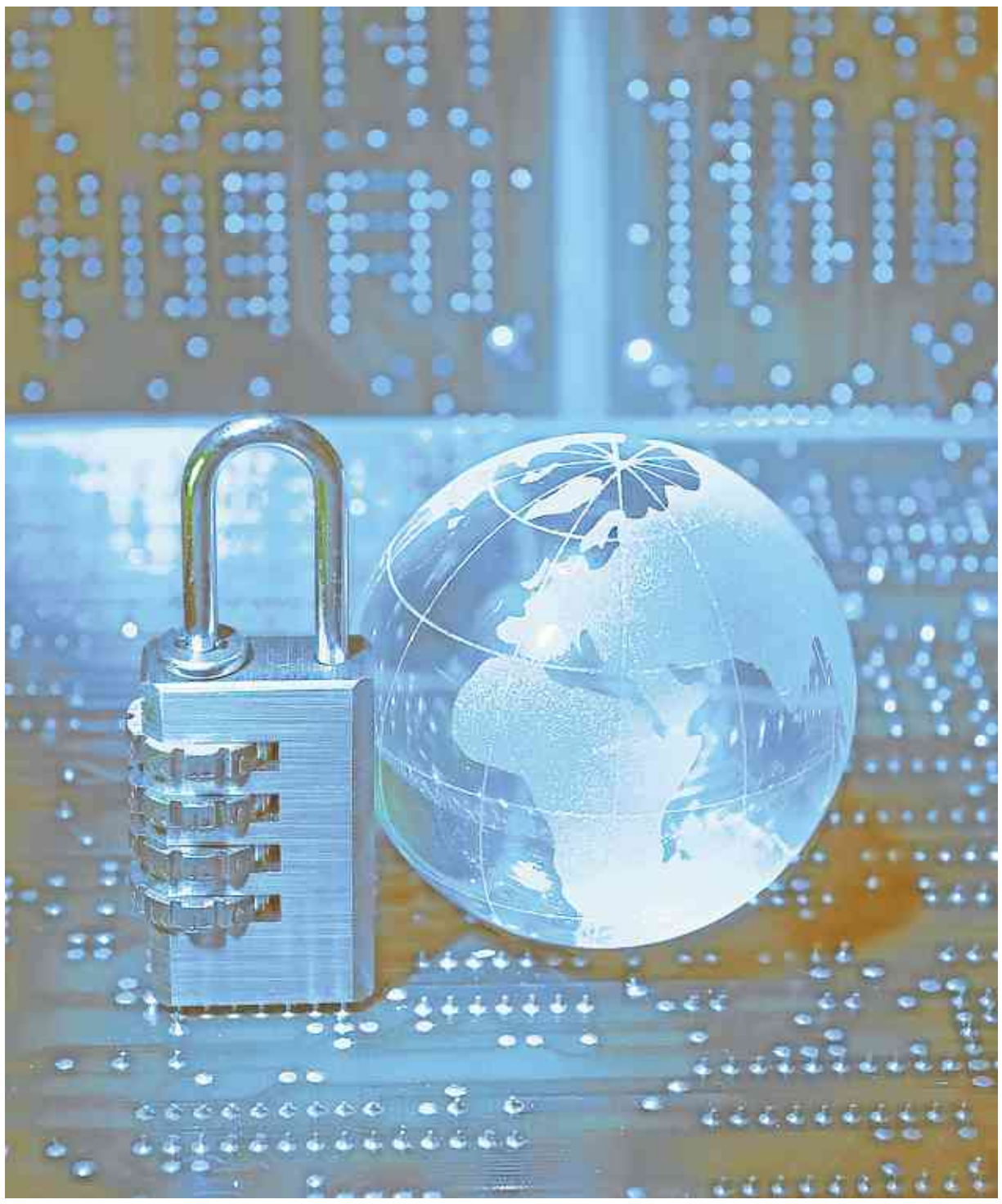
Leben

Heute: Computer & Web

Wie man seine Daten verschlüsselt

Sicherheit Allerdings kein Heilmittel gegen professionelle Spionage – Otto-Normalverbraucher kann leicht Fehler machen

Von unserem Online-Chef Markus Schwarze



Wer das Internet nutzt, macht permanent persönliche Daten bekannt. Beim Surfen im Web, beim Austausch von E-Mails und beim Hochladen von Bildern bekommen regelmäßig Serverdienste und andere diese Informationen mit, die davon normalerweise nichts zu wissen bräuchten: der Proxy-Server des Arbeitgebers beispielsweise, wenn man das in der Firma macht. Oder der durchleitende Server beim Internetprovider. Oder ein Krimineller, wenn er es darauf anlegt.

