SECURITY
FACHARTIKEL

von Sarah Gordon, Virenexpertin,
Symantec Security Response

Die heimlichen Besucher

Spyware und Adware haben sich von simplen Cookies zu ausgefeilten Überwachungsprogrammen gemausert. Das hat viele Internetnutzer kalt erwischt: Sie haben meist keine Ahnung, dass es auf ihrem Computer vor digitalen Spitzeln nur so wimmelt.

Ein nicht unbeträchtlicher Teil an persönlichen Informationen wird heutzutage online weitergegeben. Immer mehr Menschen verschicken tagtäglich E-Mails, erledigen ihre Bankgeschäfte online oder gehen im Netz einkaufen. Die fortschrittlichen Möglichkeiten, die das Internet bietet, wiegen seine Benutzer jedoch in trügerischer Sicherheit. Neuere Technologien und Übertragungswege wie DSL zusammen mit einer höheren Computergeschwindigkeit sind auch für bösartige Programme von Vorteil: Sie verbreiten sich noch schneller, exportieren vertrauliche Daten und lassen Computersysteme abstürzen.

Geheime Beutezüge

Viren, Trojanische Pferde und Würmer: das kannten wir ja alles bereits. Auch von komplexen Bedrohungen, die gleich mehrere Angriffstechniken in sich vereinen, haben wir schon gehört. Sasser, Blaster und MyDoom haben nicht nur Netzwerke lahmgelegt, auch Heimanwender hatten unter ihnen zu leiden, was weltweit für Schlagzeilen sorgte.

Anders bei Adware und Spyware. Diese Programme arbeiten im Verborgenen. Deshalb ist es auch nicht ungewöhnlich, dass auf einem Rechner mehr als ein Typ von Spyware oder Adware installiert ist. Diese Programme setzen die Privatsphäre des Anwenders, die Vertraulichkeit und Integrität seiner Daten und die Verfügbarkeit seines Rechners aufs Spiel. Im schlimmsten Fall können sie Systemressourcen fesseln und den Computer damit vollständig funktionsunfähig machen.

Sowohl Spyware als auch Adware sammeln automatisch Informationen ohne ausdrückliche Erlaubnis oder Benachrichtigung des Anwenders. Der Nutzer installiert Spyware und Adware meist unwissentlich auf dem Computer, indem er diese als Anhängsel von Shareware oder Freeware herunterlädt. Ausserdem kann man die indiskreten Programme aufgabeln, indem man auf Links auf Webseiten, in E-Mails und Instant Messaging Clients klickt.

Ein im Februar 2005 von Symantec durchgeführter Test zeigt, wie häufig Adware oder Spyware auf beliebten Websites auftritt: Ein fabrikneuer Computer wurde ohne jegliche Sicherheitssoftware ans Internet angeschlossen. Nach einer Stunde Surfen auf Webseiten für Kinder fand Symantec 359 Adware-Programme auf dem Rechner. Auf sechs Sport-Webseiten wurden 17 Adware- und zwei Spyware-Programme entdeckt. Sechs Spieleseiten enthüllten 23 Fälle von Adware und vier Fälle von Spyware. 64 Adware- und zwei Spyware-Programme wurden auf fünf Reise-Websites gefunden.

Das Kleingedruckte: Der Teufel steckt im Detail

Besonders problematisch ist, dass manche Internetteilnehmer dem Download von digitalen Spitzeln aus-

TOP-TEN-VIREN MAI 2005

Bei Sophos gemeldete Viren:

• W32/Sober-N	(43,8%)
• W32/Zafi-D	(14,5%)
• W32/Netsky-P	(13,1%)
• W32/Netsky-D	(3,1%)
• W32/Zafi-B	(2,0%)
• W32/Mytob-AZ	(1,6%)
• W32/Mytob-Z	(1,6%)
• W32/Netsky-Z	(1,6%)
• W32/Mytob-E	(1,6%)
• W32/Netsky-N	(1,4%)
• Sonstige	(16%)

Gratis-Informationen über Viren und Hoaxes auf Ihrer Website:
www.sophos.de/virusinfo

drücklich zustimmen. Wie das geht? Ganz einfach: Wer Endnutzer-Lizenzvereinbarungen beispielsweise für Freeware nicht liest und naiv ihre Bedingungen akzeptiert, läuft Gefahr, sich Spyware einzufangen. In der Regel wird auf die «Spitzelfunktionen» in den Lizenzbedingungen hingewiesen. Die Hersteller sind damit rechtlich auf der sicheren Seite. Doch nur wenige Programme präsentieren dem Nutzer einen einfach zu lesenden und klar verständlichen Vertrag.

