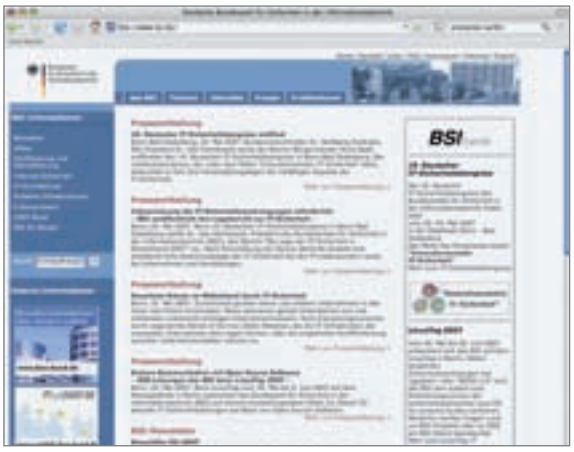
Cookies oder die Identifizierbarkeit im Internet

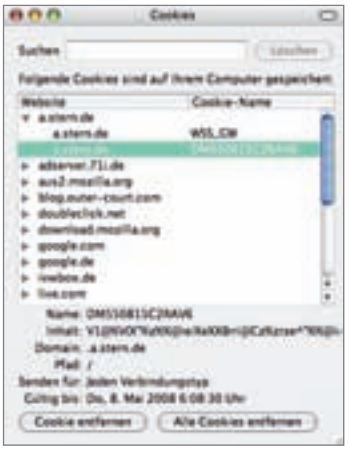
Vielleicht ist es Ihnen gar nicht bewusst, aber in Ihrem Rechner geht es manchmal zu wie in einer Backstube. Während Sie ahnungslos im Internet surfen, sammeln sich Cookies über Cookies auf Ihrer Festplatte. Leider kann man dabei nicht zwischen Chocolate Chips und Macadamia Nüssen wählen, da diese Cookies nicht essbar sind. Hinter dem unscheinbaren Namen verbergen sich kleine Datensammlungen. Warum diese Sie beim Surfen identifizierbar machen und was für andere Mechanismen es noch gibt, um Sie auszuspionieren und wiederzuerkennen, das erfahren Sie im Folgenden.

Alle Anbieter von kommerziellen Webseiten haben ein lebhaftes Interesse daran, zu erfahren wer, wann und wie oft ihre Webseiten besucht. Was dort angesehen wird und von wem, ist interessant und beeinflusst auch die weitere Gestaltung des Angebotes. Schon seit Jahren werden daher auf dem Rechner des Benutzers kleine Datenpakete abgelegt. Kommt derselbe Nutzer wieder, so wird er automatisch erkannt und sein Besuchsverhalten aufgezeichnet.

Prinzipiell wäre daran nichts allzu Schlimmes, wenn beispielsweise die Seite eines Versandhauses Sie wiedererkennt und vielleicht sogar persönlich begrüßt. Problematisch wird es erst, wenn man sich vorstellt, dass über viele Jahre diese Daten gesammelt und gespeichert werden können. Auch ist es möglich, dass mehrere Anbieter als Firmengruppe zusammengehören oder Daten abgleichen. Beliebig steigern lässt sich das ungute Gefühl bei der Vorstellung, dass außerhalb von Europa Datenschutz kaum entwickelt ist und mit diesen Nutzerprofilen auch derzeit schon Handel getrieben wird. Technisch möglich ist dabei auch eine breite Zusammenschau auf einen einzelnen Nutzer und sein gesamtes Online-Verhalten. Da wohl kaum zu entscheiden ist, wann persönliche Grenzen überschritten werden, ist ein vorsorgliches Verhalten angebracht. Folgende Regeln helfen die Sammelwut einzudämmen und zusätzlich ihre Online-Sicherheit zu erhöhen. Ganz nebenbei tun Sie dabei auch etwas für die Sicherheit der Daten, die auf Ihrem Rechner abgelegt sind.



Das Bundesamt für Sicherheit in der Informationstechnik bietet einen hilfreichen Leitfaden zur IT-Sicherheit, den jeder kennen sollte. www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf
Auf der Hauptseite (www.bsi.de) finden sich aktuelle Meldungen zu Sicherheitsthemen und vieles anderes mehr.



Im Cookie-Manager von Firefox (und anderen Browsern), den man unter Einstellungen findet, können alle Cookies, die auf ihrem Rechner hinterlegt wurden eingesehen und gelöscht werden.