Mehr und mehr Dienste behelfen sich bei diesem Dilemma durch Verschlüsselung. Passwörter etwa werden bei allen „guten" Diensten stets verschlüsselt abgespeichert, sodass nicht einmal der Administrator das Kennwort des Firmenchefs auslesen kann. Er kann höchstens ein neues Kennwort vergeben. Wenn man sich bei Google einloggt, werden plötzlich alle Google-Suchen verschlüsselt auf die US-Server des Unternehmens übertragen, sodass auf dem Weg dorthin niemand mehr mitlesen kann. Erkennbar wird dies an dem Protokoll https statt http in der Browserzeile. Beim Onlinebanking ist dies schon seit mehr als einem Jahrzehnt üblich.

Dabei ist Verschlüsselung kein Allheilmittel gegen Spionage. Wie es heißt, kann der amerikanische Geheimdienst NSA schwache Verschlüsselung aushebeln. Deswegen hat etwa kürzlich Bruce Schneier, einer der Experten auf dem Gebiet, seine digitalen Schlüssel auf eine besonders lange Länge verdoppelt. Zudem ist Verschlüsselung immer nur so gut wie das schwächste Glied in der Kette. Alles Verschlüsseln nützt nichts, wenn auf dem Rechner eine heimlich installierte Software die Tastatureingaben aufzeichnet.

Zwei Werkzeuge leisten gute Dienste beim Verschlüsseln. Das eine heißt Truecrypt. Die Software legt eine Art verschlüsselten Container auf der Festplatte an und bindet diesen Container dann wie eine eigene Festplatte ein. Um diesen Container zu öffnen, muss man ein Kennwort eingeben. Ohne Kenntnis des Kennworts sind sämtliche darin abgespeicherten Daten verloren. Einen Truecrypt-Container kann man beispielsweise auch in der Dropbox anlegen – und so seine Daten in dem populären Internet-„Cloud"-Dienst speichern, ohne dass jemand anderes darauf Zugriff erlangt. Allerdings geht das zulasten des Komforts.

Das andere passable Werkzeug zum Verschlüsseln heißt Pretty Good Privacy (PGP). Es hilft beim Verschlüsseln von E-Mails. Die Handhabung ist allerdings nicht einfach. Für Windows nützlich ist GPG4Win (www.gpg4win.org/): Es hilft beim Erstellen des benötigten öffentlichen und des privaten Schlüssels. Der öffentliche Schlüssel wird dann allgemein auf einem Schlüsselserver im Web bekannt gemacht. Wenn nun jemand mir als Autor dieses Textes eine Mail schreiben möchte, verschlüsselt er sie mithilfe meines öffentlichen Schlüssels – und nur ich kann diese Mail mit meinem privaten Schlüssel entschlüsseln. Das setzt freilich voraus, dass beide Seiten Verschlüsselung einsetzen. Und dass ich meinen privaten Schlüssel stets geheim lasse.

Das Gefährliche an der Verschlüsselung ist, dass sie von Otto-Normalverbraucher bisher selten eingesetzt wird und daher unerprobt ist. Da kann man leicht Fehler machen. Zudem sind die Werkzeuge dafür noch nicht wirklich einfach zu bedienen und manchmal schlicht falsch programmiert. In einem Festplattenspeicher von QNAP beispielsweise kann man aktuell eine komplette Festplatte verschlüsseln, bei der Festlegung des Kennworts allerdings wird stets das 16. Zeichen zum 15. Wenn man später nicht auf den Programmierfehler kommt (und das vermeintliche Kennwort an der 15. Stelle korrigiert), sind alle Daten unbenutzbar.

Im Zuge der NSA-Affäre sind zudem noch ganz andere Wege bekannt geworden, mit denen sich Daten unbefugt ausspionieren lassen. Die Monitorfrequenz lässt sich aus geringer Entfernung abhören. Bestimmte Verschlüsselungstechniken lassen sich knacken. Und mit Mikrofontechnik lässt sich das gesprochene Wort in einem Raum allein dadurch hörbar machen, dass die Schwingungen etwa auf einer Plastiktasse abgefilmt werden. Es sind unglaublich erscheinende Techniken aus einem James-Bond-Film – und Geheimhaltung wird am Ende stets zu einer Frage des Aufwands.

Lexikon der Begriffe

1 Key: Der Schlüssel in Form einer Datei. Mithilfe eines Keys lassen sich beispielsweise E-Mails verschlüsseln und entschlüsseln.

2 NSA: Der amerikanische Geheimdienst. Er nimmt Zugriff auf Verkehr im Internet, vorrangig auf Aktivitäten von Terroristen. Weil dabei auch Daten von sogenannten normalen Internetnutzern aufgenommen werden, ist der Dienst umstritten.

