

Seminar Datensicherheit – Teil II / Anhang

PC sicher konfigurieren und betreiben

© 2000-2002, Red Star Software, rss@tele-commies.de

Private Kopie und Weitergabe gestattet

Veröffentlichung nur mit Zustimmung des Autors

Version 1.6, 27. Oktober 2002

Vorwort

„Ich gehe mit einem Stock umher und zwingen alle, sich das Internet anzueignen.“ Mit diesen Worten erklärte Gennadi Sjuganow auf einem Jugendkongress der Kommunisten in Moskau am 29.10.2000 die Notwendigkeit, sich mit zeitgemäßen Medien und Werkzeugen zu befassen.

Es gibt freilich auch Daten auf dem PC, die nicht für die Öffentlichkeit bestimmt sind. Daher behandelt dieses Dokument die Datensicherheit am eigenen PC – ohne Stock :-)

Danksagung

Die Erstellung und kostenlose Verteilung dieses Readers wurde durch die finanzielle Unterstützung der DKP Darmstadt ermöglicht.

Kontaktadressen

Rainer Keil	Arno Grieger
Heinr.-Fulda-Weg 13	Odenwaldring 11
64289 Kranichstein	64354 Reinheim
Tel. 06151/788407	Tel. 06162/85351
Fax 06151/788406	Fax 06162/85351


E-Mail: info@dkp-darmstadt.de

Homepage: www.dkp-darmstadt.de

Spenden

Wenn Ihnen der Reader gefallen hat, bitten wir um eine kleine Spende (5 €) für unsere Kreiskasse (Kennwort „Internet“):

Konto Nr. 107 562 62, SEB Offenbach, BLZ 505 101 11

Überweisungsauftrag an
 **Bank für Widerstand**
 12345 Karl-Marx-Stadt

EUR-Überweisung

Empfänger: Name, Vorname / Firma (max. 27 Stellen)
 DKP Darmstadt

Konto-Nr. des Empfängers 107 562 62 Bitte deutlich schreiben! Beleg wird maschinell gelesen. Bankleitzahl 50510111

bei (Kreditinstitut) SEB Offenbach


DM od. EUR Betrag: 5,00
 E U R

Kunden-Referenznummer - noch Verwendungszweck, ggf. Name und Anschrift des Auftraggebers - (nur für Empfänger)
 Rainer User
 noch Verwendungszweck (insgesamt max. 2 Zeilen à 27 Stellen)
 Internet

Kontoinhaber: Name, Vorname/ Firma, Ort (max. 27 Stellen, keine Straßen- oder Postfachangaben)

Konto-Nr. des Kontoinhabers 20 1

111 309 - 420 837

Datum, Unterschrift


Wegen maschineller Lesung Namenszug nicht über Balken hinausziehen!

Datum _____ Unterschrift _____

Inhaltsverzeichnis

A	Anweisungen für eilige Notfälle	3
B	Literaturhinweise	4
C	Internet-Links	6
D	Software zum Umsetzen des Seminars	7
E	Empfehlenswerte Programme	10
F	Nicht empfehlenswerte Programme	18

A Anweisungen für eilige Notfälle

RESTRICTED

DESTRUCTION NOTICE

WHY —To prevent the enemy from using or salvaging this equipment for his benefit.

WHEN—When ordered by your commander.

HOW

1. Smash—Use sledges, axes, handaxes, pickaxes, hammers, crowbars, heavy tools.
2. Cut—Use axes, handaxes, machetes.
3. Burn—Use gasoline, kerosene, oil, flame throwers, incendiary grenades.
4. Explosives—Use firearms, grenades, TNT.
5. Disposal—Bury in slit trenches, fox holes, other holes. Throw in streams. Scatter.

