Linux-Viren - Mythos oder Wirklichkeit?

Marc Ruef, scip AG, maru-at-scip.ch

Nur wenige Themen hat die Gemüter so erhitzt, wie der Streitereien um Linux-Viren. Sind sie überhaupt möglich? Gibt es sie denn schon? Falls ja, welche Möglichkeiten und Auswirkungen hätten sie? In diesem Artikel wollen wir die Vorurteile diesbezüglich aus der Welt schaffen. Wir werden Trends ermitteln und die Zukunft der Linux-Viren konkretisieren.

Jürgen Kraus verfasste 1980 im Fachbereich Informatik an der Universität Dortmund eine Diplomarbeit mit dem Titel "Selbstreproduktion bei Programmen“. Der Autor schilderte in seinem Schriftstück die Konstruktion möglichst einfacher, sich selber reproduzierender Computerprogramme. Ihr Verhalten sollte demjeniger biologischer Viren sehr ähnlich sein. Grundsätzlich verfolgte Kraus einen sehr theoretischen Ansatz und ging dabei nicht auf die Sicherheitsprobleme solcher Computerviren in der Praxis ein. Die Arbeit wurde der Öffentlichkeit leider nie zugänglich gemacht und verschwand in den Archiven der Universität [BSI 1997].

Abbildung 1: Der US-Amerikaner Dr. Fred Cohen gilt als der Ur-Vater der Computerviren. Mit seiner Dissertation zum Thema hat er die technische Grundlage für moderne Computerviren geschaffen.

Dr. Fred Cohen entwickelte im Jahre 1983 zu Studienzwecken einen ersten funktionierenden Virus auf einem Digital Equipment Corporation VAX System. 1984 publizierte er seine Zeilen unter dem Titel „Computer Viruses - Theory and Experiments“ [Cohen 1984]. Da er insbesondere auf die Gefahren einging, die Computer-Viren für Rechner darstellen können, erregte seine Untersuchung auch internationales Aufsehen. Er definierte den Begriff während der Ausarbeitung seiner Dissertation folgendermassen: „Ein Computervirus ist ein Computerprogramm, das andere Computerprogramme insofern verändert, alsdass es sich selber (in einer abgeänderten Form) hineinkopiert.“

Diese Definition war für die damalige Zeit absolut ausreichend. Doch wie wir alle wissen, ist die Computertechnologie einem stetigen Wandel unterworfen. Die Definition des Begriffs Computervirus wurde immer schwieriger, denn Würmer erfüllten Cohens Definition auch, verfolgten jedoch einen Ansatz zu ihrer Verbreitung, weder die klassischen Dateiviren. „The New Hackers Dictionary“ definiert einen Virus ganz klar und grenzt ihn von einem Wurm wie folgt ab [Raymond 2002]: „[Ein Virus ist ein] Cracker-Programm, das andere Programme sucht und sie durch eine Kopie von sich selber ‚infiziert’, so dass diese zu Trojanischen Pferden werden. Wird das infizierte Programm ausgeführt, wird der Viren-Teil ebenso ausgeführt, was eine Verbreitung ermöglicht. Dies geschieht normalerweise ohne Einblicke des Benutzers. Um Gegensatz zu einem Wurm kann ein Virus ein anderes System nicht ohne Zutun infizieren.“

Man klassifiziert Computerviren in zwei Arten: Es gibt solche für Studienzwecke und solche, die „in the wild“ auftreten. Cohens Virus sollte lediglich seine Dissertation stützen, weshalb er der ersten Kategorie zugeteilt werden kann. Ein Computervirus gilt als „in the wild“, wenn er tatsächlich im Umlauf ist. Einer der ersten Viren dieser Klasse war Elk Cloner, der 1981 entdeckt wurde und Apple II-Systeme infizierte [Denning 1990]. Mitlerweile gibt es Viren für praktisch sämtliche Plattformen. Dies reicht von Amiga-Systemen bis hin zu den verschiedenen Windows-Versionen.

„Ein Computervirus ist ein Computerprogramm, das andere Programme als Wirt missbraucht.“

Sind Linux-Viren überhaupt möglich?

