DE =	EN =	PT =	VN =
Sicherheit 1/3			

Überwachung, Spionage, Datenklau? Verbraucher können sich dagegen wehren. Manchmal mit ganz einfachen Mitteln.

Unter Beobachtung. Auch im Netz sind virtuelle Spähposten installiert.

Die Amerikaner tun es, die Briten angeblich auch. Die Geheimdienste haben Interesse an unseren Daten und versuchen, möglichst viel über uns herauszufinden. Der deutschen Wirtschaft macht das inzwischen mächtig Angst. Jedes dritte Unternehmen will jetzt die Sicherheit seiner Computer, Netze, Diensthandys und Rechner überprüfen, hat das Beratungsunternehmen PwC herausgefunden. Doch was ist mit den Privatleuten? Wie kann man sich dagegen wehren, von Geheimdiensten oder auch nur von simplen Betrügern ausspioniert zu werden, die ganz schnöde an unser Geld wollen? Die Antwort ist manchmal einfacher als man denkt.

GOOGLE

Das Problem: Was weiß eigentlich die vermeintliche Datenkrake Google von mir? Wer als Besitzer eines Android-Smartphones oder aus anderen Gründen ein Google-Konto hat, kann zumindest mit einem Blick erfahren, welche Google-Dienste Daten speichern. Dieser Überblick heißt bei Google Dashboard. Um dahin zu gelangen, reicht es aus, diese beiden Worte in die Google-Suche einzugeben. Die Liste der möglichen Dienste ist lang. Dazu gehören unter anderem: Google-Konto, Android, Chrome-Synchronisierung, Cloud-Drucker, Gmail, Google-Alerts, Aufgabenplaner, Docs, Wallet, Google+, Kalender, Kontakte, News, Picasa, Play Store, Standortverlauf, Sync, Webprotokoll, Youtube. Kurzum: Aktive Google-Kontoinhaber hinterlassen eine sehr breite Datenspur. Der gläserne Netzbürger hat bei Google eine feste Adresse.

Die Lösung: Wie kann man sich davor schützen? Indem man sich zum Beispiel nach Nutzung von Google+ vom Netzwerk abmeldet, bevor eine Suche bei Google gestartet wird. Indem man sich als Android-Nutzer in möglichst wenige W-Lans automatisch einloggen lässt. Und indem man nicht jede Route mit Google Maps berechnen lässt, sondern statt dessen lieber eine Straßenkarte aufschlägt. Doch so weit geht die Angst vor den Datenkraken bei vielen Menschen nicht. „Leider haben sich die Absätze der Falk-Stadtpläne durch die Ausspähaffäre nicht erhöht“, sagt Brigitte Kehl vom Mairdumont-Verlag, der die Stadtpläne herausgibt. Mit 700 000 bis 800 000 verkauften Exemplaren pro Jahr ist man in dem Verlag aber dennoch ganz zufrieden. Topseller ist übrigens der Falk Stadtplan „Berlin“. In der Nähe der Berliner US-Botschaft und der britischen Vertretung ist es auch vielleicht ganz ratsam, sein Smartphone auszulassen und lieber mit dem Papierplan durch die Stadt zu gehen.

gezeichnet:	hpw	Datum:		eduction project	Sicherheit	translate/en_ds/p_ct/vn_ro	orign: http://www.tagesspiegel.de/wirtsc
Aenderung:	an	Datum:	24.07.2015	WIAP KFKOK	Safety	r1	datei_Wi_8_f_57_c2_r1_Sicherheit_02_d
Aenderung:	control 2	Data:		Safenwil Schweiz	spear 2	www.wiap.ch	idee of / from HPW

