zur Verfügung steht. Die meisten Internetprovider bieten ein Verfahren an, bei dem ein zufällig generierter Einmal-Code via SMS auf das Mobiltelefon des

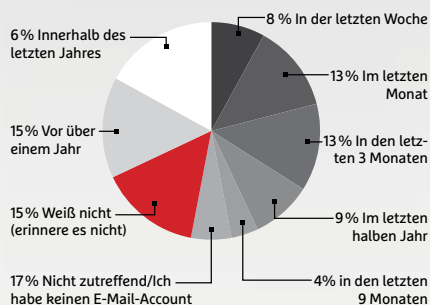
Konto-Inhabers geschickt wird. Dieser Code wird dann vom User in das entsprechende Feld im Browser eingegeben.

In der FIDO-Alliance haben sich unter anderem Samsung, Lenovo und Synaptics zusammengeschlossen, um einen Standard für sichere Authentifizierung ohne Passwörter zu schaffen. Jede Website oder Cloud-Anwendung soll so ihre User über deren FIDO-Geräte wie spezielle USB-Sticks identifizieren können. Gleichzeitig schafft die Organisation Spezifikationen für die Zwei-Faktor-Authentifizierung (U2F) über den Webbrowser. Google hat diese mit Chrome 38 implementiert und bietet sie für seine Dienste an.

Mit Windows 10 will Microsoft die Zwei-Faktor-Authentifizierung tief auf Betriebssystemebene verankern. Dabei sollen Geräte wie Desktop-PCs, Laptops oder Tablets selbst zu einem Faktor werden. Statt jedes Gerät als Faktor zu verwenden, kann aber auch ein Mobiltelefon als solcher genutzt werden. Passwörter sollen damit nach dem Willen von Microsoft künftig aussterben. Mehr dazu lesen Sie in unserem Check-up des ersten großen Updates der Windows 10 Technical Preview.  trend@chip.de

Passwörter sind unsicher

Die meisten E-Mail-Nutzer haben das Passwort für ihren E-Mail-Anbieter vor mehr als einem Jahr geändert oder wissen es nicht mehr.



Wer es hat und wer nicht

Viele Webdienste bieten bereits Zwei-Faktor-Authentifizierung an. Eine umfangreiche Liste finden Sie unter <https://twofactorauth.org>

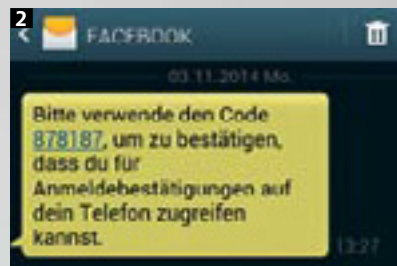
Dienst	SMS	Token	App
Amazon			
Apple			
Dropbox			
Facebook			
Google			
LinkedIn			
Microsoft OneDrive			
Twitter			
Evernote			
Yahoo Mail			
GMX			
PayPal			
eBay			

 Hat es  Hat es nicht

HOW TO

Anmeldebestätigung für Facebook einrichten

Öffnen Sie die Sicherheitseinstellungen. **1** Klicken Sie bei »Anmeldebestätigungen« auf »Bearbeiten« und setzen Sie den Haken. **2** Tragen Sie Ihre Telefonnummer ein und lassen Sie sich einen Bestätigungscode zuschicken. **3** Aktivieren Sie den Zugang per Codegenerator, um auch ohne Mobilfunk auf Ihr Konto zu kommen.



61%

der Anwender verwenden dasselbe Passwort bei mehreren Webdiensten (CSID, 2012)

31%

der Hacks in 2014 nutzten schwache Passwörter als Einbruchhilfe (Trustwave, 2014)

TREND Brennpunkt

Ein Passwort allein reicht nicht

Die Zwei-Faktor-Authentifikation (2FAS) stellt sicher, dass ein Hacker mit einem geklauten Passwort nichts anfangen kann. Sie erfordert vom Nutzer, dass er sich mit einem zweiten, unabhängigen Faktor identifiziert – etwa einem USB-Token.

1 Faktor

Etwas, das Sie wissen

Zur Anmeldung im Internet kommt meist wie gehabt die Kombination aus Benutzernamen und Passwort zum Einsatz. Für die erweiterte Verifizierung muss heute meist eine Mobilfunknummer in den Accounts angegeben werden.

2 Faktor

Etwas, das Sie besitzen/sind

Der zweite Faktor muss für hohe Sicherheit unabhängig vom ersten eingesetzt werden. Eine Anmeldung und Verifikation durch Faktor 2 auf demselben Smartphone scheidet aus.

Token

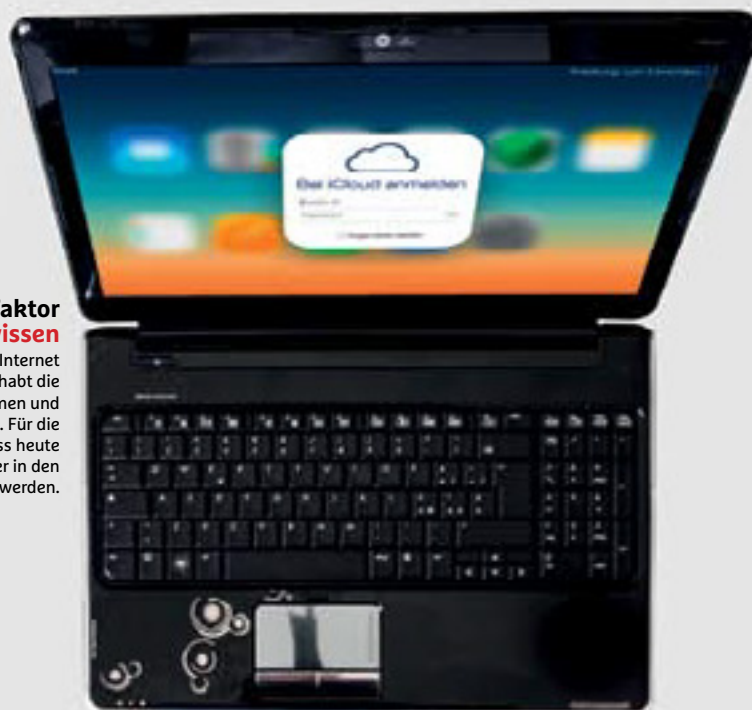
Ein Token kann etwa eine Smartcard oder ein USB-Stick mit einem speziellen Chip sein. Branchenstandards wie FIDO erlauben den Einsatz des Sticks bei mehreren Anbietern.

Handy

Der meistverbreitete zweite Faktor für die Authentifikation bei Webdiensten ist das Smartphone. Der Dienst-Anbieter kann darauf eine SMS mit einer PIN schicken, alternativ wird diese von einer App erzeugt.

Biometrie

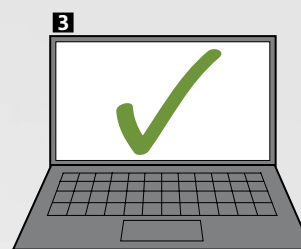
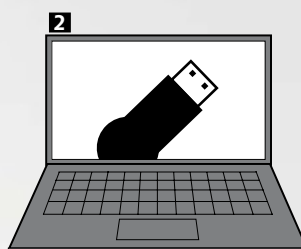
Statt eines Besitzums kann als zweiter Faktor auch ein körperliches Identifikationsmerkmal des Nutzers, zum Beispiel der Fingerabdruck eingesetzt werden.



So sieht es der User

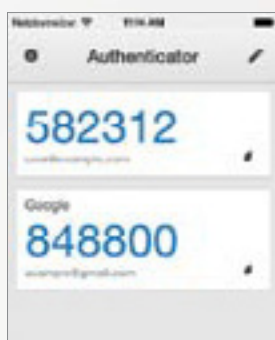
Die Authentifikation per USB-Token, wie sie etwa Google anbietet, ist besonders bequem.

- 1** Nutzernamen und Passwort werden eingegeben.
- 2** Der USB-Stick wird nach Aufforderung eingesteckt.
- 3** Der Dienst gewährt Zugriff.



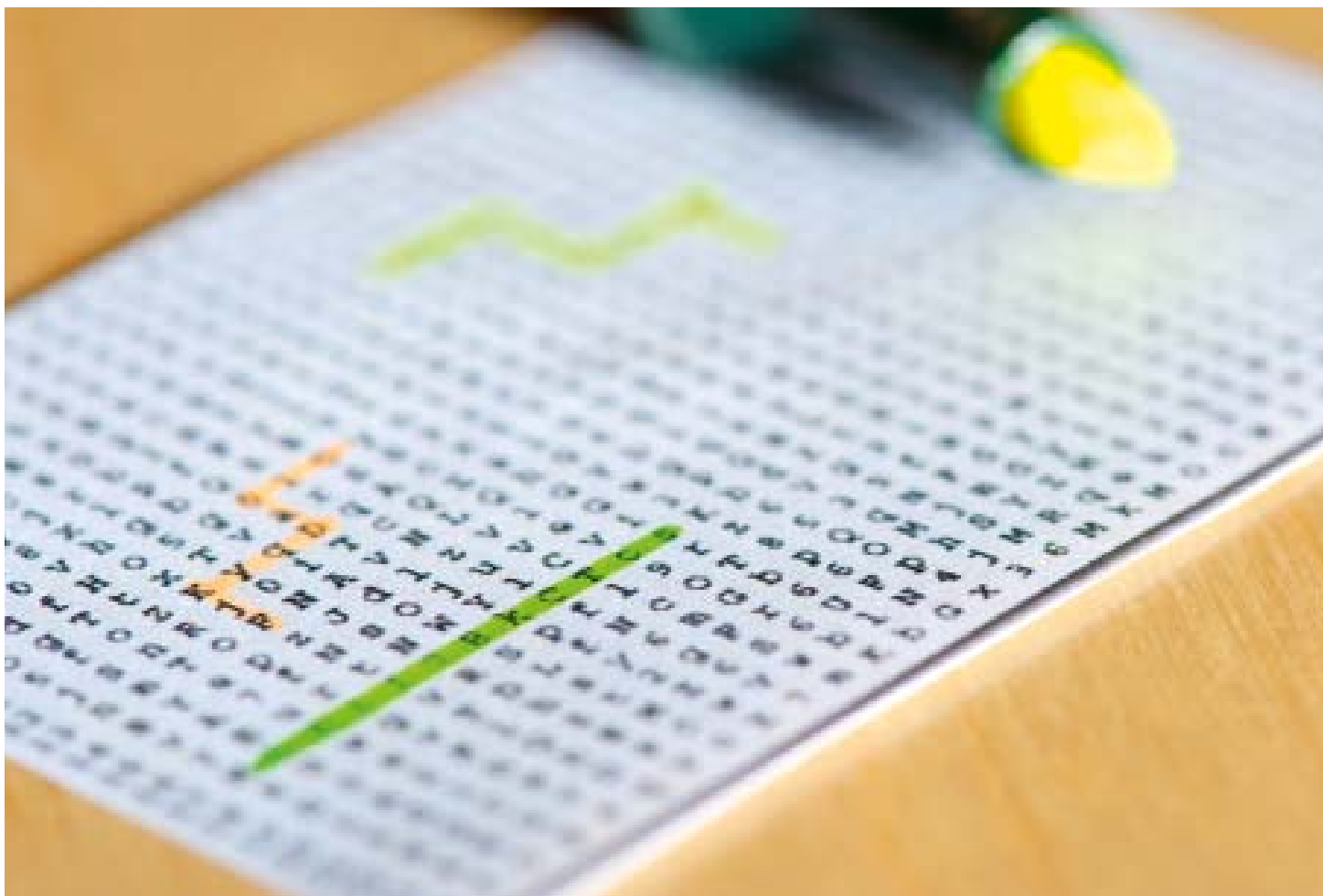
Eine App für alle

Den Google Authenticator zum Anmelden an Google- und andere Webdienste auf Basis des Time-based One-time Password Algorithm (TOTP) (Standard RFC 6238) nutzen bereits viele Anbieter, darunter Microsoft, Google, Facebook oder Dropbox. Vorteil dieser Methode: Es ist keine Webverbindung nötig, der Code wird auf dem Smartphone generiert.