3 Dropbox: Ein Dienst, bei dem man komfortabel seine persönlichen Dateien kennwortgeschützt im Internet speichern kann. Eigene Dateien lassen sich so bequem zwischen PC, Laptop, Handy und Tablet synchronisieren.

4 „Costa Concordia": Das Kreuzfahrtschiff lief vor vielen Monaten auf Grund und kippte zu 65 Grad um. In einer aufwendigen Aktion wurde es jetzt wieder aufgerichtet – Zentimeter um Zentimeter, das dauerte 19 Stunden. Videos davon sind im beschleunigten Modus sehenswert.

Serie

Schritt für Schritt ins Internet

Unsere Serie für Einsteiger

Teil 10: WLAN
Teil 11: Mit dem iPad ins Netz
Teil 12: Passwörter
Teil 13: Verschlüsselungen

Kolumne

Marcus Schwarze
zu Kameratechniken bei Smartphones und iPad

Die Zeitlupe hat Zukunft

Eine bisher vernachlässigte Funktion beim neuen iPhone ist die Zeitlupe. Diese "Slow mo"-Funktion (langsame Bewegung) zeichnet Videos automatisch im langsamen Modus auf, das heißt: mit 120 Einzelbildern pro Sekunde. Normal bei Videos sind 25 oder 30.

Mit der entsprechend unterlegten Musik entstehen so neue Effekte. Bekanntestes Beispiel ist der Hund, der sich das Wasser aus dem Fell schüttelt nach einem Bad im Meer. Oder der Sportler, der in Zeitlupe auf den Kameramann zuläuft. Die Szene eines flatternden Schmetterlings kann durch die Verlangsamung Qualität bekommen. Freilich entsteht durch diesen „Costa-Concordia"-Modus ein neues Problem: Die eigenen Videoclips anzuschauen, dauert künftig viermal so lange.

Dafür entwickeln sich die Kameras in den neuen Mobilgeräten mehr und mehr zum Ersatz für professionelle Kameras – im Video wie im Standbild. Kürzlich haben wir bei der Rhein-Zeitung allein mit der Kamera eines iPads Videos von Redaktionsbesuchen führender deutscher Politiker gemacht und sogleich mithilfe einer App namens Bambuser live ins Internet übertragen. Die Videos waren kurz darauf nicht mal mehr auf dem Aufnahmegerät, sondern nur noch im Web bei dem Dienst Bambuser. Zum Archivieren mussten wir sie von dort erst wieder herunterladen. Neuestes Redaktionsmitglied im Technikzoo sind zudem zwei Miniobjektive, die sich einfach auf ein iPhone aufstecken lassen. Ein simpler aufgeklebter Ring hält das Objektiv per Magnetkraft an der richtigen Position, und plötzlich hat man so ein vergrößerndes Makro oder ein optisches Zoomobjektiv.

Der nächste Clou digitaler Aufnahmetechnik zeichnet sich bei einem Projekt auf der Internetseite Kickstarter ab: Eine für 2014 geplante Aufsteckvorrichtung aus zwei Objektiven ermöglicht mithilfe des iPads 3-D-Scans der Umgebung. So erhält man die eigene Zimmereinrichtung in drei Dimensionen auf dem Bildschirm. Damit kann man dann bequem das neue Sofa schon mal quasi vorab virtuell einpassen. Vorausgesetzt, man hat genügend Zeit dafür: Die Zeitlupe hat Zukunft.

Die App des Monats

So behält Frau den Zyklus im Blick

Martina Koch
über die weibliche Seite des Smartphones

Die Vermessung des menschlichen Körpers durch Apps hat in den vergangenen Jahren beachtliche Ausmaße angenommen. Per App kontrollieren wir, wie viele Kalorien die Pizza hat, die wir uns in der Mittagspause reinziehen, wie viele Schritte wir beim Weg von der Couch zum Kühlschrank zurücklegen und wie sich unser Blutdruck über die Wochen verändert. Dass da der weibliche Körper nicht lange außen vor bleibt, ist klar! Es gibt eine Vielzahl von Apps, die sich mit dem Hormonzyklus der Frau beschäftigen. Die App „Period Tracker" bietet Android-Nutzerinnen eine optisch ansprechende Möglichkeit, den Überblick über den eigenen Zyklus zu behalten.

So funktioniert es: Der Period Tracker ist in erster Linie ein Kalender, in den Frau zu Beginn mit einem Klick das Startdatum der letzten Periode einträgt. Wird die App drei Monate hintereinander mit Daten gefüttert, beginnt sie selbstständig je nach durchschnittlicher Zykluslänge, den Starttermin der nächsten Periode zu berechnen. Basierend auf den Daten der Nutzerin, zeigt sie außerdem auch gleich den Eisprung und die fruchtbaren Tage an.