Spyware verbirgt ihr hässliches Gesicht

Der unlautere Einsatz von Spyware schliesst Key Logging ein (das Aufzeichnen von Tastenfolgen), die Bildschirmerfassung (Screen Shots), das Scannen des PCs sowie Datenverfälschung. Spyware ist in der Lage, E-Mails und Instant Messages abzufangen und nach sensiblen Informationen abzugrasen. Persönliche Daten wie Adressdaten, Passwörter oder Kontoinformationen und eine gehörige Portion krimineller Energie sind ausreichende Zutaten für einen Betrug, der den Anwender finanziell schädigen kann.

In seiner milderen Form kann Spyware Informationen über Anwendungen, die auf einem Computer laufen, Details über Surf- oder PC-Gewohnheiten sammeln und weiterleiten. Mit diesen Informationen finanzieren File-Sharing-Anbieter oftmals ihre kostenlos angebotenen Produkte, indem sie die gesammelten Daten an Drittfirmen verkaufen.

Adware – das kleinere Übel?

Die Gartner Marktforschungsgruppe schätzt, dass mehr als 20 Millionen Internetnutzer unwissentlich Adware installiert haben. Adware hat zwar tendenziell einen geringeren Wirkungsgrad als Spyware, wird jedoch auch immer dreister. Einfach ausgedrückt, verfolgt Adware die Internetsurfgewohnheiten und überträgt diese Informationen an Unternehmen, die den Service von einem Adware-Provider gekauft haben. Das gibt Werbern die Möglichkeit, massgeschneiderte Werbung zu schaffen, die genau den Nutzerinteressen entsprechen. Ein untrügliches Zeichen dafür, dass sich solche Werbemodule eingeschlichen haben, sind Pop-up-Fenster oder neue Werkzeugleisten mit zweifelhaftem Nutzen.

Obwohl Adware Informationen durch unerlaubten Zugriff sammelt, sind diese Daten im Allgemeinen anonym. Eine persönliche Identifizierung des Anwenders durch die von Adware gesammelten Daten ist nicht möglich.

Eine fragwürdige Eigenschaft mancher Adware-Programme ist das so genannte Browser Hijacking. Das ist die Umleitung von Browseranfragen auf fremde Internetsites. Diese Art von Adware führt Nutzer ohne ihr Wissen auf ähnlich anmutende Websites. Auch hier läuft man Gefahr, im Vorbeigehen unerwünschte Programme herunterzuladen.

Was sagt der Gesetzgeber?

Seit Ende 2003 ist die EU-Datenschutzrichtlinie für elektronische Kommunikation in Kraft, nach der unsichtbare Verfahren der Nachverfolgung, mit denen Informationen über Internetnutzer gesammelt werden können, nur verwendet werden dürfen, wenn der Anwender deutliche Informationen über den Zweck einer solchen Aktivität und das Recht erhält, diese abzulehnen. Das Strafgesetzbuch (§ 263a) sieht für den Missbrauch persönlicher Informationen zu betrügerischen Zwecken Freiheitsstrafen von bis zu fünf Jahren oder Geldstrafen vor.

Spyware und Adware kaltstellen

Die Bedrohung durch Spyware und Adware ist schwer zu fassen: zu unterschiedlich sind die Auswirkungen, zu vielgestaltig die Verbreitungswege. Auch können die Grenzen zu Viren oder Trojanern fliessend sein. Bereits 80 Prozent aller Computer beherbergen Spyware oder Adware. Das ergab eine von AOL und National Cyber Security Alliance durchgeführte Studie zur Online-Sicherheit.

Wer dennoch weiterhin alltägliche Besorgungen im Internet erledigen will, sollte seinen Rechner und seine persönlichen Daten konsequent schützen. Spezielle Antispyware-Programme halten die Spitzel vom Rechner fern. Noch besser als Einzellösungen ist Sicherheitssoftware, die nicht nur die Spitzelprogramme erkennt, sondern mit der gesamten Bandbreite an Internetbedrohungen fertig wird. Solche Programme schützen nicht nur vor bösartigem Code wie Viren, Würmern und Trojanern, sondern auch vor Sicherheitsrisiken wie Spyware und Adware sowie Spam und Phishingmails.