„Wahrscheinlich wäre all das mit Zwei-Faktor-Authentifizierung nicht passiert“

Mat Honan, Journalist,
dessen digitales Leben 2012 fast vollständig von Hackern ausgelöscht wurde – inklusive seines Laptops mit sämtlichen Fotos seiner kleinen Tochter



Unknackbare Passwörter


Standardkennwörter entschlüsseln Hacker im Handumdrehen. CHIP zeigt, wie Sie schnell sichere Passwörter finden und optimal mit ihnen umgehen

Von Jörg Geiger

Verwenden Sie sichere Passwörter? Machen Sie auf der Webseite **howsecureismypassword.net** einmal einen Blindtest. Wenn Sie etwa gern den Namen Ihrer Kinder als Passwort verwenden, geben Sie einfach fiktive Namen wie „karin“ oder „tobias“ ein. Die Webseite zeigt Ihnen an, wie lange ein normaler PC braucht, um mit einem Knack-Tool das Passwort per Brute-Force-Angriff zu ermitteln. Im Falle der Namen ist das sofort passiert. Etwas länger, nämlich sieben Stunden, dauert es, wenn Sie das Geburtsdatum hinzufügen, also etwa „karin2401“. Ein Passwort wie „sKdfj4/asl230!D_a%Up“ ist dagegen mit roher Rechenpower gar nicht zu knacken: Rund 35 Sextillionen Jahre bräuhete ein PC dazu. Das Problem im Alltag ist, dass sich solche Passwortmonster niemand merken kann. Schon gar nicht, weil man

in der Regel einige davon braucht. Mehr Zugänge erfordern Passwörter, die sich möglichst unterscheiden sollten: Windows, Mails, Online-Banking, Webshops, eBay, Dropbox, Facebook und so fort.

Eine Herausforderung im Alltag

Woher also bei Bedarf schnell ein sicheres Passwort nehmen, das man sich auch merken kann? Oder wo alternativ die Zugangsdaten so ablegen, dass niemand sie klauen kann? Der Heartbleed-Bug hat gezeigt, dass man manchmal kurzfristig eine ganze Reihe von persönlichen Kennwörtern erneuern muss. Solche Sicherheitslücken sowie Großangriffe auf Webdienstleister werden sich wiederholen. Eine Passwortstrategie muss her, und die geben wir Ihnen auf den folgenden zwei Seiten. 

testtechnik@chip.de

FOTO: NIKOLAUS SCHÄFFLER

Perfekte Passwörter

Es gibt verschiedene Wege, sichere Passwörter zu erzeugen, an die auch nur Sie sich erinnern. Wählen Sie den besten Weg für sich aus

1 Kein Recycling

Regel Nummer eins klingt trivial, wird aber leider oft nicht befolgt: Nutzen Sie für jeden Dienst ein eigenes Passwort. Der Grund: Wird das Kennwort geknackt, ist nur ein Account betroffen, und Sie können schnell Schadensbegrenzung betreiben.

2 Perfekte Zutaten

Die Passwortlänge sollte mindestens bei acht Zeichen liegen. Länger ist immer besser, ein guter Kompromiss sind zehn bis zwölf Zeichen. Ein Mix aus Groß- und Kleinbuchstaben ist Pflicht, das Einmischen von Ziffern und Sonderzeichen erhöht die Komplexität für Brute-Force-Angriffe. Wie solche Passwörter aussehen können, zeigt zum Beispiel der Webdienst gajin.at/olspwgen.php.

3 Muster statt Zeichen

Sie funktioniert wie ein Passwortzettel, ist aber viel sicherer: die Passwortkarte von Savernova. Unter chip.de können Sie die Karte herunterladen und dann ausdrucken. Die Passwortkarte ist so groß wie eine EC-Karte und enthält ein Wirrwarr aus Zeichen und Ziffern in Tabellenform (s. Bild rechts). Die Idee ist, sich EIN Muster zu merken, zum Beispiel 5x links, 5x runter. Man notiert sich den Startpunkt, der für jeden Dienst ein anderer ist – nur das Muster muss man sich merken. Im Beispiel rechts ist der Startpunkt Zeile 7/Spalte E. So erhalten Sie als Passwort »Au8S4s7tP«.

4 Individueller Baukasten

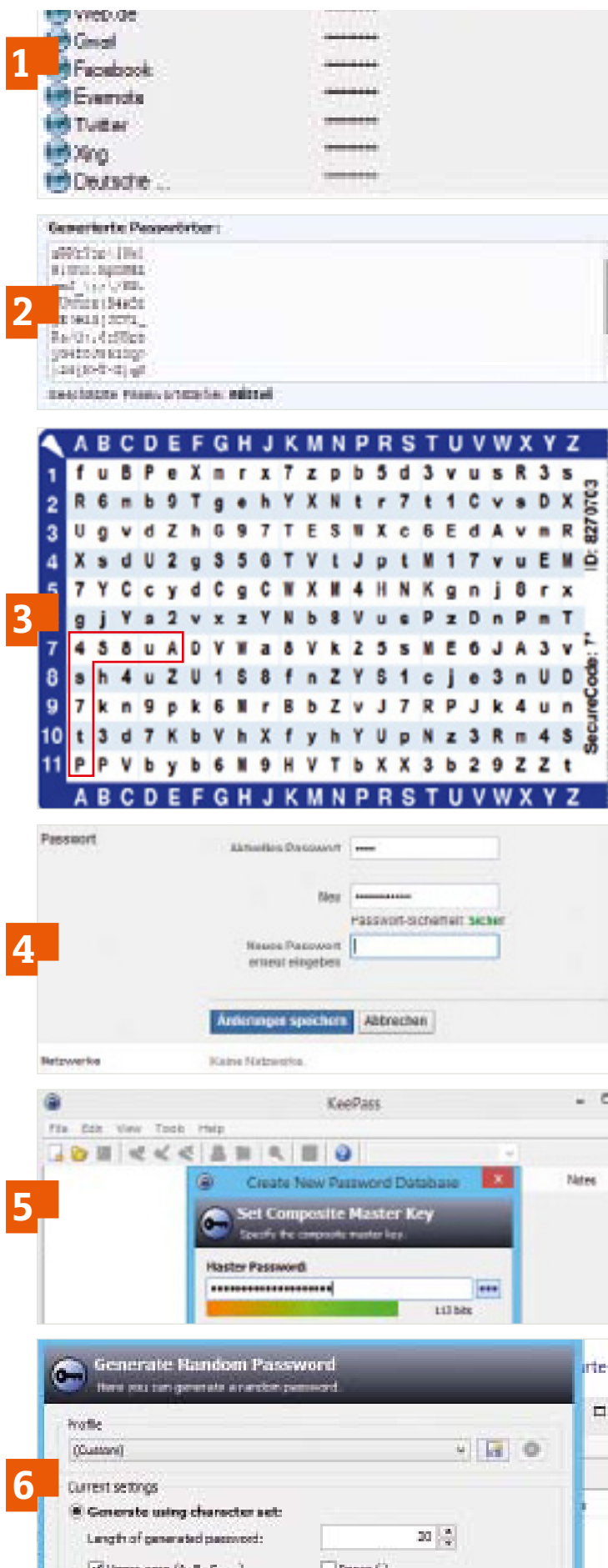
Viele unknackbare Passwörter im Kopf behalten – das klappt nur mit einem Baukasten. Ein Beispiel: Ausgangsbasis ist eine feste Größe, etwa der Name der Webseite. Für das Facebook-Log-in also »Facebook«. Lassen Sie jeden zweiten Buchstaben weg, bleibt »Fcbø«. Jetzt fügen Sie ein Datum hinzu: Vorne ergänzen Sie den Tag, hinten den Monat, jeweils als Klammer um den letzten Buchstaben. Ist das Datum der 3. Mai, wird daraus »OF3cbOo5«. Fügen Sie nach jeder Ziffer das Sonderzeichen der Zifferntaste hinzu, nach der »3« also »§« und so fort. Dann lautet das fertige Passwort »O=F3§cbO=o5%«. Prägen Sie sich den Baukasten ein, nicht das Passwort. Und wie jedes Passwort sollten Sie auch Ihre Strategie einmal pro Jahr ändern.

5 Software-Lösung

Eine gute Alternative sind Passwortmanager, die Passwörter in verschlüsselten Containern speichern. Der Zugang zum Safe selbst ist mit einem Master-Passwort gesichert. Der Vorteil: Sie müssen sich nur diesen einen Master Key merken. Ein sehr guter Passwort-Manager ist die Freeware KeePass (auf Heft-DVD).

6 Zufallsgeneratoren

Passwortmanager wie KeePass erzeugen auch Zufallspasswörter. Klicken Sie dazu unter »Tools« auf »Password Generator«.



Tipps für Passwörter

In der Praxis tauchen bei Passwörtern oft zusätzliche Stolpersteine auf: Was tun bei Zweitgeräten, Testaccounts, Passwortklau?

1 Auf andere Geräte mitnehmen

Wenn Sie mehrere Rechner nutzen, bietet sich die portable Version des kostenlosen Passwortmanagers KeePass an (auf Heft-DVD). Die angebotene ZIP-Datei lässt sich auf einen USB-Stick entpacken und mitnehmen. Um Passwörter sowohl auf dem PC als auch mobil auf Smartphone oder Tablet zu nutzen, können Sie zu den auf Seite 83 vorgestellten alternativen Strategien greifen, etwa dem Baukastenprinzip oder auch Passwortkarten.

2 Zwischen Geräten synchronisieren

Es gibt Dienste, die Ihre Passwörter automatisch mit verschiedenen Geräten abgleichen, etwa LastPass oder 1Password. Der Datensync erfolgt entweder via Cloudspeicher oder lokal. Das ist bequem, aber die Dienste sind kostenpflichtig. Wenn Sie den Passwortsafe KeePass am PC nutzen, können Sie sich mit MiniKeePass (iOS) oder KeePass-Droid (Android) Gratis-Apps holen, die die Passwortdatenbank auf Smartphone und Tablet öffnen. Für synchrone Passwortdatenbanken müssen Sie allerdings selbst sorgen: Beide Apps können Passwörter per Dropbox importieren.

Wichtig Lassen Sie den verschlüsselten Container nicht in Dropbox liegen, sondern löschen Sie ihn nach dem Abgleich.