USE ANYTHING IMMEDIATELY AVAILABLE FOR DESTRUCTION OF THIS EQUIPMENT

WHAT

1. Smash—Headset, handset, all tubes, insulation, capacitors, resistors, transformers, knobs, gearings, batteries, panels, castings, relays, switches, etc.
2. Cut—All wiring in electrical circuits, battery connecting cables, etc.
3. Burn—All instruction books, circuit diagrams, insulation, codes, etc.
4. Bend—All antenna sections, switch lever contacts, chassis, etc.
5. Bury or scatter—Where possible dispose of debris in streams or bury.

DESTROY EVERYTHING

B Literaturhinweise

Nachfolgend eine Liste empfehlenswerter Artikel zum Weiterlesen.

Literatur

- [1] Norbert Luckhard, Windows für Einsteiger – Der Weg zum sicheren PC im Netz; Sicherheit im Netz – Glossar, c't Heft 4/2000 Seite 212ff
- [2] BSI, IT-Grundschutzhandbuch; Kostenlos auf CD-ROM zu beziehen (Bestellung via EMail an gshb@bsi.de), BSI (Bundesamt für Sicherheit in der Informationstechnik) 2000
- [3] Devid Espenschied, Schlüsseldienst; Von BIOS-Passwörtern und ihrer Überwindung, c't Heft 22/2000 Seite 312ff
- [4] Thomas M. Klockow, Linux? Aber Sicher!; Host- und Netzwerk-Sicherheit bei Linux, Linux Enterprise Heft 2/2000 Seite 65ff
- [5] Karsten Sohr, Sandkastenspiele; Java-Sicherheitsmodelle, c't Heft 11/2000 Seite 226ff
- [6] Stefan Jaeger, Gesetze und Lücken; Rechtliche Schritte gegen Angriffe im Netz, c't Heft 4/2000 Seite 232ff
- [7] PC Welt, Clever partitionieren; So partitionieren Sie richtig, PC Welt Heft 10/1999 Seite 156ff
- [8] Sven Schulz, Peter Siering, Benjamin Stein, Geplanter Seitensprung; Mehrere Betriebssysteme auf einem PC einrichten, c't Heft 18/1999 Seite 36ff
- [9] Dr. Volker Zota, Digitale Wohngemeinschaften; Mehrere Betriebssysteme auf einem PC einrichten, c't Heft 16/2000 Seite 92ff
- [10] Harald Bögeholz, Laurenz Weiner, Riesige Rundablage; Daten auf großen Festplatten organisieren und sichern, c't Heft 16/2000 Seite 100ff
- [11] André Zurawski, Sicher ist sicher; Mit Netscape und Internet-Explorer risikolos surfen, PC Online Heft 9/1999 Seite 78ff

- [12] Jo Bager, Holger Bleich, Patrick Brauch, Axel Kossel, Natürliche Abwehrkräfte; Windows und Internet-Software sicher konfigurieren, c't Heft 4/2000 Seite 214ff
- [13] Peter Siering, E-Mail sicher machen; Sicherheitseinstellungen unter Windows, c't Heft 12/2000 Seite 36
- [14] Dr. Oliver Diedrich, Liebesbriefe in die Tonne; ILOVEYOU und die Konsequenzen, c't Heft 13/2000 Seite 110ff
- [15] Jürgen Schmidt, Gut gerüstet; Die Gefahren des Internet meistern, c't Heft 20/2000 Seite 116ff
- [16] Patrick Brauch, E-Mail, aber sicher; Der richtige Umgang mit elektronischer Post, c't Heft 20/2000 Seite 120ff
- [17] Norbert Luckhardt, Windows für Einsteiger; Der Weg zum sicheren PC im Netz, c't Heft 4/2000 Seite 208ff
- [18] Jürgen Schmidt, Sicherheitsrisiko Microsoft; Die Kehrseite des Windows-Komforts, c't Heft 21/2001 Seite 140ff
- [19] Martin Rost, Arnold Wallisch, Dokumente durchkeuchtet; Was Office-Dateien verraten können, c't Heft 3/2002 Seite 172ff
- [20] Holger Bleich, Axel Kossel, Abzocke abblocken; Tipps gegen ungewollte 0190-Dialer, c't Heft 1/2002 Seite 180ff
- [21] Ulrike Duhm, 0190-Abzocke; Nach Surf-Spaß pleite, com!online Heft 3/2002 Seite 20ff
- [22] Andreas Schuster, Spionageabwehr; Kostenlose Mittel gegen Trojanische Pferde, Portscans und andere Schnüffler, PC Intern Heft 8/2000 Seite 53ff
- [23] PC Welt, Spione auf Ihrem PC?; Tipps: So schützen Sie sich vor Attacken, PC Welt Heft 9/2000 Seite 206ff
- [24] PC Welt, Test: Neue Firewalls; Das leisten Desktop-Firewalls, PC Welt Heft 9/2000 Seite 220ff