Linux-Viren galten lange Zeit als unrealistisch – Ja gar grundsätzliche Utopie. Diese Ignoranz der Linux-Benutzer ist gefährlich, denn das Betriebssystem Linux bringt von Haus aus keine Schutzmöglichkeit gegen Viren mit, die nicht auch auf anderen Systemen, die ebenfalls infiziert werden können, gegeben ist. Eingefleischte Linux-Anwender pflegen bei der Diskussion um Linux-Viren stets darauf zu verweisen, dass solche auf einem durchdachten Multiuser-Betriebssystem nicht möglich seien.

An dieser Stelle muss man jedoch streng differenzieren zwischen einem „nicht möglich“ und „nicht sinnvoll“. Selbstverständlich sind Viren unter Linux möglich [Bartolich 2002]. Die Multuser-Architektur wird, sofern diese richtig um- und eingesetzt ist, die primitiven Infektions-Routinen der Viren für Singleuser-Betriebssysteme (z.B. MS DOS und Windows 9x) ins Leere laufen lassen. Schauen wir uns das Beispiel eines Shell-Skripts an, das andere Shell-Skripte mit sich selber zu infizieren in der Lage ist:

```
1     #!/bin/sh
2     for file in *.sh
3     do
4        head -n 5 $0 > $file
5     done
```

Dieser Virus, der erstmals von Eric Sesterhenn und Martin J. Münch zu Studienzwecken publiziert wurde [Sesterhenn et al. 2002], umfasst in der hier dargelegten Form lediglich 54 Zeichen. Dieses Minimum bei angenehmer Übersichtlichkeit wird dadurch erreicht, dass das besagte Shell-Skript lediglich aus einer Infektions-Routine besteht (Zeilen 2 bis 5). Auf eine Schadensroutine wird dabei verzichtet. Eine solche Einzubringen ist jedoch mit dem Hinzufügen weniger Zeilen möglich (z.B. „rm –rf /var/www“) und für den Durchschnittsanweder keine allzu grosse Herausforderung.

Programme, die sich selber reproduzieren können, und somit per se als Viren gelten, können auf Linux selbstverständlich auch in anderen Sprachen geschrieben werden. So sind auf Linux Perl-, Makro- und ELF-Viren möglich. Der Artikel „Tux erkältet sich: Linuxviren im Vormarsch“ von Martin J. Münch und Eric Sesterhenn führt sehr gut in die Möglichkeiten derer ein [Sesterhenn et al. 2002].

Das deutsche Bundesamt für Sicherheit in der Informatik (BSI) sah die Problematik der Viren auf Linux- und UNIX-Systemen im Jahre 1997 noch nicht gegeben [BSI 1997]: „[...] hardwareunabhängige Viren [sind] für das Betriebssystem UNIX nur als wissenschaftliche oder theoretische Beiträge zur Forschung, in der Praxis jedoch nicht anzutreffen.“

Die FAQ der USENET-Gruppe alt.comp.virus hat das Thema UNIX-Viren schon längst anerkannt und äussert sich zum Thema wie folgt [Harley et al. 2000]: „[Es gab] einige kleinere Linux-Viren. [...] Obschon Viren kein Hauptrisiko auf UNIX-Plattformen darstellt, benutzen Administratoren Integrity-Checker um Änderungen an den Dateien durch andere Angriffe entdecken zu können.“

Warum gibt es nur wenige Linux-Viren

Um zu verstehen, warum es nur wenige Computerviren für Linux gibt, muss man sich nach den Gründen fragen, warum jemand solcherlei Software schreibt. Ein Grossteil der Entwickler von „schädlichem“ Programmcode (z.B. Viren, Würmer und Exploits) tun dies aus reiner Freude am Forschen. Nehmen wir als Beispiel Fred Cohen, dem man wohl kaum nachsagen kann, dass er seine Dissertation und die Beispiel-Viren für bösartige Zwecke einsetzen wollte. Ihm ging es dabei einzig und allein um die Forschung im Bereich sich selber reproduzierender Software. Ein Indiz dafür, dass Cohens Viren nicht mit bösem Hintergedanken entwickelt wurden ist, dass sie bis heute nicht „in the wild“ freigelassen wurden. Wie will ein Virus ernsthaften Schaden anrichten, wenn er sich nur in abgeschotteten Test-Umgebungen bewegen darf?

