Leben

Heute: Computer & Web

Der Herzschlag als Passwort

Datensicherheit Um Hackern das Leben zu erschweren, sollte man für jeden Dienst an anderes Kennwort benutzen

Von unserem Online-Chef Marcus Schwarze

Vermutlich werden wir in ein paar Jahren darüber lächeln, wie Menschen eingangs des 21. Jahrhunderts Zugriff auf ihre Daten, das Auto, das Wohnzimmer erlangten. Dann nämlich tragen wir ein Stück Schmuck um den Arm oder eine silberne Kette um den Hals, die ganz nebenbei unseren Herzschlag misst – und per Nahfunk uns an all diesen Geräten und Räumen einloggt, die in unserer Nähe sind.

Die US-Firma Bionym bereitet genau das zurzeit vor, ein entsprechender Armreif kann unter www.getnymi.com vorbestellt werden. Die Methode: Der Rhythmus des Herzschlags ist bei jedem Menschen einmalig, und die gemessene Frequenz kann so in jedem digitalen Gerät hinterlegt und anschließend immer wieder abgeglichen werden. Zugriff erhält man nur mit dem passenden Herzschlag – fast wie mit einem Fingerabdruck im Science-Fiction-Film, nur eleganter. Getestet haben wir das allerdings noch nicht.

Wer einige Passwortregeln beachtet, der kann es Hackern schwer machen, private Daten zu erschnüffeln.

Zu viele Passwörter nötig

Bis es so weit ist, müssen wir uns noch mit Passwörtern herumschlagen. Das Fiese ist, dass diese Kennwörter nur dann sicher sind, wenn wir sie uns selbst nicht merken können und sie möglichst nur einmal pro genutztem Dienst einsetzen. Und es werden immer mehr: Man braucht ein Kennwort für das E-Mail-Postfach und den Rechnerzugang; eines für Facebook und eines für das Handy.

Nutzt man viele Dienste, gewöhnt man sich schnell daran, das gleiche Kennwort zu benutzen. Das ist aber dann misslich, falls nur einer der genutzten Dienste von Hackern gekapert wird: Unter Umständen sind dann passend zum eigenen Namen und der eigenen E-Mail-Adresse die Kennwörter im Klartext für Böslinge nachlesbar. Dann liegt es nahe, dass auch fürs E-Mail-Postfach das ausgelesene Kennwort genutzt wird. Viele Menschen machen das, nutzen also für beliebige Dienste im Internet stets das gleiche Kennwort. Sobald Hacker mit dieser Kenntnis Zugriff aufs E-Mail-Postfach erlangen, können sie auch für viele andere Dienste über die übliche Passwortherstellungsfunktion Zugang zu weiteren Diensten erlangen.

Wichtig ist es daher tatsächlich, zumindest fürs E-Mail-Postfach ein anderes Kennwort zu verwenden als für alle anderen Web-Dienste. Und es spricht wenig dagegen, die Kennwörter in einem gesondert geschützten Dokument aufzuschreiben. Im Idealfall benutzt man für jeden Dienst ein unmerkbares Kennwort großer Länge, das aus Groß- und Kleinbuchstaben besteht, Sonderzeichen und Ziffern enthält und nicht im Duden besteht. Im Alltag gelingt das durchaus mit einer Eselsbrücke: Nehmen Sie zum Beispiel die letzten drei Buchstaben eines Dienstes wie Facebook (ook), ergänzen Sie das durch die Anfangsbuchstaben eines gemerkten Satzes (NSzBdldBeDwF – um mal als Beispiel diesen Satz hier zu nehmen) und ergänzen Sie noch als Salatbeilage ein Sonderzeichen (;) sowie ein paar Zahlen wie die Zimmernummer Ihres Büros (363) – schon haben Sie mit ookNSzBdldBeDw;F363 ein denkbar sicheres Passwort in beeindruckender Länge, das auch noch für jeden Dienst unterschiedlich wäre.

