SPIEGEL ONLINE - 16. November 2001, 12:55
URL: http://www.spiegel.de/netzwelt/technologie/0,1518,167924,00.html

Safer Surfing

www.Ich_Bleibe_Anonym.de

Von Niels Gründel

Wer surft, hinterlässt unfreiwillig Spuren. Immer mehr persönliche Daten werden erfasst, der Schutz davor wird immer schwieriger. Doch noch ist es möglich, sich weitgehend anonym durch das Netz zu bewegen.


DPA
Trend: Das Sammeln persönlicher Daten

Seit dem 11. September tobt die Debatte um die Frage, ob man Datenschutzrechte nicht zu Gunsten der Sicherheit einschränken müsste. Polizeibehörden und Geheimdienste wünschen sich natürlich einen Freibrief zum Schnüffeln. Doch im Grunde ist die Diskussion fast hinfällig: Nicht nur viele Staaten, auch zahlreiche Unternehmen beanspruchen einfach dieses Recht zu schnüffeln und fragen nicht nach Gesetzen.

Mit zunehmender Verbreitung des Internet und der Telekommunikation hat sich auch das Netz um die Privatsphäre enger gezogen. Längst ist der gläserne Surfer eine Realität, und zahlreiche Überwachungssysteme bedrohen unbescholtene Bürger und Unternehmen. Das Beispiel Echelon zeigt, dass selbst befreundete Staaten nicht davor zurückschrecken, deutsche Unternehmen systematisch auszuforschen: Selbst Geheimdienste treiben heute Industriespionage, nicht zuletzt mit Hilfe des Webs.

Betroffen von legalen wie illegalen Schnüffelaktionen sind in aller Regel die Unbescholtenen. Wer wirklich etwas zu verbergen hat, greift auf die Verschlüsselung von E-Mails und für Telefonate auf abhörsichere Leitungen zurück. Für die Übermittlung von geheimen Daten ist ganz besonders die Methode der Steganografie geeignet. Dabei werden Nachrichten in Bildern versteckt und verschlüsselt. Dagegen nämlich gibt es keine erfolgreiche Überwachungs- und Entschlüsselungstechnik.

Surfen, aber anonym

Wo aber liegen nun die Risiken für den privaten Surfer, und was kann er unternehmen?

Wer über eine Standleitung für seinen Internetzugang verfügt, besitzt eine eindeutige IP-Adresse, die sich dauerhaft leicht zurückverfolgen lässt. Wer sich aber über einen der großen Provider wie T-Online, AOL oder gar per Call-by-Call ins Internet einwählt, erhält bei jedem Einwählvorgang für die Dauer der Sitzung eine andere IP-Adresse. Eine Zuordnung zum Surfer ist daher nur während der bestehenden Internetverbindung möglich, ansonsten nur für den Provider. Doch egal welchen Weg man im Internet einschlägt, die benutzten Pfade werden von den Seitenbetreibern unabhängig vom eingesetzten Webserver gnadenlos mitgeloggt.

Schließlich möchten sie alles über ihre Nutzer wissen: Von welchen Seiten kommen die Nutzer, wie lange bleiben sie, mit welchen Browserversionen betrachten sie die eigenen Seiten und welche Seiten rufen sie auf? Wer genau wissen möchte, welche Informationen er über sich preisgibt, sollte einmal bei der Verbraucherorganisation privacy.net vorbeischauen. Dort werden auf Mausklick alle persönlichen Daten präsentiert, die sich aus den übergebenen Browserinformationen online zusammenstellen lassen.

Wer nach solcher Erkenntnis doch lieber unerkannt bleiben möchte, kann sich mit einem so

genannten
Anonymizer auf seinem Weg durch das Web tarnen. Diese Hilfsseiten im Netz (wie zum Beispiel www.anonymizer.com, www.allgemeiner-datenschutz.de) wählt man direkt nach der Einwahl bei seinem Provider an und gibt hier seine eigentliche Zieladresse an.

rtl
Web-Alptraum im Film: Per Elektronik ausspioniert, entrechtet, kriminalisiert ("Das Netz" (1995) mit Sandra Bullock)

Anonymizer sorgen dafür, dass die persönlichen Daten vollständig gefiltert werden. Die Seitenbetreiber angewählter Internetseiten können so zwar noch die einzelnen Seitenaufrufe auf ihren Servern nachvollziehen, nicht aber die mit dem Browser übermittelten Daten. Stattdessen erhalten sie von den Anonymizern nur falsche oder sogar unsinnige Informationen. Für den Dauerbetrieb bietet Anonymizer.com eine kleine Ergänzung für die Toolbar des Internet Explorers.

