2007/38 Lifestyle

https://jungle.world/artikel/2007/38/zwiebel-routen

Zwiebel-Routen

Von **Burkhard Schröder**

Wer will, kann völlig anonym im Internet surfen, keine verwertbaren Spuren hinterlassen und anonym oder unknackbar verschlüsselte E-Mails schreiben. Warum das kaum jemand macht? Das Problem dabei ist die Faulheit der User. von burkhard schröder

Die Allmachtsfantasie des total gläsernen Bürgers ist sicher keine Erfindung von Innenminister Wolfgang Schäuble. Trotzdem sah es in den vergangenen Wochen so aus, als hätte man zum ersten Mal von Online-Durchsuchung, Ausspionieren von E-Mails oder Internet-Überwachung gehört. Bei der zuweilen hysterischen Debatte, die von diesen Vorschlägen ausgelöst wurde, scheint etwas vergessen zu werden: Das alles ist mit einfachen Mitteln zu verhindern.

Wer völlig anonym surfen will, muss sich um zwei Sachen kümmern. Zum einen um die Voreinstellungen des Browsers, also der Software, mit der man sich im Word Wide Web bewegt – und manchmal auf technischen Umwegen in anderen Diensten des Internet wie im Usenet. Zum anderen kann und sollte man seine eigene Identität – die unverwechselbare Rechneradresse, die man von seinem Provider jeweils zugewiesen bekommt (Internet-Protocol-Adresse) – verbergen, zum Beispiel um der geplanten Vorratsdatenspeicherung auszuweichen. Allerdings muss man eine halbe Stunde kostbarer Lebenszeit dafür verschwenden, bis man das Prinzip verstanden hat.

Wer mehr Zeit hat, kann sich auf der dem Bundesinnenministerium zugeordneten Website des Bundesamts für Sicherheit in der Informationstechnik, über alle Gefahren aufklären lassen, von einfachen Themen, etwa wie mit »aktiven Inhalten« umzugehen ist – zum Beispiel mit Cookies und Javascript –, bis zu komplizierten Dingen wie HTML-Wanzen, DNS-Spoofing oder einer »Overlapping Fragment Attack«. Dabei gilt eine einfache Regel: Kein aktiver Inhalt sollte auf den eigenen Rechner gelangen, weder Cookies noch Javascript. Noch vor wenigen Jahren war das unbequem. Viele Websites wurden dann nicht mehr korrekt angezeigt, Webdesigner brachen in Tränen aus, weil ihre bunten Einfälle per Javascript nicht mehr gebührend bewundert wurden, EDV-Veranwortliche weigerten sich, aus ihrer Kemenate zu kommen, weil die Aufgabe, technische Vorgänge auch dem dümmsten anzunehmenden User erklären zu müssen, Arbeit machte und sie ihres Herrschaftswissens beraubt hätte.

Heute geht alles viel einfacher und per Mausklick (alle Details unter: **www.awxcnx.de/handbuch.htm**). Für den Browser Firefox gibt es zum Beispiel die beiden Zusatzprogramme CookieSafe und CookieCuller. Benutzer können damit auf bestimmten

Websites die winzigen Spione flexibel erlauben oder verbieten, ohne dass man dazu umständlich in den Voreinstellungen suchen müsste.

Google hat kürzlich seine Cookie-Politik geändert und damit auf die Kritik von Datenschützern reagiert. Künftig wird Google das Nutzerverhalten mit Hilfe von Cookies nicht mehr 30 Jahren speichern wie bisher, sondern nur noch zwei – immerhin ein Fortschritt! Wer Google gebraucht und sich Cookies auf den Rechner schicken lässt, sollte konsequenterweise auch eine Webcam im Schlafzimmer installieren. Da gilt auch für die, die aus unerfindlichen Gründen meinen, Google Mail benutzen zu müssen. Wer gerne passende Werbung zum Inhalt seiner unverschlüsselten Mails eingeblendet bekommen möchte, ist dort gut aufgehoben, sollte aber niemals mehr gegen den Überwachungsstaat demonstrieren.

Eine den Cookie-Blockern vergleichbare Zusatzsoftware existiert auch für das hochgefährliche Javascript. Das PlugIn Noscript (noscript.net) schaltet die Scriptsprache bei Mozilla Firefox bei Bedarf ab. Wer andere Browser benutzt, etwa Safari für Macintosh oder Linux-Browser wie Galeon, verändert schlicht die Optionen zugunsten der Privatsphäre. Der Internet Explorer aus dem Hause Microsoft sollte nur für die sein, die perforierte Präservative benutzen – niemand wird jedoch dazu gezwungen.