- [25] Jürgen Schmidt, Block-Buster; Personal Firewalls und Anti-Viren-Software richtig einsetzen,
c't Heft 4/2000 Seite 224ff
- [26] Andreas Marx, Schutz vor Ungeziefer; Richtiger Einsatz von Antiviren-Software,
c't Heft 13/2000 Seite 114ff
- [27] Elisabeth Bauer, Patrick Brauch, Inga Rapp, Brandschutz; Zehn Personal Firewalls im Test,
c't Heft 23/2001 Seite 174ff
- [28] Andreas Marx, Patrick Brauch, Schädlingssuche; 12 Antiviren-Programme im Vergleich,
c't Heft 2/2001 Seite 102ff

C Internet-Links

Nachfolgend eine Liste empfehlenswerter Internet-Links zum Weiterlesen, Nachschlagen oder Austesten.

www.av-test.de

Unabhängige Tests von Virensclannern.

www.bsi.de

Bundesamt für Sicherheit in der Informationstechnik. Hier gibt es u.a. das „Grundsicherungs-Handbuch“ (eher für Firmen ausgelegt, aber dennoch aufschlußreich).

www.datenschutz.ch

Der Datenschutzbeauftragte des Kantons Zürich (Schweiz) bietet u.a. einen Browser-Test, mit dem sowohl die Sicherheits-Einstellungen als auch die Datenschutz-Einstellungen des eigenen Browsers überprüft werden können.

www.dkp-darmstadt.de/dasi/

Weitere Materialien zum Seminar „Datensicherheit“.

www.eicar.org/anti_virus_test_file.htm

Das Programm „EICAR.COM“ ist vollkommen harmlos und dient zum Test der korrekten Funktion eines Virensclanners.

www.fortify.net/sslcheck.html

Hier kann man überprüfen, ob der benutzte WEB-Browser eine als sicher geltende Schlüssel-Länge (≥ 128 Bit) verwendet oder wegen der (früher schärferen) US-Export-Beschränkungen auf 40 Bit Schlüssel-Länge „kastriert“ wurde.

www.heise.de/ct/antivirus/emailcheck/

Die Computerzeitschrift c't stellt eine kostenlose Prüfmöglichkeit für EMail-Programme zur Verfügung.

vil.nai.com/VIL/hoaxes.asp (englisch)

Hinweise auf Hoax-E-mails (Viren-Forschungszentrum von Network Associates).

www.symantec.com/avcenter/hoax.html (englisch)

Hinweise auf Hoax-E-mails (Viren-Forschungszentrum von Symantec).

www.symantec.com/securitycheck/ (englisch)

Die Firma Symantec bietet einen Online-Sicherheitstest an, bei dem die Absicherung des eigenen Rechners gegen Hackerangriffe, Viren und Trojaner überprüft wird.

www.t-online.de/home/Albert.Rommel/

Beschreibung zum T-Online-Zugang über das DFÜ-Netzwerk (d.h. ohne Installation der Software von der T-Online CD-ROM).

www.tu-berlin.de/www/software/hoax.shtml

Hinweise (deutschsprachig) auf Hoax-E-mails (TU Berlin).

D Software zum Umsetzen des Seminars

D.1 Vorbemerkung

Die Beurteilungen der vorgestellten Software wurde nach bestem Wissen und Gewissen, sowie unter Ausschluß jeder Gewährleistung vorgenommen.

