

Der Spyware-Konflikt – Datenschutz versus Profit

von Trend Micro

In den vergangenen drei Jahren waren die meisten Antiviren-Hersteller intensiv mit der Entwicklung neuer Strategien im Kampf gegen Spyware beschäftigt. Spyware-Programme protokollieren Benutzeraktivitäten, Surf-Gewohnheiten und getätigte Online-Käufe. Da Spyware im Hintergrund ausgeführt wird, nehmen Benutzer sie meist nicht wahr.

Werbeagenturen nutzen die durch Spyware erstellten Benutzerprofile für zielgruppengerechte Popup-Anzeigen. Spyware, die ausschließlich zu Werbezwecken eingesetzt wird, ist auch unter den Bezeichnungen „Grayware“ oder „Adware“ bekannt. Sie ist zwar unerwünscht, richtet jedoch im Gegensatz zu anderen Arten von Spyware meist keinen Schaden auf dem Computer an.

Spyware/Adware – eine Definition

Ärgernis Spyware

Obwohl Spyware in den meisten Fällen als lästig empfunden wird, besteht in der Regel kein Grund zur Panik. Die meisten Programme fallen in die Kategorie „Grayware“. Werbeagenturen nutzen sie, um Web-Browser auf bestimmte Seiten umzuleiten. Der Inhalt der dort angezeigten Werbebanner ist auf Grund der gesammelten Daten aus Suchanfragen, Surf-Gewohnheiten und getätigten Online-Käufen genau auf den Benutzer zugeschnitten. Die meisten Benutzer empfinden diese Form von Grayware als Angriff auf die Privatsphäre. Sie beklagen sich außerdem über unerwünschte Unterbrechungen und Produktivitätseinbußen. Die weitergehende Verwendung der ausspionierten und aufgezeichneten Benutzerdaten wirft darüber hinaus die Frage nach dem Datenschutz auf. Durch Grayware ermittelte Informationen können problemlos über das Internet verschickt und dann an Dritte verkauft oder weitergegeben werden.

Außer den ärgerlichen Popup-Fenstern, Browser-Hijacks und Datenschutzproblemen zählt vor allem die Beeinträchtigung der Systemleistung zu den Nebenwirkungen dieser Art von Programmen. Ed English, General Manager for Consumer Products beim Sicherheitsspezialisten Trend Micro, weiß, dass Spyware-Infektionen katastrophale Folgen haben können: „Auf einem einzigen Computer können unzählige Spyware- und Adware-Programme installiert sein. Hier nimmt die Anzahl von Popup-Fenstern schnell überhand, und die Systemleistung kommt zum Erliegen.“ „Die Installation der Grayware erfolgt übrigens meistens ohne Wissen und Einverständnis des Benutzers“, so English weiter.

Bösartige Spyware

Die eingesetzten Spyware-Techniken können jedoch auch für andere Zwecke, wie dem Sammeln von Kennwörtern, Kreditkartennummern und sonstigen vertraulichen Daten, missbraucht werden. Obwohl diese Art von Spyware nach Schätzungen von Trend Micro nur etwa 5% aller Spyware-Infektionen ausmacht, stellt sie trotzdem ein ernstzunehmendes Problem dar.

Laut einer Studie des Poinemon Instituts wurden im Jahr 2004 84% der befragten Benutzer Opfer von Spyware.

Besorgniserregend sind vor allem der hohe Verbreitungsgrad von Spyware und das Motiv für die Programmierung. Das einzige Motiv hinter der Programmierung bössartiger Spyware besteht in der Absicht, sich mit Hilfe der gestohlenen Informationen zu bereichern. Ausspioniert werden Kennwörter, Kreditkartennummern oder andere vertrauliche Daten, um Geld von Bankkonten abzuheben, im Internet einzukaufen oder sogar neue Konten unter fremdem Namen zu eröffnen.

Spyware kommt auch in der Industriespionage zum Einsatz. So erfuhr die Öffentlichkeit vor kurzer Zeit von einem spektakulären Fall, in dem ein Spyware-Programm E-Mails und andere vertrauliche Daten auf den Computern eines Unternehmens sammelte und an eine Konkurrenzfirma weiterleitete. Auch Ämter und Behörden müssen sich mit der Spyware-Problematik auseinandersetzen. Laut einem aktuellen Bericht des US-amerikanischen Government Accountability Office (GAO) verursachte Spyware in 11 von 24 befragten Behörden Produktivitätsausfälle oder vermehrte Help-Desk-Anfragen.