Darüber hinaus ist es sinnvoll, für den Versand sensibler Daten ausschliesslich verschlüsselte Internetverbindungen zu verwenden und bei der Programmkonfiguration restriktive Browsereinstellungen zu wählen. Ausserdem sollten Anwender nicht unbesehen alles herunterladen, was an Software kostenlos im Internet erhältlich ist. Vielmehr ist die kritische Aufmerksamkeit der Verbraucher gefragt. Dies gilt auch für das Lesen der Endnutzer-Lizenzvereinbarungen. Wer hier genau hinschaut, erspart sich später eine Menge Ärger. ■

+ + + NEWSTICKER + + + NEWSTICKER + + + NEWSTICKER + + + NEWSTICKER + + +

PLUG-IN FÜR VERTRAULICHE KORRESPONDENZ

Der deutsche Sicherheitsspezialist cv cryptovision hat ein E-Mail-Plug-in vorgestellt, mit dem vertrauliche Korrespondenz verschlüsselt und signiert werden kann. Das Plug-in ist kompatibel mit den drei verbreitetsten E-Mail-Plattformen MS Outlook, Novell GroupWise und IBM Lotus Notes. Dadurch ist «act s/mail» laut cv prädestiniert für heterogene Unternehmensnetzwerke.

BIG BROTHER IN US-AMERIKANISCHEN FIRMEN

Die meisten US-amerikanischen Arbeitnehmer müssen damit rechnen, dass der Chef ihre E-Mails liest, ihre Telefonate aufzeichnet und genau verfolgt, wie viel Zeit sie auf welchen Sites im Internet verbringen. Dies ergab eine Studie über elektronische Überwachung, die von der American Management Association und dem ePolicy Institute durchgeführt wurde.

«GELBER ALARM» FÜR «MYTOB.AR»

Der japanische Security-Spezialist Trend Micro hat einen globalen «Yellow Allert» ausgelöst. Die Ausbreitung des neuen Wurms «Mytob» soll damit so rasch wie möglich verhindert werden. Die Mytob-Migration «Mytob.AR» verwendet klassische Social-Engineering-Techniken, um unerfahrene Anwender hinters Licht zu führen und um Spyware- sowie Adware-Komponenten zu hinterlegen. Trend Micro will bereits über 100 Varianten des Mytob-Wurms identifiziert haben.

TROJANISCHES PFERD ALS INDUSTRIESPION

Der israelische Security-Spezialist Aladdin Knowledge Systems warnt vor der unterschätzten Gefahr, die von Trojanern ausgeht. Laut Aladdin ist es fünf israelischen Unternehmen mittels eines Trojaner-Programms gelungen, mehrere Konkurrenten perfekt auszuspionieren. Aladdin empfiehlt intelligente, proaktive Content-Security-Systeme, die einen Grossteil bislang unidentifizierter Trojaner stoppen können. *(pte/ICT)*

François Tschachtli

«Der Schlüssel liegt in der Kombination»

Interview mit François Tschachtli, General Manager Norman Data Defense Systems

François Tschachtli (39) zeichnet als General Manager für die Norman-Geschäftsstellen in der Schweiz, Deutschland und Österreich verantwortlich. Per 1. April 2004 ernannte ihn die norwegische Muttergesellschaft Norman ASA zusätzlich zum Vice President International Sales.

ICT
kommunikation

Herr Tschachtli, neue Viren und Spyware nutzen gezielt Schwachstellen bei den Anwendungen aus. Herkömmliche Antivirentools versagen im Kampf gegen diese Bedrohung immer öfter. Hat der traditionelle Virenschutz ausgedient?

François Tschachtli: Verschiedene Anzeichen deuten darauf hin. Denn klassische Antivirenscanner arbeiten bei der Enttarnung von Viren und Würmern in der Regel nach zwei unterschiedlichen Prinzipien. Ein Ansatz besteht in der Reaktion auf Code-Sequenzen und Signaturen, die für einen bestimmten Virus charakteristisch sind. Die zweite Variante ist die der heuristischen Systeme: Sie suchen nach einer bestimmten Anzahl von Merkmalen, die das Infektionsverhalten mit sich tragen. Der zentrale Schwachpunkt der genannten Verfahren zeigt sich bei der Identifizierung unbekannter Viren. Noch nicht bekannte Viren und Würmer können überhaupt nicht erkannt werden und gelangen damit trotz Anti-Virenschutz in den Computer und können so erheblichen Schaden anrichten.