D.2 Übersicht über die empfohlenen Programme

Je nach Geldbeutel und Kenntnisstand des Benutzers kommen unterschiedliche Programme in Frage. So gibt es z.B. wirklich empfehlenswerte kostenlose Programme, die jedoch nur in englischer Sprache erhältlich sind. Die folgende Tabelle gibt einen Überblick.

Festplatten-Utilities			
Programm	Preis	Sprache	Geeignet für
Partition Magic	80 €	Deutsch	Alle
WWBMU	kostenlos	Deutsch	Experten
Drive Image	71 €	Deutsch	Alle
Partition Image	kostenlos	Deutsch	Experten
Virens Scanner			
Programm	Preis	Sprache	Geeignet für
Norton Antivirus	46 € (1)	Deutsch	Alle
H+BEDV AntiVir	kostenlos	Deutsch	Alle
Firewalls			
Programm	Preis	Sprache	Geeignet für
Zone Alarm	kostenlos	Englisch	Anfänger
Sygate Personal Firewall	kostenlos	Englisch	Experten
Tiny Personal Firewall	kostenlos	Englisch	Experten
Outpost Firewall	kostenlos	Deutsch	Alle
Norton Internet Security (2)	77 € (1)	Deutsch	Alle

Legende:

- (1) Für Schüler, Lehrer und Studenten gibt es Sonderpreise
- (2) Kombination aus Firewall, Virens Scanner und Datenschutz-Filter

Man kann bei entsprechenden Computer- bzw. Englisch-Kenntnissen prinzipiell für die meisten Aufgaben mit kostenloser Software auskommen – beim Virens Scanner sollte man jedoch zu einem kommerziellen Produkt mit effektiver EMail-Filterung greifen. Für den Computer-Anwender mit wenig Geld sind auch folgende Tips interessant:

1. Die Computer-Zeitschrift „PC Praxis“ veröffentlichte in der dem Heft 01/2002 der Zeitschrift beiliegenden CD-ROM das folgende Originalprogramm (Vollversion): McAfee PGP Personal Privacy (Version 6.5.8). Die Zeitschrift kostet 3,58 € pro Heft.
2. Die Computer-Zeitschrift „PC Welt“ veröffentlichte in der dem Heft 10/2001 der Zeitschrift beiliegenden CD-ROM das folgende Originalprogramm (natürlich mit legaler Seriennummer): PowerQuest Partition Magic (Version 5.01). Die Zeitschrift kostet 3,99 € pro Heft. Auch von anderen Computerzeitschriften wurde diese Programmversion schon auf CD-ROM beigelegt.
3. Die Computer-Zeitschrift „PC Welt“ veröffentlichte in der dem Heft 08/2001 der Zeitschrift beiliegenden CD-ROM das folgende Originalprogramm (natürlich mit legaler Seriennummer): PowerQuest Drive Image (Version 3.02). Die Zeitschrift kostet 3,99 € pro Heft.
4. Die Computer-Zeitschrift „PC Welt“ veröffentlichte in der dem Heft 06/2002 der Zeitschrift beiliegenden CD-ROM das folgende Originalprogramm (für die Seriennummer muß man ein Formular auf der WEB-Site des Herstellers

PowerQuest ausfüllen und eine EMail-Adresse angeben): PowerQuest Drive Image (Version 4.0). Die Zeitschrift kostet 3,99 € pro Heft.

Ältere Ausgaben der Zeitschrift „PC Welt“ können bestellt werden (per Rechnung, plus 5 DM Porto) bei:

Computerservice Jost GmbH
Postfach 14 02 20
80452 München
Tel : 089/209 59 132
Fax: 089/200 28 111

oder unter www.pcwelt.de/shop.

Wer die oben aufgeführten Zeitschriften-Ausgaben nicht mehr bekommen konnte, sollte über einen längeren Zeitraum regelmäßig die Titelseiten der einschlägigen Computerzeitschriften studieren. Hin und wieder werden diese (und andere interessante) Programme auch in neueren Ausgaben angeboten (z.B. im Heft „PC Magazin“).

