

Schützen Sie Ihren Computer vor Schnüffelprogrammen

Im Fadenkreuz der Datenspione

Das Sammeln von Benutzerdaten über das Internet ist nicht neu. Doch immer häufiger werden auch in Standard-Software Module eingesetzt, die der Übermittlung von persönlichen Daten dienen. Unbemerkt vom ausspionierten Nutzer. Wie dieser sich schützen kann, schildert Niels Gründel.

Spyware nennt sich diese hartnäckige Art von Schnüffel-Programmen, die Benutzerdaten vom eigenen PC via Internet an Hersteller oder Vertreter weiterreichen. In diesem Zusammenhang wird oft auch der Begriff AdWare verwendet. Doch im Gegensatz zur Spyware werden bei der Benutzung von AdWare lediglich Werbebanner eingeblendet, um so die entsprechende Software zu finanzieren. Diese Vorgehensweise ist ganz offensichtlich und wird von den Anwendern akzeptiert, zumal damit noch nicht der Versand persönlicher Daten verbunden ist.

Beispiel Microsoft XP

Für Aufsehen in der Öffentlichkeit sorgen immer wieder Übergriffe von Microsoft. Die Produktaktivierung von Windows XP ist das derzeit sicherlich bekannteste und zugleich aktuellste Beispiel. Denn ohne die Datenübertragung an Microsoft ist das Betriebssystem nicht lauffähig. Doch im Zuge dieses Vorgangs werden vor allem spezifische Daten der eigenen Hardware an Microsoft übertragen. Nimmt man die Produktaktivierung per Telefon vor, kann man einer allzu detaillierten Übertragung zumindest Einhalt gebieten.

Doch auch nach einer erfolgreichen Aktivierung versuchen das Betriebssystem und andere verbundene Programme wie der Media Player oder Messenger eine bestehende Internetverbindung zur Datenübertragung zu nutzen, angeblich um den Bedienkomfort zu erhöhen. Nicht zu Unrecht führen derartige Funktionen die betroffenen Hersteller eher in Verfall, ihre Kunden auszuspionieren, vor allem, wenn man bedenkt, dass die Hersteller die Ausschaltmöglichkeit entsprechender Übertragungsmechanismen mehr oder weniger stark verheimlichen. Wer Windows XP das Spionieren abgewöhnen möchte, ist mit dem Tool XP-Antispy [1] gut bedient. Es bietet zahlreiche Einstellungen, um einzelne Funktionen zu deaktivieren.

Andere Hersteller nicht besser

Doch schon seit einigen Jahren – und fast unbemerkt von der Öffentlichkeit – sind auch zahlreiche andere Firmen der Idee verfallen, die Nutzer ihrer Software regelrecht zu durchleuchten. RealAudio sorgte mit seiner Version 8 für Aufsehen, weil Benutzer in all ihren Internetaktivitäten überwacht wurden. Dafür erhielt der Hersteller RealNetworks [2] im Jahr 2001 den Big Brother Award [3] und änderte prompt seine „Privacy Policy“, mit der das Versenden von persönlichen Kundendaten legalisiert werden sollte. Wer trotzdem auf Datenschutz besteht, dem wird die Nutzung der Software besonders schwer gemacht. „Datenschutz ist eben ein Defekt, den es auszuschalten gilt“, so umreißt Jens Ohlig vom Initiatorenteam des Big-Brother-Awards, dem FoeBuD e. V. [4] in Bielefeld, die dreisten Zugriffe der Internetspione.

