

## IT-SICHERHEIT

# Spyware – eine ernstzunehmende Gefahr

Die richtigen Informationen zur richtigen Zeit ist ein sehr wertvolles Gut. Doch die Beschaffung dieser Informationen ist nicht einfach. Eine illegale Variante um an diese Informationen zu gelangen, ist Spyware.

AUTOR: ANDREAS WISLER

**N**ach einer langen Entwicklungszeit hat Microsoft vor wenigen Tagen das Programm Defender herausgegeben. Es durchsucht den eigenen PC nach schädlichen Softwareteilen. Findet es solche, schlägt es Alarm. Defender wird in der kommenden Windowsversion Vista integriert sein, Windows XP Benutzer können es kostenlos von der Microsoft Homepage beziehen. Defender ist aber nicht das einzige Programm, das sich gegen unerwünschte Software zur Wehr setzt. Dies beweist eindrücklich, dass Spyware eine ernstzunehmende Gefahr darstellt.

## Was ist Spyware?

Als Spyware wird üblicherweise Software bezeichnet, die persönliche Daten eines PC-Benutzers, meist ohne dessen Wissen oder Zustimmung an eine dritte Person sendet. Teilweise werden die Informationen nur dazu verwendet, Werbung nach dem Geschmack der überwachten Person anzubieten. Zunehmend werden aber detaillierte Personenprofile erstellt, die für viel Geld an weitere Firmen verkauft werden.

## Wie funktioniert Spyware?

Ziel der Software ist es, dass diese bei jedem Einschalten des Computers mitgestartet wird und zwar so, dass es durch den Benutzer nicht erkannt werden kann. Immer ausgefeiltere Varianten versuchen sich so zu tarnen, dass sie auch durch Personal Firewalls nicht erkannt werden. Einmal gestartet zeichnet Spyware jede Tätigkeit des Benutzers auf. Sei dies nur

der Start von lokalen Programmen oder der Besuch von Internetseiten. In einigen Fällen wird sogar versucht, die Startseite des Browsers auf eine andere Seite umzulenken. Als besonders gefährlich gelten sogenannte Keylogger, die gleichzeitig mit den Programmen und Internetseiten auch jeden Tastenschlag aufzeichnen und an den Hersteller des Programms senden. Somit ist jedes E-Mail, jeder Brief oder gar jede Transaktion in einer Finanzapplikation aufgezeichnet und öffentlich.

## Wie bekommt man Spyware?

Niemand wird freiwillig Software installieren, in der sich Spyware versteckt. Aus diesem Grund müssen andere Wege gefunden werden. Der Einfachste ist, das Programm in einem anderen zu verstecken. Ein Trojanisches Pferd ist geboren. Aus juristischen Gründen ist bei vielen bekannten Spyware-Programmen sogar ein Hinweis in den allgemeinen Bestimmungen „versteckt“. Da diese jedoch nur in den wenigsten Fällen gelesen werden, ist der Weg frei, sich juristisch korrekt einzunisten. Die dreisteren Programme installieren sich durch Lücken in der eingesetzten Software, sei dies nun per Email (zum Beispiel via Outlook oder Outlook Express) oder per Browser (etwa beim Internet Explorer durch ActiveX). Eine weitere Variante sind Würmer, die sich selbständig durch das Internet bewegen und alle ungeschützten Systeme auf ihrem Weg infizieren.

## Wie erkenne ich Spyware?

Ein gutes Spyware-Programm werden Sie nicht ohne weiteres erkennen. Hier helfen nur Tools wie Defender oder Spybot Search &

Destroy weiter. „Billige“ Spyware erkennt man durch manipulierte Startseiten, dem wilden Öffnen von Werbefenstern ohne einen

## ZUM AUTOR

**Andreas Wisler** (Tel. 052 320 91 20), Dipl. Ing. FH, CISSP, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produkteneutralen IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. System Hardening rundet das Portfolio ab. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf [www.gosecurity.ch](http://www.gosecurity.ch) (INFONEWS) heruntergeladen werden kann. Für Blickpunkt:KMU beleuchtet er in jeder Ausgabe einen neuen Aspekt der IT-Sicherheit.



Zusammenhang zu getätigten Schritten, zusätzlichen Links in den Favoriten oder durch die Personal Firewall, welche ständig Verbindungen von lokalen Programmen ins Internet meldet.

#### Hilfe zur Selbsthilfe

An dieser Stelle kann kein Leitfaden zum Entfernen jeglicher Spyware gegeben werden. Dazu sind die Methoden einfach zu raffiniert. Sollte ein spezialisiertes Programm die Spyware nicht entfernen können, gilt es als Erstes herauszufinden, welchem Schädling man aufgesessen ist. Mit diesen Informationen gelingt es, im Internet nach der richtigen Vorgehensweise zu recherchieren. Für die meisten uns bekannten Spyware-Programme gibt es Anleitungen zum Entfernen. Neben den Ratgebern von Antiviren-Herstellern ist die Webseite <http://www.wintotal.de/Spyware/> ein guter Anlaufpunkt. Bei beinahe allen Methoden sind aber gute Kenntnisse im Bearbeiten der Registry und dem Umgang mit dem abgesicherten Modus notwendig.

#### Schutzmöglichkeiten

Damit dies gar nicht erst passieren kann, lohnt sich der Einsatz eines aktuellen Antivirenprogrammes. Viele Antivirenhersteller haben ihre Programme mit Spyware-Filtern und Erkennungsroutinen ausgerüstet. Doch ein Antivirenprogramm hilft nur, wenn auch das System aktuell ist. Installieren Sie dazu die regelmässig erscheinenden Patches. Weiter lohnt es sich, aktive Inhalte gezielt im Browser zu blockieren (beispielsweise im Internet Explorer unter Extras – Internet-Optionen – Sicherheit). Achten Sie zusätzlich bei jedem Programm darauf, was wirklich installiert wird. Lesen Sie bei Unsicherheiten die allgemeinen Bedingungen durch. Auch wenn die Versuchung gross ist, meiden Sie Webseiten mit illegalen Tools und Programmen. Hier ist die Gefahr am grössten, sich zu infizieren.

Zusätzlich gilt es im E-Mail-Programm die verfügbaren Schutzmöglichkeiten zu aktivieren. Dies sind zum Beispiel: Ausschalten der automatischen Vorschau von E-Mails und dem Download von zusätzlichen Bildern und Programmen.

Wenn Sie die obenstehenden Tipps bei Ihren Ausflügen im Internet beachten, sind Sie auch in Zukunft vor Spyware und anderen schädlichen Programmen geschützt. ◆

# InfoStore DMS

Document Management Solutions



## Sichern Sie die Infrastruktur Ihrer Prozesse.



**InfoStore ist eine Entscheidung für Sicherheit und Transparenz, für mehr Zuverlässigkeit und Effizienz in mittelständischen Unternehmen. Ob für Document-Management, Workflow oder Archivierung, Geschäftsprozessanalyse oder Effizienz bei der Kundenbetreuung. Nutzen Sie die Erfahrung aus über 900 Kundenprojekten. Unterschiedliche IT-Umgebungen, ERP-Systeme oder hochspezialisierte Branchenlösungen – InfoStore passt sich Ihren individuellen Anforderungen an. Überzeugen Sie sich unter:**

[www.solitas.com](http://www.solitas.com) oder [info@solitas.com](mailto:info@solitas.com)

TeL. +41 81 755 55 00

Fax +41 81 755 55 01

Solitas Informatik AG  
Bahnhofstrasse 21b  
9471 Buchs – Switzerland

**SOLITAS**