3 Wegwerf-Passwort schlägt Facebook

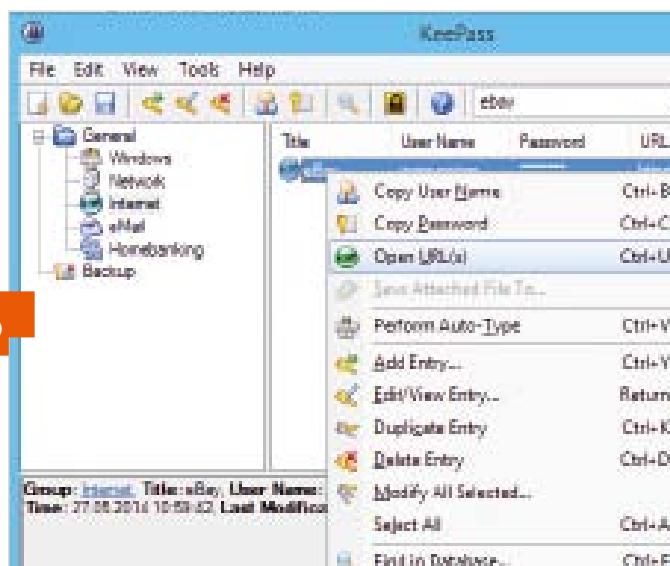
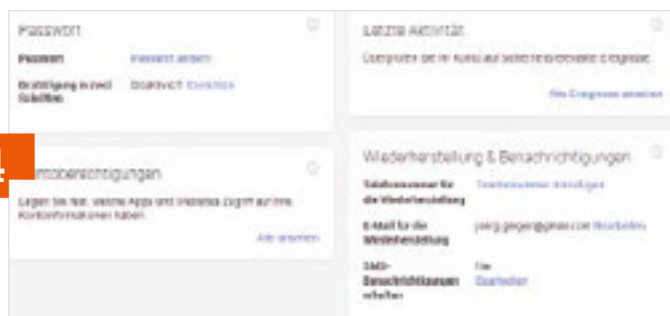
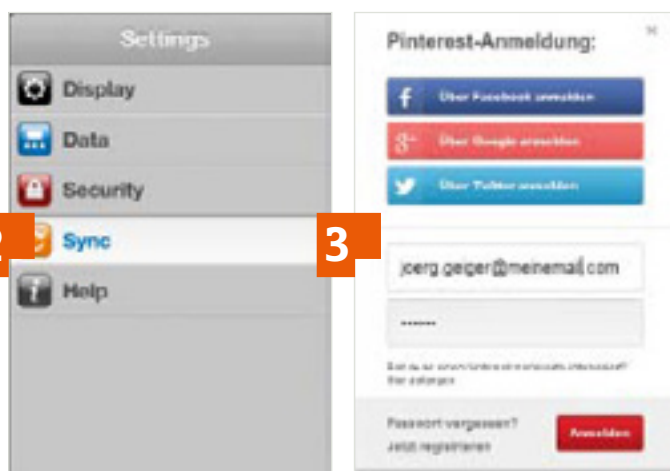
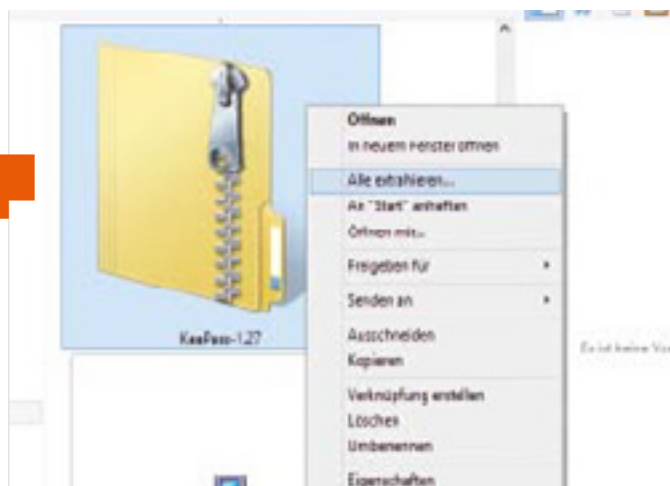
Wenn Sie gern Webdienste ausprobieren, viele davon aber anschließend wieder links liegen lassen, können Sie Wegwerfpasswörter wie »123abc« nutzen. Das Log-in mit einem einfachen Kennwort ist dann sogar die bessere Alternative zu den oft angebotenen Facebook- oder Twitter-Log-ins, denn Sie gewähren nicht unnötig Zugriff auf Ihre sozialen Netzwerke. Wichtig ist nur: Sobald Sie einen Account häufiger nutzen oder dort gar sensible Daten hinterlegen, sollten Sie sofort auf ein starkes Passwort wechseln.

4 Doppelte Sicherheit

Mehr Sicherheit als ein Passwort allein bietet die Zwei-Faktor-Authentifizierung: Zum erfolgreichen Log-in brauchen Sie neben dem Passwort noch ein zweites Geheimnis, meist einen PIN-Code. Der ist immer nur für kurze Zeit gültig und wird per SMS verschickt oder mit einer App wie Google Authenticator erzeugt. Dienste wie Gmail lassen sich auf diese Weise bereits absichern. Das geht via »Sicherheit« und »Bestätigung in zwei Schritten«.

5 Schnell zurücksetzen

Kaum eine Woche vergeht, in der nicht irgendwo Passwörter geklaut werden. Wenn Sie alle Konten übersichtlich im Passwortmanager wie KeePass haben, geht der Reset des Codes besonders schnell. Dazu suchen Sie den Eintrag für den betroffenen Dienst aus der Liste, klicken ihn mit der rechten Maustaste an und wählen »Open URL(s)«. Einmal im Jahr sollten Sie sowieso generell all Ihre Passwörter ändern.





Gehackt? So testen Sie's


Passwort-Diebstähle bei Internet-Riesen wie Adobe und eBay verbreiten Unsicherheit. Wurden auch Ihre Daten schon geklaut?

Von Jörg Geiger

Mail-Adresse und zugehöriges Passwort öffnen im Internet alle Türen, denn sie sind der Identitätsnachweis Nummer eins. Kein Wunder also, dass Hacker sich an Einbrüchen bei großen Internet-Dienstleistern versuchen, um Online-Identitäten im großen Stil zu klauen. Und sie sind dabei überaus erfolgreich. Das Hasso-Plattner-Institut für Softwaresystemtechnik in Potsdam erfasst in einer Datenbank geklaute Internet-Identitäten, die in Hackerforen und über andere dubiose Kanäle im Netz gehandelt werden. Diese Datensätze bestehen in der Regel aus E-Mail-Adressen, Namen, Geburtsdaten und oft auch zugehörigen Konto- und Kreditkartennummern sowie Adressen. Aktuell sind dort über 172 Millionen Benutzerkonten erfasst. Es ist also sehr gut möglich, dass auch ein Account von Ihnen dabei ist.

Das Hauptproblem bei Hacker-Angriffen auf Internet-Dienstleister wie eBay ist, dass viele Nutzer ihre Passwörter bei mehreren Diensten verwenden. Wird bei Adobe das Passwort erfolgreich geklaut, ist es für Hacker leicht, auszuprobieren, ob das Passwort nicht auch bei Gmail, Dropbox oder Facebook passt.

Alle Zugänge sichern und checken

Aber nicht nur im Web, auch am PC, auf Mobilgeräten und im Heimnetz verwendet oder benötigt man oft Zugangsdaten, um Inhalte zu schützen, und auch die können gehackt werden. Doch keine Angst: CHIP zeigt für alle Accounts und Geräte, wie Sie sehr einfach feststellen, ob Ihre Daten schon geklaut wurden. Außerdem haben wir die passenden Tipps parat, wie Sie wichtige Zugänge absichern. 

testtechnik@chip.de

FOTO: KLAUS SATZINGER

Dienste im Internet

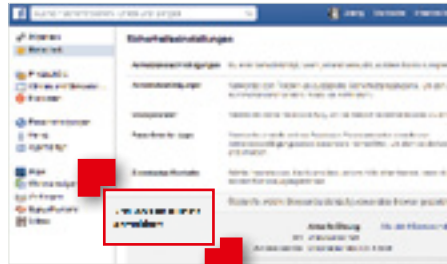
Ob Mailer, Facebook, PayPal, Adobe, Google oder Apple, alle diese Accounts werden mit Passwörtern geschützt und sind somit Hacker-gefährdet



E-Mail

Check: Der Identity Leak Checker des Hasso-Plattner-Instituts (<https://sec.hpi.uni-potsdam.de>) der Uni Potsdam prüft nach, ob Ihre Mail-Adresse zusammen mit Name, Kreditkartennummer, Bankkonten und anderen persönlichen Daten in Hackerkreisen gehandelt wird. Damit könnte ein Fremder sogar Ihre komplette digitale Identität annehmen und missbrauchen. Um den Check zu starten, müssen Sie nur Ihre E-Mail-Adresse eingeben und auf »E-Mail-Adresse prüfen« klicken. Wichtig: Ihre Mail-Adresse wird weder gespeichert noch an Dritte weitergegeben. Der Check prüft Ihre Mail-Adresse gegen eine ständig aktuell gehaltene Datenbank mit kompromittierten Accounts und schickt das Ergebnis des Checks an die angegebene Mail-Adresse.

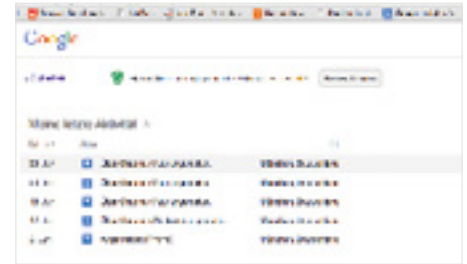
Tipp: Falls Sie nicht betroffen sind, brauchen Sie auch nichts zu unternehmen. Wurde aber die Mail-Adresse gehackt, sollten Sie für alle Dienste, mit denen diese Adresse verknüpft ist, das Passwort ändern. Tauchen in den Datensätzen auch Kreditkartennummern auf, sollten Sie umgehend Ihre Bank über den Diebstahl informieren. Bei gehackten Kontonummern prüfen Sie alle Transaktionen mindestens einmal pro Woche.



Facebook

Check: Für viele Nutzer ist Facebook der Internetdienst überhaupt. Auch Hacker knöpfen sich bei Phishing-Angriffen am liebsten das soziale Netzwerk vor. Was viele nicht wissen: Mit einem eingebauten Check kann man sehr leicht nachprüfen, ob sich Dritte schon mal in Ihren Facebook-Account gehackt haben. Klicken Sie dazu in Facebook oben in der Leiste ganz rechts auf den kleinen Pfeil. Im Drop-Down-Menü wählen Sie »Einstellungen« und danach »Sicherheit«. Gehen Sie jetzt neben dem Eintrag »Von wo aus Du Dich anmeldest« auf »Bearbeiten«. Dort sehen Sie, mit welchen Geräten und von welchen Orten aus bereits auf Ihr Facebook-Konto zugegriffen wurde.

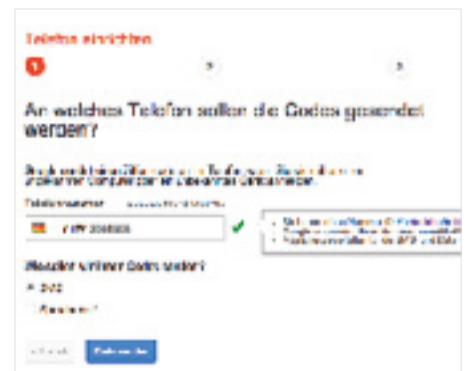
Tipp: Sollte ein unbekanntes Gerät in der Liste stehen, klicken Sie neben dem Eintrag auf »Aktivität beenden«. Danach wählen Sie links im Menü »Allgemein« und ändern Ihr »Passwort«. Für mehr Sicherheit, zumindest für Facebook im Browser, sorgt unter »Sicherheit« der Punkt »Anmeldebestätigung«. Wenn Sie dort den Sicherheitscode aktivieren, ist beim erstmaligen Login von einem unbekannten Gerät aus ein zusätzlicher PIN-Code nötig, den Sie auf Ihr Handy geschickt bekommen.



Google

Google-Check: Hacker lieben auch Google-Accounts. Der Grund: Hat man einen Gmail-Account geknackt, kann man die »Passwort-Vergessen«-Funktionen anderer Dienste nutzen. Diese senden dann einen Passwort-Reset-Link an die Gmail-Adresse und die digitale Identität ist futsch. Doch auch Google hat einen Hacker-Check eingebaut. Wenn Sie angemeldet sind, reicht ein Besuch der Seite <https://www.google.com/settings/security>. Dort klicken Sie unter »Letzte Aktivität« auf »Alle Ereignisse ansehen« und sehen dann die letzten Logins.

Tipp: Sind bei den Logins unbekannte Geräte gelistet, sollten Sie schnell Ihr »Passwort ändern«. Praktisch: Google platziert den passenden Link dafür auf der Übersichtsseite. Außerdem bietet Google schon länger eine 2-Faktor-Authentifizierung an: Neben Mail-Adresse und Passwort brauchen Sie dann für das Login auch noch einen PIN-Code. Den erzeugt die App Google Authenticator, die es kostenlos für Android und iOS gibt. Um die 2-Faktor-Authentifizierung zu aktivieren, klicken Sie unter »Sicherheit« neben dem Eintrag »Bestätigung in zwei Schritten« auf »Einrichten«. Ein Assistent führt Sie durch die Konfiguration.



Computer und Software

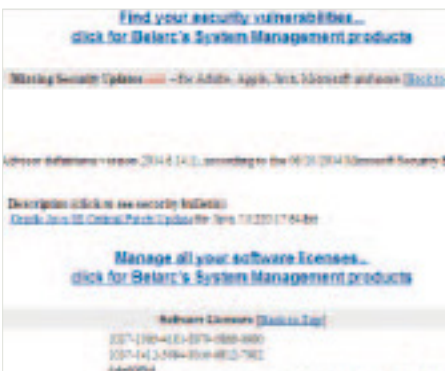
Ihr PC oder Notebook kann Sicherheitslücken aufweisen, über die Hacker an Ihre Daten kommen können. Doch auch hierfür gibt es Check-Seiten im Web



System

Check: Zwar haben Sie schon eine gute Basis-Sicherheit, wenn Sie Ihr Windows 7 oder 8 sowie all Ihre Programme per Update stets aktuell halten und einen Virenschanner installieren. Um aber ganz sicherzugehen, dass Ihr System keine größere Lücke aufweist, lassen Sie das kostenlose Tool Belarc's Security Advisor laufen: belarc.de/de/free_download.html. Es informiert Sie über aktuelle Sicherheitseinstellungen von Windows und prüft, ob eine Firewall aktiv ist und der Virenschanner wirklich auf dem neuesten Stand ist. Starten Sie das Programm durch Doppelklick auf das Icon und klicken Sie auf »Continue«, um den System-Check zu starten. Nach wenigen Minuten wird Ihnen im Browser ein Report angezeigt.