Aber – ach! – manche Dienste erlauben solche langen Kennwörter nicht. Noch schlimmer: Einige Dienste im Web speichern die Kennwörter ihrer Kunden im Klartext. Im Notfall hat dort zwar dann der Administrator Zugang auf Ihre Daten, aber vielleicht auch der Praktikant. Eine Notwendigkeit dafür gibt es bei einem schlüssigen Sicherheitskonzept nicht. Über die Passwortwiederherstellung sollte der Kunde stets sein Kennwort zurücksetzen können, indem er eine E-Mail an sein E-Mail-Postfach erhält. Als Nutzer kann man sich aber nie sicher sein, wie ein Dienst die Kennwörter speichert, daher die Grundregel: stets ein anderes Kennwort.

Was ist heute noch sicher?

Ich persönlich speichere meine Kennwörter und Zugänge in einer Textdatei auf dem Rechner und bei Google Docs. Da es auf Dauer nervig ist, die Kennwörter für die vielen Dienste nachzulesen und einzutippen, speichere ich sie zusätzlich mithilfe einer besonderen Browsererweiterung bei einem US-Dienst namens LastPass. Bei jeder Eingabeforderung wird dann das Kennwort automatisch vorausgefüllt. Das ist praktisch im Alltag, aber auch bedenklich: In Zeiten von NSA-Skandal und Snowden ist bei mir persönlich das Vertrauen geschwunden, dass meine Kennwörter tatsächlich sicher bei einer beliebigen amerikanischen Firma oder überhaupt irgendwo im Internet gespeichert lagern.

Erste Versuche mit einer gespeicherten Textdatei auf einem eigenen Mini-Server bei mir im Keller laufen, im Prinzip könnte dafür der USB-Stick, eingesteckt an dem DSL-Router des heimischen Internetzugangs, reichen. Die Krux ist stets der Zugriff von unterwegs via Handy oder Laptop darauf.

Per VPN, also einer geschützten Verbindung, klappt das schon per Handy und iPad, aber das komfortable Vorausfüllen von Eingabefeldern gelingt darüber noch nicht. Denn bei allen Wünschen nach Sicherheit muss es auch praktikabel bleiben. Vielleicht weist die Idee eines Armbands, das den Herzschlag misst, in Zukunft den besseren Weg.

Serie

Schritt für Schritt ins Internet

Unsere Serie für Einsteiger

Teil 8: Web-Perlen
Teil 9: Wikipedia
Teil 10: WLAN
Teil 11: Passwörter

Lexikon der Internetbegriffe

1 VPN: Eine verschlüsselte Verbindung zu einem ausgewählten Netzwerk, beispielsweise der eigenen Firma. Per VPN (virtuelles privates Netzwerk) kann man sich von unterwegs sicher in das Netz seiner Firma einwählen und so an alle relevanten Daten gelangen.

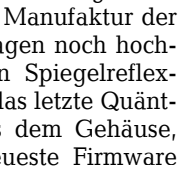
2 Passwort: Für fast alle Dienste im Internet muss man sich stets per Nutzernamen und einem Passwort anmelden. Das Passwort kennt man in der Regel nur selbst.

3 https: Anstelle der gängigen Protokollkennung http (ohne s) wird das https für gesondert geschützte Übertragungswege ins Internet verwendet. Dabei werden die Daten auf dem Weg durchs Netz verschlüsselt und können unterwegs nicht ausgelesen werden. Bei der Eingabe von Kennwörtern sollte man also stets darauf achten, dass die Adresszeile im Browser eine https-Seite ist, um sicherzustellen, dass die Daten verschlüsselt übertragen werden.

4 Zwei-Wege-Authentifizierung: Dieses neuere Verfahren gebraucht stets zusätzlich zum Kennwort einen zweiten Weg fürs Anmelden an einem System. Will man etwa ein E-Mail-Postfach von Googlemail nutzen, dann kann man in den Einstellungen diese Zwei-Wege-Authentifizierung einstellen. Dann erhält man stets eine SMS mit einer zusätzlichen Nummer, die einzutragen ist, sobald man das Postfach von einem anderen Rechner als üblich aufruft. So soll sichergestellt werden, dass kein Unbefugter auf das Postfach zugreift.