Die verschiedenen Arten von Viren, Würmern und Trojanern werden nicht nur raffinierter, sondern sind auch immer enger miteinander verknüpft. Ist unter diesen Umständen ein umfassender Schutz der IT-Umgebung überhaupt noch zu erreichen?

Der Schlüssel liegt in der Kombination von verschiedenen Lösungen. Die wichtigste Massnahme ist die Installation einer persönlichen Firewall, die die Online-Aktivitäten des Rechners überwacht und einschränkt. Spy- und Malware ist zwar nicht immer einfach zu finden und von der Festplatte zu verbannen, doch helfen findige Softwareprogramme dabei, diese zu entfernen. Daneben entwickeln Softwarehersteller kontinuierlich spezifische Programme und Updates, die immer neu auftretende Varianten von altbekannten Spionen effektiv aufspüren und eliminieren. Solche Software bieten Echtzeitschutz gegen ungewollte Software und stellen eine optimale Ergänzung zu Virenscannern und Firewalls dar.

In jüngerer Zeit ist viel vom Day Zero-Angriff die Rede. Was versteht man darunter?

Tatsächlich ist dieser Begriff zu einem der gängigsten Schlagworte in der IT-Sicherheit geworden. Der «Day Zero»-Angriff ist eine Attacke, die noch an dem Tag erfolgt, an dem eine Schwachstelle aufgedeckt wird.

Wie lässt sich der Schaden abweisen, der durch einen solchen Angriff auf das Internet entsteht?

Proaktive Erkennung – die Fähigkeit, eine Bedrohung im Moment ihres Entstehens zu identifizieren und zu eliminieren – ist in diesem Fall ein Muss. Zu diesem Zeitpunkt kann es bereits zu spät sein, weil viele Organisationen vielleicht schon infiziert sind. Denn sechs bis 24 Stunden liegen im Schnitt zwischen dem Moment, in dem ein neuer Virus zuschlägt, bis zu dem Zeitpunkt, da User auf die aktualisierten Erkennungsdateien zugreifen können. Dass so ein Verfahren keinen Echtzeitschutz vor neuen und unbekannten Viren bietet, versteht sich von selbst.

Wie kann ein Virus daran gehindert werden, seine Aktivitäten auf den Systemen der Anwender zu entfalten?

Die beste Methode besteht darin, eine verdächtige Datei in einer sicheren Umgebung auszuführen. In anderen Worten: den Virus einfach das tun lassen, was er tun will. Auf diese Weise wird jede unbekannte und verdächtige Datei, die sich auf dem Computer «niederlassen» möchte, isoliert und daran gehindert, das System während der Analyse zu infizieren. Wenn der Virus seine Aktivitäten entfaltet, überwacht und analysiert die proaktive Lösung das Verhalten der verdächtigen Datei. Danach entscheidet das System, ob die Datei unter Quarantäne gestellt wird, oder ob sie im echten System gespeichert werden darf. In diesem Fall handelt es sich um eine vollständig, simulierte Rechnerumgebung, die sich in einem isolierten Bereich auf dem realen Computer befindet und Teil des Virenprüfprogramms ist. Und auch dem Hacker und Virenprogrammierer wird ein Strich durch die Rechnung gemacht: Die verdächtige Datei «weiss» nichts davon, dass sie in einer simulierten Welt operiert.

Welche Zukunftsprognosen können für den IT-Security-Markt gemacht werden?

Die Herausforderungen im Sicherheitsbereich scheinen im Vergleich zu den vergangenen Jahren keineswegs kleiner geworden zu sein. In den ersten Monaten dieses Jahres zeichnete sich deutlich ab, dass es hinsichtlich der aktuellen Bedrohungslage einen grundlegenden Wandel gibt. Vorfälle, wie die Verbreitung von Malware via MSN Messenger, die explosionsartige Zunahme von Malwarevarianten (Bots) und die Tatsache, dass die Autoren zu ihren Wurzeln zurückkehren, indem sie sich der altbewährten Methode des Social Engineering bedienten, lassen die allgemeine Marktsituation aus der Sicherheitsperspektive in einem neuen Licht erscheinen. Unabhängig von den zur Verbreitung eingesetzten Mitteln konnten wir beobachten, dass die verschiedenen Arten von Malware – das Zusammenspannen von Viren und Trojanern – immer enger miteinander verknüpft sind. Zudem verfolgt die heutige Malware-Szene handfeste finanzielle Interessen. Dieser Trend wird sich mit aller Wahrscheinlichkeit im Laufe des Jahres weiter fortsetzen. ■

***Interview:** Jürg Buob*