Grayware hingegen soll das Surf-Verhalten und besondere Interessen von Benutzern ausspionieren, damit die Werbeaktionen besser an die Zielgruppe angepasst werden können. Der Markt für Technologien zum Erstellen von Benutzerprofilen wird auf 1,4 bis 2 Milliarden US-Dollar geschätzt.

Die rechtliche „Grauzone“

Spyware bzw. Adware wird als „Grayware“ bezeichnet, wenn sie nicht ausschließlich gute oder schlechte Eigenschaften hat.

Die meisten Benutzer empfinden Spyware/Grayware als Eingriff in die Privatsphäre und sind deshalb auf der Suche nach Tools, mit denen Spyware blockiert und entfernt sowie Neuinfektionen verhindert werden können. Da Spyware jedoch erst installiert wird, nachdem der Benutzer dem Lizenzvertrag (EULA) zugestimmt hat, sei Grayware nach Meinung ihrer Hersteller völlig *legal*. In letzter Zeit kam es vermehrt zu Anzeigen von

Grayware-Herstellern, die Anbietern von Sicherheits-Software die Entwicklung und Implementierung von Anti-Spyware-Lösungen untersagen wollten.

Die Sicherheitsbranche fordert nun ihrerseits Gesetze, die den Vertrieb von Anti-Spyware auf ein sicheres rechtliches Fundament stellen. Benutzer sollen die Möglichkeit haben, nach unerwünscht installierten Programmen zu suchen und diese zu entfernen. Auch Informationen über die Funktionsweise von Grayware und Spyware sollen weiterhin frei verfügbar sein.

Wissen ist Macht

In vielen Staaten prüft man derzeit Gesetzesentwürfe zum Schutz von Benutzern vor Spyware und Grayware. Eine einheitliche Gesetzgebung in den einzelnen Ländern ist allerdings nicht zu erwarten. Die Verbreitung von Spyware wird aber auch durch ein Verbot nicht verhindert werden können. Abgesehen von leistungsstarker Technologie bleibt die Aufklärung der Benutzer deshalb die wichtigste Verteidigungstaktik im Kampf gegen unerwünschte Computer-Programme.

Die Sicherheitsexperten von Trend Micro weisen darauf hin, dass es vor allem wichtig ist, die Endbenutzer-Lizenzvereinbarung aufmerksam zu lesen. Vor dem Klick auf die „Akzeptieren“-Schaltfläche sollte sich der Benutzer über die möglichen Folgen des Software-Downloads im Klaren sein. Endbenutzer-Lizenzvereinbarungen enthalten nicht selten Klauseln, die den Software-Anbieter dazu berechtigen, weitere Programme ohne Ankündigung auf dem Computer zu installieren. Einige Lizenzvereinbarungen verlangen, dass der Benutzer auf seine Datenschutzrechte verzichtet und der Aufzeichnung seiner Computer-Aktivitäten und Eingaben (z. B. von Kennwörtern oder PINs) zustimmt.

Lizenzvereinbarungen, die folgende Klauseln enthalten, sollte der Benutzer grundsätzlich nicht zustimmen:

- Jederzeit beliebige Informationen und Angebote des Anbieters sowie seiner Partnerfirmen und Kunden an den Benutzer zu senden.
- Von der Internet-Verbindung des Benutzers Gebrauch zu machen.
- Den Computer des Benutzers beliebig zu nutzen oder anderen Parteien den Zugriff darauf zu ermöglichen.
- Dateien auf dem Computer des Benutzers zu speichern bzw. von dort herunterzuladen.

- Ohne Ankündigung oder Einverständnis seitens des Benutzers Software anderer Hersteller auf dem Computer des Benutzers zu installieren.
- Undeutliche Bestimmungen bezüglich des Rechts des Benutzers, die Software oder Programme anderer Hersteller nach Anklicken von „Akzeptieren“ zu deinstallieren sowie ein begrenztes Recht zur Beendigung der Vereinbarung seitens des Benutzers.
- Erlaubnis zum Sammeln vertraulicher Daten auf dem Computer des Benutzers. Geringe Einschränkungen bezüglich der Auswahl dieser Daten, deren weiterer Verwendung und eventueller Nutznießer.
- Inhalte der Lizenzvereinbarung (inklusive der Datenschutzbestimmungen) jederzeit unangekündigt und ohne Einverständnis des Benutzers zu ändern. In vielen Fällen wird vom Spyware-Hersteller darauf hingewiesen, dass der Benutzer gehalten ist, sich auf der Website des Anbieters über mögliche Änderungen zu informieren.

