Privatsphäre und Datensicherheit

Unsichtbar im Netz

Wer seine Daten nicht preisgeben will, muss sich aktiv schützen – von E-Mail-Kommunikation bis Verschlüsselung. So leicht gelingt das

Kampf gegen Big Brother: Sich im Internet abzusichern zahlt sich aus

Big Brother is watching you." Als George Orwell seinen Roman „1984" nach dem Zweiten Weltkrieg veröffentlichte, schien das alles eine nette Anti-Utopie zu sein. Doch heute ist der bekannteste Spruch aus dem Buch – „Der große Bruder sieht dich" – im Licht der NSA-Spionage-Skandale aktueller als je zuvor. Denn: Egal, was Sie machen, sei es einkaufen, surfen oder E-Mails absenden, überall hinterlassen Sie Spuren und öffnen den Viren, Spionage-Programmen und Cyber-Kriminellen die Hintertür zu Ihrem Rechner und Ihren Daten. Was tun?

Grundlagen der Online-Sicherheit. Als Faustregel gilt: Sicherheits-Updates des Betriebssystems und von installierten Programmen wie Java oder Adobe PDF immer auf dem neuesten Stand halten. Das gilt auch für Browser und deren Plug-ins wie Media Player oder Adobe Flash. Außerdem: „Verschlüsseln Sie Ihre Festplatte: Das ermöglichen die meisten Betriebssysteme über die Einstellungen. Sollte Ihr Rechner verloren gehen oder gestohlen werden, sind Ihre Daten gesichert", empfiehlt Anne Roth, Netz- und Medienaktivistin und Mitarbeiterin der internationalen Nicht-Regierungsorganisation Tactical Technology Collective.

Surfen: nicht ohne Weiteres. Wer surft, muss doppelt aufpassen. So empfehlen Experten, den Rechner nicht direkt über ein Kabel mit dem Internet zu verbinden, sondern lieber über einen Router (also WLAN benutzen). Grund: Der Router arbeitet als eine Art Firewall, er lässt von außen nichts nach innen. Wichtig ist: Wenn Sie WLAN verwenden, sollten Sie in den Einstellungen des Routers die Verschlüsselungsmethode WPA2 mit einem sicheren Passwort und nicht WEP oder WPA auswählen. Damit verringern Sie die Gefahr, dass der Datenverkehr von Dritten ausgelesen wird. Das betrifft allerdings nur das private Netzwerk. Im offenen WLAN wie etwa bei Starbucks muss man schon in Kauf nehmen, dass der Datenverkehr nicht verschlüsselt läuft und jeder mitlesen kann.

Allerdings gibt's auch hier eine Abhilfe: Benutzen Sie beim Surfen das sichere Protokoll HTTPS – das sieht man dann links in der Adressleiste im Browser. In der Regel sind die Verbindungen über dieses Protokoll verschlüsselt. Aber auch hier finden sich Sicherheitsfallen. Denn es kann passieren, dass der Datenverkehr von Kriminellen umgeleitet wird. In diesem Fall bekommt man eine Sicherheitswarnung, dass das Zertifikat ungültig ist. In solchen Fällen – vor allem wenn man den Fehler sonst nie gehabt hat – darf man nie auf „O.k." klicken, sondern muss die Seite sofort verlassen. Falls Sie nicht sicher sind, ob Ihr Datenverkehr gerade gefährdet ist, schauen Sie sich das Schlösschen in der Adressleiste oben links an. Es sollte geschlossen sein – dann sind Ihre Daten bei der Übertragung verschlüsselt.

E-Mails gegen Mitleser und Hacker absichern. Achten Sie auf die eingehenden E-Mails, und geben Sie private Daten nie heraus. Wenn die E-Mails verdächtige Dateien oder Links enthalten, können Sie sie auf der Seite virustotal.com überprüfen. „In der Regel empfiehlt es sich, für E-Mails ein Mail-Programm wie Thunderbird zu benutzen und nicht Webmail", sagt Anne Roth. „Außerdem kann man verschiedene Mail-Adressen für verschiedene Zwecke verwenden." ■ ▷

NATALIA KARBASOVA

INTERVIEW

„Komplettschutz gibt es nicht"

