

Sicher Surfen II: Von Cookies und Cookiemonstern

Georg Wagner

25. Mai 2001

1 Was sind Cookies ?

Cookies (cookie: Keks, Guetzli) sind kurze Informationen, die von den Internet-Browsern (Netscape, Internet Explorer) in einer Datei abgelegt werden. Die Datei in der die Cookies abgelegt werden, kann cookies.txt, cookies oder MagicCookie heissen¹. Da Cookies in einer Datei abgelegt werden, bleiben sie über längere Zeit - auch wenn der Rechner zwischendurch ausgeschaltet wird, erhalten.

Die Ablage eines Cookies wird von aussen veranlasst, meist von der Web-Seite, die Sie gerade besuchen. Wenn Sie mit Ihrem Browser im Internet unterwegs sind, so sammeln Sie also unentwegt Cookies (Kekse) ein.

Abgelegt wird der Cookie aber von dem Browser auf Ihrem Rechner. Die Browser lassen sich so einstellen, dass sie vor dem Abspeichern eines Cookies fragen, ob man damit einverstanden ist. Wenn nein wird der Cookie nicht abgelegt. Leider wird so häufig nachgefragt, dass es extrem störend ist.

Cookies haben gute und negative Seiten, um in der Analogie zum Keks zu bleiben: Es gibt süsse und bittere Cookies

1.1 Der süsse Cookie

Cookies können bestimmte Voreinstellungen speichern, auf die beim nächsten Besuch der zugehörigen Webseite zurückgegriffen werden kann. Sind Sie Kunde einer Webfirma oder einer Online-Bank, so müssen Sie nur einmal angeben, in welcher Sprache Sie z.B. die Webseite sehen möchten. Es lassen sich weitere arbeitssparende und harmlose Verwendungen von Cookies denken.

1.2 Der bittere Cookie

Viele Organisationen nutzen Cookies, um jeden Besuch, jeden Mausklick auf ihrer Webseite festzuhalten. Auf diese Weise können Interessen festgestellt und festgehalten werden. Diese werden Ihrer Cookie-ID zugeordnet. Dieser Cookie-ID kann nun nach Auswertung Ihrer Surfgeohnheiten ein Interessenprofil zugeordnet werden. Wenn nun ein Internet-Surfer

mit dieser Cookie-ID eine Web-Seite besucht, kann die zu diesem Profil passende Werbung eingeblendet werden.

Weiss eine solche Organisation auch noch Ihre Email-Adresse oder gar Ihren Namen, kann sie diese für einen Adressenhandel verwenden. Wird z.B. festgestellt, dass Sie sich speziell für Autos interessieren, könnte Ihre Adresse an Autofirmen verkauft werden. Diese könnte Ihnen dann gezielt per Email Werbung zusenden. Mithilfe der Cookies können also Anwenderprofile, die Ihre Surfgeohnheiten und Interessen festhalten, erstellt werden. Für ein Beispiel einer solchen Anwendung lesen Sie bitte im Anhang den Abschnitt über *doubleclick*. Wenn Ihre Identität nur einer Firma im Internet bekannt wird, kann dies heissen, dass sie an hunderte andere weiterverkauft werden kann. Weitere Anwendungen, um in Ihr Privatleben einzudringen, lassen sich leicht vorstellen.

2 Beurteilung: Cookies und Sicherheitsrisiken

Ein direktes Sicherheitsrisiko liegt nicht vor. Cookies sind passiv, sie enthalten nur Daten. Cookies ermöglichen keinen direkten Zugriff auf Ihren Rechner.

- Ausserdem können mit Cookies nur Daten erfasst werden, die auch ohne Cookies erfasst werden können und jeder Web-Seite, die Sie besuchen ohnehin bekannt sind.
- Cookies ermöglichen aber die Persistenz - also die Dauerhaftigkeit - der über Sie erfassten Daten. Der Cookie kann nämlich beliebig lange auf Ihrer Festplatte liegen bleiben.
- Die Gefahr der Cookies liegt in der Erstellung von Anwenderprofilen. In diesen Punkten ähneln sie z.B. der Migros-Cumulus-Karte. Auch hier werden Ihre Kaufgeohnheiten systematisch erfasst. Im Gegensatz zur Cumulus-Karte ist Ihr Name - falls Sie ihn nicht freiwillig zusammen mit Ihrer Email-Adresse bekannt gegeben haben - nicht fest mit einem Cookie verbunden.

Cookies können viele Funktionen haben. Eine sehr wichtige Aufgabe der Cookies besteht darin, einen

¹Microsofts Internet Explorer legt die Cookies in einem Ordner namens "Cookies" als einzelne Dateien ab.

gläsernen Internetbesucher zu schaffen, um gezielt Werbung schalten zu können.

