Special Innovation

Waffen gegen „wilde Tiere“

Die Zahl der kriminellen Angriffe auf Computer nimmt ständig zu. Als Gegenmittel arbeiten Wiener Forscher an einer neuen Sicherheitssoftware, die Schwachstellen bisheriger Programme beseitigt. In Zukunft sollen nicht die Viren selbst, sondern ihr übliches Verhalten aufgespürt werden.

Ernst Brandstetter

Mehr Schutz für Computersysteme: 2006 wurde im Schnitt an jedem zweiten Tag ein „Trojaner-Attack“ gemeldet. Foto: Siemens

2006 war zwar das erste Jahr seit Beginn der Analysen durch das IT-Security-Unternehmen Message Labs, das nicht von einem erheblichen Viren-Ausbruch in der Größenordnung von Sobig, Mydoom oder Netsky geprägt war. Wirklich besser wurde die Situation dennoch nicht: Eine von rund 68 E-Mails weltweit war mit einem Virus infiziert; durchschnittlich jede 274. E-Mail war eine Phishing-E-Mail. Spams machten bereits 86,2 Prozent des weltweiten Mail-Verkehrs aus. Erheblich zugenommen hat auch die Bedrohung durch gezielt agierende Trojaner, die ausdrücklich für den unbefugten Zugriff auf vertrauliche Informationen erstellt werden: Trat Ende 2005 ein solches Schadprogramm pro Woche auf, waren es Ende 2006 bereits zwei pro Tag.

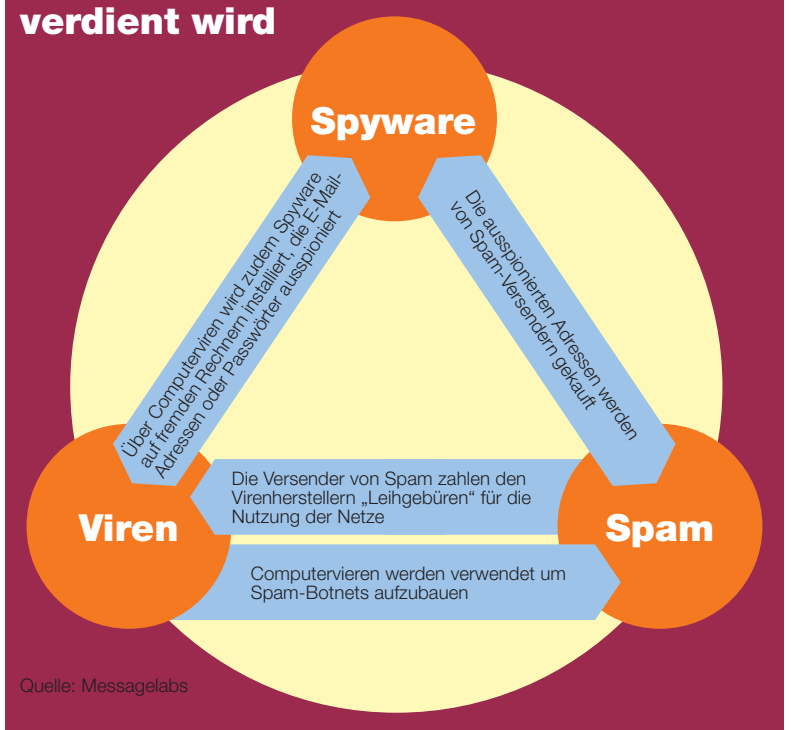
Österreich liegt mit einer Spam-Rate von 50,6 Prozent über und mit einer Virus-Rate von 1,39 Prozent (jede 71. E-Mail) unter dem weltweiten Durchschnitt. „Es gibt einen starken Trend hin zu Trojanern und Würmern“, erklärt der Geschäftsführer von Secure Business Austria, Markus Klemen. Secure Business Austria ist das erste österreichische Kompetenzzentrum, das sich in Zusammenarbeit mit den Technischen Universitäten von Wien und Graz sowie der Universität Wien die Erforschung von praxisrelevanten Sicherheitsthemen zum Ziel gesetzt hat.

Aktuelles Hauptthema ist eine neue Basis für künftige Systeme zur Abwehr von schädlicher Software. Diese Programme tauchen mittlerweile in so vielen Varianten auf, dass eine Suche, wie sie aktuell üblich ist, bald nicht mehr zielführend sein wird. Klemen: „In den Datenbanken der Hersteller von Antiviren-Software finden sich inzwischen rund 200.000 Programmbeispiele, es wird immer schwieriger, die Daten up to date zu halten. Außerdem dauert die Suche in den riesigen Datenbanken bald zu lange.“ Stattdessen forschen die Experten von Secure Business Austria an einem neuen Erkennungsprinzip: Man beobachtet, welche Aktivitäten ein Wurm oder Virus setzen kann und wie diese Aktivitäten beschrieben werden können, um sie für spätere Vergleiche heranzuziehen. Klemen: „Dazu gibt es einen leicht verständlichen bildhaften Vergleich. Vereinfacht gesagt hat man bisher von allen bekannten wilden Tieren Fotos gemacht und sie für einen späteren Vergleich gespeichert. In Zukunft wird man die Wildtiere erkennen, indem man bestimmte Verhaltensweisen, wie etwa Aggressivität oder die Neigung, Menschen zu attackieren, als Klassifikationsmerkmale heranzieht.“ Ein zweites Problem sind gefährliche Websites. Hier arbeiten die Forscher an einem Programm, das gewissermaßen alle möglichen Websites abklappert und analysiert und so frühzeitig etwa gefälschte Bank-Homepages, wie sie bei Phishing-Attacken verwendet werden, aufdeckt.