Ein anderer Teil der Viren-Programmierer fröhnt ihrer Tätigkeit aufgrund des Triebs nach Anerkennung, Ruhm und Popularität. In der Aggressionspsychologie spracht man von einer Erlangungs-Aggression. Bei dieser hat es der Aggressor (der Viren-Entwickler) auf die Durchsetzung seiner Ziele (Befriedigung seines Narzissmus) abgesehen [Fromm 1973, Nolting 1978]. Genau dieser Charakter ist es, der die Verbreitung von Viren vorantreibt, denn nur so kann er seine Ziele durchsetzen. Wird ein Virus bekannt, vor allem durch eine fortwährende Medienberichterstattung, hat der Entwickler sein Ziel erreicht – Er findet darin seine Bestätigung und befriedigt so seinen Narzissmus.

„Ein Computervirus ist auf jedem System denkbar, das sich frei programmieren lässt.“

Ein Grossteil der Computerviren ist nur für eine bestimmte Plattform entwickelt worden. Es gibt zwar einige Hybrid-Viren, die sich auf verschiedenen Betriebssystemen verbreiten können. Diese sind jedoch sehr selten gesehen, da sie einen Mehraufwand bei der Entwicklung erfordern: Der Viren-Programmierer muss quasi eine Portierung seiner Software machen.

Multiuser-Betriebssysteme sind jedoch sehr undankbar bei der Verbreitung von Computerviren – Weshalb die Aussage, dass Viren auf Linux „nicht sinnvoll“ sind ein grosses Stück Wahrheit in sich trägt. Gehen wir davon aus, dass sich der Benutzer mruef auf unserem

Debian GNU/Linux einen Perl-Virus durch das Herunterladen eines vermeintlich nützlichen Skripts eingefangen hat. Diese bösartige Software durchsucht sämtliche Verzeichnisse nach Perl-Skripten, die es infizieren könnte. Da der Benutzer mruef nur sehr beschränkten Zugriff im System hat (zum Beispiel nur Schreibrechte in seinem eigenen Home-Verzeichnis), kann sich die Infektion auf keine für das System lebenswichtigen Dateien (z.B. in /usr/bin) ausbreiten: Der Benutzer – und somit sein Virus, der dessen Privilegien geerbt hat - hat halt einfach keine Schreibrechte.

Nicht umsonst wird in den gängigen Newsgruppen immerwieder darauf hingewiesen, dass auf einem Linux-System das Arbeiten mit administrativen Rechten eine Gefahr darstellt. Denn fängt sich der Administrator einen Virus ein, erbt der Virus seine Rechte und hat somit Zugriff auf sämtliche Systemdateien. Sowohl die Infektion als auch die Schadenroutine kann dann wichtige Dateien des Betriebssystems betreffen.

Popularität steigert das Interesse

Linux ist sowohl im Server- als auch im Workstation-Bereich auf dem Vormarsch, keine Frage. Die Popularität eines Systems, einer Software oder Lösung bringt jedoch auch immer gewisse Nachteile mit sich. Einer dieser Nachteile ist die erhöhte Aufmerksamkeit, die die Angreifer den populären Produkten schenken. Eine gefundene Sicherheitslücke im Microsoft Internet Information Server (MS IIS, www.microsoft.de) erregt viel mehr Aufmerksamkeit, weder eine Schwachstelle in einem unbekannten Webserver-Produkt. Schwachstellen im real-time Betriebssystem QNX (www.qnx.com) werden weniger entdeckt und publiziert, weil nur sehr wenige Menschen Interesse an diesem Produkt zeigen. Laut der Verwundbarkeits-Datenbank von SecurityFocus.com, sind bisher nur zwei Schwachstellen in diesem relativ unpopulären Betriebssystem bekannt geworden. Dieses Total ist bestimmt nicht so niedrig, weil QNX weniger Sicherheitslücken hat, weder andere Betriebssysteme.