FOCUS-MONEY: Ist es noch möglich, die eigene Privatsphäre im Internet komplett zu schützen?
Josef Reitberger: Komplettschutz gibt es nicht. Wer im Internet einkauft, wer in sozialen Netzwerken unterwegs ist und wer E-Mails schreibt, der kann nachverfolgt werden – selbst wenn die E-Mails verschlüsselt sind, denn der Adressat ist offen lesbar.
MONEY: Woher weiß ich überhaupt, ob ich überwacht werde?
Reitberger: Wenn derjenige, der es macht, keine Fehler begeht, dann kann ich die Überwachung nicht bemerken. Eingeschleuste Trojaner sollten vom installierten Virenscanner erkannt werden. Das Beispiel Stuxnet zeigt aber, dass das nicht immer so sein muss. Das Schadprogramm Stuxnet ist über eine ungepatchte Betriebssystem-Schwachstelle eingeschleust worden, die Anti-Viren-Software konnte ihn nicht sehen.
MONEY: Was ist der erste Schritt zu mehr Datensicherheit?
Reitberger: Die Erkenntnis, dass Daten, die ins Internet gelangen, nicht mehr zurückzuholen sind. Jeder, dem das bewusst ist, wird ein Auge darauf haben, welche Daten er über sich preisgibt. Zum Beispiel wird er dann eine Gratis-Spiele-App, die Zugriff auf die Kontaktliste auf dem Handy haben will, nicht installieren.
MONEY: Was sind die wichtigsten Bereiche, die geschützt werden müssen?
Reitberger: Bank-Zugangsdaten und Zugangsdaten zu den E-Mail-Accounts – dieser Punkt wird gern unterschätzt, aber über E-Mail-Accounts lässt sich sehr viel anderes knacken! Auch Smartphones insgesamt: Sie ermöglichen ein komplettes Positionstracking, weil Kamera und Mikrofon integriert sind und deshalb als Universalwanzen missbraucht werden können.
MONEY: Was machen Sie persönlich für mehr Datensicherheit?
Reitberger: Ich arbeite privat mit Linux, ich lösche nach dem Beenden des Browsers alle Cache-Dateien, den Verlauf, alle Cookies. Ich benutze eine der großen integrierten Security-Suites auf dem Windows-Rechner (Kaspersky Pure 3.0). Für private E-Mails verwende ich PGP-Verschlüsselung, wo es geht, Daten, die ich auf Online-Festplatten ablege, werden zumindest als Zip-Datei mit Passwortschutz verpackt oder in sogenannte Truecrypt-Container verschlüsselt abgelegt.

Josef Reitberger, Chefredakteur des Computermagazins „CHIP"

Foto: 123RF

Foto: CHIP

Datensicherung

Verschlüsseln, speichern, löschen

Dokumente, Excel-Rechnungen, Power-Point-Präsentationen – auf die Sicherheit solcher Daten achten die Nutzer in der Regel zu wenig. Dabei kann jeder ein Dokument mit privaten Daten öffnen. Um das zu vermeiden, verschlüsseln Sie wichtige Dokumente mit dem Programm TrueCrypt. Die Software kann außerdem die Dateien in einem unsichtbaren Container verstecken. Vergessen Sie auch nicht, die Daten, die Sie bei den Cloud-Diensten wie Dropbox ablegen, abzusichern und zu verschlüsseln. Nutzen Sie möglichst europäische Cloud-Anbieter wie Wuala.

Was viele nicht wissen: Gelöschte Daten, auch wenn der Papierkorb entleert wurde, kann man mit ein paar Tricks wieder herstellen. Damit gelöschte Dokumente tatsächlich weg sind, lassen Sie das Programm Eraser laufen. Und wenn Sie eine Datei zufällig – aber nicht mit Eraser – entfernt haben, können Sie diese auch selber wieder herstellen. Das kostenlose Programm Recuva ist dann die erste Wahl.

Ganzheitliche Verschlüsselung

Die Freeware TrueCrypt kann die Festplatte oder einen USB-Stick verschlüsseln. Um Daten zu öffnen, braucht es dann ein Passwort.

Daten sichern mit einem Klick

Mit AxCrypt verschlüsseln Sie Ihre Daten mit dem Rechtsclick. Das ist einfacher als TrueCrypt und passt gut für den Alltag.

Daten ausradieren

Das kostenlose Programm Eraser für Windows löscht sicher Ihre Daten. Alternative: die Löschfunktion bei AxCrypt.

Cloud ohne Reue

BoxCryptor verschlüsselt Ihre Daten für die Cloud und funktioniert auf allen Plattformen. Alternative: Cloudfogger.

Dokumente wiederherstellen

Die Freeware Recuva kann Ihre Dokumente wieder herstellen, falls Ihr Rechner abgestürzt ist oder Dateien zufällig gelöscht wurden.

Kommunikation

E-Mail und Chat: So hört keiner mit

Der erste Schritt zu mehr Sicherheit beim Absenden und Empfangen von E-Mails auch in offenen WLANs: Kreuzen Sie die Option SSL/TLS in den Einstellungen Ihres E-Mail-Programms an, sei es Thunderbird oder Microsoft Outlook. SSL und TLS sind Verschlüsselungsprotokolle, die bei der E-Mail-Kommunikation die gleiche Rolle spielen wie HTTPS beim Surfen. Als Nächstes können Sie das kostenlose E-Mail-Programm Thunderbird von Mozilla mit seiner Erweiterung Enigmail herunterladen. Sie hilft, Nachrichten verschlüsselt zu verschicken.

Wenn Sie Ihre E-Mails von Ihrem GoogleMail-Konto doch im Browser aufrufen müssen, stellen Sie am besten die Anmeldebestätigung in zwei Schritten ein. Jedes Mal, wenn Sie sich von einem unbekannten Rechner einloggen, wird ein zusätzliches Kennwort an Ihr Handy geschickt. Klar, dann hat Google Ihre Handy-Nummer, das ist allerdings sicherer, als wenn Sie Ihr ganzes E-Mail-Konto opfern.