Manche Betreiber von Suchmaschinen wie ask.com werben damit, dass sie das Verhalten der Surfer nicht ausspionieren wollen. Das ist Werbung und Augenwischerei. Selbst wenn die Behauptung stimmt, was niemand nachprüfen kann, sollte nicht irgendeine Firma für die Sicherheit beim Surfen veranwortlich sein, sondern die Nutzer selbst. Wer mit seinem Rechner bewusst und vernünftig umgeht, muss nicht das Schloss vor die Tür nageln, sondern setzt sich mit der Software so auseinander wie mit einem Auto, für das man immerhin einen Führerschein machen muss: Man muss nicht den Motor auseinanderbauen, aber das Lenkrad vom Ersatzreifen unterscheiden können.

Die virtuelle Tarnkappe beim Surfen ist etwas komplizierter, aber nicht nur etwas für Technik-Freaks. Vor einigen Jahren förderte das Bundeswirtschaftsministerium den Java Anon Proxy (anon.inf.tu-dresden.de/index_en.html), eine kostenlose Software für alle Betriebssysteme, welche die IP-Adressen verschleiert. Das Programm wird heute noch angeboten, in einer kostenlosen Version, die halbwegs Anonymität garantieren kann, und in einer Bezahlversion, die den Datenstrom über so viele Rechner leitet, dass dieser selbst von allen Schäubles dieser Welt und ihren Helfershelfern nicht mehr dem Urheber zugeordnet werden kann. Das Prinzip ist schlicht, die Software selbst für Windows-Laien einfach zu installieren. Sie funktioniert wie ein so genannter Proxy, eine Art virtueller Zwischenrechner, der mit Hilfe einer Kaskade angeschlossener Rechner die IP-Adresse schreddert. Steht nur einer der beteiligten Computer im Ausland, würde es den Strafverfolgungsbehörden nichts nützen, wenn sie alle deutschen Rechner beschlagnahmen und forensisch analysieren – es käme nur Datenschrott heraus.

Nach einem ähnlichen System arbeitet die Anonymisierungstechnik Tor (The Onion Routing). Das hört sich geheimnisvoller an, als es ist. Wer die Standard-Software dazu benutzt – einen Tor-Server beziehungsweise das Tor-Netzwerk –, bekommt von der anspruchsvollen Technik gar nichts zu sehen. Das »Zwiebel-Routen« verhindert, dass der Betreiber einer Website erkennen kann, wer sich gerade auf seiner Seite befindet. Während die Rechner beim Java Anon Proxy jeweils wie Kaffeemühlen mit den eingespeisten Daten umgehen, sie aber am Ausgang wieder zusammensetzen, ohne dass der Weg der Puzzleteilchen zurückverfolgt werden könnte, arbeiten

Tor-Server mit der Methode, dass innerhalb des Netzes der angeschlossenen Computer die IP-Adressen immer wieder ausgetauscht werden. Der einzelne Rechner gibt »nach außen« seine Individualität auf, versteckt sich hinter einer großen Masse und setzt sich immer wieder eine andere Maske auf.

Auch hier ist der Browser Mozilla Firefox klar im Vorteil: Das Plugin Torbutton schaltet per Mausklick die Anonymität auch beim Betriebssystem Windows ein und aus. Beim Macintosh-Rechner leisten Vidalia und Privoxy mit einer verständlichen grafischen Oberfläche ähnliche Dienste. Bei Linux werden Tor und vergleichbare Programme gleich mitgeliefert. Es geht sogar noch einfacher: Der PrivacyDongle des »Vereins zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V.« zum Beispiel ist ein kleiner USB-Stick, der die Software TorPark enthält. Damit ist die anonyme Kommunikation im World Wide Web sofort möglich, ohne vorher irgendetwas installieren zu müssen. Der PrivacyDongle wird über eine freie USB-Schnittstelle mit dem Rechner verbunden; wenn man auf das Programm-Icon klickt, wird ein Firefox-Browser gestartet, der sich sofort mit dem Tor-Netzwerk verbindet.

Wer gern paranoid ist, kann natürlich immer noch eins draufsetzen – etwa mit der kostenlosen Software anon-web-vm für die virtuelle Maschine des VMware Players – oder sich gar am I2P (Invisible Internet Project) beteiligen. Diese oder ähnliche schon existierenden Projekte der Open Source Community sind der digitale Alptraum aller Zensoren und anderer Internet-Kontrolleure, jedoch für den normalen Nutzer meistens technisch zu aufwändig und zu anspruchsvoll. Wer sich damit beschäftigt, kann vollkommen anonym surfen, jedwede Überwachung und Speicherung der Daten läuft ins Leere.

Natürlich gibt es zu jeder der Anonymisierungstechniken eine oder mehrere Verschwörungstheorien, warum sie dennoch alles belauschen können; das gilt auch für die Verschlüsselungssoftware Pretty Good Privacy, die E-Mails für Spione unlesbar macht. Fragt man nach den technischen Details, entpuppen sich diese Theorien ausnahmslos als unausgegorenes Halbwissen und weitgehend faktenfrei.