Das freie Betriebssystem Linux wird also immer interessanter für Angriffe, Viren und Würmer. Dieses steigende Interesse ist zum Beispiel aus der Defacement-Statistik von Attrition.org ersichtlich. Diese bekannte Webseite sammelt Informationen über verunstaltete Webseiten – Sogenannte Defacements. In ihrer OS-Statistik halten Sie vom August 1999 bis 17. Mai 2001 fest, welche zugrundeliegenden Betriebssysteme der verunstalteten Webseite am meisten betroffen waren [Dickerson et al. 2001]. Windows NT erfreute sich während dieser Zeit grosser Beliebtheit als Webserver-System. Praktisch in jedem Monat führt das Microsoft-Betriebssystem die Statistik an. Windows 2000 taucht erstmals in den Statistiken im Monat März 2000 auf. Die ersten fünf Monate wurden im Schnitt 2.5 Defacements durchgeführt. Danach steigt die Kurve linear an. Dies deutet darauf hin, dass a) mehr Windows 2000-Webserver eingesetzt wurden und b) es mehr Angreifer auf dieses relativ junge System abgesehen haben. Das UNIX-Derivat Solaris der Firma Sun Microsystems Inc. (www.sun.com) war eher weniger betroffen. Dafür ist diese Kurve sehr konstant; im Schnitt bei etwa 43 Defacements pro Monat.

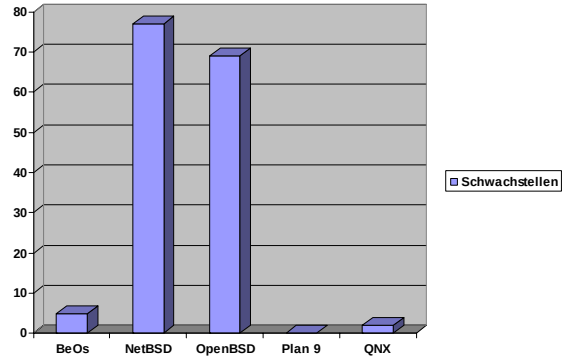

Abbildung 2: DIe geringe Anzahl der Sicherheitslücken alternativer Betriebssysteme geht einher mit ihrer Unpopularität und dem fehlenden Interesse der Viren-Entwickler.

Für uns von eigentlichem Interesse ist natürlich die Anzahl der Defacements, die das Linux-Betriebssystem betroffen haben. Von August 1999 bis August 2000 lagen die Defacements bei rund 70 Stück pro Monat. Danach sind zwei Anstiege zu erkennen. Der erste erfolgte im August 2000 und der zweite Januar und Februar 2001. Sodann wurden pro Monat etwa 212 Defacements von Linux-Webservern gezählt. Man kann also davon ausgehen, dass zur Zeit des ersten Ausschlags das Linux-Betriebssystem von den Angreifern ins Visier genommen wurde. Das Interesse am UNIX-Derivat liess bis heute nicht nach.

Selbstverständlich kann die Statistik für Webseiten-Defacements nicht so ohne Weiteres für die Verbreitung von Linux-Viren herhalten. Viele andere Faktoren spielen da auch eine Rolle. Es zeigt jedoch trotzdem deutlich, dass die Popularität eines Systems Aufmerksamkeit erregt. Und wo Aufmerksamkeit ist, werden eher Fehler entdeckt. Leider existieren keine Aufzeichnungen über die Anzahl und Verbreitung von Linux-Viren der letzten Monate. Es ist aber

damit zu rechnen, dass die Trends im Defacement-Bereich auch auf die der Computerviren abgebildet werden kann. Es ist nun jedoch nicht damit zu rechnen, dass eine wahre Flut an Linux-Viren über uns hereinbrechen wird. Klassische Computerviren wurden in den letzten Jahren immer uninteressanter für ihre Entwickler – Es steckt doch viel mehr Potential in Computerwürmern, die sich zum Beispiel über Emails verbreiten (z.B. Melissa). Viele Virenentwickler haben der Szene den Rücken gekehrt und beschäftigen sich nun mit anderen Dingen...

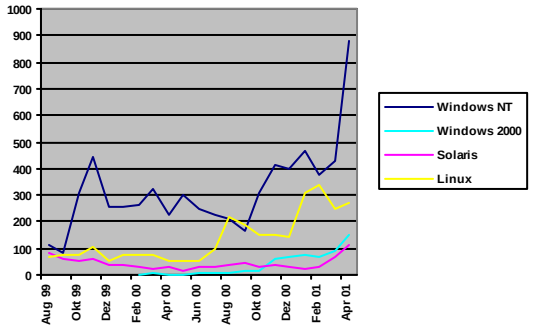

Abbildung 3: Die zunehmende Anzahl der für ein System gefundenen Sicherheitslücken hat mit der steigenden Verbreitung und mit dem zunehmenden Interesse der Hacker und Cracker zu tun.