Die auf den Zeitschriften-CDs enthaltenen Programme sind nicht die jeweils aktuellste Version, jedoch für die besprochenen Zwecke völlig ausreichend.

D.3 Hinweise zu Kauf und Einsatz der Software

Antiviren-Programme bieten nur begrenzte Sicherheit. Die aktuelle Software zur Erkennung und Bekämpfung von Viren kann immer nur auf bekannte Viren reagieren, ist somit zeitlich immer etwas im Rückstand. Zusätzlich entsteht eine Verzögerung dadurch, daß man sich ja nicht täglich die neueste Version seiner Virens Scanner-Software als Update herunterladen und installieren kann.

Man sollte auf keinen Fall mehrere Virens Scanner gleichzeitig installieren, auch nicht testweise – nach einem derartigen Test auf einem PC waren die Icons auf dem Windows-Desktop durcheinander, der Maustreiber erkannte eine zusätzliche Maus und die Internet-Verbindung hatte Benutzernamen und Paßwort „vergessen“.

Achtung: Ein gewisses Restrisiko bleibt immer beim Ändern bestehender Partitionen (z.B. Stromausfall), selbst bei kommerziellen Programmen.

Nochmal zur Erinnerung: Ein Boot-Manager mit Paßwort schützt nur, wenn man das Booten von Diskette oder CD-ROM unterbindet.

Für sämtliche nachfolgend beschriebene Software gilt, keine veraltete Version zu kaufen:

- Virens Scanner müssen aktuelle Erkennungs-Signaturen für Viren haben.
- Partitionierungs-Software muß auch Festplatten > 8 GB unterstützen.
- Image-Backup Software muß auch Festplatten > 8 GB unterstützen und nach Möglichkeit direkt auf CD-Rs/CD-RWs speichern können (Wichtig: Kompatibilität mit dem verwendeten CD-Brenner prüfen!).

- Die eingesetzte Software muß unter den eingesetzten Betriebssystemen (z.B. MS-Windows XP, Linux) lauffähig sein.

Der Autor kann leider nicht ständig neue Versionen der Software kaufen bzw. Testversionen herunterladen. Daher sind die angegebenen Programmversionen im Zweifelsfall diejenigen, die der Autor selbst getestet hat, auch wenn es bereits eine neuere Version geben sollte.

Preisvergleich lohnt sich beim Softwarekauf, wie man an den jeweils angegebenen Straßen- (bzw. Versand-) und Listenpreisen sieht. Viele Softwarehersteller (u.a. Microsoft, Borland, Symantec) bieten für Schüler, Studenten und Lehrer deutlich ermäßigte Preise für ihre Software an.

E Empfehlenswerte Programme

E.1 Einleitung

Der Autor stellt verbreitete und bewährte Software vor, überwiegend kommerzielle. Natürlich können nicht alle Programme auf dem Markt behandelt werden, d.h. hier nicht aufgeführte Programme müssen deshalb nicht unbedingt schlecht sein. Bei der Auswahl wurden überwiegend Programme berücksichtigt, die in deutscher Sprache erhältlich sind.

E.2 Partition Magic

Name	Version	Hersteller
Partition Magic	8.0	PowerQuest
Programmtyp	Partitionierung und Boot-Manager	
Preis	69 € (Straßenpreis) / 80 € (Liste)	

Partition Magic kann neue Partitionen anlegen und bestehende Partitionen ohne Datenverlust verkleinern, vergrößern, verschieben oder mit anderen Partitionen zusammenfügen – sinnvoll z.B. zwecks Freimachen von Plattenplatz für Installation von Linux oder einer zweiten Windows-Installation.

Die Software enthält auch einen Boot-Manager, mit dem man auch festlegen kann, welche Partitionen für welches Betriebssystem sichtbar sein sollen. Ein Paßwortschutz ist möglich, jedoch durch Booten von Diskette leicht zu umgehen.

