



Wer sich im Internet inkognito bewegen will, muss ausgeklügelten DATEN-SELBSTSCHUTZ betreiben



Anonym im Netz

VON NIELS BOEING

Im Internet weiß keiner, dass du ein Hund bist.“ Kein Bild hat den Mythos des Internets als anonymen Datenraum besser getroffen als Peter Steiners berühmte Karikatur im US-Magazin „The New Yorker“ vom Juli 1993. Zwei Hunde sitzen da vor dem Rechner und chatten. Längst aber gibt es eine aktualisierte Version. „Hallo Hundes-User 39 (Promenadenmischung, hauptsächlich Labrador, mag Peperoni)... Profil wird aktualisiert“ steht da auf dem Bildschirm, auf den die Hunde starren.

Das ist nicht übertrieben. Im Jahre 2000 sind viele User ein offenes Buch für geschickt programmierte Websites: IP-Adresse des eigenen PCs während der Online-Session; E-Mail-Adresse; Domain-Name des Servers, über den man ins Netz geht; Adresse der zuvor besuchten Website; Inhalte versteckter interaktiver Dateien – all das ist leicht von außen abrufbar. Ganz ohne Hacken, nur mit ein paar Programmzeilen im Code einer Seite.

Grund zur Verzweiflung ist dies nicht. Je nachdem, wie anonym und abgeschottet ein User surfen möchte, hat er gewisse Schutzmöglichkeiten. Die einfachste, wenn auch schwächste, ist die Anpassung des Browsers. Noch vertraut ein Großteil der User den laxen Voreinstellungen bei der Installation – wenn sie überhaupt wissen, dass sie eine Wahl haben im Umgang mit potenziellen Web-Schnüfflern.

Das sind in erster Linie aktive Inhalte und Cookies. Aktive Inhalte sind kleine Zusatzprogramme, die, in den Programmiersprachen Java oder Javascript erstellt oder auf Microsofts Active-X-Technologie aufbauend, Websites interaktiver machen – und durchaus mehr, als Usern lieb sein kann. Im Prinzip können mit ihrer Hilfe diverse Daten auf dem eigenen Rechner ausgespäht und übers Netz an ihren Schöpfer gesendet werden.

Sie lassen sich aber ganz einfach deaktivieren: im Internet Explorer (IE) 5.0/5.5 den Menüpunkt „Extras/Internet-Optionen/Sicherheit“ aufrufen, im neuen Fenster den Button „Stufe anpassen“ anklicken und dann die Deaktivierung von ActiveX und Java auswählen; im Netscape Navigator 4.x unter „Bearbeiten/Voreinstellungen/Erweitert“. Allerdings muss man dann in Kauf nehmen, dass manche Websites nicht mehr funktionieren.

Obwohl Cookies seit längerem durch die Medien geistern und ein Liebling aller Netz-Pessimisten sind, fällt vielen Usern noch immer nichts dazu ein: Nach einer Umfrage des Pew Internet & American Life Pro-

ject wussten 56 Prozent der US-User im August 2000 nicht, was ein Cookie ist, und nur 10 Prozent hatten sie im Browser deaktiviert.

Ruft man etwa einen Online-Shop oder eine Portalseite auf, werden diese kleinen Dateien vom Web-Server auf dem eigenen Rechner abgelegt. Sie speichern, welche Produkte man angeklickt oder wie man die Portal-seite nach persönlichen Vorlieben umgestaltet – „personalisiert“ – hat. Diese Informationen bleiben so für spätere Seitenabfragen erhalten.

Damit umgehen Website-Betreiber das Problem, dass Privatnutzer nicht anhand der IP-Adresse ihres Rechners identifizierbar sind. Denn diese wird ihnen bei jeder Online-Session vom Provider neu zugewiesen. Cookies dagegen enthalten eine Identifikationsnummer, die den Rechner permanent erkennbar macht, sowie weitere, oft nicht nachvollziehbare Informationen.

Was drin steht, lässt sich überprüfen: Gibt man `JavaScript:alert(document.cookie)` ins Adressfeld des Brow-

sers ein, öffnet sich gegebenenfalls ein kleines Fenster mit dem Dateinhalt. Beispiel bei Amazon.de: „ubid-acbde=227-5473590-2348542; x-acbde=oyd43Yvx91ECnm VGV6TahS1PJm0Qi3pT...“ In der Regel wird sich dahinter nichts Illegales verbergen.

Wer dem dennoch misstraut, kann Cookies blockieren, und zwar wieder über die Browser-Voreinstellungen: im IE 5.0/5.5 unter „Extras/Internetoptionen/Sicherheit“ in der Einstellung „hoch“ oder über den Button

„Stufe anpassen“ im daraufhin erscheinenden Fenster; im Netscape Navigator 4.x unter „Bearbeiten/Voreinstellungen/Erweitert“.

Das kann dazu führen, dass auch harmlose Sites nicht mehr einwandfrei funktionieren. Deshalb sperrt man besser ganz gezielt Cookies von Servern aus, deren Datenschutzverhalten unklar ist. Wer mit älteren Browsern arbeitet, kann dies mit Blockier-Programmen wie „Cookie Cleaner“ oder „Cookie Cutter“ oder umfassenderer Schutz-Software wie Norton Internet Security tun. Hier setzt man die Domain-Namen etwa von dubiosen Werbebanner-Diensten auf den Index. Wer mit den neuen Browsern IE 5.5, iCab (www.icab.de) oder Netscape 6.0 arbeitet, kann das dort im eingebauten Cookie-Manager tun.