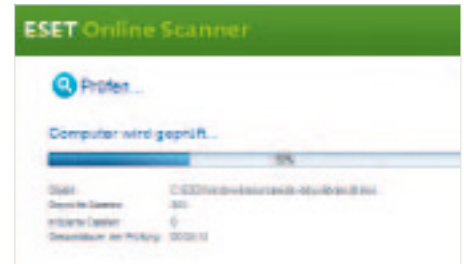
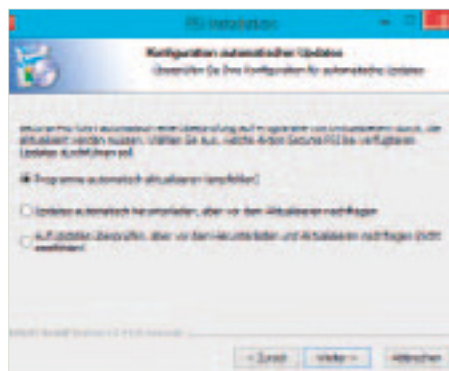
Tipp: Das Tool kommt ohne schicke Grafik und prüft nur die Basics, aber die müssen auf jedem System stimmen. Wird beispielsweise gemeldet, dass der Virenschanner veraltet ist, sollten Sie ihn sofort aktualisieren; fehlt ein Update, lassen Sie sich anzeigen, um welchen Patch es sich handelt, und installieren Sie ihn nach. Der übersichtliche »Security Benchmark Score«, mit dem Sie den Sicherheitsstatus auf einen Blick sehen, ist leider nur bis Windows 7 verfügbar.



Browser

Check: Firefox, Chrome und Internet Explorer gehören zu den am meisten genutzten Programmen überhaupt. Deshalb stehen sie besonders weit oben auf der Abschlusliste von Hackern. Für Ihren Browser sollten Sie deshalb einen gesonderten Security-Check machen. Surfen Sie dazu in Ihrem Browser die Seite botfrei.de/browsercheck an und klicken Sie auf »Browsercheck starten«. Der Dienst wird vom Anti-Botnet-Beratungszentrum angeboten und prüft Ihren Browser sowie die installierten Plug-ins.

Tipp: Findet der Test eine veraltete Browser-Version oder angegraute Plug-ins, dann sollten Sie die angezeigten Links nutzen und so schnell wie möglich die notwendigen Updates einspielen. Um für die Zukunft alle Updates immer gleich am Start zu haben, empfehlen wir die Freeware Secunia Personal Software Inspector. Installieren Sie das Tool und wählen Sie dabei »Programme automatisch aktualisieren« aus. Ist der Inspector einmal mithilfe von »Jetzt überprüfen« eingeschaltet, überwacht er die installierten Programme auf Updates und spielt diese in den meisten Fällen ein. Software, bei der diese Automatik nicht funktioniert, wird Ihnen gesondert angezeigt.



Viren

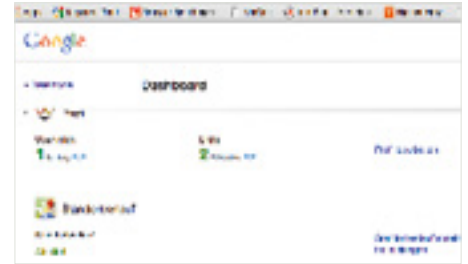
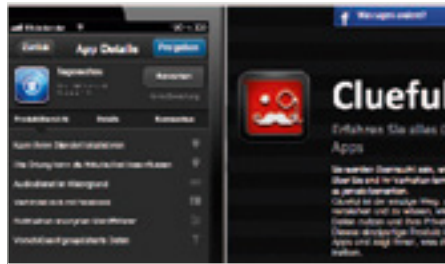
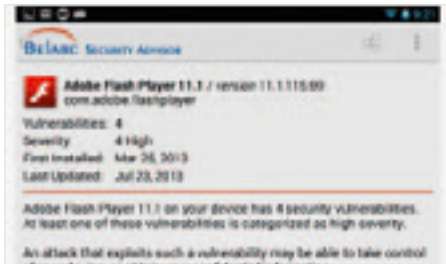
Check: Wenn Sie schon einen Virenschanner installiert haben, ist kein Viren-Check mehr nötig? Ganz sicher können Sie nie sein, denn Sie dürfen nicht davon ausgehen, dass ein Antivirentool immer alles erkennt. Eine zweite Meinung schadet daher nicht. Mit dem ESET Online Scanner auf eset.com/de/home/products/online-scanner führen Sie sehr einfach einen Viren-Check aus. Er funktioniert parallel zu Ihrem bereits installierten Virenschutz. Klicken Sie auf der Webseite auf »ESET Online Scanner starten«, und der Viren-Check beginnt.

Tipp: Wer neben dem Virenschanner einen zusätzlichen permanenten Schutz haben will, der kann sich das kostenlose Malwarebytes Anti-Exploit installieren. Die Freeware kommt dem bereits installierten Virenschanner nicht in die Quere, denn sie arbeitet daneben als zweite Schutzebene und konzentriert sich auf die Sicherheit von Browsern und Drittanbieter-Tools. In der kostenlosen Version bewacht Anti-Exploit die großen Browser Internet Explorer, Firefox, Chrome und Opera. Außerdem dichtet es Java-Lücken ab. Praktisch: Anti-Exploit muss nur installiert werden. Einzustellen brauchen Sie nichts, der Schutz greift sofort.



Smartphone und Tablet

Mobilgeräte geraten zunehmend in den Fokus von Hackern. Denn ihre Verbreitung steigt, ihre Funktionen sind für den User oft undurchsichtig – und sie gehen leicht verloren



System

Check: Wie bei Windows gibt es auch auf Mobilsystemen eine Grundabsicherung. Dazu gehören ein aktuell gehaltenes Betriebssystem, sinnvolle Sicherheitseinstellungen und unter Android ein Virenschutz. Ein kurzer Check schafft Klarheit: Android-Nutzer können zur kostenlosen App Belarc Security Advisor greifen, die über 400 Schwachstellen in Android und populären Apps prüft. Einen System-Check unter iOS macht die kostenlose Version der App Lookout.

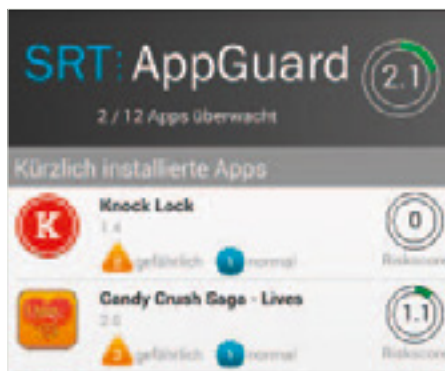
Tipp: Android-Nutzer sollten sich an den gefundenen Sicherheitslücken orientieren und Apps sowie das Betriebssystem aktualisieren. Um ein neueres Android einzuspielen, navigieren Sie in den Einstellungen zu »Über das Telefon« oder »Info zu Gerät« und dort zum Unterpunkt »Software-Update«. iOS-Nutzer erhalten zwar für System-Updates eine Push-Nachricht, meist ist aber der Weg zu Fuß schneller: Wenn Sie in »Einstellungen | Allgemein« den Punkt »Softwareaktualisierung« aufrufen, prüft das System, ob es aktuell ist. App-Updates sehen iOS-Nutzer leicht an einem Hinweis auf dem App-Store-Icon. Unter »Updates« erledigen Sie das mit »Alle aktualisieren« für sämtliche Apps in einem Rutsch.



Apps

Check: Was darf eine App auf Ihrem System anstellen? Mitunter mehr als Ihnen lieb sein kann. Zwar ist ein gut gemeinter Tipp, die Berechtigungen einer App vor der Installation zu prüfen, meist wird das aber nicht gemacht. Android-Nutzer lassen sich mit der Gratis-App aSpotCat anzeigen, welche bereits installierten Apps sich welche Berechtigungen nehmen. iOS-Nutzer steuern die Seite cluefulapp.com an und können so die Berechtigungen einzelner Apps einsehen.

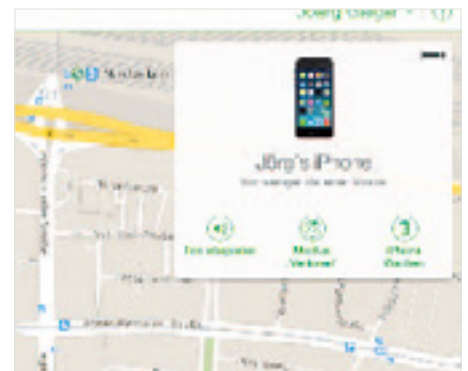
Tipp: Wenn Sie sich mit App-Berechtigungen nicht auseinandersetzen wollen, können Sie eine App natürlich einfach löschen. Doch oft kommt das nicht in Frage. Android-Nutzer haben dann ein Problem, denn Google bietet kein Berechtigungs-Management an. Der kostenlose SRT AppGuard (auf srt-appguard.com) kann zwar einer App bestimmte Berechtigungen nachträglich wegnehmen. Doch Vorsicht: Dann funktioniert das Auto-Update nicht mehr. iOS-Nutzer können die App-Berechtigungen dagegen einfach unter »Einstellungen | Datenschutz« anpassen. Dort sieht man, welche Apps auf Kontakte, Fotos oder andere Daten zugreifen. Ein Fingertipp in die Rubrik schaltet Berechtigungen gezielt aus.



Ortung

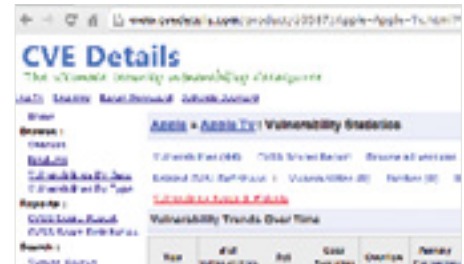
Check: Bei Smartphones und Tablets stellt sich nicht nur die Frage »Wurden Sie schon gehackt?«, sondern oft auch »Wurden Sie schon geklaut?«, denn Mobilgeräte sind ein beliebtes Ziel von Dieben. Für den Fall eines Diebstahls sollten Sie vorbereitet sein. Prüfen Sie also, ob sich Ihre Mobilgeräte orten lassen. iOS-Nutzer aktivieren unter »Einstellungen« und »iCloud« den Dienst »Mein iPhone suchen«. Damit eine Ortung unter Android funktioniert, müssen Sie den Standortzugriff zum einen in den Einstellungen Ihres Gerätes und zum anderen über das Dashboard Ihres Google-Kontos (<https://www.google.com/settings/dashboard>) aktivieren.

Tipp: Im Falle eines Diebstahls oder Verlusts können sich iOS-Nutzer unter icloud.com mit ihrer Apple ID anmelden und ihr Gerät orten. Das klappt automatisch, auf Wunsch können Sie auch noch einen Signalton abspielen oder das Gerät löschen. Android-Nutzer loggen sich für die Ortung bei play.google.com ein, klicken auf »Einstellungen« und wählen dort den »Android Geräte-Manager« aus. Auch hier funktioniert die Ortung automatisch für alle Android-Systeme ab Version 2.2.



Heimnetz und Co.

Router und sogar Home-Entertainment-Geräte wie Fernseher sind inzwischen ebenso anfällig für Hacker-Angriffe wie PCs und Handys



Router

Check: Statt sich einzelne PCs, Smartphones oder Tablets vorzunehmen, greifen Hacker gern DSL-Router an, die sämtliche Geräte eines Haushalts ins Netz bringen. Wer daher den Router kontrolliert, der kontrolliert auch die dahinter arbeitenden Geräte. Unter **checkmyrouter.org** können Sie sehr einfach prüfen, ob Ihre FritzBox oder ein anderer Router anfällig für Sicherheitslücken wie den UPnP-Bug (Universal Plug and Play) ist. Zum Redaktionsschluss war Checkmyrouter aber wegen Wartungsarbeiten nicht erreichbar. Eine Alternative ist ShieldsUP unter <https://www.grc.com/shieldsup>.

