Die Presse, 12. Mai 2000

Virus-Erfinder: "Rückverfolgung aussichtslos"

Virus-Programmierer sind schwer zu enttarnen. Ermittler müssen sich auf Fehler oder Hinweise verlassen. Der Loveletter-Virus-Verdächtige Onel de Guzman gab an, er könnte das Virus versehentlich verschickt haben.

WIEN (bau). Computer-Experten sind sich einig: Den Programmierer eines Virus zu enttarnen, ist sehr schwierig bis unmöglich. Es sei denn, er hinterläßt Hinweise im Virus-Code. Wie der Programmierer des kürzlich weltweit aufgetretenen Loveletter-Virus. "Er hat praktisch sein Pseudonym, seinen Standort und weitere Angaben einfach in den Viren-Code reingeschrieben", weiß Nicolas Ehrschwendner von Attingo Software, der das Loveletter-Virus analysiert hat. Warum? "Möglicherweise wollte er damit etwas beweisen oder jemanden beeindrucken."

Ein Ansatz, der zur zweiten Möglichkeit führt, einen Virus-Programmierer zu schnappen. Weniger eine hochtechnische Analyse, sondern eher "Kommissar Zufall" scheint dort eine Rolle zu spielen. "Meistens ist es so, daß jemand plaudert", sagt Ehrschwendner. Virus-Programmierer, wie auch Hacker, werden oft von Spieltrieb geleitet. "Da gibt es rivalisierende Gruppen, die ständig zeigen wollen, wer der bessere ist." Oft führen solche Hinweise zur Ausforschung. Dadurch, daß sich die Programmierer sicher fühlen, finden sich sogar sämtliche Beweise noch an Ort und Stelle.

"Den Ausgangspunkt eines Virus zurückzuverfolgen ist praktisch aussichtslos", erklärt auch Peter Rogy von Schoeller Network Control, dessen Firma Sicherheitsüberprüfungen von Firmen-Netzwerken durchführt. Bei Hackern haben Systemadministratoren oft die Möglichkeit zurückzuschlagen. Hacker, die gezielt von außen in Firmen-Netzwerke eindringen, hinterlassen Spuren. "Eindringlinge kann man über ihre IP-Adresse zurückverfolgen."

Versierte Hacker verstehen es aber, diese Spuren zu verschleiern. "Man kann über verschiedenen Server als Zwischenstation in ein System eindringen. Eine Rückverfolgung wird dadurch zumindest erschwert". Es gibt auch Internet-Provider, die einen anonymen Zugang über Kreditkarten anbieten. "Oft werden gestohlene Kreditkartennummern dafür mißbraucht", meint Ehrschwendner. Wenn die Einwahl dazu noch via Wertkarten-Handy erfolgt, ist eine Identifikation fast unmöglich.