

Zusammenfassung

Spyware ist ein Programm, das den User ausspioniert. Diese kleinen Programme gelangen über im Internet verbreitete und zum Download bereitstehende Software (Freeware und Shareware,

daher meist kostenlos), aber auch per CD-ROM und DVD auf die Rechner. Bestimmte proprietäre Softwareprogramme enthalten ebenfalls Spyware.

Inhalt

- 1 Was ist Spyware? →
- 2 Wer ist betroffen? →
- 3 Wie funktioniert Spyware? →
- 4 Ist Spyware legal? →
- 5 Vorbeugende Massnahmen →



1 Was ist Spyware?

Spyware ist ein Softwareprogramm, das den User ausspioniert. Es ist ein Haupt- oder Unterprogramm, das entwickelt wurde, um persönliche Daten über seinen Anwender, ohne dessen vorherige Genehmigung, zu erfassen und über das Internet oder ein beliebiges anderes EDV-Netz an seinen Entwickler oder an Dritte zu

senden. Spyware hat zum Ziel die Gewohnheiten des Internetnutzers auszuspionieren und die erfassten Informationen anschliessend, ohne sein Wissen, an die Urheber und Entwickler der Software zu übertragen, um eine gigantische Datenbank mit Informationen zu versorgen.

2 Wer ist betroffen?

Alle Personen, die das Internet nutzen, sind betroffen. Die Zahl der betroffenen Anwender lässt sich nur schwer einschätzen, da die Spyware im Allgemeinen im Hintergrund und völlig ohne Wissen des Computerbesitzers ausgeführt wird. Und selbst wenn sich die Anwender über die Existenz bewusst sind, sehen viele die Spyware nicht als eine Bedrohung sondern höchstens als irgend-

einen Nachteil an. Sie unternehmen daher nichts, um die Spyware zu beseitigen, und warnen ihren Netzwerkadministrator nicht. Die explosionsartige Zunahme von Spam-Mails in den vergangenen zwei Jahren ist jedoch ein Beleg für den Ernst des Spyware-Problems.

3 Wie funktioniert Spyware?

Spyware wird im Allgemeinen beim Surfen im Internet oder beim Laden von kostenlosen Programmen (Freeware) oder Werbefprogrammen (Adware) eingefangen. Am häufigsten ist Spyware in Instant Messaging Programmen (ICQ), Audioprogrammen (RealPlayer) und "Peer-to-Peer"-Programmen

(Kazaa, Limewire) zu finden. Die Spyware selbst ist ein autonomes Programm oder mit einem zu einem anderen Zweck dienenden Programm verknüpft. Spyware verwendet also Techniken aus dem Social Engineering oder der Trojanischen Pferde an.

3.1 Spyware-Typen

„**Zu Werbezwecken dienende Spyware**“ erfasst Daten über die Anwender und interagiert sichtbar mit ihnen, indem sie die Anzeige von gezielten Werbebannern generiert, die Anzeige von Pop-up-Fenstern auslöst oder den Inhalt der besuchten Webseiten verändert, um beispielsweise kommerzielle Links hinzuzufügen. Dies ist die gängige Spyware. Ihre Existenz wird normalerweise in der Lizenzvereinbarung der betroffenen Software erwähnt, häufig jedoch in zweideutigen Ausdrücken und/oder in einer Fremdsprache, was zur Folge hat, dass der Anwender nicht richtig informiert ist.

„**Spione**“ erfassen ebenfalls Daten über den Benutzer, dies geschieht jedoch völlig im Verborgenen. Die Überwachung und die mögliche Weiterverwendung der erfassten Daten erfolgen ohne Wissen des Benutzers. Die Daten dienen im Allgemeinen statistischen Zwecken, dem Marketing, zum Debuggen oder zur technischen Wartung bzw. zur Überwachung des Cyber Space. Die Existenz dieser Spionageprogramme wird den Benutzern bewusst verschwiegen.

„**Integrierte (oder interne) Spyware**“ ist eine Routine, die in den Quellcode einer Software, die über eine eigene Funktion verfügt, integriert wurde, um es ihr zu ermöglichen, Informationen zu erfassen und über das Internet zu übertragen. Diese Spyware wird separat heruntergeladen oder bei der Installation anderer kostenloser Programme, bei denen es sich im Allgemeinen ebenfalls um Spyware handelt, aufgrund von Abkommen zwischen den Urhebern der Software angeboten. Dies ist insbesondere bei Gator, New.net, SaveNow, TopText, Alexa und Webhancer der Fall.

Während der Anwender im Internet surft, kann die auf seinem Computer gespeicherte Spyware Informationen erfassen, die sein System verlangsamen oder die Vertraulichkeit oder

Integrität seiner Daten gefährden. Diese Spyware kann die Liste der besuchten Internetseiten speichern, das Verlaufsprotokoll des Internet-Browsers, die Cookies, die Informationen über die installierten Programme und sogar die auf der Festplatte vorhandenen Daten untersuchen und ausnutzen. Spyware stellt eine Verletzung der Privatsphäre der Opfer dar.

„**Externe Spyware**“ ist eine autonome Anwendung. Sie ist mit einer anderen Software verknüpft und kommuniziert mit jener. Ihre einzige Funktion besteht darin sich der „Client Relation“ zu bemächtigen: Datenerfassung und -übertragung, Anzeige von Werbebannern etc. Diese Spyware wird von Werbeunternehmen oder spezialisierten Unternehmen wie etwa Radiate, Cydoor, Conducent, Onflow oder Web3000 entwickelt, mit denen Urheber von Softwareprogrammen ebenfalls Abkommen abschließen. Die Spyware von Cydoor ist beispielsweise mit der „Peer-to-Peer“-Software KaZaA verknüpft und wird gleichzeitig mit dieser Software installiert.