Es handelt sich um ein leistungsfähiges und zuverlässiges Programm mit gutem technischen Support durch den Hersteller, das gegenüber FDISK einigen Komfort bietet, dafür aber extra Geld kostet.

Man kann sich das Geld allerdings sparen, wenn man seine Festplatte löscht und – nachdem wir ja jetzt wissen, worauf's ankommt – Betriebssystem und Anwendungen neu installiert, und zwar gleich auf von Anfang an richtig angelegten Partitionen.

Siehe auch den Tip auf Seite 8 (Partition Magic 5.0 kostenlose Vollversion auf Zeitschriften-CD).

E.3 WWBMU Bootmanager

Name	Version	Hersteller
WWBMU	6.2	Wolfgang Wirth
Programmtyp	Boot-Manager	
Preis	Freeware / Kostenlos	

Hinweis: Die Beschreibung beruht auf der dem Autor verfügbaren Vorgängerversion 6.1.

Dieser Bootmanager ist für den privaten Einsatz kostenlos.

Das Programm bietet folgende Funktionen:

- Auswahl einer aktiven aus maximal 4 primären Partitionen.
- Versteckt die nicht aktiven primären Partitionen, das Programm kann jedoch logische Laufwerke nicht verstecken.
- Multi-User Modus mit Paßwort möglich.
- Partitionen anlegen und löschen.

Leider gibt es kein ausdrucksbares Handbuch, nur eine Online-Hilfe. Diese Hilfedatei ist jedoch gut und humorvoll geschrieben.

Das Programm ist empfehlenswert und bietet auch eine Deinstallationsroutine.

E.4 Drive Image

Name	Version	Hersteller
Drive Image	2002	PowerQuest
Programmtyp	Image Backup Software	
Preis	64 € (Straßenpreis) / 71 € (Liste)	

Drive Image sichert komplette Festplattenpartitionen. Es erkennt alle verbreiteten Dateisysteme (FAT16, FAT32, NTFS, HPFS, Linux Ext2, Swap). Bei Bedarf können einzelne Dateien aus den Backups extrahiert werden.

Die Software erzeugt Image-Dateien und legt sie auf Wechselmedien oder Netzlaufwerken ab. Das Programm läuft im MS-DOS-Modus, allerdings mit einer grafischen Benutzeroberfläche. Das Programm kann die Image-Dateien auch auf mehrere Teile aufteilen. Images können ab Version 4.0 direkt auf einen CD-Brenner gesichert gespeichert werden. Diese dürfen aber nicht am USB-Port, der parallelen oder einer PCMCIA-Schnittstelle angeschlossen sein. Auch Streamer-Bandgeräte werden leider nicht unterstützt. PowerQuest veröffentlicht die Liste der unterstützten CD-Brenner auf seiner Website – es ist empfehlenswert, dort nachzuschauen ob der eigene CD-Brenner unterstützt wird: www.powerquest.com/driveimage/cdlist.html.

Dem Programm, das sich an fortgeschrittene Anwender richtet, liegt ein ausführliches Handbuch bei.

Der Autor führte einen aufwendigen Backup-Test mit Drive Image durch. Partitionen mit FAT16, NTFS und Ext2 Dateisystemen wurden auf CDs gesichert und auf einer zweiten Festplatte wiederhergestellt. Nach der Wiederherstellung

wurden sämtliche Dateien anhand mathematischer Prüfsummen mit dem Original verglichen, wobei keine Fehler festgestellt werden konnten.

Die Software ist etwas pingelig mit den Einträgen der Partitionstabelle, man sollte vermeiden die Festplatte mit verschiedenen Tools zu partitionieren.

Der Autor setzt Drive Image selbst ein und empfiehlt es zur Datensicherung. Das Programm ist zwar 50% teurer als das Konkurrenzprodukt von Norton/Symantec – dafür funktioniert es aber wenigstens.

Siehe auch den Tip auf Seite 8 (Drive Image 4.0 kostenlose Vollversion auf Zeitschriften-CD).