Surfregel Nummer 1

Verwenden Sie einen sicheren Browser in einer aktuellen Version. Nur so kann man die Risiken minimieren. Der Microsoft Internet Explorer gehört leider nicht in diese Kategorie und ist bekannt für seine zahlreichen Sicherheitslücken, auch und besonders, weil er so tief ins Betriebssystem integriert ist. Bessere Alternativen sind da Firefox und Opera. Die aktuellen Versionen finden Sie unter:
www.mozilla-europe.org/de/products/firefox/
www.opera.com/products/desktop/?htlanguage=de/

Wie Sie die Einstellungen anpassen können, um die Sicherheit zu erhöhen finden Sie hier:
www.heise.de/security/dienste/browsercheck/anpassen/

Surfregel Nummer 2

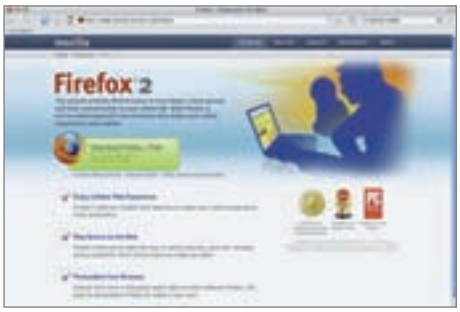
Auch der beste Browser ist nur so gut wie das Betriebssystem, auf dem er läuft. Viele Sicherheitslücken können nur im Betriebssystem beseitigt werden. Aktualisieren Sie daher Ihr Betriebssystem regelmäßig auch wenn es lästig ist.

Surfregel Nummer 3

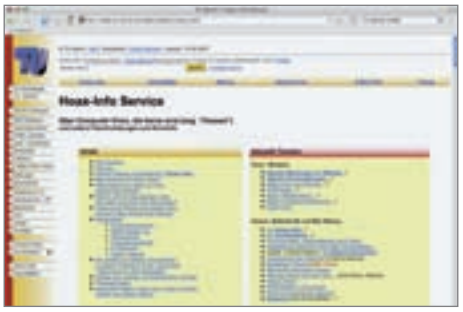
Machen Sie sich mit dem Cookie-Manager Ihres Browsers vertraut und verwenden Sie ihn regelmäßig. Cookies können dafür sorgen, dass eine Webseite mit persönlichen Voreinstellungen angezeigt wird, sie können auch persönliche Daten enthalten, die Sie auf einer Webseite angegeben haben wie zum Beispiel Bestellungen. Zugang zu Daten auf Ihrem Rechner haben Sie nicht. Ob das das Risiko des Missbrauchs und der Datensammlung rechtfertigt, muss jeder selbst entscheiden. Mit dem Cookie-Manager können Sie unerwünschte oder gleich alle Cookies von Ihrem Rechner löschen. So können Sie den häufigsten Identifizierungsmechanismus selbst umgehen. In Firefox lassen sich auch Regeln formulieren nach denen zum Beispiel nur bestimmten Webseiten das Ablegen von Cookies erlaubt wird.

Surfregel Nummer 4

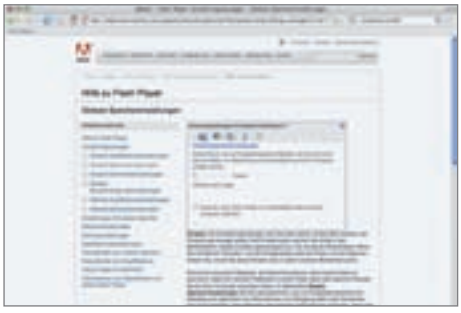
Schalten Sie Ihren Rechner regelmäßig ganz aus. Das ist natürlich nur sinnvoll, wenn Sie ihn tatsächlich einige Stunden oder länger nicht benötigen. Es spart Energie, verringert den Verschleiß und macht ihn wesentlich weniger



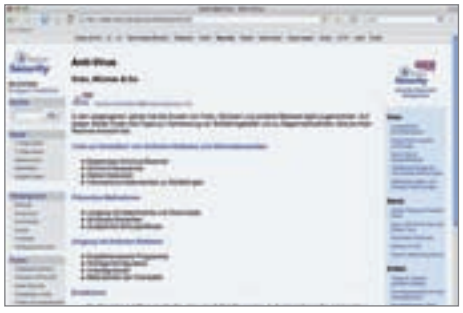
Einer der sichersten Browser, wenn man die neueste Version verwendet, ist Firefox. Außerdem werden verschiedenste Web-Standards sehr gut unterstützt. www.mozilla-europe.org/de/products/firefox/



Als Startpunkt für Informationen zu E-Mailscherzen, aktuellen Viren und anderen Gefahren bietet sich der Informationsdienst der TU-Berlin an. www.tu-berlin.de/www/software/hoax.shtml



Unscheinbar und gut verborgen zeigen sich die Einstellungen des fast überall installierten Flash-Players nur bei Aufruf der richtigen Adresse: www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager03.html



Eine ständig aktualisierte Übersicht zu erhältlichen Virenschutzprogrammen gibt es beim Heise-Verlag: www.heise.de/security/dienste/antivirus/

angreifbar als einen Rechner, der 24 Stunden angeschaltet und online ist. Eine Schaltsteckdose ist die einfachste und hundertprozentige Lösung, um auch den teilweise stromfressenden Stand-by-Betrieb von Computer und Peripherie zu unterbinden. Natürlich können Sie auch die DSL- oder Kabelmodemeinheit an eine Schaltsteckdose hängen und diese regelmäßig abschalten.