Normalanwender stellen ein Risiko dar

Die Popularität eines Systems stellt insofern ein Risiko dar, da es mehr Aufmerksamkeit der potentiellen Angreifer erhält. Wir haben dies gesehen. Popularität bringt auch ein Mehr an Normalanwendern mit sich, die sich an den neuen Trend heranwagen wollen. So auch Linux, das zunehmends für normale Endanwender ohne tiefschürfende Technik-Kenntnisse interessant wird. Auch wenn es viele eingefleischte Linux-Fans nicht gern hören, haben anwenderfreundliche Distributoren wie SuSE (www.suse.de) oder Red Hat (www.redhat.com) einen beachtlichen Beitrag zur Vereinfachung und dadurch zur höheren Verbreitung von Linux beigetragen.

Normalanwender pflegen es jedoch nicht sonderlich genau mit der Sicherheit zu nehmen. Das Absichern des eigenen Systems wird dann zum Glücksspiel: Man arbeitet sowieso immer als root, da man so am wenigsten behindert wird und Mailanhänge werden noch geoffnet, bevor man überhaupt den Inhalt des Mails gelesen hat. Dieser Umstand ist der zweite Hauptantrieb für die Verbreitung von Viren.

Was tun gegen Linux-Viren? Grundsätzlich gilt im Umgang mit Viren auf Linux das Gleiche, wie auch auf anderen Betriebssystemen [scip 2003]. Stellen Sie Ihren PC im BIOS so ein, dass er direkt von der Festplatte bootet und beim Aufstarten gar nicht erst auf Disketten- und Netzwerklaufwerke zugreift. Damit beugen Sie Bootsektor-Viren vor. Vermeiden Sie grundsätzlich das Öffnen unangeforderter Dateien (z.B. per Email) und Dateien unbekannter Herkunft.

Bei Multiuser-Betriebssystemen ist es von Vorteil, wenn man seine alltägliche Arbeit mit normalen Benutzerrechten ausführt. Wird auf diesem Account ein Virus eingefangen, kann sich dieser in erster Linie nur mit den Privilegien des infizierten Kontos verbreiten. Zugriffe auf wichtige Systemdateien sind dann bei einem richtig konfigurierten System nicht möglich.

Überprüfen Sie bestmöglich jede Datei, die von Ihrem Rechner benutzt werden soll, durch mindestens eine aktualisierte Antiviren-Software. Es bieten sich dafür verschiedene Lösungen (z.B. Amavis, Clamav und F-Prot Antivirus) an. Durchsuchen Sie alle (festen) Datenträger in regelmässigen Abständen mit einer aktualisierten Antiviren-Software nach bösartigen Programmen. Dies ist vor allem bei Dateiservern wichtig, auf denen viele verschiedene Dateien abgespeichert werden. Benutzt eine Grosszahl der Clients Windows, können Sie vielleicht durch diesen Schritt frühzeitig die Ausbreitung eines Windows-Virus in Ihrem Netzwerk entdecken.
In den meisten Fällen wird ein Computervirus erst durch seine Auswirkungen erkannt. Dies reicht von unnormalen Verhalten des Computers über Verzögerungen beim Öffnen, Bearbeiten und Schliessen von Dateien und den Rückgang des Arbeitsspeichers und des Speicherplatzes auf beschreibbaren Datenträgern bis hin zu Programmabstürze bei zuvor fehlerfrei funktionierenden Programmen und Veränderte oder fehlerhafte Dateien. Breitet sich ein Virus über ein Netzwerk aus, können zudem unerklärliche Netzwerkkommunikationen und eine Verlangsamung der Netzwerkverbindungen hinzukommen.

„Die fehlende Vorsicht der Benutzer macht Computerviren überhaupt erst möglich."