E.5 Partition Image

Name	Version	Hersteller
Partition Image	2.1	Wolfgang Wirth
Programmtyp	Image Backup Software	
Preis	Freeware / Kostenlos	

Mit Partition Image lassen sich 1:1-Kopien von Partitionen anlegen und zu-rücksichern.

Die Sicherungen werden in Dateien geschrieben, wobei eine Aufteilung auf mehrere Dateien möglich ist, so daß diese auf CD-Rs oder andere Medien passen.

Die Software kann leider weder Daten komprimieren noch die unbenutzten Sektoren weglassen. Daher erzeugt dieses Programm die größten Backup-Dateien im Vergleich zu den kommerziellen Konkurrenten. Die Backup-Dateien können auch nicht direkt während des Backups auf CDs „gebrannt“ werden. Man kann die Backup-Dateien jedoch auf Festplatte speichern und später auf CD-Rs brennen.

Leider gibt es kein ausdrucksbares Handbuch, nur eine Online-Hilfe.

Das Programm hat weniger „Features“ als die kommerziellen Image Backup Programme, aber es versieht auch zuverlässig seinen Dienst.

Das Programm ist empfehlenswert. Mit den kommerziellen Programmen spart man hingegen Zeit und CD-Rohlinge, da deren Image-Dateien deutlich kleiner sind (Faktor 2-3) und auch direkt auf CDs gebrannt werden können.

E.6 PGP

Name	Version	Hersteller
PGP	7.0	Network Associates
Programmtyp	Verschlüsselungs-Software	
Preis	Freeware (für private Verwendung, ohne PGPdisk) / ca. 40 € (kommerzielle Version mit PGPdisk)	

PGP ist bekannt als Verschlüsselungstool für E-Mails. Darüber hinaus bietet PGP weitere, weniger bekannte, nützliche Funktionen:

- PGPtools kann mit „Wipe Disk“ sämtlichen freien Festplattenplatz (der ja noch Reste von geheimen Dateien enthalten kann) mehrmals überschreiben

und so effektiv löschen. PGPtools ist auch in der kostenlosen PGP-Version enthalten.

- PGPdisk (nur in der kommerziellen PGP-Version enthalten) kann ein verschlüsseltes „Laufwerk“ anbieten, das nur mit korrektem Schlüssel und Passphrase gelesen werden kann. Dieses Programm ist einfach genial!

Der Autor bemerkte beim Test einen Programmfehler in PGP: Wenn die vom Benutzer gewählte „Passphrase“ einen Umlaut enthielt, ließen sich die auf der PGPdisk gespeicherten Daten nicht mehr lesen (die Passphrase wurde beim Entschlüsseln nicht akzeptiert)!

Ein Nachteil der Software ist die undurchsichtige Vertriebspolitik des Herstellers für die kommerziellen Versionen. Man muß lange suchen, bis man einen Händler findet. Auch für Privatanwender gibt es ein gutes Argument zum Kauf der kommerziellen Version von PGP, nämlich das Tool „PGPdisk“. Leider hat Network Associates beschlossen, die Weiterentwicklung der kommerziellen PGP-Produkte einzustellen.

Die Praxis der Verschlüsselung soll in Teil IV des Seminars behandelt werden.

Siehe auch den Tip auf Seite 8 (PGP 6.5.8 kostenlose Vollversion auf Zeitschriften-CD).

E.7 Norton AntiVirus 2003

Name	Version	Hersteller
Norton Antivirus	2003	Symantec
Programmtyp	Virenschanner	
Preis	39 € (Straßenpreis) / 46 € (Liste)	

Der Virenschanner ist auch für Computerlaien leicht zu bedienen, bezüglich der Virenerkennung jedoch nicht ganz so gut wie das Konkurrenzprodukt „VirusScan“ von McAfee. Insbesondere bei der Erkennung von Trojanern und BackDoor Software schneidet das Programm nicht so gut ab. Bei der Reparatur von virenbefallenen Dateien oder Rechnern soll die Software jedoch brauchbar sein, d.h. weniger schlecht als andere Programme.

