TECHNIK

Surfen mit der **Zwiebeltaktik**

Wie man heimliche Verfolger im Internet mit einfachen Mitteln ausbremsen kann – Eine Übersicht

VON STEFFEN HAUBNER

Es scheint dieser Tage kaum ein anderes Thema zu geben: Wie können wir Internet- und Mobiltelefonnutzer uns wirksam vor den Spionage-Attacken des US-Auslandsgeheimdienstes NSA schützen. Ohne auf den Komfort zu verzichten, an den wir uns mittlerweile so sehr gewöhnt haben? Verunsichert werden die Anwender auch durch Meldungen, dass die NSA angeblich in der Lage ist, jede Verschlüsselung zu knacken. Tatsächlich gibt es Experten zufolge keinen Schutz, den Spione nicht irgendwann überwinden können. So gelingt es den NSA-Spitzeln immer wieder, Sicherheitslücken auszunutzen, um sich Zugang zu Rechnern zu verschaffen. Doch das belegt nur, wie wichtig grundlegende Sicherheitsmaßnahmen sind. Denn: Auch wenn ein hundertprozentiger Schutz nicht möglich ist, so sollte man den Datendieben ihr illegales Handwerk doch so beschwerlich wie möglich machen. Mit den richtigen Software-Tools ist das gar nicht so schwer.

Das „Tor"-Projekt

Wer im Internet nicht auf Schritt und Tritt verfolgt werden und zudem anonym bleiben will, sollte sich einmal das „Tor"-Projekt ansehen. Die Abkürzung steht für „The Onion Router". Der Name leitet sich vom englischen Wort für „Zwiebel" ab. Jede Anfrage, die man ins Internet schickt, wird dabei über mehrere Rechner innerhalb eines Netzwerks weitergeleitet und immer wieder ver- und entschlüsselt. Am Ende ihres Weges kann die Information zwar gelesen, aber nicht mehr auf einen Nutzer zurückgeführt werden. Dieses System erinnert an die Schalen einer Zwiebel, was den etwas eigenwilligen Namen erklärt. Auch wenn es kompliziert klingt: Die Anwendung ist recht einfach. Laden Sie von der Webseite

» **https://www.torproject.org/**

das „Tor Browser Bundle" herunter. Mit dem Pfeilmenü unterhalb des Download-Buttons können Sie Ihre bevorzugte Sprache wählen. Die Software ist für Windows, Mac OSX, Linux und Android verfügbar.

Nach dem Herunterladen entpacken Sie das Programm mit einem Doppelklick in ein Verzeichnis auf Ihrer Festplatte oder einen USB-Stick. Nach einem weiteren Doppelklick auf „Start Tor Browser.exe" öffnet sich das Kontroll-Panel „Vidalia" und versucht automatisch, eine Verbindung herzustellen. Bei Erfolg öffnet sich eine spezielle Firefox-Version, die nicht zu verwechseln ist mit dem Firefox-Browser, der wahrscheinlich bereits auf Ihrem PC installiert ist. Ist das so weit geschafft, können Sie sofort anonym surfen.

Leider hat das Ganze mehrere Haken. So können Sie sich keine Online-Videos mehr anschauen. Um beispielsweise in den Genuss eines Youtube-Clips zu kommen, müssen Sie Ihren normalen Browser starten und sind dann natürlich nicht mehr anonym. Zudem ist die Surfgeschwindigkeit merklich verlangsamt, der Umweg über das Zwiebel-Netzwerk fordert hier seinen Tribut.

Im Alltag bietet sich „Tor" deshalb vor allem an, wenn Sie im Internet Informationen suchen, die niemanden etwas angehen. Um wirklich anonym zu bleiben, müssen Sie zudem einige Verhaltensregeln beachten:

1 Sie sind nur geschützt, wenn Sie den „Tor"-Browser benutzen und dessen Voreinstellungen beibehalten.

2 Installieren Sie keine Erweiterungen wie Flash, RealPlayer oder Quicktime.

3 „Tor" benutzt die Applikation „HTTPS Everywhere", um Ihre Anonymität auch auf der Zielseite zu wahren. Das funktioniert aber nur auf Seiten, die verschlüsselte Verbindungen ermöglichen, also Seiten, die mit „https://" beginnen.

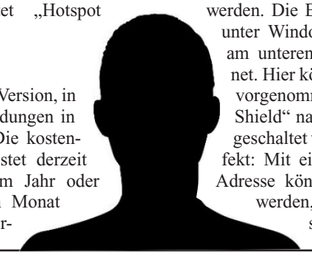
4 Ihre Anonymität ist nicht mehr gewährleistet, wenn Sie sich bei Diensten wie Mail-Provider, Bank oder Facebook anmelden, externe Dokumente öffnen oder Filesharing-Netzwerke benutzen.

5 Hundertprozentige Anonymität kann auch „Tor" nicht garantieren. Aber je mehr Nutzer das System regelmäßig einsetzen, desto besser funktioniert es.