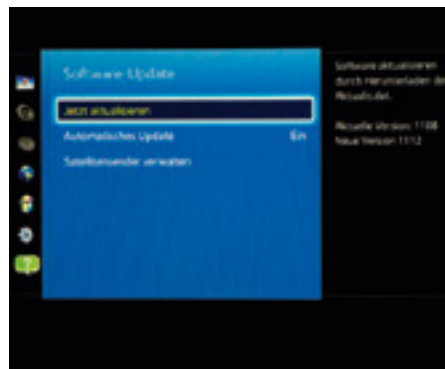
Tipp: Egal ob FritzBox oder Router von anderen Herstellern wie Asus oder Linksys, die Firmware, also die Geräte-Software auf dem WLAN-Router, sollte immer aktuell sein. Bei der FritzBox lässt sich die Firmware einfach über das Web-Interface (Adresse fritz.box) aktualisieren. Klicken Sie dort auf »Assistenten« und danach auf »Update«. Dann wird geprüft, ob für Ihre FritzBox eine neue Firmware zur Verfügung steht. Ist das der Fall, können Sie das Update mit einem Klick einspielen. Bei anderen Routern funktioniert dies ähnlich. Suchen Sie hierzu nach Menüpunkten wie »Firmware-Update«.



Smart TV

Check: Smart TVs spielen ihre Vorteile erst mit einer Internetverbindung aus. Diese und die Möglichkeit, Apps zu installieren, machen sie anfällig für Angriffe. Denn auch bei Smart TVs kommen Standard-Protokolle und -Dateiformate zum Einsatz. Leider existiert kein spezieller Security-Test für Smart TVs, zu unterschiedlich arbeiten die Geräte der verschiedenen Hersteller. Momentan müssen Sie noch selbst die genaue Modellnummer herausfinden (steht oft auf der Geräterückseite) und anschließend auf den Herstellerseiten gezielt nach Informationen rund um die Sicherheit suchen. Häufig helfen die Support-Foren mit Nutzerberichten schneller weiter als die von den TV-Herstellern gepflegten Seiten.

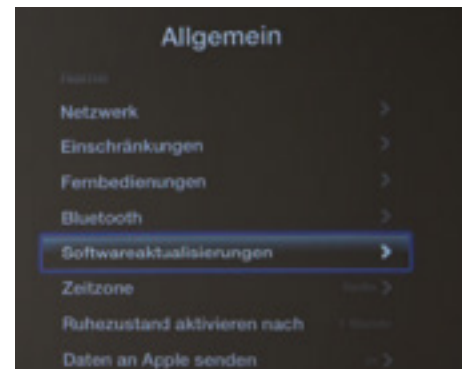
Tipp: Wichtig für die Sicherheit auf dem Smart TV ist eine aktuelle Firmware. Die lässt sich meist auf zwei Wegen einspielen: entweder direkt am TV-Gerät mit aktiver Internetverbindung oder via USB-Stick. Am Gerät kann die Firmware bei Philips unter »Einstellungen« und »Software-Aktualisierung« aufgespielt werden. Bei LG heißt der passende Menüpunkt meist »Support«, bei Samsung finden Sie die Funktion unter »Hilfe« oder ebenfalls »Support«.



Entertainment

Check: Auch was sich neben dem Smart TV an Geräten im Wohnzimmer versammelt, kommt nicht mehr ohne Internet aus und ist somit anfällig für Angriffe. Gemeint sind Apple TV, PlayStation, Xbox und andere Home-Entertainment-Geräte. Einen einheitlichen Security-Check gibt es aber auch für diese Geräte nicht. Erste Anlaufstellen für Security-News sollten wie bei Fernsehern die Hersteller-Webseiten sein. Als zweite Option legen wir Ihnen die Webseite **cvedetails.com** ans Herz. Dort werden Sicherheitslücken herstellerübergreifend gesammelt. So können Sie beispielsweise nach Apple TV suchen und die Sicherheitslücken der letzten fünf Jahre ansehen.

Tipp: Auch bei der Entertainment-Hardware ist eine aktuelle Firmware wichtig. Meist lässt sie sich direkt über das Gerät einspielen, bei Apple TV über »Einstellungen | Allgemein | Software aktualisieren«. Bei der PlayStation 3 führt der Weg zur neuen Firmware über »Einstellungen | System-Aktualisierung | Aktualisierung über Internet«. Auch für die Xbox 360 erledigen Sie dies am einfachsten direkt: Klicken Sie dazu die Guide-Taste am Controller und wählen Sie »Einstellungen | Systemeinstellungen«.





Der Trick mit dem Stick

Wenn Hacker auf Passwortjagd gehen, ist niemand sicher. Es sei denn, Sie legen Ihre Kennwörter verschlüsselt auf einem sicheren Stick ab

Von Markus Hermannsdorfer

Viele Firmen, darunter Sony und Adobe, fielen in den vergangenen Jahren Hackern zum Opfer, die dabei millionenfach Passwörter klauten. Diese Passwortlisten zeigten, dass viele User oft entweder unsichere Passwörter wie „123456“ oder dasselbe Passwort für mehrere Dienste verwenden. Das erleichtert Hackern ihre Angriffe ungemein, ist aber zugleich verständlich: Wer kann sich schon Dutzende hochkomplexe Kennwörter merken?

Eine simple Lösung ist der unter die Tastatur geklebte Notizzettel. Kein Hacker kann sie von dort stehlen, dafür müssen Sie aber ständig auf Personen achten, die sich in der Nähe Ihres Rechners aufhalten. Und es nützt nichts, wenn Sie an einem fremden Rechner sitzen und sich von dort bei einem Webdienst einloggen wollen.

Das Gratistool KeePass 2 Portable (auf Heft-DVD unter dem CHIP-Code Passwort) löst dieses Dilemma. Dafür benötigen Sie nur einen USB-Stick mit rund zehn MByte freiem Speicherplatz, auf dem Sie das Tool installieren. Fortan müssen Sie sich nur noch ein Passwort merken – das für den Stick. Denn auf diesem speichert KeePass die Log-in-Daten Ihrer Webdienste in einer verschlüsselten Datenbank, die durch das Masterpasswort geschützt ist. Den Stick brauchen Sie immer nur dann am Rechner einzustecken, wenn ein Dienst die Eingabe eines Kennwortes fordert. Trojaner, die Passwörter klauen, kön-

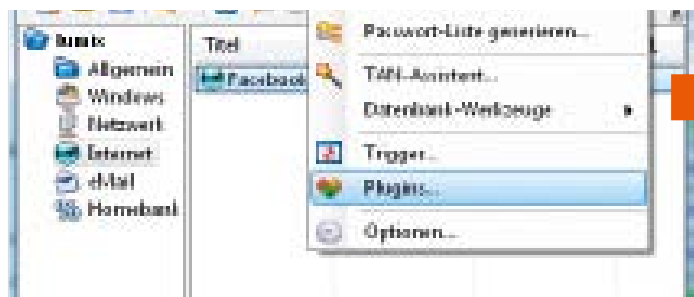
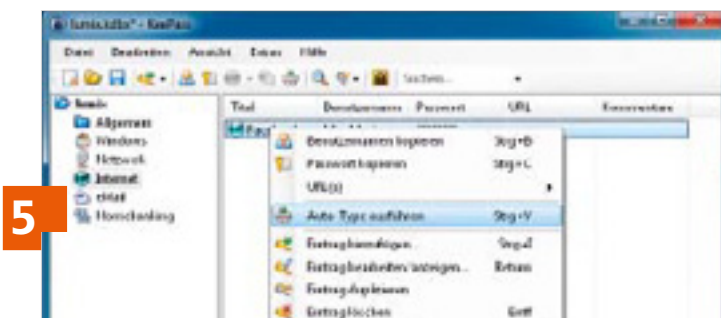
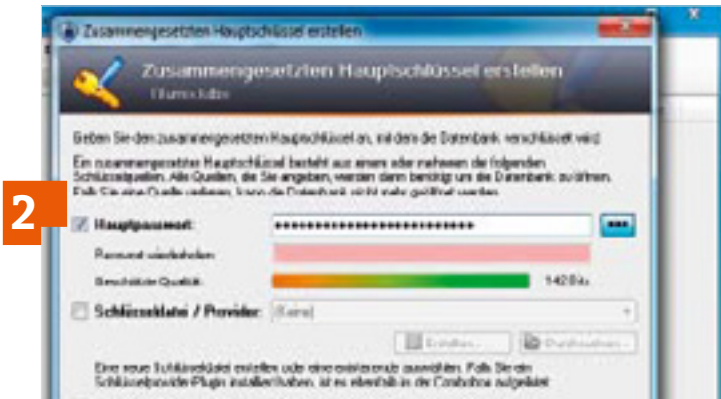
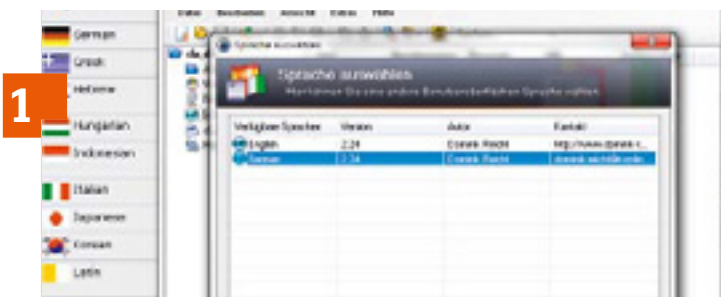
nen damit nichts mehr ausspionieren. Und weil Sie sich nicht mehr Dutzende Passwörter einprägen müssen, können Sie nun für jeden Webdienst ein neues, wirklich sicheres Kennwort verwenden. Wie Sie KeePass einrichten, erklären wir in den folgenden sechs Schritten.

So geht's 1 Passwortsafe einrichten

Stecken Sie einen leeren, formatierten USB-Stick am PC ein, entpacken Sie die Datei »KeePass-2.24.zip« auf den Stick und doppelklicken Sie auf »KeePass.exe«. Aktivieren Sie nach dem Start die automatische Suche nach Updates per Klick auf »Enable«. Dann wählen Sie »View | Change Language« und klicken auf »Get more languages«. Laden Sie die deutsche Sprachdatei von der nun geöffneten Webseite per Klick auf »German | 2.24+«. Die ZIP-Datei entpacken Sie auf den USB-Stick. Danach gehen Sie wieder zu »View | Change Language«, wählen »German« und starten KeePass per Klick auf »Ja« neu.

2 Masterpasswort festlegen

Wählen Sie »Datei | Neu« und geben Sie als Speicherort für die Passwortdatenbank den USB-Stick an. Im folgenden Fenster legen Sie bei »Hauptpasswort« ein Kennwort fest. Das müssen Sie bei jedem Start von KeePass eingeben. Wir empfehlen, mindestens 15 Buchstaben,



Die besten Erweiterungen für KeePass

Statten Sie Ihren Passworttresor mit zusätzlichen Funktionen aus, etwa einem Backup oder einer Kennwortübertragung für Handys

Name	Beschreibung
DataBaseBackup	Erstellt eine Sicherung Ihrer Passwortdatenbank, für den Fall, dass der USB-Stick gestohlen wird oder verloren geht
Twofish Cipher	Fügt einen fast unknackbaren Verschlüsselungs-Algorithmus hinzu; beachten Sie, dass KeePass hierdurch langsamer wird
KeeAgent	Blockiert Lausangriffe, indem es Ihre Log-in-Daten über eine verschlüsselte SSH-Verbindung überträgt
KeyExchanger	Speichert das Masterpasswort auf dem Handy; via Bluetooth können Sie dann Ihren Passwortsafe auf dem PC öffnen
KeeForm	Öffnet auf Knopfdruck Ihre Lieblingswebsites und trägt dort automatisch die Anmeldeinformationen ein

Zahlen und Sonderzeichen zu verwenden, zum Beispiel die Anfangsbuchstaben der Worte und die Satzzeichen eines für Sie leicht zu merkenden Satzes. Bestätigen Sie das Masterpasswort mit »OK«, und geben Sie der Datenbank im nächsten Fenster einen Namen.