5 NSA: Die National Security Agency der USA, ein Geheimdienst, hat laut Enthüllungen ihres früheren Administrators Edward Snowden auf Millionen Verbindungsdaten im Internet zugegriffen und macht das noch heute. Dabei wurden und werden nach bisheriger Erkenntnis Datenpakete aus Knotenpunkten im weltweiten Internet, E-Mails inklusive, ausgeleitet und in einem eigenen Netzwerk abgespeichert. Alle hier genannten Ratschläge können nicht ausschließen, dass die US-Behörde im Falle des Falles Zugriff auf beliebige E-Mails erlangt. Ohne eine eigene spezielle Verschlüsselung, die zurzeit leider noch kompliziert ist und auch beim Empfänger einer E-Mail Kenntnisse über Verschlüsselung erfordert, kann man heute leider nicht sicher sein, dass die persönliche Kommunikation wirklich geheim bleibt.

Kolumne



Marcus Schwarze zu den nervigen Dingen des Digitalen

Ein Update vom Update vom Update ...

Sie sind die lästigen Begleiterscheinungen des digitalen Alltags: Updates. Mal eben die Rhein-Zeitung auf dem Handy lesen? Es steht ein Update für diese App zur Verfügung. Am Rechner den Firefox-Browser gestartet? Es gibt ein Update für Firefox. Den Windows-Rechner nach dem dreiwöchigen Urlaub einschalten? Bitte installieren Sie die folgenden Sicherheitsupdates, das Update für das Virenschutzprogramm. Und nach diesem Update das Update zum Update.

Man fragt sich: Warum können die nicht einfach fehlerfreie updatelose Software herstellen? Selbst der Fernseher, heiliger Gral abendländischer Sofakultur, fordert nun das Update der TV-Programm-Übersicht, und die Manufaktur der bis vor ein paar Tagen noch hochwertig gepriesenen Spiegelreflexkamera nutzt erst das letzte Quäntchen Leistung aus dem Gehäuse, wenn man die neueste Firmware 2.0.3.4 installiert.

Der Nutzen ist häufig minderwertig. In der Praxis bekommt man durch Updates Dinge wie den neuen Sender Universal bei Sky oder die Möglichkeit, Fotos direkt von der Kamera jetzt auch auf dem neuesten Canon-Drucker auszudrucken. Das Update hier auf dem einen Gerät erfordert dann meist ein weiteres Update dort auf dem Drucker, für den Zugriff via Windows 7 möge man bitte auch auf Windows 8 updaten, wenngleich dann möglicherweise Schwierigkeiten mit dem NAS-Server der Baureihe QNAP auftreten, zu denen man sich dann bitte direkt an QNAP wenden möge. Die antworten dann mit einer Bitte um ein Update!

Alles Lamentieren aber hilft nichts. Normalerweise behebt ein Update Fehler der Vorgängerversion. Auch auf dem Handy, dem Fernseher und der Spiegelreflexkamera sind Updates wichtig, um neue Angriffsmöglichkeiten zu unterbinden. Es gibt keine Alternative zum Update. Schon bereitet einer dieser digitalen Götter heutiger Zeit, Apple, das Update ohne Nachfrage vor. Da wird dann ohne weiteres Zutun und ohne weitere Nachfrage das Update einfach installiert. Wenn danach das eine oder andere nicht mehr funktioniert, haben die Hersteller einfach nicht ordentlich gearbeitet. Die müssen dann ein Update bereitstellen, das ordentlich funktioniert und auch das nächste Update toleriert. Vermutlich stehen wir an der Schwelle zu einem neuen Zeitalter, in dem wir die dauernden Updates im Hintergrund nicht mehr bemerken. Das wäre ja mal etwas wirklich Neues.

Kompakt

Sind APP-Wettervorhersagen wirklich zu gebrauchen?