Shareware besonders betroffen

Besonders kritisch stehen Datenschützer der Firma Radiate/Aureate gegenüber, deren Softwarepaket für Shareware-Autoren gedacht ist und inzwischen in unzählige Programme Einzug erhalten hat. Nach Angaben von Radiate wird das Zusatzprogramm in mehr als 300 Softwareprodukten eingesetzt. „Wird die Aureate-Software Bestandteil eines anderen Programms, so hat der Autor die

Möglichkeit, das Verhalten seiner Nutzer nachzuverfolgen. Er erfährt beispielsweise alles über die Windows-Registry, das Surfverhalten, andere installierte Software und aufgerufene Werbebanner“, so ein Insider. „Die Firmen der Shareware-Software senden ihren Kunden dann nicht nur E-Mails, in denen sie über Updates informieren, praktisch sind sie auch dazu im Stande, Raubkopien aufzuspüren.“

Die Eintragungs-Software HelloEngines [5] von sofTrans [6] aus Reinheim übermittelt Registrieredetails und gleicht sie mit illegalen Codes ab. „Stellt das Programm dabei fest, dass ein illegaler Code verwendet wird, verweigert es seinen Dienst. Es werden aber nicht einmal dann die Daten des offensichtlichen Raubkopierers an uns übermittelt, weil das datenschutzrechtlich nicht zulässig wäre. In den letzten Jahren haben wir über 300.000 Registrierungen mit illegalen Freischaltcodes erhalten. Und der Datenbankabgleich sollte dem illegalen Treiben lediglich etwas entgegenwirken“, so Stelios Tsaousidis, Geschäftsführer der sofTrans (jetzt AceBIT).

Von Promo- und Rankware [7], einer Suchmaschinen-eintragungs- und Optimierungssoftware, wird berichtet, dass auch sie Daten an den Hersteller übermittelt, mit der die Nutzer identifiziert werden und bei Verstößen eine E-Mail mit Androhung einer Strafanzeige erhalten sollen.

Andere Programme, die wegen ihrer Spionage-technologie immer wieder genannt werden, sind beispielsweise CuteFTP 3.5, edonkey2000, Eudora, Go!Zilla und Zip Express 2000. Insgesamt sollen es aber weit mehr als 500 Programme sein, rund 300 arbeiten mit der Technologie von Radiate/Aureate. Unterschiede gibt es oft sogar in den diversen Programmversionen eines Herstellers: Besitzt eine bestimmte Version eines Programms Spyware-Technologie, muss das nicht zwangsläufig bedeuten, dass dies in allen anderen Versionen auch so ist oder dass die Technologie noch in der neuesten Version enthalten ist. Manche Software-Hersteller wägen inzwischen ab und verzichten wegen des Negativ-Images, das mit dem Spyware-Einsatz zwangsläufig verbunden ist, bei neuen Versionen auf dessen Einsatz.

Strafbares Verhalten?

Unlautere Absichten mögen bei den wenigsten Herstellern im Vordergrund stehen, doch die Übermittlung von Nutzer-spezifischen Daten zur weiteren Verwendung durch den Hersteller oder einen Vertriebspartner stellt ohne die ausdrückliche Erlaubnis des Anwenders einen Eingriff in die persönlichen Rechte dar, der nach Angaben des Berliner Datenschutzbeauftragten [8] unter gewissen Umständen sogar strafrechtliche Konsequenzen nach sich ziehen kann. Nach seiner Einschätzung dürfte die Erhebung personenbezogener Daten eines Nutzers im Rahmen eines Tele- oder Mediendienstes regelmäßig



BigBrotherAward-Statue des FoeBuD e.V. Bielefeld.

einen Verstoß gegen die Unterrichtspflicht aus § 4 Abs. 1 Teledienstschutzgesetz (TDDStG) sowie § 18 Abs. 1 Mediendienste-Staatsvertrag (MDStV) darstellen; gleichzeitig stelle dies eine Ordnungswidrigkeit dar, die mit einer Geldbuße bis zu 50.000 Euro geahndet werden könne.