3 Ablage eines Cookies verhindern.

Es gibt mehrere Methoden die Ablage eines Cookies zu verhindern:

1. Im Browser ausschalten: Einfach aber lästig, da immer wieder nachgefragt wird.
2. Die Datei cookies.txt schreibschützen. Da die Browser die Cookies anfangs im Speicher halten, gehen die Cookies nach dem Ausschalten verloren. Sie sollten aber auf jeden Fall kontrollieren, ob wirklich keine Cookies abgelegt wurden.
3. Programme, die die Cookies in der Cookie-Datei anzeigen und verwalten. Am Ende einer Internet-Sitzung können Sie mithilfe eines solchen Programms, die Inhalte der Cookie-Datei anzeigen und gegebenenfalls löschen.
4. Proxy-Filter: Dies sind spezielle Programme die sich zwischen Ihrem Browser und dem Internet einhängen. Aller Datenverkehr läuft über diese Proxy-Filter. Meistens lassen sich diese Filter so konfigurieren, dass z.B. Ihre Online-Bank Cookies ablegen darf, während alle anderen Cookies automatisch verworfen werden. Der Proxy-Filter agiert gewissermaßen als Cookie-Monster, der alle unerwünschten Cookies auffrisst. Meistens kann ein Proxy-Filter auch noch Werbung ausfiltern, sodass Sie weniger von blinkender Werbung gestört werden. Einige Proxy-Filter erlauben sogar die Anonymisierung Ihrer IP-Adresse, sodass nicht zurückverfolgt werden kann, von woher Sie die Verbindung zu einer Webseite aufgebaut haben.

Die Methoden 1 - 3 haben folgende Nachteile:

- Belästigung durch ständiges Nachfragen, ob Cookies abgelegt werden dürfen
- Bei den Veränderungen an der Cookie-Datei sind Fachwissen und Disziplin erforderlich.

Ich bevorzuge daher die Methode 4. Gelegentlich verwende ich Methode 3 zur Kontrolle, ob wirklich alles funktioniert. Im folgenden Abschnitt werden Programme beschrieben, die als Cookiemonster agieren können.

4 Cookiemonster

Zur Umsetzung der Methode 4 eignet sich der Internet Junkbuster besonders. Er ist für diverse UNIX-Betriebssysteme, Windows und Macintosh frei erhältlich².

4.1 The Internet Junkbuster

Dieses Programm hat folgende Eigenschaften:

- Arbeitet als Proxy, also als ein eigenständiges Programm, das zwischen dem Browser und dem Internet steht. Jede http-Nachricht (http-request) - also alles was Ihr Browser sendet oder empfängt - wird überprüft und nur gemäss den Regeln in einer Block-Datei weitergegeben.
- Kann mit jedem Browser verwendet werden.
- Quellcode ist vorhanden, seine Arbeitsweise kann also überprüft werden.
- Stoppt alle Cookies, ausser denen die man ausdrücklich zulässt.
- Die Weitergabe anderer Informationen - z.B. verwendetes Betriebssystem, verwendeter Browser, welche Webseite angeklickt wurde oder Hardware und Softwareinformationen über den verwendeten Computer³ - wird ebenfalls verhindert.
- Anonymes Surfen ist bei entsprechender Konfiguration ebenfalls möglich.

Installation des Internet JunkBusters

1. Die zip-Datei ijb20.zip nach C:/Programme auspacken
2. Ein geeignete Blockfile aus dem Internet besorgen
3. Starten des Internet Junkbusters automatisieren (Link in Autostart-Ordner setzen).
4. Im Browser die Option "Manual Proxy Configuration" anwählen und folgende Punkte setzen:
 - HTTP Proxy: localhost 8000
 - Security Proxy localhost 8000
 - Die anderen Proxies sollten auf: proxy.provider.ch 8080 gesetzt sein (genaue Angaben sind Provider-spezifisch).

²The Cookie Server - funktioniert ähnlich wie der JunkBuster, kümmert sich aber nur um Cookies und läuft nur unter Windows. Sollte nur ohne den JunkBuster verwendet werden.

³Solche Angaben gibt Ihr Browser von sich aus weiter.

4.2 Was ist in der Keksbüchse?

Zusätzlich sollten Sie ein Programm zur Kontrolle und Pflege der Cookie-Datei(en) verwenden. Geignet ist z.B. :

- Cookie Cruncher
- Cookie Killer

Mithilfe dieser oder ähnlicher Programme können Sie sich den Inhalt der Keksbüchse - der Cookie-Datei(en) - ansehen und einzelne Cookies gezielt löschen.