Ausprobiert Stiftung Warentest: Temperaturangaben sind in Ordnung, Probleme gibt es beim Niederschlag

Man hat es geahnt: „Wetterapps liefern häufiger falsche Informationen“, sagt Prof. Uwe Ulbrich vom Institut für Meteorologie an der FU Berlin. Die Güte der Vorhersage hängt von der Aufbereitung der Wetterdaten ab. „Dabei gibt es einen Widerstreit zwischen den Kosten für die Interpretationssoftware und den Einnahmen für die Dienste aus Werbung oder kostenpflichtigen Apps.“ Die Stiftung Warentest hat Wetterapps verglichen. Ihre Prognosen für neun Städte weltweit mussten sich gegen jene lokaler Wetterstationen behaupten. Die meisten Apps lieferten dabei insgesamt ordentliche Vorhersagen. Besonders bei der Temperatur schnitten die meisten Anwendungen recht gut ab: „Die Abweichungen betrugen im Mittel zwischen 1 und 1,5 Grad Celsius.“ Problematischer ist die Aussagekraft digitaler Wetterhäuschen beim Niederschlag.

Einrastfunktion hilft

Handicap. Ob zum Sperren des Bildschirms oder zum Kopieren von Text: Oft genug müssen Windows-Nutzer im Computeralltag zwei oder mehr Tasten gleichzeitig drücken. Wer das nicht kann, zum Beispiel wegen eines körperlichen Handicaps, dem steht seit XP die sogenannte Einrastfunktion zur Verfügung. Aktiviert wird sie durch fünfmaliges Drücken der Umschalttaste.

Interesse an schlauer Uhr

Smartwatch. Jeder siebte Bürger (16 Prozent) will sich eine Smartwatch kaufen. Das geht aus einer repräsentativen Umfrage des Meinungsforschungsinstituts Aris hervor. Gut ein Fünftel der Teilnehmer (22 Prozent) kann sich das immerhin vorstellen. Insgesamt interessieren sich damit 38 Prozent für die Armbanduhr, die sich mit dem Internet verbinden kann.

Unterdrücken nutzlos

Überwachung. Handy und Festnetztelefon lassen sich so einstellen, dass die eigene Nummer beim Anruf nicht übertragen wird. Vor Überwachung durch den Netzbetreiber oder staatliche Behörden schützt das allerdings nicht.

WLAN nur sporadisch

Kamera. Immer mehr moderne Digitalkameras können per WLAN ins Internet gehen. Nutzer sollten die Funktion aber nur einschalten, wenn sie wirklich gebraucht wird. „Das ist schon ein ziemlicher Stromfresser“, sagt die Stiftung Warentest. Über den drahtlosen Internetzugang können die Geräte etwa Bilder bei Fotodiensten oder in soziale Netzwerke hochladen, andere lassen sich darüber fernsteuern. Vor allem unterwegs verbraucht ein aktiviertes WLAN viel Strom, weil es permanent nach verfügbaren Netzwerken sucht.

Anbieter genau prüfen

Onlineshopping Schnäppchenseiten oft unseriös

Surfen Jugendliche in eher unbekannten Onlineshops, sollten sie als Erstes einen Blick ins Impressum werfen. Am besten googeln sie auch gleich den Namen des Anbieters. „So erfahren sie, ob es schon Probleme oder Beschwerden gibt“, sagt Thomas Bradler von der Verbraucherzentrale Nordrhein-Westfalen. Besondere Vorsicht ist bei Anbietern aus dem Ausland geboten – denn da gelten oft andere Regeln.

Bei Schnäppchen freuen sich Jugendliche besser nicht vorschnell über den niedrigen Preis. „Je günstiger ein Schnäppchen ist, desto kritischer werde ich“, sagte Bradler. Denn zu oft handelt es sich bei Schnäppchenseiten um falsche Shops: Das Geld ist weg, und die Ware kommt nie an. Für sicheres Onlineshopping empfiehlt Bradler zwei Gütesiegel: Die Gütesiegel „Safershopping“ und „Trusted Shops“ zeichnen Onlineshops unter anderem für Daten- und Zahlungssicherheit aus. Die Tipps für Jugendliche gelten auch für Erwachsene. Für Minderjährige ist es gar nicht so einfach, im Internet einzukaufen. Unter 18 Jahren ist es nicht möglich, einen wirksamen Vertrag zu schließen – es sei denn, Jugendliche haben die Einwilligung ihrer Eltern oder bezahlen bar mit ihrem Taschengeld.