



Spurlos surfen

Technisch lassen sich die meisten Datenspuren verwischen. Nur wenige Anwender dürften die umständlichen Schutzmaßnahmen jedoch anwenden.

■ Es gibt eine Reihe von Möglichkeiten und Tools, um sich effektiv gegen Datenspionage und Web-Zensur zu schützen. Wichtig ist zunächst die Frage: Wovon genau braucht man den Schutz? Denn Daten können an zwei Stellen ausgeforscht werden: Entweder indem der Internet-Verkehr belauscht wird oder durch den direkten Zugriff auf den Rechner. In diesem Artikel widmen wir uns vor allem der ersten Art des Lauschangriffs, da diese sich besonders gut für eine „virtuelle Rasterfahndung“ ausnutzen lässt.

Erste Schritte. Ein Abhören des Internet-Verkehrs zu verhindern, ist insofern nicht trivial, als die Daten den Rechner ja nicht versehentlich verlassen. Wer im Internet surft, kommt nicht umhin, sich bei seinem Provider einzuloggen, URLs anzufordern oder seine E-Mails abzurufen. Alle diese Daten lassen sich bequem mitprotokollieren. Da sich die Übermittlung nicht vermeiden lässt, kann die Privatsphäre nur hergestellt werden, wenn die Daten für Fremde möglichst unbrauchbar sind.

Kann der Nutzer seine E-Mails noch in Eigenregie mit Tools wie PGP oder GnuPG verschlüsseln, so wird dies schon schwieriger, wenn es ums Surfen geht. Der Nutzer hinterlässt hierbei gleich drei Datenspuren: Zunächst wird beim Internet-Provider festgehalten, wann der eigene Rechner mit welcher IP-Adresse ans Netz geht. Zudem werden die URLs per GET-Anweisung verschickt, die angewählte Adresse also im Klartext übermittelt. Auch die Antwort (die HTML-Seite) wird in der Regel im Klartext zurückgeliefert, solange keine SSL-Übertragung erfolgt. Angewählte und erhaltene Internet-Inhalte sind daher jederzeit nachvollziehbar. Als dritte Datenspur werden dem angewählten Server, ebenfalls im Klartext, Daten über die eigene Client-Konfiguration übermittelt. Darunter sind:

- die im Browser eingestellte E-Mail-Adresse,
- die Betriebssystem-Version,
- die genaue Version des Webbrowsers,

- IP-Adresse oder Host-Name des Rechners,
- eventuell zuvor gesetzte Cookies,
- die zuvor besuchte URL (Referrer).

Partner gesucht. Um alle diese Datenspuren zu verwischen, bedarf es der Hilfe Dritter. Einigermassen bequem geht das mit so genannten anonymen Proxys. Bei einem Proxy handelt es sich um einen Server, der zwischen dem Client- und dem Zielrechner steht. Der Client übermittelt seine Daten (z.B. eine URL-Anforderung) an den Proxy-Rechner. Dieser reicht die Anfrage an den Zielrechner weiter, der die Antwort über den Proxy an den Client zurückleitet. In der Folge „sieht“ der Zielrechner lediglich den Proxy und erfährt nichts über den Client. Am einfachsten lässt sich ein anonymer Proxy mit einem Web-Interface nutzen, beispielsweise der kostenlose @nonymouse (<http://nonymouse.com>). Bequemer geht es, wenn der Proxy in den Browser-Einstellungen abgespeichert wird. Eine Software, die diese Schritte abnimmt, zugleich eine ganze Reihe anonymer Proxys mitbringt und diese auf Status und Geschwindigkeit überprüft, heißt Anonymity 4 Proxy (www.inetprivacy.com/a4proxy) und ist als Demo kostenlos, als Vollversion für 35 US-Dollar erhältlich.

Unsichtbar. Mit diesen Schritten ist die Privatsphäre allerdings lediglich zu einem Teil hergestellt. Zwar ist das dezentrale Sammeln von Daten durch Web-Server weitgehend unterbunden. Zentrale Abhörmaßnahmen, etwa durch staatliche Stellen, greifen aber weiterhin. Da die URL-Anfragen im Klartext übertragen werden, lassen sich die Zugriffe an zentralen Stellen nach wie vor protokollieren. Als Lösung bietet es sich an, auch diese Daten unbrauchbar zu machen, sprich: zu verschlüsseln. Zu diesem Zweck wurde der Dienst Rewebber (www.rewebber.de) ins Leben gerufen, der ursprünglich von der Fernuniversität Hagen entwickelt wurde, inzwischen aber von der ISL Internet Sicherheitslösungen GmbH, Hagen, betrieben wird. Leider verlangt ISL für den ursprünglich kostenlosen Service inzwischen eine Abonnement-Gebühr. Mit Preisen ab 20,88 Euro für eine dreimonatige Nutzung des Advanced-Services ist der Dienst zudem alles andere als günstig.

