# Spyware, Cookies und lästige Mitbewohner

Der allgemein verbreitete Glaube, man sei im Internet besonders „anonym“ unterwegs, kann heute leider nicht mehr bestätigt werden. Zu viele Schnüffelmechanismen und –programme sind inzwischen erfunden, die diese Anonymität leicht durchbrechen. Wir wollen nun einen Überblick geben, welche technische Möglichkeiten es überhaupt gibt, um Ihre Privatsphäre zu verletzen und wie Sie sich gegen diese hinterhältigen Plagegeister schützen können.

## *Ihre IP-Adresse – ein erster Anhaltspunkt*

Wenn Sie mit Ihrem Computer im Internet unterwegs sind, so ist Ihr PC durch die IP-Adresse weltweit auf jedem Webserver, den Sie besuchen, sichtbar. Diese Adresse (z.B. 195.72.22.20) besteht aus 4 Zahlen, die jeder Betreiber einer Webseite sehen kann (natürlich nur wenn Sie diese auch anklicken), womit eine theoretische Rückverfolgbarkeit ihres Rechners gegeben ist (das hängt vor allem von rechtlichen Vorgaben ab). Dass Ihre IP-Adresse je nach Internetprovider immer gewechselt wird, oder ob Sie über einen Proxyserver im Internet surfen, kann diese Rückverfolgbarkeit nicht wirklich verhindern. Es gibt jedoch einige mehr oder weniger „windige“ Angebote zum „anonymen“ Surfen, die tatsächlich Ihre Spuren im Internet (das geht über spezielle Proxyserver) zu verwischen vermögen – gern gesehen in der Hackerszene, die nicht gerne ihre Identität preisgibt.
Jedenfalls ist die IP-Adresse eher Anhaltspunkt für die Verfolgung von Straftätern und nicht besonders gut geeignet, z.B. Statistiken über Ihr Surfverhalten anzulegen (zumindest wenn Sie keine fixe IP-Adresse haben).

## *Cookies – schon besser identifiziert*

Cookies sind kleine Textdateien, die von Ihrem Webbrowser auf Ihrem Computer gespeichert werden, und beim Surfen der entsprechenden Webseite auch „mitgeteilt“ werden. Das ist so ähnlich, als würden Sie jedes Mal beim Einkaufen einen Ausweis hinlegen müssen, in dem seltsame Vermerke über Ihren Einkaufskorb gemacht werden. Was der Webseitenbetreiber mit den gesammelten Information macht, bleibt

**IP-Adresse** … eindeutige Adresse eines Computers oder Netzwerks im Internet
**Proxyserver** … Server im Internet, der Ihre IP-Adresse durch seine eigene ersetzt.
**Cookie** … kleine Textdatei auf Ihrem Computer, die erlaubt, dass Sie von Webseiten „wiedererkannt“ werden.
**Webbrowser** … Software zum Ansehen von Internetseiten (z.B. Internet Explorer, Firefox, Netscape, etc.)
**Spyware** … Software, die Daten ihres Computers sammelt und preisgibt, Werbefenster anzeigt, etc.
**Popup** … Selbsttätig öffnende Fenster mit z.B. Werbebotschaften

dem Besucher weitestgehend verschlossen. Die Möglichkeiten reichen vom „überhaupt nichts“ mit den Cookie-Informationen anstellen bis zu „jeden Mausklick“ auf jede Seite registrieren und speichern. Sie können Cookies zwar jederzeit im Browser abschalten, bekommen dann aber als Nebeneffekt geliefert, dass viele Webseiten überhaupt nicht mehr funktionieren (diese wirken dann irgendwie „vergesslich“). Die Lösung dafür ist, dass Sie nur sogenannte „Session-Cookies“ akzeptieren können, die immer nur für eine Sitzung auf einer Webseite gelten und dann vom PC gelöscht werden. Damit sind Sie nur für die Viertelstunde bei der Webseite als „eine Person“ erkennbar – beim nächsten Besuch hat Sie die Webseite „vergessen“, da Ihr Browser das Cookie von Ihrem PC entfernt hat.

## Spyware

Etwas schlimmer wird’s mit der sogenannten „Spyware“, also kleinen Schadprogrammen bzw. geänderten Einstellungen des Webbrowsers ohne Ihre Zustimmung. Die Programme installieren sich meist selbst beim Besuch zweifelhafter Webportale, meist durch Nutzung diverser Sicherheitslücken Ihres Webbrowsers. Sie erkennen die Fieslinge manchmal durch unvermutete Einblendung von Werbefenstern ohne Zusammenhang mit einer bestimmten Webseite. Die Bandbreite reicht von eher harmlosen Popups bis zur Änderung von Webbrowser- oder Netzwerkeinstellungen ohne Ihr Wissen, sodass die Grenzen zum Virus schon fast erreicht werden.
Genauso wie für den Virenschutz gibt es auch Maßnahmen gegen die Spyware-Finsterlinge, sehr bekannt sind die Programme „Ad-Aware“ (auch gratis für Privatanwender) oder „HijackThis“. Beachten Sie bitte, dass auch diese Programme – genau wie die Virenschutzprogramme - Aktualisierungen brauchen, um Sie vor neuen Bedrohungen zu schützen. Es wäre auch nicht das erste Mal, dass ein unbedarfter Anwender sich selbst aus dem Internet aussperrt, weil das Abhaken von gewissen Einstellungen bei „HijackThis“ wohl etwas zu gut gemeint war. Verwenden Sie also bitte diese Programme nur nach intensiver Lektüre der Hilfeseiten.

Falls Sie Detailfragen zu den besprochenen Themen haben, senden Sie bitte Ihre E-Mail an:
**Müller & Kanduth OEG**
**support@mko.at**