Anhang

Doppelklick geht auf den Keks

Wenn Sie einen Blick in die Datei cookies.txt werfen, werden Sie mit hoher Wahrscheinlichkeit einen Eintrag (Cookie) mit dem Namen "doubleclick.net" finden. Höchstwahrscheinlich haben Sie nie eine Web-Seite mit diesem Namen besucht. Wie kommt dieses Cookie dann in Ihre Datei? Die Idee hinter den Cookies war doch, bestimmte Informationen festzuhalten, falls Sie eine Web-Seite mehrmals besuchen.

Was passiert hier? Doubleclick ist eine Marketing-Firma, die Daten über Web-Benutzer sammelt und weiterverkauft. Die Suchmaschine AltaVista ist z.B. ein Kunde von Doubleclick. Wenn Sie also AltaVista's Suchseite benutzen, setzt diese einen Cookie für Doubleclick auf Ihrem Rechner ab. Gleichzeitig wird eine zugehörige ID an Doubleclick gesendet. Doubleclick wird nun darüber informiert, welche Web-Seiten Sie besuchen und was Sie interessiert. Diese Daten legt Doubleclick in einer Datenbank ab. Das gleiche geschieht bei Web-Seiten anderer Doubleclick-Kunden.

Haben Sie dann einen Doubleclick-Cookie, wird, wenn Sie nun die Seite eines Doubleclick-Abonnenten besuchen, Ihr Doubleclick-Cookie gelesen, an Doubleclick gesendet und die bei Doubleclick gespeicherte Information abgerufen. Danach blendet die Webseite Werbung ein, von der angenommen wird, dass sie Ihren Interessen entspricht. Wenn Sie gerne gezielt Werbung erhalten, mögen Sie das Ganze relativ harmlos finden. Oder Ihnen gehen die ständigen Versuche AltaVista's den Doubleclick-Cookie abzulegen zwar auf den Keks, aber die Erfassung Ihrer Surfgewohnheiten ist Ihnen egal. Aber hier werden Daten über Sie ohne Ihr Wissen erfasst und weiterverkauft.

Stellen Sie sich vor, dass staatliche Stellen oder politische Gruppierungen solche oder ähnliche Mechanismen verwenden. Dann sind wir nicht mehr weit vom "Big Brother" oder "Gläsernem Bürger" entfernt.

Die Keksbüchse wird voll

Im Internet gibt es Firmen, die sich darauf spezialisiert haben, das Verhalten einzelner Benutzer zu analysieren. Ich möchte hier die Adressen einzelner Firmen angeben, und diejenigen, die Englisch lesen können, können dann diese Internetseiten besuchen und sich die Möglichkeiten der Netzanalyse erklären lassen. Fangen wir bei *Adlink*⁴ an. Diese Firma untersucht sowohl das Leseverhalten der Internet Besucher, verwaltet aber auch gleichzeitig die Werbung von Firmen. Es gibt einen engen Zusammenhang zwischen Werbung im Internet und den Cookie-Sammlern. Durch Analyse des Verhaltens der Benutzer kann auf die Interessen der Benutzer geschlossen werden und entsprechende Werbung geschaltet werden. Derjenige, der werben möchte, kann sicher sein, dass seine Werbung die gewünschte Zielgruppe erreicht.

Die Cookie-Hamster

Die Firma *Adlink* hamstert die Cookies nicht alleine, sondern zusammen mit vielen anderen Web-Seiten. Falls Sie die eingesammelten Cookies einmal anschauen, so stellen Sie möglicherweise fest, dass sie von vielen Stellen gesammelt wurden. Dies muss aber nicht heißen, dass diese Cookie-Sammlungen von verschiedenen Gruppen getrennt analysiert werden. Die Cookies können von den verschiedenen Rechnern wiederum zentral gesammelt und analysiert werden. Die Internet-Firma *Keynote*⁵ bietet z.B. komplexe Netzanalysen an und arbeitet mit der Firma *Adlink* zusammen.

Keks für Keks

Die Site *Hitbox*⁶ sammelt fleissig Cookies und erstellt daraus eine Art Hitparade, die wiederum im Internet abrufbar ist. Diese Hitparade hat natürlich zwei Funktionen. Zum einen findet man heraus, welche Internetseiten beliebt sind, zum anderen kann man durch die Analyse des Surfverhalten gezielte Werbung anbieten.

Deutsche Kekse

Die Cookie-Sammelleidenschaft grassiert nicht nur in Amerika. Auch in Deutschland werden Cookies gesammelt. Die Seite *Doppelklick*⁷ ist ein Beispiel für eine deutschsprachige Seite. Und auf der Unterseite *Preis-Doppelklick-Werbung*⁸ finden Sie eine sehr detailliert abgefasste Preisliste.

⁴<http://www.adlink.de>

⁵<http://www.keynote.com>

⁶<http://www.hitbox.com>

⁷<http://www.doppelklick.net>

⁸http://www.doppelklick.net/sitemap.html?sitemap_main_li.html