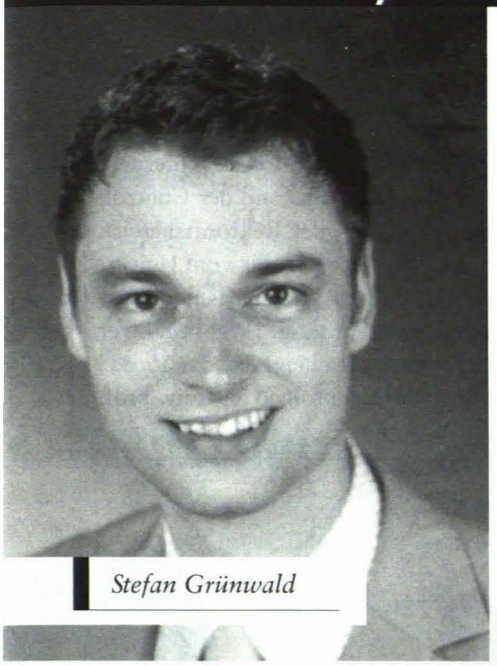
Internet / Neue Medien / Trends



Stefan Grünwald

Plagegeister

Aus wieder einmal ziemlich aktuellem Anlass ist eine Beschäftigung mit Viren und Würmern angebracht. Die Problematik beinhaltet technische, organisatorische, soziale und rechtliche Aspekte. Die sozialen Komponenten liegen am veränderten Benutzerverhalten des mittlerweile zum Massenmedium gewordenen Internets. Die grundlegenden Entwicklungen des Netzes wurden in den 1960er, 1970er und 1980er Jahren getätigt, wobei damals die heutige Struktur und Verbreitung des Internets nicht absehbar. Gerade unter Wissenschaftlern waren die Offenheit und der effiziente freie Informationsaustausch durch das Internet zentrale Faktoren; die Teilnehmer kannten und vertrauten sich. Darüber hinaus war die kommerzielle Nutzung verboten und Viren stellten noch kein Problem dar, unter anderem weil die Teilnehmer die prinzipiellen Gefahren kannten und sich entsprechend verhielten. Mit der Ausbreitung des Netzes zu einem alltäglichen Medium zur Kommunikation und Information seit Mitte der 1990er Jahre änderte sich die Anwenderstruktur grundlegend, vor allem weil die Bedienung stark vereinfacht wurde. Dadurch wurde der Zugang erleichtert, aber die darunter liegende Komplexität der Netzwerktechnologie und die Gefahren durch den Anschluss an ein globales Netz blieben dieselben – sie wurden nur vor dem Anwender versteckt. Die "Teilnahme" am Internet bleibt potenziell gefährlich. Den Anwendern wurde und wird eine heile Internet-Welt vorgegaukelt, die so nicht existiert. Der beste Schutz vor unerwünschten Plagegeistern und Verletzungen der Privatsphäre war, ist und bleibt ein angepasstes Verhalten im Umgang mit dem Medium Internet, und damit lassen sich fast alle Schadensfälle vermeiden.

Auch wenn Antivirensoftware-Hersteller die Wichtigkeit ihrer Produkte betonen, und durch die aktuellen Viren und Würmer ihre Umsätze in die Höhe schnellen, sind Virenscanner nur ein minimaler Baustein auf dem Weg zur Datensicherheit, da das Problem nicht gemildert, sondern nur Symptome bekämpft werden. Darüber hinaus besteht die Gefahr, dass sich Anwender in falscher Sicherheit wiegen und ihr Verhalten nachlässiger wird. An und für sich ist die Virenproblematik momentan ein Phänomen der Windows-Welt, die durch die Homogenität der verwendeten Anwendungssoftware, durch konzeptionelle Schwächen von Windows und durch die Produktstrategie von Microsoft, welche die einfache Bedienung in den Vordergrund stellt, ausgelöst wurde. Usability und Sicherheit lassen sich aber nicht uneingeschränkt vereinen! Linux-Anwender sollten sich jetzt aber nicht zurücklehnen und in Schadenfreude verfallen, da mit einer weiteren Verbreitung des freien Betriebssystems sicherlich auch der Reiz für Programmierer von schädlicher Software ansteigen wird. Dennoch sind zwei Faktoren, welche der Verbreitung von Viren entgegenstehen, ein gewisser Schutz, nämlich die grundsätzlich mehr auf Sicherheit ausgelegte Struktur von Unix-Systemen und eine Heterogenität bei der Verwendung von Anwendungssoftware. Darüber hinaus kommt bei Linux als Open-Source Software noch das Mehraugenprinzip zum Tragen, da tausende Entwickler weltweit daran arbeiten, sowie die schnellere Reaktionszeit bei auftretenden Sicherheitslücken. Bei Windows kann ein Virenersteller davon ausgehen, dass 80 – 90 % der Benutzer Outlook als E-Mail-Programm einsetzen und die Schwächen und Fehler dieser Software sind allgemein bekannt. Damit kann ein Schädling "perfekt" angepasst werden, und seiner lawinenartigen Ausbreitung steht nichts mehr im Wege.

Wie sieht jetzt ein optimales Sicherheitskonzept aus, und welche Maßnahmen können getroffen werden, um Daten von Unternehmungen und Privatpersonen zu schützen? Primär sollte aktuelle und damit möglichst fehlerfreie Software eingesetzt werden. Durch die Wahl der Anwendungssoftware kann ebenfalls ein großer Beitrag zu mehr Sicherheit geleistet werden. Daneben spielt der angepasste Umgang mit den Internetdiensten eine zentrale Rolle (z.B. der Verzicht auf "HTML-E-Mails"), wobei auch dazugehört, dass man sich laufend über aktuelle Gefahren informiert. Die Integration einer Firewall, und damit die Trennung der lokalen Netze vom Internet, sollte Profis vorbehalten bleiben, da sie ein hohes Kompetenzniveau bezüglich Netzwerk- und Systemtechnik voraussetzen. Deshalb können auch so genannte "Personal-Firewalls" nur bedingt zu einer steigenden Datensicherheit beitragen, weil wieder gilt: Sicherheit im Internet ist ein komplexes Themengebiet, welches nicht durch das Anklicken von ein paar Knöpfen zu erreichen ist. Hat man die genannten Aspekte berücksichtigt und einen Rechner mit ausreichender Leistung am Schreibtisch stehen, kann man durch den Einsatz eines Virenscanners noch ein paar Promille mehr an Datensicherheit herausholen. ;-)

Stefan Grünwald