Übellaunig, frustriert, gereizt? Einige Frauen fühlen sich in bestimmten Phasen des Zyklus nicht besonders wohl – weil sie körperliche Beschwerden haben oder sich einfach dünnhäutiger fühlen. Daran wird auch der Period Tracker nichts ändern. Dafür bietet er aber hübsche kleine Symbole für alle erdenklichen Stimmungslagen und Beschwerden, die sich antippen und im Profil speichern lassen. Im Verlauf der Wochen und Monate lässt sich dann überprüfen, ob bestimmte Symptome immer wieder auftreten – und vielleicht doch besser mit einem Arzt abgeklärt werden sollten.

Und was bringt das Ganze? Wichtig ist es, vorab erst einmal zu sagen, was das Ganze nicht bringt: Die App ist ausdrücklich nicht zur Vermeidung einer Schwangerschaft geeignet. Wer denkt, Verhütungsmittel in Zukunft nur noch dann nutzen zu müssen, wenn der Period Tracker fruchtbare Tage anzeigt, muss auf Überraschungen gefasst sein. Der Hormonzyklus jeder Nutzerin tickt anders – und unter Umständen nicht synchron mit der App. Seine Stärke hat der Period Tracker als Gedächtnisstütze: Nach einigen Monaten berechnet die App zuverlässig den Starttermin für die nächste Monatsblutung. Für den Besuch beim Frauenarzt lassen sich die Daten zudem an eine E-Mail-Adresse exportieren.

Optik für Mädchen: Der Period Tracker ist sehr übersichtlich und liebevoll gestaltet: Hier flattern Schmetterlinge und Vögel, warme Pastelltöne überwiegen. Das ist überaus nett anzuschauen, aber auch sehr brav und niedlich. Ich würde mir für die nächste Version als Optik irgendwas mit Star Wars wünschen. Oder mit Batman.

Manko: Die ursprüngliche App ist englischsprachig, über die Einstellungen lassen sich andere Sprachen, unter anderem Deutsch, auswählen. Die Übersetzung ist allerdings recht rustikal geraten. Unter dem Symbol, das die fruchtbaren Tage anzeigt, stand in der ersten deutschen Version etwa „Trächtigkeit", was von der Begriffswahl her nicht nur eigen, sondern auch sachlich falsch ist. Wenn irgendwie möglich, ist die englische Standardeinstellung die bessere Wahl.

Preis: Die App gibt es als kostenlose Version mit Werbeeinblendungen im Google Playstore. Wer keine Werbung mag, kann die App für 1,54 Euro käuflich erwerben.

Eine App (Von Application, dem englischen Wort für Anwendung) ist ein Programm für Smartphones oder Tablet-Computer. Die Vielfalt der Programme reicht von kleinen Helferlein bis hin zu Spielen mit Suchtpotenzial. Unsere Redakteure Martina Koch und Andreas Jöckel testen monatlich Apps für iPhone und Android im Wechsel und stellen sie auf dieser Seite vor.

Zweitrechner für Onlinebanking

Schutz Alternativ anderes Betriebssystem einsetzen

Sichere Computer brauchen in der Regel einen Virenscanner und Programme, die immer auf dem neuesten Stand sind. Wer sich beim Onlinebanking und anderen sensiblen Geschäften im Netz besonders absichern will, kann aber auch zu radikaleren Maßnahmen greifen. Erik Tews vom Center for Advanced Security Research (Cased) empfiehlt zum Beispiel, zwei verschiedene Computer einzusetzen: „Einen nehme ich eher für die Abgründe des Internets, einen für sensiblere Sachen." Besonders viel können muss der Zweitrechner dabei nicht – eventuell tut es schon ein alter PC, der ansonsten nutzlos herumsteht.

Noch günstiger ist es, nur einen Rechner zu verwenden und den für Onlinebanking und Co. von USB-Stick oder einer CD mit einem anderen Betriebssystem hochzufahren. Ins Internet kommt der Nutzer so trotzdem, das neue Betriebssystem schirmt sensible Daten aber vom Rest des Rechners und Gefahren aus dem Netz ab. Tews empfiehlt für Boot-Stick und -CD Linux-Distributionen wie Knoppix oder Ubuntu, die es kostenlos im Netz gibt und die sich oft direkt auf einer CD oder einem Stick installieren lassen.

Der Rechnerstart von UBS-Stick oder CD klingt zwar kompliziert, ist aber auch für Laien kein Problem. „Das geht in der Regel automatisch oder mit einer Tastenkombination", erklärt der Experte. „Und im Betriebssystem müssen Sie höchstens noch das WLAN einrichten und für Onlinebanking nur den Browser starten." Läuft der Browser, funktioniert das Surfen mit Linux so wie unter Windows.