Bei Verdacht auf einen Virenbefall sollte man grundsätzlich Ruhe bewahren, um in der Hitze des Gefechts versehentlich keinen zusätzlichen Schaden anzurichten. Beenden Sie schnellstmöglich sämtliche Arbeiten auf dem

System. Trennen Sie die Netzwerkverbindung Ihres Computers, um eine Verbreitung über das Netzwerk zu verhindern. Schalten Sie den Rechner wie gewohnt ab und lassen Sie ihn ausgeschaltet. Sofern ein Anhaltspunkt auf die Existenz eines Computervirus ausgemacht werden konnte, informieren Sie sich über dieses schädliche Programm, um seine Funktionsweise und Auswirkungen zu verstehen. Unerfahrene Benutzer sollten keinesfalls alleine infizierte Dateien und Programme bereinigen. Handelt es sich um einen bisher unbekannten Computervirus, informieren Sie die Hersteller von Antiviren-Software und Sicherheits-Gruppen.

Fazit

Ein sich selber reproduzierendes Programm gilt als Computervirus (Diese Definition ist nicht ganz korrekt, denn Würmer weisen diese Eigenschaft ebenso auf). Ein jedes Betriebssystem stellt die Möglichkeit zur Verfügung, selber reproduzierende Programme zu erstellen.

Singleuser-Betriebssysteme begünstigen die Verbreitung solcher Computerviren, da sämtliche Benutzer administrative Rechte haben und ein eingefangener Virus mit den Privilegien des Benutzers agieren. Auch auf Multiuser-Betriebssystemen, wie Linux auch eins ist, sind Computerviren möglich. Halten sich jedoch sämtliche Anwender daran, den Grossteil ihrer täglichen Arbeit als normale Benutzer und nicht als root durchzuführen, erbt der Computervirus nur sehr wenig Rechte. Ihm ist sodann die Infektion systemwichtiger Daten nicht möglich, da schlichtweg die Lese- und Schreibrechte fehlen. In der Vergangenheit wurden jedoch auch schon Linux-Viren gesichtet, die durch das Ausnutzen einer lokalen Schwachstelle administrative Rechte erlangen konnten.

Je populärer ein Produkt wird, desto mehr Leute interessieren sich für dieses und umso mehr potentielle Angreifer beschäftigen sich damit. Die Defacement-Statistiken von Attrition.org haben gezeigt, dass mit der zunehmenden Verbreitung von Linux auch die Übergriffe auf dieses Betriebssystem sprunghaft angestiegen sind. Dieser Trend ist in seinen wichtigsten Punkten auch auf die Entwicklung der Computerviren für das freie System anwendbar.
Die Popularität, Verbreitung und Vereinfachung eines Produkts zieht unweigerlich normale Endanwender an, die nur ein sehr bedingtes technisches Grundwissen mitbringen. Diese stellen sodann die potentiellen Opfer dar, die ein Teil des Lebenszyklus eines Computervirus werden können.

Der Autor

Marc Ruef arbeitet als Security Consultant bei der schweizer Firma scip AG (http://www.scip.ch), welche sich auf Sicherheitsberatungen im Bankenumfeld spezialisiert hat. Er hat eine Vielzahl an Artikeln, Büchern und Übersetzungen im Bereich Computersicherheit publiziert, betreut einige namhafte internationale Projekte auf diesem Gebiet und unterrichtet an diversen Fachhochschulen sowie Universitäten.

Literaturverzeichnis

Bartolich, Alexander, 2002, The ELF Virus Writing HOWTO, http://www.lwfug.org/~abartoli/virus-writing-HOWTO/ html/; Dieses ziemlich unorthodoxe Howto führt sehr gut und umfassend in das Schreiben von ELF-Computerviren ein.

BSI, 1997, Informationen zu Computer-Viren, Geschichte der Computerviren, http://www.hu-berlin.de/bsi/viren/kap1/kap1_1.htm; Ein schon etwas älteres Dokument aus der BSI-Reihe. In diesem werden die Grundlagen Computerviren besprochen. Neben einem historischen Abriss werden auch der Aufbau und der Umgang mit sich selber reproduzierenden Programmen erläutert.