3 Sicheren Desktop aktivieren

Damit Trojaner nicht Ihr KeePass-Kennwort mitlesen, sollten Sie den von der Windows-Benutzerkontensteuerung bekannten Secure Desktop nutzen. Dafür gehen Sie in KeePass zu »Extras | Optionen | Sicherheit«, scrollen im Feld »Optionen« nach unten und setzen einen Haken bei »Hauptschlüssel auf sicherem Desktop eingeben«.


4 Kennwörter hinterlegen

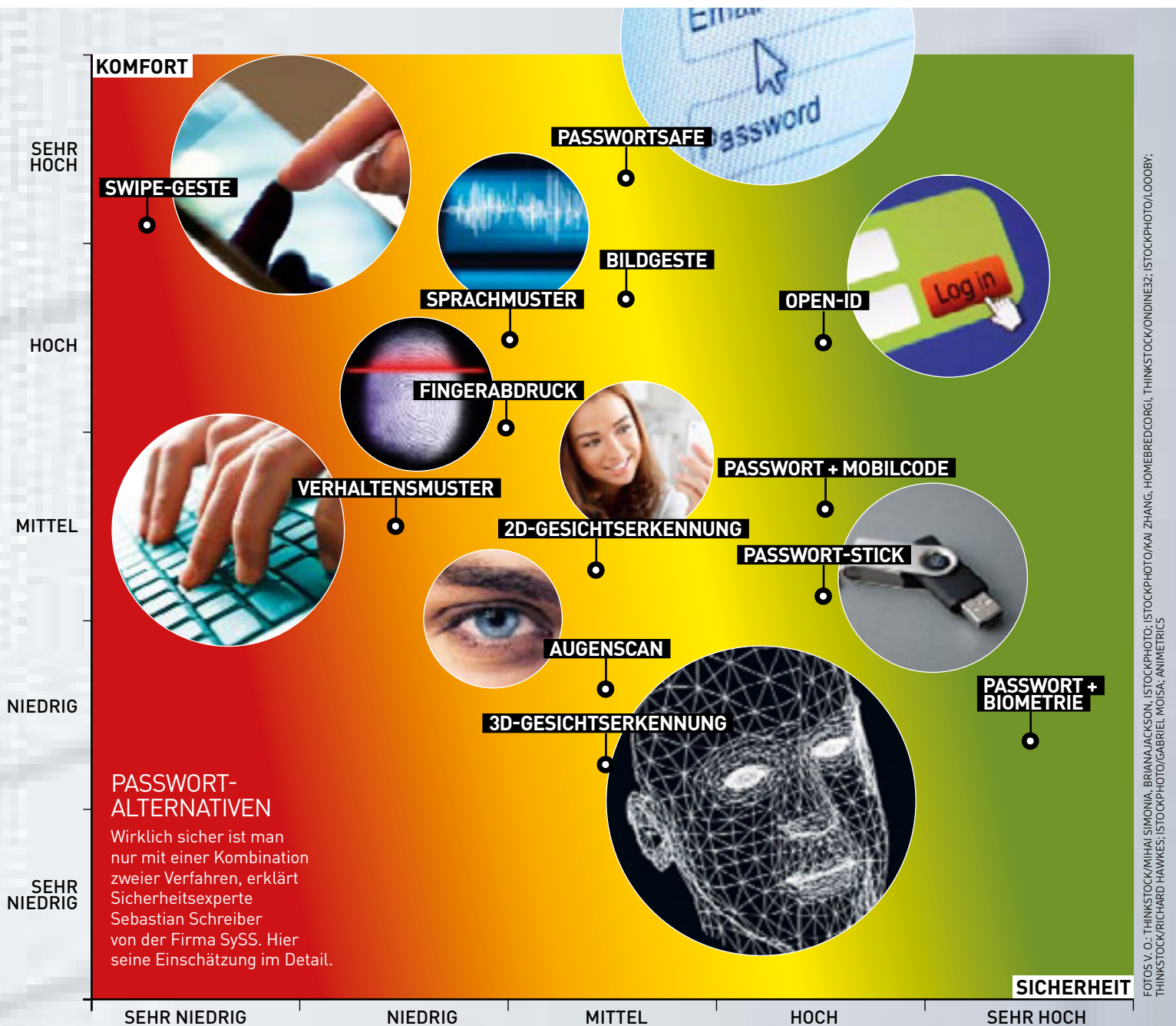
Ihre Kennwort-Datenbank zeigt links Kategorien wie »Windows« oder »Internet« an. Wählen Sie einen Bereich und klicken Sie in der Symbolleiste auf den Schlüssel. Tragen Sie im folgenden Fenster den Namen, die URL und Ihre Log-in-Daten für einen Dienst ein. Da Sie sich dessen Passwort nicht mehr merken müssen, können Sie bei dem Dienst ein neues, komplexes Passwort vergeben, das Sie etwa auf passwort-generator.com erstellen lassen.

5 Automatische Anmeldung nutzen

Wollen Sie sich mit KeePass bei einem Dienst einloggen, öffnen Sie dessen Seite und starten KeePass. Klicken Sie mit der rechten Maustaste auf den Dienst in der KeePass-Datenbank und wählen Sie »Auto-Type ausführen«. Das Tool kopiert nun die Log-in-Daten in das Eingabefeld der Webseite. Achten Sie darauf, dass Sie exakt die URL eingeben, die in der Datenbank steht, sonst reagiert KeePass nicht.

6 Passwortsafe sinnvoll erweitern

Wollen Sie KeePass erweitern, rufen Sie über »Extras | Plugins | Mehr Plugins herunterladen« eine Webseite mit nützlichen Upgrades auf (unsere Empfehlungen finden Sie in der Tabelle oben). Nun laden Sie von der Website die ZIP-Datei per Klick auf den Plug-in-Namen herunter und entpacken sie auf den Stick. Sie starten KeePass neu und gehen auf »Extras«. In dem Menü finden Sie unten die Plug-ins, welche Sie von dort ausführen können.  testtechnik@chip.de



PASSWORTade

Hackerattacken und Lücken in Hard- und Software bedrohen Ihre Webidentität. Was tun? Packen Sie das Passwort in einen Safe, auf einen Stick – oder verzichten Sie ganz darauf

VON CLAUDIO MÜLLER

Ein sehr berühmter Sicherheitstipp stammt von dem Wissenschaftler Clifford Stoll: „Behandle Dein Passwort wie Deine Zahnbürste: Lass niemanden heran und wechsele es alle sechs Monate.“ Doch mit Passworttipps ist es wie mit Glückskeks-sprüchen. Der psychologische Wohlfühleffekt ihrer leicht bekömmlichen Weisheiten ist groß. Ihre tatsächliche Schutzwirkung eher gering. Sie sind zu simpel für eine komplexe Welt mit Tausenden Onlinebanken, -shops und Webdiensten, mit Millionen Mobilgeräten, die alle per Passwort geschützt werden wollen.

Denn anders als die Zahnbürste kann man Passwörter nicht ausschließlich zu Hause aufbewahren. Sie liegen immer auch in Datenbanken auf den Servern der Webdienste, manchmal nur schwach verschlüsselt, damit Sie sich dort einloggen können. Und diese Server werden gehackt. Sony hat es schon erwischt, genauso Yahoo, Gamigo, LinkedIn oder zuletzt Evernote (siehe rechts). Ob man sein Passwort kurz zuvor geändert oder es schon seit Jahren verwendet hatte, ob man auf ein kurzes wie [12345] oder ein komplexes wie [Hc84#6gBm7§_v] vertraute – es spielte keine Rolle. Bei diesen Angriffen waren alle Passwörter betroffen.

Hacker sind mindestens so clever wie Sie

Dummerweise sind Sie bei Webdiensten auf Passwörter angewiesen, denn andere Möglichkeiten bieten die meist nicht. Doch ein sicheres, aber leicht zu merkendes Kennwort zu erstellen, ist leicht – wenn man die Tricks der Hacker kennt. Verwenden Sie keine echten Wörter, nicht einmal dann, wenn Sie etwa das „i“ durch eine „l“ oder das „E“ durch eine „3“ ersetzen. Bei Angriffen mit einem festen Passwortbestand (Wörterbuchattacken) probieren Passwortknacker inzwischen selbst diese Varianten automatisiert durch. Auch zu kurz sollte das Kennwort nicht sein. Denn sogar kryptische Zeichenketten knacken Brute-Force-Angriffe in weniger als einer Minute, wenn sie nur sechs Zeichen lang sind (laut der Seite [howsecureismypassword.net](#)). Und vor allem sollten Sie nie ein Passwort mehrfach verwenden. Knackt der Hacker diesen Generalschlüssel auf einer Seite, wären dann auch Ihre anderen Accounts gefährdet.

Eine leicht anwendbare Passwortstrategie verrät uns Markus Jakobsson, leitender Wissenschaftler für Nutzersicherheit bei PayPal. Sein Tipp: „Kombinieren Sie ein Masterpasswort mit einem seiten-spezifischen Passwort.“ Das Masterpasswort – zum Beispiel Hc84# (keine Initialen oder Ihr Geburtsdatum!) – ergänzen Sie mit einer für jede Website einzigartigen Zeichenkette. „Vermeiden Sie dabei vorhersehbare Zeichen, etwa den Namen der Seite“, sagt Jakobsson. Nehmen Sie stattdessen etwa „Ozean*8“ für Facebook (abgeleitet vom Facebook-Blau und der Zeichenzahl des Dienstes). Die seiten-spezifischen Passwortteile können Sie laut Jakobsson aufschreiben und in Ihrer Brieftasche oder zu Hause aufbewahren – bloß nie zusammen mit dem Masterpasswortteil.

Ähnlich kreativ sollten Sie auch die Sicherheitsfragen zur Passwortwiederherstellung beantworten, die oft Teil der Registrierung bei einer Website sind. Ihre Lieblingsfarbe ist Rot? Das errät jeder Angreifer. Auch hier lässt sich die Jakobsson-Strategie anwenden. Die Lieblingsfarbe könnte dann etwa lauten: Ma+§Bordeauxrot§ (Ma für Mailaccount). Wenn Sie für die Passwortwiederherstellung zudem eine alternative Mailadresse angeben können, tun Sie das. Am besten legen Sie sich eine ausschließlich für diesen Zweck an.

Damit Ihnen im Worst-Case-Szenario, dem gehackten E-Mail-Konto, keine Kettenreaktion gekapeter Accounts droht, sollten Sie dieses Konto besonders schützen. Die Mailadresse ist nicht nur der Anker Ihrer digitalen Identität. Sie ist bei vielen Webdiensten auch der Nutzernamen und dient der Passwortwiederherstellung. Wer →

DIE HÄUFIGSTEN PASSWÖRTER

Über zwölf Jahre sammelte Sicherheitsforscher Mark Burnett Passwörter aus offenen Quellen, etwa per Google durchsuchbare Datenbanken. Das sind die beliebtesten:

password	2000	hockey	dallas
123456	jordan	george	yankees
12345678	superman	charlie	123123
1234	harley	andrew	ashley
qwerty	1234567	michelle	666666
12345	fuckme	love	hello
dragon	hunter	sunshine	amanda
pussy	fuckyou	jessica	orange
baseball	trustno1	asshole	biteme
football	ranger	6969	freedom
letmein	buster	pepper	computer
monkey	thomas	daniel	sexy
696969	tigger	access	nicole
abc123	robert	123456789	thunder
mustang	soccer	654321	ginger
michael	fuck	joshua	heather
shadow	batman	maggie	hammer
master	test	starwars	summer
jennifer	pass	silver	corvette
111111	killer	william	taylor

17%

ALLER NUTZER VERWENDEN REALE WORTE ODER NAMEN ALS PASSWORT

DIE GRÖSSTEN PASSWORT-HACKS



Sony PlayStation Network (77 Mio. Accounts):

Die Mutter aller Passworthacks bedrohte im April 2011 alle PSNetwork-Accounts. Neben Passwörtern konnten die Angreifer auch Kreditkartendaten auslesen. Sony nahm den Dienst daraufhin für 24 Tage vom Netz.



Evernote (50 Mio. Accounts):

Im März gab der Daten- und Notizspeicherdienst einen Hackerangriff bekannt, bei dem 50 Millionen Datensätze (Username, Mailadresse, verschlüsseltes Passwort) kompromittiert wurden.



Gamigo (8,24 Mio. Accounts):

Der deutsche Onlinespiele-Anbieter Gamigo wurde im Februar 2012 gehackt, im Juli tauchten die Passwörter mit den E-Mail-Adressen im Web auf. Bis heute die größte bekannte Passwortsammlung eines einzelnen Hacks.