Dafür wird eine zuverlässige Verschlüsselung der angewählten URLs garantiert. Die Verschleierung wird mittels asymmetrischer Verschlüsselung (Public-Key) erreicht. Die resultierende „URL“ gibt keinen Aufschluss über die ursprüngliche URL. Sie besteht aus der Adresse des Rewebber-Servers, einem Präfix und der chiffrierten URL. Durch diesen Vorgang entsteht eine anonymisierte Angabe nach dem Muster: www.rewebber.de/surf_encrypted/MTCTFC3oiN... Da auch das zurückgelieferte Dokument verschlüsselt wird, lassen sich kaum Spuren verwerten.

Neue Ansätze. Mit diesem Verfahren ist bereits viel gewonnen. Die protokollierbaren Daten sind beinahe wertlos, auch gängige Zensurmaßnahmen werden problemlos ausgehebelt, da diese in der Regel mit Sperrlisten bestimmter Wörter und/oder Domains arbeiten. Allerdings gibt es zwei Lücken: Zum einen muss der Rewebber zuverlässig außer Reichweite desjenigen sein, der die Rechner belauschen will. In einem totalitären System

URLs

Anonym bleiben
Anonymer Proxy (Web-Interface)
■ <http://nonymouse.com>

Anonymity 4 Proxy
■ www.inetprivacy.com/a4proxy/

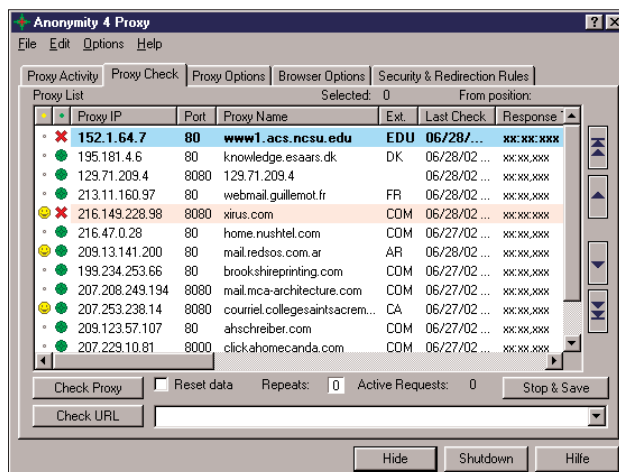
Anonymer Proxy (verschlüsselt)
■ www.rewebber.de

Projekt Peekabooty
■ www.peek-a-booty.org

Projekt Free Bird
■ www.photono-software.de


muss er also außerhalb des Landes stehen. Zum anderen muss der Rewebber erreichbar bleiben. Das ist nicht ganz einfach: Schließlich lässt sich eine Internet-Adresse, so sie einmal bekannt ist, in zentralistischen Strukturen leicht sperren.

Mit „Peekabooby“ und „Free Bird“ wurden jüngst zwei Programme ins Beta-Stadium entlassen, die auch diese vorerst letzten Lücken stopfen wollen. Beide Projekte setzen auf ein ähnliches Konzept: Anstatt einen zentralen Proxy wie Rewebber zu nutzen, sollen diese Aufgabe weltweit verteilte Rechner übernehmen. Wer die Programme auf seinem Rechner startet, verbindet seinen Rechner mit einem eigens zu diesem Zweck eingerichteten Peer-to-Peer-Netz. Jeder Computer in diesem Netz fungiert fortan als Teil des weltweiten Proxy-Server-Netztes. Sobald ein Nutzer eine URL nachfragt, reicht das System die Anfrage an die anderen an-



Das Programm „Anonymity 4 Proxy“ bringt reichlich Adressen von vertrauenswürdigen Proxy-Servern mit

geschlossenen Computer weiter. Nutzer in Ländern mit liberaler Gesetzgebung helfen auf diese Weise Anwendern in totalitären Systemen. Die Kommunikation ist bei beiden Projekten ebenfalls verschlüsselt, so dass eine staatliche Firewall keine Möglichkeit hat, die Daten zu prüfen. Durch den Ad-hoc-Character des Netzes ist es auch kaum möglich, einzelne IP-Nummern zu sperren.

Ausblick. Der Ausflug in die Technik zeigt zweierlei: Zum einen ist eine weitgehend anonyme Kommunikation im Internet möglich. Zum anderen ist Anonymität ein durchaus schützenswertes Gut. Nur auf diese Weise ist es möglich, Zensurmaßnahmen schon im Ansatz zu verhindern. Es bleibt jedoch zu vermuten, dass auch die hier gezeigten Ansätze ein bekanntes Schicksal erleiden werden: hoch gelobt, aber in der Praxis kaum genutzt.  Dominik Grollmann