3.2 Exemples

Cydoor - ist eine Spyware, die während des Surfens im Internet Pop-up-Fenster öffnet. Ausserdem leitet Sie alle Internet-Anfragen an Drittserver weiter, um Ihre Gewohnheiten zu erfassen. Cydoor kann nicht mittels der Windows-Funktion „Uninstall“ deinstalliert werden, und es steht keine Deinstallationsroutine zur Auswahl.

Gator - bietet eine scheinbar nützliche Funktion an, die jedoch sehr gefährlich ist. Das Programm bietet die Möglichkeit, sich den Namen des Anwenders, Passwörter und die Informationen der für den Zugang zu e-Commerce-Seiten verwendeten Karten zu merken. Diese Informationen werden auf Ihrem Computer gespeichert. Obwohl die Daten verschlüsselt werden, können sie von Gator oder von Eindringlingen abgefragt werden.

4

Ist Spyware legal?

Laut der europäischen Gesetzgebung hat „jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz“ (Konvention zum Schutze der Menschenrechte und Grundfreiheiten). Die Richtlinie 95/46 der Europäischen Gemeinschaft besagt, dass personenbezogene Daten, daher alle Informationen über eine bestimmte oder bestimmbar natürliche Person, und die Verarbeitung dieser Daten „...ohne ausdrückliche Einwilligung der betroffenen Person“ unzulässig ist. “

Die Richtlinie 2002/58 der Europäischen Gemeinschaft behandelt den Status von Spyware und anderen gleichartigen Technologien. Sie besagt folgendes: „(...) So genannte „Spyware“, „Web-Bugs“, „Hidden Identifiers“ und ähnliche Instrumente können ohne das Wissen des Nutzers in dessen Endgeräte eindringen. Sie können Zugang zu Informationen

erlangen, oder die Nutzeraktivität zurückzuverfolgen. Damit können sie eine ernsthafte Verletzung der Privatsphäre dieser Nutzer darstellen. Die Verwendung solcher Instrumente sollte nur für rechtmässige Zwecke mit dem Wissen der betreffenden Nutzer gestattet sein. “

Die Gesetzgebung schützt also die Rechte des Internetnutzers. Wenngleich einige Fälle vor Gericht gelandet sind (zum Beispiel der Fall des Unternehmens Doubleclick, das im Jahr 2002 in den USA zur Zahlung von 450.000 Dollar und zur Wahrung der Privatsphäre der Internetnutzer verklagt wurde), fällt jedoch jedes, mit der Nutzung des Internets in Zusammenhang stehende Problem, nur schwer in einen legalen Rahmen. Bis die rechtliche Seite eindeutig geregelt ist, kommt der Internetnutzer nicht umher, Massnahmen zu ergreifen, um sein Privatleben zu schützen.

5

Vorbeugende Massnahmen

Der Schutz vor Spyware ist nicht einfach. Eine Anti-Virus-Software erkennt sie nicht, da es nicht den gesamten Programmcode prüft, sondern sich auf die Erkennung zuvor identifizierter Signaturen beschränkt. Ausserdem ist Spyware kein Virus. Die Verwendung einer richtig konfigurierten Firewall (eine Firewall, die gleichzeitig die ein- und ausgehenden Datenströme analysiert) kann eventuell Spyware erkennen, die versucht, Daten nach aussen zu senden. Wenn der Rechencode jedoch zum Senden einer Datei per E-Mail an einen unerwünschten Empfänger führt, hat die Firewall keine Möglichkeit zu erkennen, ob eine E-Mail absichtlich oder ohne Wissen des Anwenders gesendet wird und blockiert den Versand daher nicht. Eine der existierenden Möglichkeiten zur Erkennung einer Spyware auf einem Rechner ist die Beobachtung des Paketflusses. Ist dieser wesentlich höher als der üblicherweise über die Firewall oder das Modem fliessende Paketstrom, könnte Spyware auf dem Rechner installiert sein. Aber selbst dann ist diese nur schwer zu identifizieren.

Es gibt im Internet zahlreiche Webseiten, die auf Spyware verweisen. Aber keine dieser Seiten kann für sich beanspruchen, über eine umfassende Liste der existierenden Spyware-Programme zu verfügen. Ebenso ermöglichen bestimmte Tools die Erkennung von Softwareprogrammen, die mit Spyware verknüpft sind, aber die Verwendung dieser Tools gewährleistet keinen 100%igen Schutz des PC.

Aus diesen Gründen wurden Anti-Spyware-Programme nach dem Modell von Anti-Viren-Programmen entwickelt. Diese erkennen Spyware auf der Grundlage von Signaturen. Die selbst von Laien leicht zu bedienenden Programme ermöglichen das Aufspüren von Spyware, selbst wenn diese nicht aktiv ist. Eine permanente Aktualisierung der Signatordateien ist jedoch unbedingt erforderlich.

Nützliche Links:

- ➔ <http://www.spychecker.com/>
Spyware-Suchmaschine
- ➔ <http://www.zonealarm.com/>
Persönliche Firewall von ZoneLabs
- ➔ <http://www.lavasoftusa.com/default.shtml.en>
AdAware - Anti-Spyware von Lavasoft
- ➔ <http://www.safer-networking.org/fr/index.html>
Spybot - Anti-Spyware
- ➔ <http://www.cases.public.lu/publications/dossiers/spyware/index.html>
Anti-Spyware von Microsoft