


Spyware, Adware and Under-Wear



Immer mehr werden Internetnutzer von so genannter "Spyware" heimgesucht. Was bedeutet das? Bei Spyware handelt es sich um kleine Programme, welche durchs Internetsurfen und Downloads unbemerkt auf Ihr System gelangen. Es handelt sich um Würmer, Trojaner, Dialer usw. Diese Programme senden dann, sobald eine Internetverbindung besteht, Daten von Ihrem PC ins Internet (an Hacker, Mail-Sammler usw.). Es werden dabei teilweise auch sehr vertrauliche Daten gesendet. Sie merken jedoch davon nichts – das ist auch die Gefahr!

Die Programmierer der verseuchten Freeware Programme trifft an dieser Entwicklung aber nicht die Hauptschuld, schliesslich wollen sie nur für ihre Arbeit bezahlt werden. Der User ist mal wieder der Leidtragende, wird doch sein System nun mit Cookies, Registry- u. System-Einträgen „zugemüllt“ und permanent ausgespäht.

Definition Adware – Spyware (nach www.whatis.com)

Unter *Adware* wird jede Art von Programmen verstanden, in welcher Werbebanner (engl: advertising banners) eingeblendet werden. Dabei können die Werbebanner als separate PopUp-Windows oder in Anzeigefeldern direkt im Programm auftreten.

Der Programmierer setzt Adware ein, um sich damit zu finanzieren. Er blendet gegen Bezahlung ein Werbebanner in sein Programm ein. Diese Art von Werbung ist unbeliebt und nicht jeder, der die Werbung sieht, interessiert sich auch dafür und klickt sie an.

Spyware bezeichnet im allgemeinen Sinn jede Technologie, die dabei hilft, Informationen über eine Person oder ein Unternehmen zu erfassen, ohne deren Wissen.

Im Zusammenhang mit dem Internet wird unter Spyware ein Programm verstanden, das auf einem Computer installiert wurde mit dem Ziel, geheime Informationen über den Benutzer zu erhalten und diese via Internet an den Hersteller der Software oder an diverse Werbezentralen zu übermitteln.



Funktionsweise/Techniken

Die womöglich grösste Gefahr für Ihre Privatsphäre geht heute wohl von den Werbefirmen aus. Dank Cookies, Clear-Gifs und Spyware ist es Unternehmen relativ problemlos möglich, Bewegungsbilder Ihrer Surfgeohnheiten zu erstellen. Die dabei verwendeten Techniken sind einfach. Sie nutzen Funktionen, die aus unserem Web-Alltag nicht mehr wegzudenken und deshalb auch nur schwer abzublocken sind. Im Folgenden zeigen wir die meistverbreiteten Techniken auf:

Technik	Massnahmen
<p>Cookies Cookies ("Kekse") sind kleine Textdateien, die beim Besuch einer Website auf Ihrem Computer abgelegt werden und beim zweiten Besuch vom Bereitsteller der Homepage gelesen werden können. Sie beinhalten entweder Informationen vom Server der besuchten Webseite oder Angaben die der Surfer macht.</p>	<p>→ Browser Policies → Datenschutzeinstellungen</p>
<p>Clear-GIF's aka. Web-Bugs Web-Bugs oder auch "clear GIFs" sind meist kleine, 1*1 Pixel grosse GIF-Dateien, die in anderen Grafiken, E-Mails, o. ä. versteckt werden können. Sie ermöglichen ein Tracking des Benutzers, indem sie seine IP-Adresse, besuchte URL, Datum/Uhrzeit, sein Browsertyp sowie zuvor gesetzte Cookie-Informationen an einen Web-Server übermitteln.</p>	<p>→ Blocken „berüchtigter“ Domains</p>
<p>Banner-Ads Ähnlich wie Clear-Gifs. Problem: Banner-Ads stammen meist von einem Dritt-Server, an welchem mehrere Firmen angeschlossen sind. Für diese Dritt-Firma ist es ein Kinderspiel, Surfgeohnheiten festzustellen.</p>	<p>→ Blocken „berüchtigter“ Domains</p>