LinkedIn (6,5 Mio. Accounts):

Das Businessnetzwerk wurde im Juni gehackt, die Passwörter erschienen in einem russischen Webforum.



Yahoo (450.000 Accounts):

Die im Juli 2012 veröffentlichten Passwörter von Yahoo Voices waren unverschlüsselt, die Hacker konnten sie also direkt weiterverwenden, etwa um sie an Yahoo-Mailaccounts auszuprobieren.



Twitter (250.000 Accounts):

Im Februar, kurz nachdem chinesische Hackerangriffe auf große US-Dienste wie Facebook, Twitter, Apple oder die New York Times bekannt wurden, tauchten 250.000 Log-in-Datensätze zu Twitterkonten im Web auf.

Ihren Mailaccount kontrolliert, kann sich also bei vielen Diensten problemlos die Log-in-Daten zuschicken lassen. Damit kauft er zum Beispiel mit Ihren hinterlegten Bezahlinformationen im Online-shop ein, sieht Ihre persönlichen Fotos im Webspeicher an oder tritt in Ihrem Namen in sozialen Netzwerken auf. Ein Horrorszenario.

E-Mail: Doppelt schützt besser

Es ist vollkommen unverständlich, warum viele E-Mail-Provider (darunter GMX oder Microsoft) keine zweite Sicherheitsstufe neben dem Passwort anbieten. Sicherheitsexperten wie Sebastian Schreiber von SySS nennen das Single Point of Failure, denn wer das Passwort kennt, kann den Account übernehmen. Nur wenige Anbieter unterstützen die Zwei-Faktor-Authentifizierung (siehe rechts). Neben dem Passwort müssen Sie sich dabei mit einem meist achtstelligen Zahlencode authentifizieren. Den bekommen Sie entweder per SMS zugeschickt oder erzeugen ihn mit einer App auf dem Smartphone. Wer sich einmal so authentifiziert hat, kann das dabei verwendete Gerät als vertrauenswürdig definieren. Bei zukünftigen Log-ins an diesem Gerät genügt dann wieder das normale Passwort. Bei Anmeldeversuchen von einem unbekannten Gerät bekommen Sie aber eine SMS zugeschickt. Und so haben Sie gleichzeitig ein Warnsignal, ob sich irgendjemand in Ihren Mailaccount hacken will.

In Google, neben Yahoo der einzige große Mailanbieter mit Zwei-Faktor-Authentifizierung, richten Sie die Methode so ein: Klicken Sie im Gmail-Postfach auf den Pfeil rechts oben und wählen Sie »Konto | Sicherheit | Bestätigung in zwei Schritten | Einstellungen«. Ein Assistent führt Sie durch die weiteren Schritte. Halten Sie dabei das Handy parat, um den ersten Code per SMS zu empfangen. Bei anderen Anbietern finden Sie diese Einstellungen üblicherweise im Nutzerkonto unter »Sicherheit« oder »Kontoeinstellungen«.

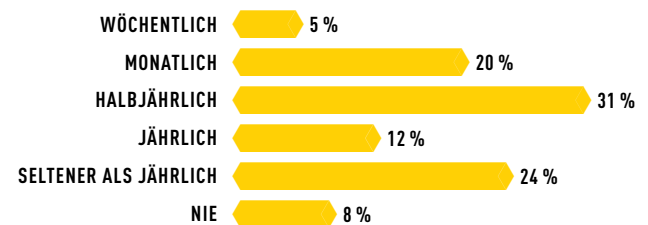
Eine zweite Sicherheitsstufe bedeutet natürlich: weniger Komfort. Zudem dürfen Sie nicht vergessen, die hinterlegte Mobilnummer zu ändern, wenn Sie mal eine neue haben. Eine bequemere Lösung sind Passwortsafes, zum Beispiel LastPass (auf Heft-DVD). LastPass speichert Ihre Log-in-Daten in einem mit 256 Bit verschlüsselten und per Masterpasswort geschützten Onlinespeicher. Über synchronisierte Browser-Plug-ins und Apps können Sie sich damit auf allen Geräten in Ihre Webkonten einloggen. Auf Wunsch füllt LastPass die Log-in-Felder automatisch aus. Das hat zwei Vorteile: Sie brauchen sich keine Passwörter mehr merken, und Keylogger-Trojaner können keine Passworteingaben von der Tastatur mitschneiden. Das große Risiko von Passwortsafes: Wer Ihr Masterpasswort klaut (vom PC oder vom Server des Anbieters), kennt all Ihre Log-in-Daten.

Ähnlich bequem sind OpenID-Verfahren, bei denen Sie sich eine universell nutzbare persönliche Kennung generieren lassen können, meist in Form einer URL. Diese URL geben Sie dann statt des Passworts ein. Ein echter Sicherheitsgewinn, denn jede Passworteingabe ist ein Sicherheitsrisiko. OpenID-Lösungen sind elegant, wenn auch nur so sicher wie die Server der Anbieter. Neben Google, Facebook oder Mozilla gibt es auch unabhängige wie myOpenID. Der einzige Nachteil: Sie können OpenIDs nur auf Seiten nutzen, die das Verfahren unterstützen – und das sind aktuell nicht sehr viele.

Windows: Passwort für die Hosentasche

Mit den oben genannten Passwortregeln können Sie auch die Windows-Parole kreieren und so Ihren Rechner schützen. Doch statt es über die Tastatur einzugeben, sollten Sie einen USB-Stick als virtuellen Schlüssel verwenden. Den können Sie wie einen echten immer bei sich tragen. Seit Windows Vista bietet Microsoft dafür eine integrierte Lösung an, allerdings nur in den Versionen Ultimate und

SO HÄUFIG WECHSELN NUTZER IHR PASSWORT



ZWEI-FAKTOR-AUTHENTIFIZIERUNG

Sehr sicher ist nur, wer mindestens zwei Verfahren nutzt, also das Passwort ergänzt. Das ist in der Regel ein Zahlencode, den Sie per SMS oder App auf das Smartphone bekommen.

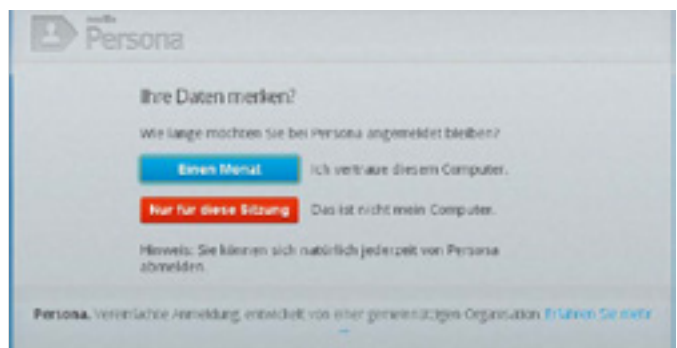


ANBIETER	METHODE
GOOGLE-DIENSTE	per SMS oder Authenticator-App
MICROSOFT SKYDRIVE, XBOX	per SMS oder an alternative E-Mail-Adresse
PAYPAL	per Codegenerator oder SMS
FACEBOOK	per SMS oder die Facebook-App
DROPTBOX	per SMS oder Googles Authenticator-App
LASTPASS	per Googles Authenticator-App
YAHOO MAIL	per SMS oder Sicherheitsfrage
WORDPRESS	per Googles Authenticator-App
DE-MAIL	per SMS, neuem Personalausweis oder Signaturkarte
APPLE ID, iCloud	per SMS (bisher nur USA, UK)



OPENID

Bei OpenID-Verfahren müssen Sie sich nicht mit Benutzername und Passwort anmelden, sondern nur mit Ihrer OpenID, meist eine URL. Noch unterstützen das nur wenige Seiten.



Enterprise (beziehungsweise Windows 8 Pro). Mit der BitLocker-Laufwerksverschlüsselung kodieren Sie Ihre Datenpartition und schützen sie entweder per PIN-Code oder per Stick (unsere Empfehlung). Der USB-Stick enthält dabei eine Schlüsseldatei, die das Laufwerk entsperrt, sobald Sie den Rechner starten. Einrichten können Sie dies unter »Systemsteuerung | System und Sicherheit | BitLocker-Laufwerksverschlüsselung«. Folgen Sie nach einem Klick auf »BitLocker aktivieren« einfach der Einrichtungsroutine.

Wer BitLocker nicht nutzen kann, installiert das Tool USBLogon (auf Heft-DVD). In dem Tool wählen Sie den USB-Stick aus und legen fest, ob der Log-in automatisch erfolgt, wenn der Stick angeschlossen ist, und was der Rechner tun soll, wenn Sie den Stick abziehen (etwa Standby, runterfahren oder Bildschirmschoner). Der Stick meldet Sie dann in Windows an. Lediglich auf die Festplattenverschlüsselung von BitLocker müssen Sie verzichten. Mit dem Tool TrueCrypt (ebenfalls auf Heft-DVD) können Sie die aber selbst nachrüsten.

Smartphone: Verräterische Schmierfinger

Nach Webdiensten und dem Rechner bleibt jetzt nur noch, Ihre Mobilgeräte zu schützen. Die bewahren nahezu unser gesamtes digitales Leben in komprimierter Form in ihrem Flashspeicher – und sind oft absurd schwach geschützt. Gegen einige ihrer Sicherheitslücken ist man machtlos. Angreifer konnten etwa beim iPhone und beim Samsung Galaxy SIII über die Notruffunktion im Sperrbildschirm die Telefonsperre umgehen. Bei Mobilgeräten sind Sie zudem davon abhängig, welche Gerätesicherung und Nutzerauthentifizierung sie überhaupt bieten. Biometrische Verfahren sind leider immer noch kaum über den Prototypstatus hinaus (→ S. 26).

Bei den meisten Mobilgeräten können Sie neben der PIN-Nummer der SIM-Karte lediglich einen Sperrcode anlegen – eine vierstellige PIN oder eine Swipe-Geste über ein Raster von neun Punkten. Die IT-Sicherheitsfirma Symantec fand bei einer Analyse gestohlener Smartphones heraus, dass 40 Prozent der Geräte mit dem Code [1234] gesichert waren. Auch wenn ein Telefondieb nur drei Versuche für die Eingabe hat, auf solche Codes kommt er vermutlich schnell. Ähnlich unsicher sind die Gesten, die man über die Fingerabdrücke auf dem Display nachvollziehen kann (Smudge-Attack).

Im Vergleich zu Apple und Google ist Microsoft schon einen Schritt weiter beim Schutz mobiler Geräte. In Windows 8 können Sie nämlich Bilderpasswörter nutzen. Dabei zeichnen Sie Gesten auf einem Bild, etwa einen Punkt, einen Kreis oder eine Linie zwischen zwei Bildelementen. Der Vorteil: Die Gesten sind ähnlich sicher wie komplexe Passwörter, lassen sich aber auf Touchgeräten komfortabler eingeben. Zudem funktionieren sie auch am PC, wo Sie die Gesten per Maus nachzeichnen. Und so richten Sie ein Bilderpasswort ein: Öffnen Sie die Charm Bar [Win]+[C] und gehen Sie auf »Einstellungen | PC-Einstellungen | Benutzer«. Dort kreieren Sie ein Windows-Kennwort und klicken danach auf »Bildcode erstellen«. Folgen Sie nun dem Einstellungsassistenten. Unser Tipp: Verwenden Sie keine Punktgesten, sondern nur Linien und Kreise. Die sind sicherer, da sie sowohl Positions- als auch Richtungsdaten enthalten. Außerdem sollten Sie keine vorhersehbaren Gesten wählen, etwa ein Kreis um ein Gesicht. Vor allem am PC ist diese Methode ein hervorragender Ersatz für das Passwort, da hier nicht einmal Wischspuren auf einem Display zurückbleiben. Wer unsere Passwortstrategien befolgt, braucht die Parolen (im Gegensatz zur Zahnbürste) auch nicht regelmäßig zu wechseln. Es sei denn, Passwort, Stick oder Smartphone waren in falschen Händen. Dann sollten Sie bei allen Accounts das Kennwort ändern. Sicher ist sicher. ☑

TESTTECHNIK@CHIP.DE

SWIPE

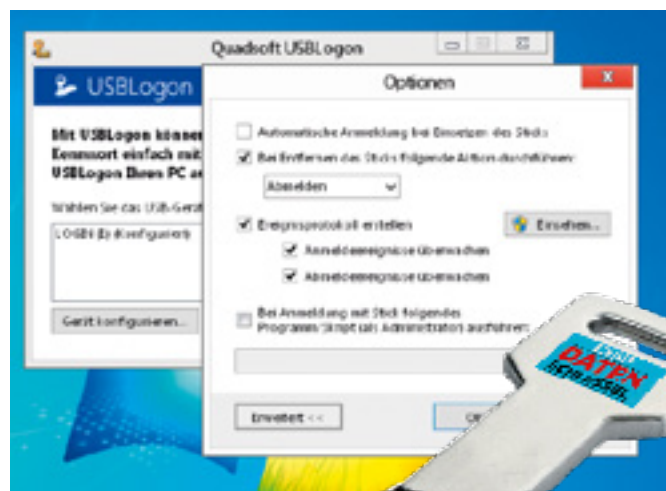
Swipe-Gesten sind simpel, und damit gefährlich. Denn die Touchgesten kann man bei guten Lichtverhältnissen als Fingerspuren auf dem Display sehen. Dann muss man nur noch die Richtung der Geste ausprobieren und das Gerät ist entsperrt.