Noch komfortabler ist ein Tool wie der Stealther, der auf dem eigenen PC installiert wird und die Funktionalität der Anonymizer-Webseiten übernimmt, also die Tarnung im Netz. Die Vollversion von Stealther kostet 79 Mark. Aber die Sicherheit der Zivilgesellschaft hat eben ihren Preis - wie ja auch unsere Politiker nicht müde werden zu betonen.


SPIEGEL ONLINE
Kabel/Server: Wer liest mit?

Doch auch auf dem eigenen Rechner bleiben oft zahlreiche Surfspuren im weltweiten Web: temporäre Internetdateien, die History, Favoriten und unbemerkt angelegte Cookies.

Theoretisch lassen sich alle diese Spuren nach jedem Besuch des Internet von Hand löschen. Leichter geht es mit Überwachungshilfen der meisten Personal Firewalls oder mit speziellen Säuberungstools wie etwa dem Washer (für Windows oder Mac). Cookies können inzwischen in allen Browsern der neueren Generation recht gut kontrolliert werden.

Auch E-Mails lassen sich anonym versenden

Ähnliche Anonymität lässt sich auch beim Versenden von E-Mails erreichen. Im Internet bietet diese Möglichkeit zum Beispiel die Seite Allgemeiner Datenschutz (www.allgemeiner-datenschutz.de). Für den Dauergebrauch wesentlich bequemer sind allerdings Tools wie Ghost Mail oder Potato. Auch hier bleibt die eigentlich Mailadresse sicher verborgen. Allerdings kann dabei jede beliebige Absenderadresse gewählt werden, ohne dass der Empfänger es merken kann. Insofern besteht hier natürlich auch die Gefahr eines Missbrauchs - und entsprechend ist der Ruf solcher Dienste. In bester Gesellschaft befindet man sich dort nicht unbedingt.

Wer mit Spuren im Netz leben kann, sollte zumindest eigene E-Mails verschlüsseln

Wem zwar die Spuren beim Versenden von E-Mails egal sind, nicht aber die Gefahr, dass Fremde den Inhalt der Nachricht mitlesen, sollte seine E-Mails unbedingt verschlüsseln. Online geht das beim Web-Mailprovider web.de, allerdings mit einer nur recht schwachen Verschlüsselung und der unverschlüsselten Übertragung zwischen dem eigenen Rechner und web.de. Als sehr sicheres Angebot gilt PrivacyX, wenngleich E-Mails manchmal etwas länger für den Weg zum Empfänger benötigen.

Wer einen E-Mail-Client auf seinem Rechner nutzt, kann zur Verschlüsselung das sehr beliebte PGP - Pretty Good Privacy integrieren. Plug-ins sind für die meisten E-Mail-Clients verfügbar, die maximale Verschlüsselungsstärke ist extrem hoch. Sie liegt bei 2048 Bit. Für Privatanwender ist der Einsatz kostenlos möglich. Ebenfalls kostenlos, aber (noch) nicht ganz so verbreitet ist der GNU Privacy Guard.

In den USA hat längst die Debatte darüber begonnen, ob Privatpersonen eine

Verschlüsselung von E-Mails verboten werden sollte. Sollten sich die USA für ein Verbot entscheiden, besteht die Gefahr, dass dies Beispielcharakter haben könnte. Weltweit ist der Trend festzustellen, E-Mail-Kommunikation analog zur Telefon-Kommunikation zu betrachten. Die vor kurzem vom Kabinett abgenickte Telekommunikations-Überwachungs-Verordnung TKÜV zeigt, wohin die Reise geht: Richtung Überwachungs-Freibrief für Behörden und eingeschränkte Schutzrechte für Verbraucher.

Weitere Informationen rund um den Datenschutz und das anonyme Surfen bietet das "Virtuelle Datenschutzbüro".

Zum Thema:

Zum Thema im Internet:

- Anomynizer.com
  http://www.anonymizer.com
- Stealther
  http://stealther.com
- Washer
  http://www.webroot.com/washer.htm
- Potato
  http://www.theinternet.cc/potatoware/pot
- GhostMail
  http://www.er.uqam.ca/merlin/fg591543/gm
- moderner-datenschutz.de
  http://www.moderner-datenschutz.de
- Datenschutz.de
  http://www.datenschutz.de
- "Allgemeiner Datenschutz"
  http://www.allgemeiner-datenschutz.de
- PrivacyX
  http://www.privacyx.com
- PricacyNet
  http://www.privacy.net
- Pretty Good Privacy
  http://www.pgpi.org
- Platform for Privacy
  http://www.w3.org/p3p
- Electronic Privacy Information Center
  http://www.epic.org/
- Die Überwachunsstudie der Privacy Foundation
  http://www.privacyfoundation.org/workplace/technology/extent.asp
- Open-Source-Verschlüsselungssoftware GnuPG
  http://www.gnupg.org
- US-Bericht zur Anonymität im Internet
  http://www.usdoj.gov/criminal/cybercrime/unlawful.htm