Wissen Sie, was Ihr Computer anstellt?

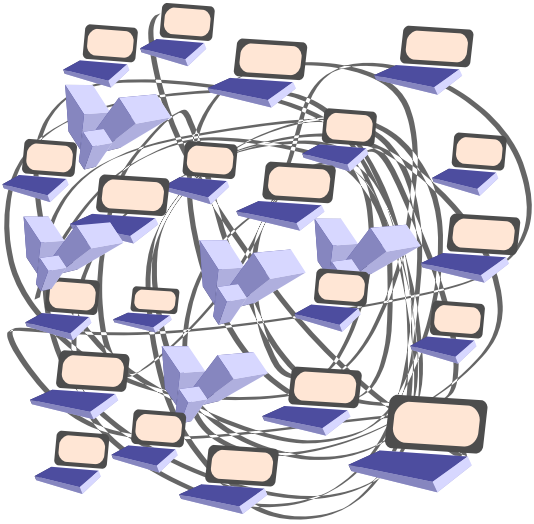
"Natürlich", werden Sie sagen. "Meine Textverarbeitung schreibt Texte, mein Mailprogramm verschickt Mails, und mein Musikprogramm lädt bei meinem Lieblingshändler Musik herunter, die ich mir immer wieder anhören kann." Natürlich, das sind die Funktionen, von denen Sie wissen, aber ist das wirklich alles?

Seit Jahren ist unbekannt, welche Daten Windows bei der Registrierung an Microsoft schickt. Viele Programme besitzen Spionagefunktionen, die Ihre Verhaltensdaten sammeln, und vor wenigen Monaten löschte Amazon bereits gekaufte und bezahlte Bücher von den Kindle-E-Book-Lesegeräten, weil es zum Streit mit der Verwertungsgesellschaft gekommen war.

Transparenz: Mehr als eine blinkende Werbeeinblendung!

Wenn Sie sicher sein wollen, dass Ihre Daten wirklich nicht in falsche Hände geraten, brauchen Sie vertrauenswürdige Software. Quelloffene Software, so genannte "Open Source", liegt grundsätzlich im Quelltext vor. Gerade bei größeren freien Projekten gibt es einige hundert Menschen weltweit, die mit der unabhängigen Qualitätskontrolle befasst sind.
Offensichtliche Schadfunktionen gelangen so erst garnicht an die Verbraucher.

Sie sind Teil eines Netzwerks



Wenn Sie eine Information anfordern, melden Sie sich aktiv (und in der Regel mit Ihrer realen Identität) und bitten um Darstellung beispielsweise einer gewünschten Webseite. Dabei durchqueren Ihre Anfragen Router, eine Art Knotenpunkte. Das heißt, dass Sie nicht etwa von Ihrem Rechner auf direktem Wege beim Internetdienst anfragen, sondern viele, viele andere auf Ihrem Weg dorthin mitlesen können, was genau Sie gerade anfordern.

Weil Ihre Privatsphäre kostbar ist

Mit einem freien und offenen Betriebssystem, etwa einer Linux-Distribution, können Sie sicher gehen, dass Ihr PC nicht heimlich "nachhause" telefoniert. Weitere Schutzmaßnahmen sind angemessene Verschlüsselungsprogramme, die dafür sorgen, dass ausschließlich Sie und die gewünschte Empfängerin oder Empfänger die Nachricht erhalten. Die unten erwähnten Programme sind "Open Source" und **kostenlos** erhältlich. Sie helfen Ihnen dabei, Ihre Privatsphäre im Internet zu wahren.

* Das weltweite **Tor-Anonymisierungsnetz** wird von tausenden Freiwilligen unterstützt, die das Programm weiterentwicklen, verständliche Dokumentation schreiben oder schlicht einen Knotenrechner betreiben.

* Ihre Festplatten und USB-Sticks können Sie mit dem quelloffenen **Truecrypt** verschlüsseln, das neben den üblichen Funktionen die Verschlüsselung mit einem zweiten Passwort anbietet, das man notfalls preisgeben kann, bei dessen Verwendung der Rechner aber nur "harmlose Daten" speichert.

* Effektiven Rundum-Schutz bieten auch die Linux-Betriebssysteme, die als **Live-CD** ohne Installation vom Laufwerk aus verwendbar sind und keine Änderungen an Ihrem System durchführen. Praktisch: Sie arbeiten sicher und anonym und probieren ohne ungewünschte Folgen ein neues (freies) Betriebssystem aus (z.b. mit **Polippix** oder der **Privacy-CD**)

Ihr Interesse ist geweckt?!

Besuchen Sie uns auf unserem Treffen:
jeden 3. Samstag im Monat, 18 Uhr im Klein-Bon(n)um
(Paulstraße 5, 53111 Bonn)

E-Mail: bonn@vorratsdatenspeicherung.de
Web: http://bonn.vorratsdatenspeicherung.de

Der Arbeitskreis Vorratsdatenspeicherung (AK Vorrat) in Bonn ist eine an Datenschutz interessierte Gruppe, die sich gegen Überwachung im Allgemeinen und im Besonderen gegen die Vorratsdatenspeicherung einsetzt. Einige von uns beschäftigen sich begesitert mit Open Source.

V.i.S.d.P.: S. Kasem, J.R. Selzer c/o AK Vorrat Bonn, Wolfstraße 10, 53111 Bonn