DE =	EN =	PT =	VN =
Sicherheit 2/3			

MAILS

Das Problem: Wer eine E-Mail verschickt, muss sich bewusst sein, dass es in etwa so ist, als würde er eine Postkarte versenden. Ab dem Zeitpunkt, wo sie im Briefkasten gelandet ist, ist sie für jeden einzusehen. Denn die meisten Anbieter von E-Mail-Konten verschlüsseln die elektronischen Nachrichten nicht oder nur rudimentär. Wer beispielsweise sein E-Mail-Konto bei einem US-Anbieter hat, muss damit rechnen, dass die Mail von Berlin nach München einen Umweg über die Server in den USA nimmt – und dort von den Geheimdiensten gescannt wird. Gleiches gilt natürlich, wenn unverschlüsselte Mails von einem deutschen Anbieter an eine Adresse in den USA gehen.

Die Lösung: Es gibt durchaus Möglichkeiten, die elektronische Post vor dem Zugriff Unbefugter zu schützen – praktisch mit einer Art versiegeltem Briefumschlag. Die Verschlüsselungstechnologie PGP zum Beispiel ist beinah so alt wie das Internet selbst. Sie gewährleistet, dass lediglich der Empfänger den Inhalt lesen kann. Allerdings ist die Installation nicht ganz einfach. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt auf seiner Internetseite beispielsweise Gpg4win. Hinter dem kryptischen Namen verbirgt sich ein Programmpaket zur sicheren E-Mail- und Datei-Verschlüsselung für das Betriebssystem Windows von Microsoft. Es ist kompatibel mit den Versionen XP, Vista, Windows 7 und 8. Laut den Sicherheitsexperten ist Gpg4win benutzerfreundlich. Auch ein Handbuch sei enthalten. Wer auf Nummer sicher gehen will, sollte vertrauliche Unterlagen ohnehin nicht auf elektronischem Weg verschicken, sondern dem leicht angejahrten Werbespruch der guten alten Bundespost folgen: Schreib' mal wieder. Beim Einschreiben kann man jedenfalls sicher sein, dass die Sachen ankommen – ungelesen und beim richtigen Empfänger.

BANKING

Das Problem: Daten sind wertvoll, Geld aber noch mehr. Kein Wunder, dass Hacker seit jeher versuchen, die Konten der Bankkunden leer zu räumen. Geheimnummern werden ausgespäht, Kreditkartennummern kopiert. „Es ist ein Wettlauf mit den Kriminellen", sagt Kerstin Altendorf vom Bankenverband.

Die Lösung: In diesem Wettlauf setzen die Banken auf immer verfeinertere Techniken. Die M-Tan etwa, die aufs Handy geschickt wird und als Eintrittskarte fürs nächste E-Banking genutzt wird. Oder die Chip-Tan, bei der man die Transaktionsnummer mit einem speziellen Gerät, dem Tan-Generator, aus einem QR-Code herausliest. Eine Verschlüsselung, die fast schon agentenreif ist. Genauso wie die HBCI-Technik, bei der man seine Chipkarte in einen Kartenleser, die Pin eingibt und dann erst seine Transaktionsnummer bekommt.
Wie kann es passieren, dass dennoch Langfinger aufs Konto zugreifen? Glaubt man den Banken, haben in den meisten Fällen die Kunden eine Mitschuld, weil sie ihre Computer nicht ausreichend schützen oder sich die M-Tan auf dasselbe Handy schicken lassen, mit dem sie dann auch die Bankgeschäfte ausführen. Oder sie machen ihre Überweisungen gleich von der Arbeit aus – ohne den nötigen Datenschutz. Dafür spricht, dass die Banken die meisten E-Bankinggeschäfte morgens vor neun, in der Mittagspause und kurz vor 18 Uhr registrieren. An HBCI oder sonstiges ist im Büro natürlich nicht zu denken.

gezeichnet:	hpw	Datum:		eduction project	Sicherheit	translate/en_ds/p_ct/vn_ro	orign: http://www.tagesspiegel.de/wirtsc
Aenderung:	an	Datum:	24.07.2015	WIAP KFKOK	Safety	r1	datei_Wi_8_f_57_c2_r1_Sicherheit_02_d
Aenderung:	control 2	Data:		Safenwil Schweiz	spear 2	www.wiap.ch	idee of / from HPW