www.securityresearch.at

Kriminelle Geschäfte

Wie mit Schadsoftware Geld verdient wird



Quelle: Messagelabs

Die Kombination von Viren und Spam ist die wichtigste Praxis von Web-Betrügern. Die Verteilung von rund 80 Prozent aller im Umlauf befindlichen Spam-Nachrichten erfolgte 2006 über Botnets, die speziell für diesen Zweck von entsprechenden Virenstämmen erzeugt wurden. Botnets (die Kurzform von Roboter-Netzwerk) sind fernsteuerbare Netzwerke von PC im Internet, die aus untereinander kommunizierenden Bots bestehen. Diese Kontrolle wird durch Würmer oder Trojanische Pferde erreicht, die den Computer infizieren und dann auf Anweisungen warten. Die Netzwerke können so beispielsweise für die Verbreitung von Spam verwendet werden, meist ohne dass die betroffenen PC-Nutzer etwas davon mitbekommen.

Markus Klemen: „Waren es früher vor allem Hacker, die aus Spaß Viren konstruierten, so wird Schadsoftware heute zunehmend von Kriminellen eingesetzt, um damit Geld zu ergaunern.“

Die Dunkelziffern werden steigen

economy: ***Schadsoftware und Spams werden zu einer immer schlimmeren Plage. Was sind die aktuellen Trends?***

Markus Klemen: Früher waren es vor allem Hacker, die Virenprogramme oder andere schädliche Software in Umlauf brachten und sich freuten, wenn die Zeitungen darüber berichteten. Jetzt sind immer mehr Kriminelle am Werk, die mit Schadsoftware Geld verdienen wollen. Daran ändert auch nichts, dass die Virus-Rate seit 2004 leicht sinkt. Die Betroffenen sollen nämlich nichts mehr von der Infizierung ihrer Computer merken. Diese Dunkelziffer wird künftig wesentlich steigen.

Wie verdienen die Internet-Kriminellen ihr Geld?

Ein Supergeschäft ist momentan das Verleihen von Botnets *(siehe Kasten)*. Die aktuellen Gebühren für die Verwendung von Botnets belaufen sich pro Woche auf etwa 50 bis 60 US-Dollar *(rund 38 bis 46 Euro, Anm. d. Red.)* für 1.000 bis 2.000 gekaperte Computer. Welche Kosten genau anfallen, hängt davon ab, wie die ferngesteuerten Zombie-Rechner verwendet werden.

Bisher wurde Microsoft kritisiert, das Betriebssystem Windows würde es den Kriminellen besonders einfach machen. Wie wird das bei Windows Vista?

Wir arbeiten schon seit Längerem mit Vista und sehen ein Problem, das bei allen Virtualisierungsprodukten, beispielsweise auch VM-Ware, droht. Dazu muss man erklären, worum es sich handelt. Bei derartiger Software ist die tatsächliche Benutzeroberfläche nicht ident mit dem Basis-Betriebssystem. Mit VM-Ware lassen sich mehrere Computer mit verschiedenen Betriebssystemen gleichzeitig darstellen. Wenn aber das unsichtbare Basis-Betriebssystem geknackt wird, hat man praktisch keine Chance, das auf der normalen Betriebsebene festzustellen.

Wann wird Ihre neue Viren-Software fertig?

Wir wollen in zwei bis drei Jahren einen Prototypen vorstellen können.

Wie groß ist Secure Business Austria, und was machen Sie sonst noch?

Das Zentrum arbeitet seit April 2006 und hat jetzt 25 Mitarbeiter. Insgesamt sollen es 30 bis 35 werden.

Gibt es noch andere Arbeitsschwerpunkte?

Ein weiteres Projekt ist E-Health. Hier wollen wir in einem Jahr einen stabilen Prototypen für die Anonymisierung von Patientendaten vorstellen. Dieses Thema wird ja derzeit auch in der Öffentlichkeit intensiv diskutiert. *bra*

Das Special Innovation entsteht mit finanzieller Unterstützung von ECAustria. Die inhaltliche Verantwortung liegt bei *economy.*

Redaktion:
Ernst Brandstetter