Cohen, Fred, 1984, Computer Viruses – Theory and Experiments, Computers & Security, Volume 6, 1987, Seiten 22 bis 35; Dr. Fred Cohen war einer der ersten, der sich intensiv mit Computerviren und ihren Auswirkungen auf bestehende Computersysteme beschäftigte.

Denning, Peter, 1990, Computers Under Attack: Intruders, Worms, and Viruses, ACM Press; Ein historischer Abriss der Entwicklung von Computerviren, der sehr gut die Anfänge der Szene-Bewegung skizziert.

Dickerson, Matt, Brian, Martin, 17. Mai 2001, OS Statistics: August 1999 to Present, Attrition.org, http://www.attrition.org/mirror/attrition/os.html;
Eine der wenigen Statistiken, die verlässlich über die Anzahl der verunstalteten Webseiten und die zugrundeliegenden Betriebssysteme berichtet. Leider wurde Sie nur von August 1999 bis Mitte Mai 2001 geführt.

Harley, David, Wenzel, George, Burrell, Bruce, 23. März 2000, alt.comp.virus FAQ Part 2/4, http://www.faqs.org/faqs/computer-virus/alt-faq/part2/; Diese FAQ fasst die wichtigsten und am meisten gestellten Fragen in der USENET-Gruppe alt.comp.virus zusammen. Eine gute

Quelle, um die grundlegenden Fragen zum Thema Computerviren zu beantworten.

Fromm, Erich, 1973, Anatomie der menschlichen Destruktivität, Rowolth Taschenbuchverlag, ISBN 3-499-17052-3; Erich Fromms umfassende Abhandlung über die Aggression gilt als eines der Standardwerke in der Aggressionsforschung. Sehr genau und unvoreingenommen durchleuchtet er vergangene Theorien und versucht neue Thesen zu entwickeln.

Sesterhenn, Eric, Münch, Martin J., 2002, Tux erkältet sich: Linuxviren im Vormarsch, Linux Enterprise, Ausgabe 12/2001, http://www.codito.de/text/linviren.html; Ein revolutionärer deutschsprachiger Artikel zum Thema Linux-Viren ist hier Eric Sesterhenn und Martin J. Münch gelungen. Sehr detailliert und mit Beispielen werden die Möglichkeiten dargelegt. Ein Muss für jeden Linux-Benutzer.

Nolting, Hans-Peter, 1978, Lernfall Aggression, Rowolth Taschenbuch Verlag, ISBN 3499602431; Hans-Peter Nolting ist mit diesem Buch eine hervorragende Zusammenfassung zeitgenössischer Aggressionstheorie gelungen. Sein Buch hat zwar, wie der Titel schon vermuten lässt, das Schwergewicht bei der Lerntheorie – Trotzdem werden auch andere Theorien neutral und objektive betrachtet. Eine gute Einführung in das Thema der Aggressionspsychologie.

Raymond, Eric, The New Hackers Dictionary, http://www.catb.org/~esr/jargon/html/entry/virus.html; Dieses umfassende Wörterbuch erklärt die Begriffe aus den Bereichen Computer, Hacking und Cracking. Eine gute Stütze, will man sich an ein neues Thema heranwagen und kommt nicht mit allen Begriffen zurecht.

Ruef, Marc, Gieseke, Wolfram, Rogge, Marko, Velten, Uwe, September 2002, Hacking Intern, Data Becker, Düsseldorf, ISBN 381582284X, http://www.amazon.de/exec/obidos/ASIN/381582284X/; Dieses Buch führt den Leser in die Welt der Computersicherheit ein. So werden klassische Themen wie Mapping, Scanning, Auswertung und Angriffe beschreiben. Aber auch Computerviren, Trojanische Pferde sowie Firewall- und Intrusion Detection-Systeme werden erläutert.

scip AG, 2003, Merkblatt Computerviren, http://www.scip.ch/publikationen/merkblaetter/computerviren/; Dieses Merkblatt der schweizer Security-Firma scip AG hält die wichtigsten Informationen zum Thema Computerviren bereit. Sehr schnell kann man so die Grundlagen wieder auffrischen.

Impressum

scip AG
Technoparkstrasse 1
CH-8005 Zürich
T +41 44 445 1818
mailto:info-at-scip.ch
http://www.scip.ch

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich IT-Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams im Jahre 2002 waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigen. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.