DE =	EN =	PT =	VN =
Sicherheit 3/3			

Die Lösung: Wer seine Bankgeschäfte online erledigen will, muss seinen Computer mit Firewalls sichern und auch beim Versenden der Transaktionsnummern auf ein sicheres Verfahren achten. Man kann sich aber natürlich auch in der Bankfiliale an den Automaten stellen und seine Überweisungsdaten in den Automaten tippen. Dann ist man garantiert vor dem Ausspähen geschützt, zumindest vor dem elektronischen. Allerdings wird das Ganze ab dem nächsten Jahr noch mühseliger als heute. Im Zuge der Sepa-Einführung muss man ab Februar nächsten Jahres bei Überweisungen immer die 22-stellige Nummer eintippen. Und: Man muss aufpassen, dass Diebe nicht mit Kameras oder Attrappenapparaturen die Geheimnummer ausspähen. Ganz ohne ist das also auch nicht.

KARTEN

Das Problem: Nur Bares ist Wahres, hieß es in der Zeit vor dem Plastikgeld. Heute zahlen viele Kunden selbst Kleinbeträge mit EC- oder Kreditkarte. Und hinterlassen dabei Daten. Beim Zahlen mit Kreditkarte geht der Datenstrom vom Händler über die Händlerbank zum Kartenunternehmen, dann weiter an die kartenausgebende Bank – und zurück. Allerdings hat das Kreditkartenunternehmen nur die Kartennummer, nicht den Namen des Karteninhabers. Wer sich dahinter verbirgt, weiß nur die Bank, von der der Kunde die Kreditkarte bekommen hat und von der er auch die Monatsabrechnung erhält. Bei dubiosen Zahlungsaufforderungen nimmt das Kreditinstitut Rücksprache mit dem Kunden, notfalls kann man aber auch später noch seine Abrechnung anfechten.

Die Lösung: Wer möglichen Abrechnungsproblemen und Betrügereien aus dem Weg gehen und keine Datenspuren hinterlassen will, hat aber auch eine Option: Er kann eine Prepaid-Kreditkarte kaufen und mit dieser bis zu einem bestimmten Betrag anonym bezahlen.

APPS

Das Problem: Smartphones gehören inzwischen zum Standard und auch Tablet-Computer sind mittlerweile alles andere als eine Randerscheinung. Wir schätzen die Vorzüge der digitalen Helfer. Egal, ob Fahrpläne, Spiele oder Chats – über die Programme auf den Geräten können wir von überall aufs Internet zugreifen und kommunizieren. Doch was die Applikationen (Apps) währenddessen im Hintergrund treiben, bleibt dem Nutzer in der Regel verborgen. Kostenlose Apps finanzieren sich normalerweise über Werbung. Insofern sind Anbieter an möglichst vielen Daten der Nutzer interessiert, die sie gegebenenfalls an andere Unternehmen weitergeben können. So kommt es vor, dass Spiele-Apps den Standort übermitteln oder Wetterdienste auf die Kontakte des Nutzers zugreifen wollen.

Die Lösung: Wer Apps nur von großen Plattformen wie dem Google Play Store oder dem App-Store von Apple bezieht, kann davon ausgehen, dass sie dort zumindest rudimentär überprüft wurden. Experten empfehlen zudem, die Allgemeinen Geschäftsbedingungen des App-Anbieters vor dem Herunterladen zu lesen. Sowohl Apples iOS-Betriebssystem als auch Googles Android registriert, welche App sich welche Zugriffe etwa zum Adressbuch verschafft. In der Systemsteuerung können Nutzer diese Berechtigungen einsehen – und die App entfernen, wenn sie ihnen zu neugierig erscheint.