Surfregel Nummer 5

Vermeiden Sie das Herunterladen unnötiger Dateien besonders von Ihnen unbekannten Quellen oder Webseiten, die Sie zum ersten Mal besuchen. Sich zu fragen, ob der Bildschirmschoner, Desktophintergrund oder ein Hilfsprogramm wirklich notwendig sind, kann unnötige Aufräumarbeiten und auch Sicherheitsrisiken vermeiden helfen. Gerade in scheinbar harmlosen Dateien stecken immer wieder Schadprogramme. Wer ganz auf Nummer sicher gehen will, der kann sich auf die Zusammenstellungen von renommierten Computerzeitschriften entweder im Heft oder auf den Webseiten der Verlage umsehen. Dort finden sich bewährte Hilfsmittel aber auch Spiele, Bildschirmschoner usw. die von Redakteuren getestet wurden.

Surfregel Nummer 6

Kontrollieren Sie die Einstellungen Ihres Flash Players. Einige Webseiten benützen dieses Format, um Dateien auf Ihrem Rechner abzulegen, die Sie erkennbar machen. Einstellung für maximale Speichergröße und andere Parameter finden Sie unter der Adresse:
www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager03.html
Wenn Sie diese auf 0 KB einstellen und den Haken vor „Nachfragen" anklicken, sind Sie vor unerwünschten Flash-Dateiablagen auf Ihrer Festplatte sicher.

Surfregel Nummer 7

Installieren Sie einen Virenschutzmechanismus und aktualisieren Sie ihn regelmäßig. Nur so können Sie sich vor Datenverlust schützen und die Weitergabe von infizierten Nachrichten und Dateien vorbeugen. Aktuelle Lösungen sowie Erklärungen zu den Schädlingstypen finden Sie unter:
www.heise.de/security/dienste/antivirus/
www.tu-berlin.de/www/software/antivirus.shtml#univ

Surfregel Nummer 8

Beteiligen Sie sich nicht an (manchmal sehr verlockend klingenden) Online-Preisausschreiben! Hier werden Ihre Daten erhoben und Sie werden um den Preis einer Teilnahme vollständig identifizierbar. Kein Anbieter hat im großen Stil etwas zu verschenken. Alle Gewinne (wenn es sie denn gibt) sind bewusst kalkulierte Kosten für die erhaltenen Adressen, die oft auch weiterverkauft werden.

Alle Maßnahmen, um sich anonym im Web zu bewegen sind fruchtlos, wenn Sie sich selbst den Anbietern preisgeben.

Surfregel Nummer 9

Per E-Mail werden Sie manchmal mit den absonderlichsten Nachrichten auf eine Webseite gelockt. Die allermeisten dieser Nachrichten dienen ebenfalls nur der Validierung ihrer E-Mail-Adresse (wie gehabt zum Weiterverkauf) und versuchen zusätzlich noch persönliche Daten aus Ihnen herauszulocken. Manche dienen auch nur dazu, eine Nachrichtenflut zu verbreiten, wenn jeder Nutzer die Nachricht wie gefordert an alle Freunde weiterleitet. Jugendliche Hacker können sich damit in ihren Kreisen Prestige erwerben.

Für solche und andere Scherze hat sich der Begriff „Hoax" etabliert. Einen umfangreichen Informationsdienst zu aktuellen und früheren kursierenden Nachrichten unterhält die TU-Berlin unter:
www.tu-berlin.de/www/software/hoax.shtml

Surfregel Nummer 10

Derzeit gibt es zwei praktikable Möglichkeiten, sich anonym durchs Netz zu bewegen. Beide Angebote nutzen ähnliche Techniken, die durch mehrfache Umleitung in einem speziellen Servernetz eine Identifizierung beinahe vollständig unmöglich machen. Etwas Zeit zur Installation und dem Studieren der Anleitung sollte man allerdings schon mitbringen:
http://anon.inf.tu-dresden.de/
http://tor.eff.org/

Sorgen Sie angemessen für sich, Ihre Daten und Ihren Computer. Denn es gibt immer wieder Spannendes, Interessantes und Hilfreiches im Web zu entdecken.

Dr. Marc M. Batschkus,
Institut für Ethnomedizin,
Melusinenstraße 2, 81671 München,
E-Mail: mmb@institut-ethnomed.de