Die Gesetzeslage

Zur Gesetzeslage: Werden die personenbezogenen Daten im Rahmen eines Tele- oder Mediendienstes auf der Inhaltebene beispielsweise nach dem Bundesdatenschutzgesetz erhoben, ist im Einzelfall zu überprüfen, ob der Einsatz der Spyware auch unter diesem Aspekt als Ordnungswidrigkeit (§ 43 Abs. 2 Nr. 1 oder Nr. 3 BDSG) zu werten ist. Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet oder wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abrufen oder sich oder einem anderen aus automatisierten Verarbeitungen verschafft. Eine Ordnungswidrigkeit kann dann sogar mit einer Geldbuße bis zu 250.000 Euro geahndet werden (§ 43 Abs. 2, 3 BDSG). Erfolgt die Tat in Bereicherungs- oder Schädigungsabsicht, kommt auch die Einleitung eines Strafverfahrens in Betracht (§ 44 BDSG). Das ist zumindest dann denkbar, wenn Spyware solche Funktionen nutzt, die alle Tastatureingaben mitloggen und diese übermitteln. Dadurch würden auch geheime Zugangsdaten protokolliert und übermittelt. Im Extremfall versendet der Spion auf der Festplatte die Zugangsdaten zum eigenen Bankkonto.

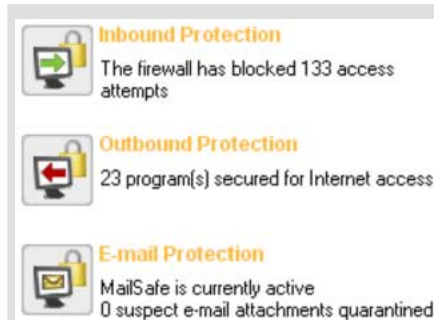
Hartnäckige Spione

Das besonders Heimtückische an Spyware ist ihre Hartnäckigkeit. Denn selbst wenn man verseuchte Programme vom Rechner löscht, verbleiben häufig gewisse DLL-Dateien und Registry-Einträge weiter auf dem Rechner. Und sie übermitteln auch weiterhin und unbremst Informationen über die eigenen Surfgewohnheiten an die entsprechenden Hersteller.

Um seinen eigenen PC vor Spyware zu schützen, eignet sich das Tool Ad-Aware [9] von Lavasoft. In der kostenlosen Version filtert es die bekanntesten Akteure aus dem Spyware-Bereich und hält vor allem die Registrierungsdatenbank von Windows sauber. Die Plus-Version für rund 19 € enthält eine Erweiterung, die mit fast allen Spy-Systemen zurechtkommt, also auch Systeme wie Cydoor [10] und Doubleclick [11] aufspürt und das sogar in Echtzeit während einer Neuinstallation.

Schutz durch Firewall

Die beste Wahl ist eine Firewall auf dem eigenen Rechner, die den Spionagetools weitgehend das Handwerk legt. Desktop-Firewalls wie Zone Alarm untersuchen sämtlichen ein- und ausgehenden Datenverkehr auf gefährliche Inhalte. Einige testen potenziell schädli-



Zone Alarm: Hier wird angezeigt, wie viele Zugriffe auf den Rechner die Firewall registriert hat. Unten: Diesem Buch aus dem Verlag Markt und Technik, das die Anwendung von Zone Alarm haarklein und verständlich erklärt, liegt eine CD mit der Vollversion bei.

Auch andere PC-Schutzprogramme werden vorgestellt. Dazu gibt's Tipps, wie man sein Computer-System optimal einstellt, Filter konfiguriert, E-Mails verschlüsselt u.v.m. ISBN: 3827262895



che Anwendungen sogar zuerst in isolierter Umgebung auf ihre tatsächliche Gefahr. Diese Variante führt je nach Rechnerleistung leider zu einiger Verzögerung.

Im Gegensatz zu den inzwischen weit verbreiteten Virenskannern kennen neue Desktop-Firewalls keine Muster gefährlicher Programme mehr. Sie funktionieren nach einem letztlich ebenso einfachen wie wirkungsvollen Prinzip, das sich deren Entwickler vom Java-Entwickler Sun [12] abgeschaut hat: Prinzipiell ist alles erlaubt, solange die eingehenden Applikationen nicht versuchen, auf Systemressourcen wie Laufwerke oder Dateien zuzugreifen. Damit wird auch vermieden, dass die Firewall-Software ständigen Updates unterliegt. Ein weiteres Plus liegt darin, dass sogar fehlerhaft programmierte Applikationen lauffähig bleiben, ohne Schaden anrichten zu können. Sie führen die Applikationen in einer sicheren Umgebung aus, der so genannten Sandbox (Sandkasten). Nur lokale Anwendungen haben einen vollständigen Zugriff.