SICHERHEIT 
KOMFORT 



PASSWORTSTICK

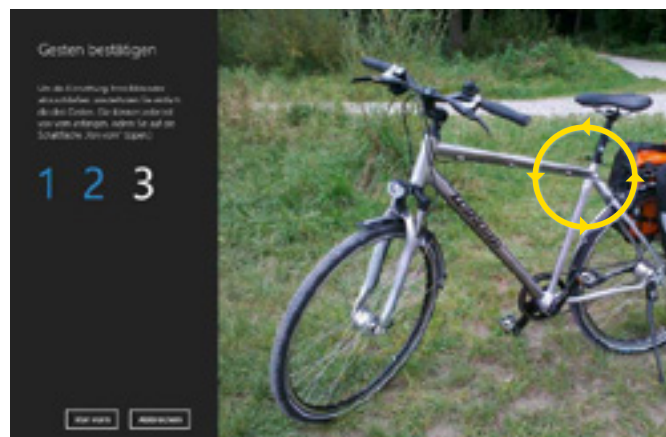
Windows per Passwortstick zu schützen (oder bei BitLocker ganze Partitionen zu verschlüsseln), ist simpel – man darf das kleine Teil nur nicht verlieren.



SICHERHEIT 
KOMFORT 

WINDOWS-8-BILDERPASSWORT

Drei verschiedene Gesten auf einem Foto sind für Angreifer schwer nachzuvollziehen. Für User ist das auf Touchgeräten aber viel einfacher, als ein komplexes Passwort einzutippen.

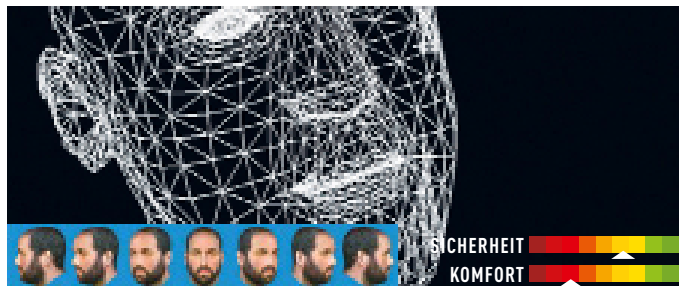


SICHERHEIT 
KOMFORT 



Log-in per Blick

Flughäfen oder Polizeibehörden setzen schon seit Jahren Augenscanner ein. Die erkennen Menschen anhand der Kapillaren in der Netzhaut oder der Struktur der Iris. Unter optimalen Bedingungen ist diese Erkennung nahezu fehlerfrei. Doch Lichteinfall oder auch Verletzungen des Auges können die Identifikation stören. Zudem konnten Irisscanner schon durch Fotos des Auges überlistet werden. Und die meist mit Infrarottechnik arbeitenden Scanner taugen nicht für den Einsatz in Mobilgeräten – anders als die App EyeVerify. Die fotografiert Ihre Augen und erkennt Sie anhand der Adern im Augapfel, wofür laut Anbieter schon Kameras ab zwei Megapixel genügen. Von den vier Augenabdrücken – jeweils links und rechts der Iris in beiden Augen – muss nur einer übereinstimmen, damit die App das Telefon entsperrt. Auch mit einem blauen Auge können Sie also Ihr Handy freischalten und den Arzt rufen. Damit die Software ein Foto von einem echten Menschen unterscheiden kann, verändert sie zufallsgesteuert den Kamerafokus und prüft die Reaktion des Auges. EyeVerify soll im Sommer 2013 auf den Markt kommen.



3D-Gesichtsanalyse

Seit Android 4.0 kann man Smartphones per Gesichtserkennung entsperren. Die Face-Lock-Funktion arbeitet zuverlässig, allerdings nur bei guten Lichtverhältnissen. Bei Gegenlicht, etwa Sonnenschein, braucht es mitunter etliche Versuche. Ließ sich Face Unlock anfangs noch per Foto überlisten, muss man heute blinzeln, um zu beweisen, dass man wahrhaft ein Mensch ist. PC-User können mit der Software Blink (auf Heft-DVD) ebenfalls eine Gesichtserkennung nutzen. Die oft verwendete 2D-Erkennung authentifiziert Sie anhand von etwa 80 Merkmalen (Augenabstand, Breite der Nase), die sie per Berechnung eines Wertes oder Musterabgleich analysiert. Da eine 2D-Erkennung weder fehlerfrei noch fälschungsresistent ist, geht der Trend aber zum weniger lichtabhängigen 3D-Gesichtsscanner. Eine mikrometergenaue Vermessung der Gesichtsoberfläche, die sogar aus Fotos errechnet werden kann, soll Menschen zuverlässiger identifizieren. Eine zusätzliche Oberflächentexturanalyse der Haut unterscheidet sogar eineiige Zwillinge. Militärs und Polizei nutzen das schon heute, etwa mit der Smartphone-App FaceR MobileID von Animetrics.



VoiceTAN fürs Banking

Stimmerkennung in Alltagsgeräten ist wegen der Hintergrundgeräusche oft schwierig. Stimmfrequenzanalysen oder Mustererkennungsalgorithmen funktionieren bislang zuverlässig nur in stillen Umgebungen. Daher arbeiten Forscher intensiv an der Verbesserung der Geräuschunterdrückung. Funktioniert die Technik, wird sie vor allem für Bankgeschäfte mit dem Smartphone interessant, da sich die Stimme über die Telefonverbindung prüfen lässt. Ein Ansatz ist Voice TAN des deutschen Finanzdienstleisters GFT. Dabei spricht man bei der Registrierung einen vierstelligen Zahlencode dreimal ins Telefon, woraus ein Sprachmuster erzeugt wird. Nach der Eingabe von Überweisungsdaten erhält man einen automatischen Anruf, bei dem man diesen Code wiederholt. „Der Prototyp hat aktuell eine Erkennungsgenauigkeit von etwa 85 Prozent“, sagt Bernd Kohl von GFT. Bis zum Marktstart will man das aber noch verbessern. Eine ähnliche Lösung stellte die Firma VoiceVault im März vor. Sie erlaubt auch komplexe Eingabephrasen, etwa ganze Sätze in jeder beliebigen Sprache, was die Zuverlässigkeit noch einmal erhöht.

Fingerabdruckscan

In Notebooks, Tastaturen oder externen USB-Scannern gibt es Fingerscanner schon seit Jahren. Gerüchten zufolge könnte auch das iPhone 5 einen im Home-Button haben. Ein interessantes Projekt ist myIDkey, ein per Fingerabdruck gesicherter USB-Stick, der Passwörter, Dokumente oder Bilder verschlüsselt speichert. Er verbindet sich per USB oder Bluetooth mit Geräten oder zeigt die Log-in-Daten auf einem Display an, erzeugt sichere Passwörter und löscht die Daten nach mehreren Fehlversuchen. Ab August soll er für etwa 100 US-Dollar auf den Markt kommen.

SICHERHEIT 
KOMFORT 




Verhaltensmuster

Auch die Interaktion mit Geräten erzeugt ein einzigartiges Muster. Die schwedische Firma BehavioSec hat dafür eine Erkennungssoftware entwickelt. Diese prüft eingegebene Passwörter oder Gesten nicht nur auf Korrektheit, sondern auch, wie sie eingegeben werden. Zu den analysierten Faktoren zählen die Tippgeschwindigkeit und der Tipprhythmus. Bei Touchscreens erkennt die Software den Druck und den Winkel der Gesten, an der Maus die Mausbeschleunigung und die Klickfrequenz. Diese Methode wäre ein einfacher Weg, eine weitere Sicherheitsstufe anzubieten.

SICHERHEIT 
KOMFORT 



Impressum

Chefredakteur	Josef Reitberger (verantwortlich für den redaktionellen Inhalt)
stellv. Chefredakteur	Andreas Hentschel
Art Direction	Stephanie Schönberger
Chefin vom Dienst	Verena Flurschütz
News	Niels Held (Lt看. Print), Markus Schmidt (Lt看. Online); Caren Stella Geiger, Dominik Hayon, Rupert Mattgey, Claudio Müller, Frederik Niemeyer
Test & Technik	Martin Michl (Lt看.); Benjamin Hartlmaier, Fabian von Keudell, Peter Krajewski, Markus Mandau, Christoph Schmidt, Andreas Vogelsang
Multimedia	Andreas Hentschel (Lt看.); Peter Deppner (Lizenzen), Karsten Bunz, Patrick Dörfel
Red. Tablet-Edition	Dominik Hoferer
Testcenter	Wolfgang Pauler (Testchef CHIP); Torsten Neumann (Teamleiter Testcenter), James Curtis, Tomasz Czarnecki, Werner Gaschar, Christoph Giese, Grzegorz Glonek, Stephan Hartmann, Leopold Holzapfel, Martin Jäger, Robert Kraft, Martin Nowakowski, Sven Sebastian, Jacek Wojtowicz
Grafik	Antje Küther (Lt看.); Janine Auer, Esther Göddertz, Doreen Heimann, Isabella Schillert, Andreia Margarida da Silva Granada, Veronika Zangl
Schlussredaktion	Renate Feichter, Birgit Lachmann, Angelika Reinhard
Bildredaktion	Jennifer Heintzschel, Gertraud Janas-Wenger
Bildbearbeitung	Gisela Zach
Assistenz	Verena Flurschütz (Redaktion) Monika Masek (Testcenter)
CHIP Online	Martin Gollwitzer (Chefredakteur CHIP.de), Carl Schneider (Chefredakteur CHIP.de), Lisa Brack (Stellv. Chefredakteurin), Dr. Wiebke Hellmann (Lt. Redakteurin), Florian Holzbauer (Lt. Redakteur), Michael Humpa (Teamleiter Downloads & Apps), Beate Kipphardt (Teamleiterin Software & OS), Michael Ludwig (Ressortleiter), Alexander Schauer (CvD & Lt. Schlussredakteur), Kirstin Dedic, Saskia Dittrich, Markus Grimm, Benjamin Heinfling, Andreas Nolde, Matthias Röbler, Dennis Schöberl, Sebastian Schoener, Manuel Schreiber, Christian Schwalb, Rian Voß, Moritz Wanke, Dominik Zientek Thomas Mayrhans (Director Product)
Anschrift der Redaktion	St.-Martin-Straße 66, 81541 München Tel. 089 746 42-502 (Redaktion), -253 (Testcenter), -120 (Fax)
Geschäftsführung	Thomas Koelzer (CEO) Markus Scheuermann (COO)
Executive Director	Florian Schuster
Director Distribution	Andreas Laube
Herstellung	Andreas Hummel, Frank Schormüller Medienmanagement Vogel Business Media GmbH & Co. KG 97064 Würzburg
Vertrieb	MZV GmbH & Co. KG 85716 Unterschleißheim Internet: www.mzv.de
Verlag	CHIP Communications GmbH St.-Martin-Straße 66, 81541 München Tel. 089 746 42-0, Fax: 089 746 42-120
 <small>a BurdaTech company</small>	Die Inhaber- und Beteiligungsverhältnisse lauten wie folgt: Alleinige Gesellschafterin ist die CHIP Holding GmbH mit Sitz in der St.-Martin-Straße 66, 81541 München.
Verleger	Prof. Dr. Hubert Burda