Spyware ohne Lizenzvereinbarung

Zusätzlich zu den oben genannten Argumenten, die widerlegen, dass eine Lizenzvereinbarung für die Spyware-Industrie eine rechtlich einwandfreie Basis schaffen würde, verzichten manche Hersteller sogar völlig auf die *Endbenutzer-Lizenzvereinbarung*. Die Produkte dieser Hersteller werden beim Download anderer Programme oder beim Hijacken rechtmäßiger Software praktisch „beiläufig“ mitinstalliert. Dieser Vorgang findet ohne Ankündigung und ohne Einverständnis des Benutzers statt.

Dazu meint Ed English: „Ein Benutzer, der eine Website besucht, auf der Spyware zum Download angeboten wird, kann in der Regel davon ausgehen, dass diese Programme keinen Schaden anrichten, rückstandslos deinstalliert werden können und die Lizenzvereinbarungen unmissverständlich formuliert sind. Da die Website des Herstellers aber nicht der einzig mögliche Vertriebskanal für die Spyware ist, kann noch keine Entwarnung gegeben werden. Selbst wenn auf der Website rechtlich unbedenkliche Programmversionen angeboten werden, können sich Benutzer auch anderswo mit der Spyware infizieren, z. B. beim Download rechtmäßiger Software aus dem Internet. In solchen Fällen gibt es dann natürlich weder Lizenzvereinbarungen noch Deinstallationsprogramme.“

Woher kommen also diese Spyware-Versionen und wie gelangen sie auf den Computer? Eine typische Infektionsquelle sind Websites mit pornografischen Inhalten. Viele dieser Seiten installieren ohne Ankündigung oder Zustimmung des Endbenutzers Spyware auf dem Computer. Die Betreiber wissen, dass Besucher solcher Websites gerne anonym bleiben. Selbst wenn die Spyware entdeckt wird, bleiben Beschwerden aus. Je anstößiger der Inhalt, umso idealer der Nährboden für Spyware.

Wissen als Waffe im Kampf gegen Spyware

Laut David Perry, dem Global Director of Education bei Trend Micro, können Benutzer ihr Infektionsrisiko reduzieren, indem sie einige klare Verhaltensregeln befolgen und die genannten Spyware-Fallen umgehen. „Sind Spyware-Programme erst einmal installiert, lassen sie sich nur schwer aufspüren und entfernen. Benutzer müssen hier in aller Regel auf den Einsatz professioneller Sicherheits-Software zurückgreifen.“

Perry betont außerdem, dass man als Benutzer eine Lizenzvereinbarung in unbekannter Software nicht einfach „wegklicken“ sollte, ohne sich darüber zu informieren, welche Bestimmungen sie enthält. Für ihn ist das Internet „nur dann eine Bereicherung, wenn die Benutzer auch die Risiken kennen und dementsprechend handeln. Surfen macht nur mit der Gewissheit Spaß, dass keine wildfremden Personen an Ihrem Online-Leben teilhaben.“

Lösung in Sicht

Die Antiviren-Branche entwickelt sich zunehmend zu einer Branche für Computersicherheit. Sowohl Privatanwender als auch Firmenkunden erwarten von ihrem Sicherheitsanbieter immer zuverlässigeren Schutz, um Risiken zu erkennen und vorzubeugen.

Benutzer müssen sich in Zukunft noch stärker für ihr Recht einsetzen, Programme nach Belieben zu löschen und die automatische Installation unerwünschter Software zu unterbinden. Benutzer sollten *keinesfalls* Lizenzvereinbarungen akzeptieren, deren Bestimmungen dieses Recht in irgendeiner Art und Weise einschränken, da sie sonst selbst eine rechtliche Grundlage für den Datenmissbrauch schaffen.

Da kein Ende der Spyware-Problematik abzusehen ist, können die Bedeutung von Benutzerrechten und das Engagement von Sicherheitsexperten nicht hoch genug eingeschätzt werden. Spyware, wie wir sie heute kennen, wird durch neue Technologien abgelöst werden, die vor der Privatsphäre der Benutzer nicht Halt machen. Vor allem die

Sicherheitsexperten sind gefragt. Sie müssen neue Strategien entwickeln, um die Benutzer vor Datenmissbrauch und moralisch bedenklichen Methoden zu schützen.

Benutzerrechte und Aufklärungskampagnen stehen also heute und in Zukunft im Mittelpunkt erfolgreicher Verteidigungsstrategien.

Für weitere Informationen über Trend Micro klicken Sie bitte hier: <http://www.trendmicro.de/tc>