Die Identifizierbarkeit des Users beim Surfen anhand seiner vorübergehenden IP-Adresse ist damit jedoch noch nicht ausgeschaltet. Wer unerkannt bei einer Website reinschauen möchte, kann ihre Adresse auf der Seite www.anonymizer.com eingeben. Diese leitet den Surfer dann unerkannt weiter.

Das sind nur Teillösungen. Ganz nervöse Zeitgenossen sollten deshalb zu einer echten Netz-Tarnkappe greifen: der Software „Freedom“ der kanadischen Firma Zeroknowledge.com. Mit ihrer Hilfe lassen sich Schein-Identitäten aufbauen, so genannte Nym (kurz für Synonym, siehe Kasten), die die eigene Online-Herkunft verschleiern.

Freedom baut auf einem Netzwerk von derzeit 81 Freedom-Servern, davon 19 in Europa, auf. Jede Mail und jeder Website-Aufruf, die der Freedom-Nutzer abschickt, wird über bis zu drei Server weitergeleitet, dazwischen ver- und entschlüsselt, und gelangt erst dann zum Zielrechner. Der erkennt als Absender immer nur einen anonymisierten Nutzer `nym@freedom.net`. Gerade so, als ob dieser maskiert aus einem dichten Cyber-Nebel auftaucht und sich dorthin wieder zurückzieht. Und sämtliche Cookies, die von Websites platziert werden, landen in einer virtuellen „Keksdose“ innerhalb der Software Freedom, die einen Zugriff auf vertrauliche Daten unterbindet.

Allerdings hat auch diese Lösung zwei Schönheitsfehler. Je mehr Freedom-Server dazwischengeschaltet werden, desto langsamer wird die Übertragung auf Grund der dazwischenliegenden Verschlüsselungsschritte. Und: Der Freedom-Nutzer ist auf die Redlichkeit der Firma Zeroknowledge angewiesen – ganz ohne Vertrauen geht es nicht.

SERVICE

Testen Sie die Browser-Einstellungen und den SICHERHEITZUSTAND IHRES NETZ-ZUGANGS:
▶ beim NIEDERSÄCHSISCHEN DATENSCHUTZBEAUFTRAGTEN:
www.lfd.niedersachsen.de/service/service_selbst.html
▶ im BROWSER-CHECK des Computermagazins „c't“:
www.heise.de/ct/browsercheck

INTERNET-TARNKAPPEN:
▶ Unerkannt Websites aufrufen kann man:
online über WWW.ANONYMIZER.COM oder vom eigenen PC mit der Software **JAVA ANON PROXY JAP** (kostenlos herunterladbar unter jap.inf.tu-dresden.de)

▶ Völlige Anonymität beim Surfen und Mailen bietet **FREEDOM** (siehe Text). Die Software selbst gibt es kostenlos unter www.freedom.net. Drei Testgutscheine für je eine 30-Tage-Tarnidentität gibt es kostenlos, danach kosten fünf Gutscheine für ein Jahr 50 Dollar (56 €)

WEITERE INFOS:
im VIRTUELLEN DATENSCHUTZBÜRO der Landesdatenschutzbeauftragten, www.datenschutz.de

DIE WOCHE BRINGT ES AUF DEN PUNKT.

DAS GESCHENK-ABO

KEIN BLATT FÜR DEN DURCHSCHNITT – 52 X INTELLIGENT LESEN

Verschenken Sie einfach DIE WOCHE zu Weihnachten.
Und ein ganzes Jahr lang kommt Lesen ins Haus.

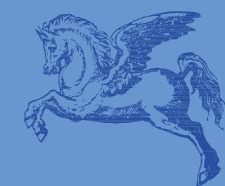
SIE SPAREN 10 %

Für nur DM 3,50 (1,79) pro Ausgabe statt DM 3,90 (1,99) im Einzelverkauf kommt DIE WOCHE direkt zu Ihnen ins Haus.

IHR GESCHENK!

Bis zum 20. 12. anrufen oder E-Mails, und das Original kommt pünktlich zum Fest! Oder „last minute“ einfach anrufen, DIE WOCHE bestellen, Gutschein ausschneiden, unterschreiben und gerollt an den Weihnachtsbaum hängen. Intelligente Weihnachten!

WIDERRUFGARANTIE: Diese Bestellung können Sie innerhalb von 14 Tagen widerrufen. Eine Mitteilung an DIE WOCHE, Leserservice, Postfach 60 04 69, 22204 Hamburg, genügt. Die Frist beginnt mit Absendung dieser Bestellung (Poststempel).



GESCHENKGUTSCHEIN

EIN JAHR LANG DIE WOCHE.

EINES DER INTELLIGENTESTEN ABONNEMENTS DEUTSCHLANDS.



MIT DEN BESTEN WÜNSCHEN VON

DIE WOCHE BRINGT ES AUF DEN PUNKT.

JETZT ANRUFEN: 0180 / 5 110 110
(DM 0,24/Min.)

ODER PER E-MAIL: ABO@WOCHE.DE
(Bitte immer Aktions-Nr. 2045-13692 mit angeben)