BILDER: FOTOLIA/JAMESCHIPPER

Virtual Private Networks

Virtuelle private Netzwerke sind eine Alternative, wenn man sich mit den „Tor"-Einschränkungen (siehe Kasten links) nicht abfinden möchte. Doch auch sie haben einen Nachteil: Nach Meinung von Experten sind die NSA-Spione in der Lage, VPN-Verbindungen zu knacken. Außerdem setzt die Verwendung ein gewisses Vertrauen in den Anbieter voraus. Die VPN-Technik ist aber beispielsweise dann nützlich, wenn man in einem öffentlichen Netzwerk surft. Passwörter und sensible Daten bleiben dann in einer Art Tunnel verborgen, die sogenannte IP-Adresse, mit der der Nutzer identifizierbar ist, wird durch eine ausländische Kennzahl ersetzt. Damit werden auch Datensammler ausgebremst, die den Weg des Nutzers durch das Netz nachverfolgen und diese Informationen an Dritte weitergeben, also auch an die NSA. Die Spione müssen sich also selber bemühen, an die Daten zu kommen. Eine solche Lösung bietet „Hotspot Shield".



Unter der Adresse

» **www.hsselite.com**

gibt es eine kostenlose Version, in der man Werbeeinblendungen in Kauf nehmen muss. Die kostenpflichtige Variante kostet derzeit rund 30 US-Dollar im Jahr oder knapp drei Dollar im Monat und wartet mit erweiterten Funktionen und höherer Surfgeschwindigkeit auf. Die Software ist für Windows, Mac, iOS und Android erhältlich. Nach Download und Installation kann „Hotspot Shield" auf die deutsche Version umgestellt werden. Die Benutzeroberfläche wird unter Windows über die Taskleiste am unteren Bildschirmrand geöffnet. Hier können alle Einstellungen vorgenommen und „Hotspot Shield" nach Bedarf ein- und ausgeschaltet werden. Netter Nebeneffekt: Mit einer amerikanischen IP-Adresse können Inhalte aufgerufen werden, die für deutsche Nutzer sonst gesperrt sind.

Alternative Suchmaschinen

Womit verdienen Google und Facebook ihr Geld? Durch die Monetarisierung von Nutzerdaten! Mittlerweile gilt es als so gut wie erwiesen, dass diese Firmen Millionen Dollar für ihre Kooperation mit der NSA kassiert haben. Umso erstaunlicher, dass Google als Suchanbieter noch immer beinahe eine Monopolstellung innehat.

Gibt es keine Alternativen? Doch, die gibt es! Der deutsche „Suma EV – Verein für freien Wissenszugang" unterhält die Metasuchmaschinen „MetaGer.de" und „MetaGer2.de", die konsequent auf Datenspeicherung verzichten. Um ihren Nutzern relevante Resultate anbieten zu können, werden dabei viele kleine Informationsquellen gebündelt. Per Voreinstellung entscheiden die Nutzer selbst, welche davon in die Ergebnisse einfließen sollen und welche nicht. Mit individueller Konfiguration, einem eigenen Ranking-Verfahren und einer Unterteilung der Suchergebnisse in Kategorien wird den Nutzern eine sehr brauchbare Alternative zu Google geboten.

Ganz ähnlich arbeitet auch die Suchmaschine „DuckDuckGo", die 2008 von dem MIT-Wissenschaftler Gabriel Weinberg gegründet wurde. Der Schutz der Privatsphäre ihrer Nutzer hat für die Betreiber nach eigenem Bekunden oberste Priorität. Konkret bedeutet das: Es werden keine Daten gespeichert oder Profile angelegt. Kein Wunder also, dass die Suchanfragen in direkter Folge des NSA-Skandals auf mehr als zwei Millionen pro Tag emporschnellten. Darüber sollte man allerdings nicht vergessen, dass „DuckDuckGo" wie alle US-Unternehmen der Auskunftspflicht gegenüber den Behörden unterliegt. Außerdem benutzt die Suchmaschine Server des Amazon-Konzerns, der angeblich ebenfalls mit der US-Administration kooperiert.

Gleichwohl ist es unstrittig, dass mehr Vielfalt bei den Suchanbietern dem Datenschutz und der Meinungsvielfalt im Internet förderlich ist. Klicken Sie auf der „DuckDuckGo"-Seite unten rechts auf „More" und „Settings", um Einstellungen vorzunehmen und die Suchmaschine bei Bedarf auf die deutsche Sprachversion umzustellen.

» **http://metager.de/**
» **https://metager.de/neu/**
» **https://duckduckgo.com**

Browser-Erweiterungen

Sie können auch den von Ihnen präferierten Browser mit diversen Erweiterungen gegen Angriffe wappnen. Die äußerst nützliche Seite

» **http://fixtracking.com/**

ist ein weiteres Projekt der „DuckDuckGo"-Betreiber und unbedingt einen Besuch wert. Leider steht die Seite überwiegend nur in englischer Sprache zur Verfügung. Wählen Sie über die Pfeiltasten im Banner unter dem Enten-Logo den Browser aus, den Sie benutzen. Passend dazu werden Ihnen dann Einstellungen und Erweiterungen für Ihren Browser empfohlen. Dazu gehört etwa „DoNotTrackMe" – ein Add-on, das verhindert, dass man Ihren Weg durch das Netz nachverfolgt.

„HTTPS Everywhere", das auch Teil des „Tor"-Pakets ist, sucht automatisch nach jenen Versionen von Webseiten, bei denen Daten verschlüsselt übertragen werden. Auch die „DuckDuckGo"-Suchmaschine lässt sich als Plug-in direkt in den Browser einbinden.

Auf diese Weise surfen Sie künftig nie mehr ungeschützt. Die Belohnung für den Aufwand: Das gute Gefühl, dass Sie der NSA Ihre Daten nicht auf dem Silbertablett präsentieren.