Sicheres E-Mail-Programm

Das E-Mail-Programm Thunderbird mit seiner Erweiterung Enigmail lässt Sie vertrauliche E-Mails verschicken.

E-Mails verschlüsseln

Gpg4win für Windows verschlüsselt Ihre E-Mails und funktioniert mit Outlook und Thunderbird. Alternative für OS X: GPGTools.

E-Mails anonym verschicken

TorBirdy ist eine Erweiterung für den Browser Mozilla Firefox, die Ihnen erlaubt, E-Mails über das Tor-Netzwerk zu verschicken.

Google-Mail-Alternative

Riseup ist ein alternativer E-Mail-Anbieter, der besonderen Wert auf Privatheit und Sicherheit legt.

Jitsi statt Skype

Mit der Open-Source-Software Jitsi führen Sie sichere Videokonferenzen. Für Text-Chats: Pidgin (Windows/Linux) oder Adium (OS X).

Surfen

Spurenlos im Netz unterwegs

Surfen kann heikel werden, wenn jeder Schritt im Netz von Dritten mitverfolgt werden kann. Um anonym zu surfen, nutzen Sie die kostenlose Software Tor. So funktioniert es: Bevor Sie sich mit einer Internet-Seite verbinden, wird die Anfrage durch das Tor-Netzwerk geschleust und kommt dann von dem zufällig ausgewälten Server an. So kann Sie keiner zurückverfolgen. Auch wichtig: Beim Einloggen auf unterschiedlichen Seiten immer unterschiedliche Passwörter benutzen. Ein Passwort sollte mindestens aus acht Zeichen – Buchstaben, Zahlen und Sonderzeichen – bestehen. Vergessen Sie Kombinationen wie „qwertz" oder „12345", die werden in ein paar Sekunden geknackt. Am besten setzen Sie einen Passwort-Manager ein, der sich Ihre Passwörter für unterschiedliche Seiten merkt und selbst nur ein Kennwort braucht, dafür aber ein langes und sicheres. Überprüfen Sie die Sicherheit Ihres Passworts auf der Seite www.howsecureismypassword.net.

Anonym surfen

Die Freeware Tor versteckt Ihre IP-Adresse. Dritte wissen dann nicht, wo Sie sich gerade befinden. Alternative: JonDonym.

Passwort-Manager einsetzen

Benutzen Sie den Passwort-Manager KeyPass, um Kennwörter sicher zu verwalten. Als Alternative: LastPass.

Aktive Inhalte blockieren

Die Firefox-Erweiterung No Script unterbindet fremde Inhalte und schützt den Browser vor Infektionen.

Surfspuren und Verlauf löschen

CCleaner löscht unter anderem den Browserverlauf und Cookies – Textdateien, die Daten über besuchte Web-Seiten speichern.

Schluss mit Datensammlern

Die Browser-Erweiterung DoNotTrackMe blockiert personalisierte Werbung und lässt das Setzen der Cookies nicht zu.

Mobil

Tablets und Smartphones sichern

Mobile Geräte haben oft ernsthafte Sicherheitslücken. Die Entwicklung der Schadprogramme für mobile Geräte nimmt zu, die Virenscanner sind allerdings noch nicht ganz ausgereift. So schneidet die Sicherheitsapp Lookout in einem Test am besten ab – allerdings hat auch sie 20 Prozent der Schadprogramme nicht erkannt. Das heißt: Auch wenn Sie einen Virenscanner installiert haben, bedeutet das noch längst keine hundertprozentige Sicherheit. Daher: Nicht jede App installieren und immer schauen, ob die App und die Quelle vertrauenswürdig sind ! Dabei sollten Sie darauf achten, welche Berechtigungen die App braucht. Manche Apps, die alle Daten auslesen können, braucht man ja erst gar nicht.

Wie auch für Rechner gilt für Smartphones und Tablets: Immer Updates installieren und Daten-Back-ups erstellen. Um den Zugang zu Ihrem Gerät zu erschweren, benutzen Sie den Sperrcode.

Sicherer Virenscanner

Die App „Lookout Security & Antivirus" ist gut, gibt aber wie jede andere Sicherheitsapp keine hundertprozentige Garantie.

What'sApp-Ersatz

Die iOS- und Android-Chat-App „Threema" verschlüsselt die Daten. Ihr Gesprächspartner muss sie auch installieren.

Anonym mobil surfen

Um auf Ihrem Android-Gerät sicher zu surfen, installieren Sie den Browser Orweb. Alternative für iOS: Onion Browser.

Installierte Apps kontrollieren

Mit der kostenlosen App „Guard" haben Sie die Kontrolle über die Berechtigungen Ihrer installierten Apps.

Verschlüsselt chatten

Die kostenlose App „Gibberbot" verschlüsselt die Nachrichten auf Ihrem Android-Gerät. Alternative für iOS: „ChatSecure".