<p>Phonehome-Programme Darunter versteht man Software, die nach dem Spyware-Prinzip unbemerkt über das Internet Kontakt zu seinem Hersteller aufnimmt, Seriennummer weitermeldet und abgleicht, oder unerwünscht nach Updates anfragt.</p>	<p>→ Firewall rules LAN>WAN → Beachten von Lizenzbedingungen</p>
<p>Trojanische Pferde Ein Virus richtet meist sehr schnell Schäden an, die der PC-Nutzer schnell entdeckt, Trojaner arbeiten aber im Hintergrund und werden oft sehr spät oder manchmal auch gar nicht entdeckt. Abgesehen davon erlaubt ein Trojaner oft den vollständigen Zugriff auf den befallenen PC. Trojaner können als Mischform zwischen Virus und Spyware angesehen werden und gelten als deren übelste Sorte.</p>	<p>→ Firewall rules LAN>WAN → Sicherheitsrichtlinien bei Userberechtigungen</p>
<p>BHO Ein „Browser Helper Object“ ist eine DLL, die es dem Entwickler erlaubt, plug-ins für Internet Explorer zu schreiben und IE komplett zu kontrollieren. Die API ist ziemlich komfortabel. Beispiele sind Toolbars, Alexa, GetRight, Go!Zilla oder die Einbettung von Adobe Acrobat Reader.</p>	<p>→ BHO's komplett ausschalten → Userberechtigungen</p>

Gefahren, Risiken

Mit Spyware verseuchte Programme können Nutzerdaten jeglicher Art sammeln und diese ungefragt an den Hersteller des Programms übermitteln. Der Hersteller erhält so Informationen, wer seine Software benutzt und wie viele Programme im Umlauf sind. Durch die Spyware kann ein Software-Hersteller auch Raubkopien ausfindig machen.

Weiters können Clickstreams des Anwenders mitgeschrieben und daraus Logfiles generiert werden. Eine Online-Werbefirma erhält so beispielsweise Informationen darüber, wie das Surfverhalten der verschiedenen Personen aussieht. Diese Informationen werden in einer Datenbank gespeichert. Mit Hilfe der so erhaltenen Nutzerprofile können Personen direkt und mit für sie abgestimmter Werbung attackiert werden.

Spyware läuft im Hintergrund ab ohne das Wissen des Anwenders. Zu Spyware gehören also auch die heimlichen Update-Funktionen diverser Programme. Diese wählen sich ins Internet ein und laden automatisch ein Update herunter. Durch eine heimliche Verbindung kann auch gleich die Software online verifiziert werden, ohne dass der Benutzer davon etwas erfährt.

Eine weitere Gefahr birgt Spyware, die Tastatureingaben mitschreiben kann, damit auch Passwörter, ID's oder gar Kreditkartennummern. Diese Informationen werden dann per Internet zum Spion gesendet

Die aber wohl gefährlichste Art von Spyware kann alle Informationen zu Festplatteninhalten oder aus der Windows Registry übertragen. Der Protokoll-Empfänger erhält ein komplettes Benutzerprofil der Person, das neben ihren persönlichen und ggf. vertraulichen Daten auch alle auf ihrem Rechner installierten Programme sowie dessen Konfiguration offen legt.

Bei folgenden Namen (Werbeagenturen, Softwarehersteller) ist Vorsicht geboten, da hier Spyware im Spiel ist: OfferCompanion, Webhancer, Gator, Cydoor, SaveNow, Radiate (früher Aureate), Timesink und Conducent.

Links

Anti-Spyware Tools <http://www.lavasoft.de/> - Ad-Aware, Lavasoft
<http://www.pestpatrol.com/> - PestPatrol
<http://grc.com/optout.htm> - OptOut

Artikel http://www.sicherheit-online.net/html/body_spyware.html - Spyware, Phonehome
<http://www.sitepoint.com/article/888/51>, Adware and Underwear
http://www.clickz.com/aff_mkt/aff_mkt/article.php/1483761 - The Big Lie