Allen Firewall-Systemen ist gemeinsam, dass sie sämtliche Ports (Datenausgänge) überwachen. Die Ports ermöglichen parallel arbeitende Dienste wie Internet, Mail oder Datenübertragung. Alle Standard-Dienste verwenden immer denselben zugeordneten Port, für Internet beispielsweise Port 80, für Mailverkehr per SMTP (Simple Mail Transfer Protocol) standardmäßig Port 25 und Mails per POP (Post Office Peer-to Peer Protocol) Port 110. Viele Anwendungen nutzen eigene Ports. So verwendet die „advert.dll“ der Aurore-Software beispielsweise Port 1749. Will man die dauernden Warnmeldungen einer bestimmten Anwendung vermeiden, muss man den Zugriff über diesen Port in der Desktop-Firewall explizit zulassen. Kennt man eine

Anwendung nicht, so sollte man dies allerdings tunlichst vermeiden.

Schwieriger und teilweise sogar unmöglich wird es selbst für die Desktop-Firewalls, wenn die Spyware ihre Daten über den Port 80 nach außen schafft, denn der wird schließlich für den Internetzugang benutzt. „Darüber hinaus gibt es sogar Programme, die sich zum Beispiel als so genanntes Browser Help Objects (BHO) im Internet Explorer installieren. Andere wiederum täuschen einfach vor, dass sie der gerade verwendete Internet-Browser seien“, so der Spyware-Experte Markus B. aus Hannover. „Auf jeden Fall aber schafft eine Firewall eine gewisse Sicherheit, nur hundertprozentig sicher kann man sich leider nie sein. Die beste Sicherheit kann man erreichen, wenn man Anti-Spyware mit einer Desktop-Firewall kombiniert und bei neuen Programmen immer mit dem Schlimmsten rechnet.“

Preiswerter Schutz

Wer keine Angst vor dem Einsatz englischsprachiger Software hat, kann sich gut und teilweise sehr preiswert auf dem Sharewaremarkt bedienen, als Privatperson mitunter sogar kostenlos. Ein bekanntes Programm ist „ZoneAlarm“ [13], das alle Windows-Betriebssysteme unterstützt. Es ist für Privatanwender sogar kostenfrei und arbeitet sehr effektiv. Eine deutsche Anleitung findet sich im Internet unter der Adresse www.zonealarm.de.

Hilfreiche Links

- [1] Tool XP-Antispy – www.xp-antispy.de
- [2] RealNetworks – www.realnetworks.com
- [3] Big Brother Award – www.big-brother-award.de/2001/.tec/
- [4] FoeBuD e. V. – www.foebud.org
- [5] Eintragungs-Software HelloEngines – www.hello-engines.de
- [6] soffTrans – www.softtrans.de (www.acebit.de)
- [7] Promo- und Rankware – www.iok.net
- [8] Berliner Datenschutzbeauftragten – www.datenschutz-berlin.de
- [9] Ad-Aware – www.lavasoftusa.com/downloads.html
- [10] Cydoor – www.cydoor.com
- [11] Doubleclick – www.doubleclick.com
- [12] Sun – www.sun.com
- [13] ZoneAlarm – www.zonelabs.com/store/content/home.jsp

So erkennt man Spyware

- verminderte Rechenleistung, Browser wird langsamer (kann auch andere Ursachen haben)
- veränderte oder zusätzliche Menüleisten im Browser
- unbekannte Icons in der Taskleiste
- häufige Pop-Up-Banner, auch bei Seiten, die derartige Werbung eigentlich gar nicht geschaltet haben
- es erscheint eine andere Browser-Startseite als die von Ihnen eingestellte

Spyware-Listen und -Datenbanken

Datenbanken: www.spychecker.com
www.tom-cat.com/spybase/index.html
www.cyberspalace.de/hm/sicher1.htm