

# Moderne K@mmernjäger

Von Professor Dr. Thomas J. Schult

Geht der Rechner ans Netz, drohen Viren und andere Angreifer mit ihrem Besuch. An einem gesicherten Computer liegen daher ständig elektronische Kammerjäger auf der Lauer: Virenschutzprogramme sorgen für saubere Rechner. Aber wie lernen sie, Freund und Feind zu unterscheiden?

explore: INFOBOX

## Wichtige Fachbegriffe

**Viren** sind Programme, die sich von selbst verbreiten, meist mithilfe eines als „Wirt“ dienenden anderen Programms. In der Regel haben sie eine schädliche Wirkung: Sie verlangsamen beispielsweise Computer oder zerstören Dateien. Früher wurde der Begriff nur für solche Schädlinge verwendet, die sich an andere Computerdateien anhängen.

**Polymorphe Viren** sind schwierig zu entdecken, weil sie ständig ihre Gestalt verändern. Teile von ihnen können ihr Aussehen etwa nach einem Zufallsprinzip verändern, ohne dass sich dadurch das Verhalten des Virus ändert.

**Würmer** sind Viren, die keinen Wirt für die Verbreitung benötigen. Sie vermehren sich von selbst und nehmen einen immer größeren Teil des zur Verfügung stehenden Speichers in Beschlag.

**Trojaner** sind Viren, die eine andere Identität vorgaukeln. Sie geben etwa vor, ein nützliches kostenloses Programm zu sein, um sich bei Computeranwendern einzuschleichen, sind aber tatsächlich Viren, die beispielsweise Passwörter ausspionieren wollen.

**Virens Scanner** sind Programme, die einen Computer oder einen Datenträger daraufhin überprüfen, ob er von Viren befallen ist. In der Regel können sie die Viren dann auch beseitigen.

**Signaturen** sind charakteristische Bitfolgen in Viren, vergleichbar den Fingerabdrücken bei Menschen. Ein typischer Virens Scanner prüft eine Festplatte, indem er bekannte Signaturen in allen gefährdeten Dateien auf der Platte sucht.

Eine **Firewall** besteht aus Hard- oder Software, um ein lokales Netzwerk oder einen einzelnen Computer mit Internetverbindung vor Gefahren aus dem Internet zu schützen, etwa vor Viren oder Hacker-Angriffen.

**Router** sind Geräte, mit denen sich mehrere Computer einen Internetanschluss teilen können.

Früher ließen sich die ungebetenen Gäste klar einteilen: Die klassischen Viren hängen sich an Dateien, *Würmer* machen sich ohne Wirt breit, *trojanische Pferde* kommen im Gewand eines erwünschten Gastes – so genannte Hintertüren öffnen den Rechner und lassen weiteres Gesindel herein. Diese Trennung hat sich mittlerweile überholt; neuere Schädlinge kombinieren solche Fähigkeiten.

Unabhängig vom Schädlingstyp müssen Hersteller von Antivirensoftware wie McAfee oder Symantec ihre Programme immer noch mit viel Handarbeit trainieren. Typische Bit-

folgen (*Signaturen*) verraten manchen Eindringling, so dass dieser erkannt und ausgemerzt werden kann. Die beim Anwender installierte Software holt sich dann Signaturenlisten in regelmäßigen Abständen von der Website des Herstellers.

*Polymorphe Viren*, die sich in immer neuem Code verstecken, können sich jedoch nur durch ihr Verhalten verraten. *Virens Scanner* werden dafür mit Listen untypischer Aktionen versehen, die sie im Auge behalten sollen. Wenn auf einmal die Festplatte formatiert werden soll, treten die Scanner auf den Plan. Oder sie führen verdächtige

Programme in einer abgeschlossenen Umgebung aus und studieren ihr Verhalten.

*Firewalls*, die Schutzwälle von Rechnern am Netz, darf ein Anwender übrigens selbst trainieren: Er kann die elektronischen Brandmauern mit den typischen Netzaktivitäten am betreffenden Arbeitsplatz vertraut machen. Später können die Firewalls dann auf Abweichungen vom gewohnten Datenverkehr mit Warnungen reagieren. Was man beachten sollte, um sich vor ungebetenen Gästen zu schützen, erklärt Daniel Bachfeld (siehe: *explore: INTERVIEW*). ■



Oft unerkannt vom Benutzer greifen Viren & Co. den Rechner an. Eine Firewall ist ein absolutes Muss.

## explore: INTERVIEW

**Was sind nun die wichtigsten Maßnahmen, mit denen sich der Besitzer eines Computers schützen kann? Dazu fragte explore-Autor Professor Dr. Thomas J. Schult Daniel Bachfeld vom Informationsdienst heise Security.**

**explore:**  
Muss ich eigentlich auch einen Rechner schützen, der überhaupt nicht am Internet hängt?

Daniel Bachfeld:  
Ja, weil auch Datenträger verseucht sein können. Bei gepressten CDs oder DVDs kann man mittlerweile ziemlich sicher sein, dass sie sauber sind. Bei gebrannten Scheiben ist die Gefahr schon größer. Ein Virens Scanner kann da Sicherheit geben.

**explore:**  
Wenn ich eine Internetverbindung habe: Welche Sicherheitsmaßnahmen sollte ich ergreifen?

Daniel Bachfeld:  
Vier Dinge sind zu beachten: Firewall, Updates, Mail-Anhänge und Virenschutz. Eine Firewall brauchen Sie, wenn Sie nicht an einem Router hängen oder wenn Sie drahtlos surfen. Dann aktivieren Sie beispielsweise die Firewall von Windows XP. Erste Aktion im Internet sollte es sein, das aktuelle Sicherheitsupdate von der Microsoft-Site zu holen und das Betriebssystem so einzustellen, dass künftige Updates automatisch übertragen werden. Anhänge von E-Mails sollten Sie nur öffnen, wenn Sie vom Absender wirklich eine Datei erwarten.

**explore:**  
Soll ich mir auf jeden Fall einen Virens Scanner kaufen?

Daniel Bachfeld:  
Virenschutz muss nichts kosten. AVG Anti-Virus beispielsweise reicht meistens aus und kostet nichts. Das Programm holt sich automatisch die neuesten Signaturen. Es gibt natürlich noch bessere Virens Scanner, aber die sind nicht mehr gratis.

## explore: INFOBOX

### Sicherheits-Links

Sicherheits-Infos: [www.heise.de](http://www.heise.de)  
AVG-Virens Scanner: <http://free.grisoft.com>  
McAfee Virens Scanner: [www.mcafee.com/de](http://www.mcafee.com/de)  
Symantec Virens Scanner: [www.symantec.com/region/de](http://www.symantec.com/region/de)