Die Benutzeroberfläche ist verständlich und „designmäßig“ unaufdringlich. Die Aktualisierung per Internet ist leicht zu bedienen und funktioniert zuverlässig (sofern der Symantec-Server nicht gerade überlastet ist). Die CD-ROM ist bootfähig, um im Notfall ohne lauffähiges Betriebssystem einen Virenschanner durchzuführen (funktioniert leider nicht mit NTFS-formatierten Partitionen).

Eine spürbare Verlangsamung des PC (beim Hochfahren des PCs und beim Starten von Programmen) ist festzustellen, siehe Kapitel E.13.

Noch ein Hinweis: Man sollte mit dem Programm eine „Emergency-Diskette“ anlegen. Auf die erste Diskette sollte man auch noch die Programmdatei „SMART-DRV.EXE“ auf die Diskette kopieren und per Editor in der „AUTOEXEC.BAT“ aktivieren, was den Virenschanner der kompletten Festplatte gewaltig beschleunigt.

Ein empfehlenswertes Programm.

E.8 H+BEDV AntiVir Personal Edition

Name	Version	Hersteller
AntiVir PE	6.12	H+BEDV Daten-technik
Programmtyp	Virenschanner	
Preis	Freeware (für private Verwendung) / Kostenlos	

AntiVir PE scannt einzelne Dateien oder Verzeichnisse bzw. Festplatten nach Viren (on-demand). Weiterhin werden gelesene oder erzeugte Dateien auf Viren überwacht (on-access).

Das Programm ist recht übersichtlich und problemlos zu konfigurieren. Per Internet kann die Software aktualisiert werden. Eine Notfall-CD bzw. -Diskette fehlt in der Freeware-Version.

Das Programm schneidet bei der Erkennung von Viren nicht schlecht ab, jedoch weniger gut als z.B. die kostenpflichtigen Produkte von Norton oder McAfee. Ein Nachteil der Software sind die laut Testberichten häufigen Fehlalarme. E-Mails werden leider nicht beim Empfang gescannt, d.h. an E-Mails angehängte Viren werden erst beim Versuch des Ausführens festgestellt! Bei der Beseitigung von Viren aus befallenen Dateien ist die Software jedoch weniger leistungsfähig – aber wir hatten uns ja vorgenommen, den Virenschanner vorher zu installieren, nicht nachher!

Das Programm ist für den privaten Gebrauch kostenlos.

Ein empfehlenswertes Programm.

E.9 Zone Alarm

Name	Version	Hersteller
Zone Alarm	2.6	Zone Labs
Programmtyp	Software-Firewall	
Preis	Freeware / Kostenlos	

Zone Alarm überwacht als Software-Firewall die TCP/IP Verbindungen in das und aus dem Internet.

Der Anwender kann die Programme auf seinem PC angeben, die Verbindungen ins Internet aufbauen dürfen. Man kann den Betrieb von Servern auf dem eigenen PC grundsätzlich unterbinden – eine sinnvolle Option, da es sich hier meist um Trojaner handelt.

Sowohl die angezeigten Alarme wie auch der „Not-Aus“ Knopf sind sehr plakativ gehalten. Das Programm ist vielleicht nicht das optimale Spielzeug für den Netzwerk-Experten, für den „Normal-Anwender“ jedoch gut verständlich und nachvollziehbar: die Konfiguration bietet relativ wenige, aber brauchbare Einstellungsmöglichkeiten.

Zone Alarm berücksichtigt auch Internetverbindungen über die proprietäre T-Online Software.

Das Programm behauptet auch, einen Schutz gegen Viren in E-Mails zu bieten. In Tests war von diesem Schutz jedoch nicht viel festzustellen.

Das Programm ist für den privaten Gebrauch kostenlos. Das Programm ist in englischer Sprache, eine separate deutsche Anleitung existiert jedoch im Internet.

Ein empfehlenswertes Programm, der Einsatz ist sinnvoll in Kombination mit einem Virens scanner.

E.10 Sygate Personal Firewall

Name	Version	Hersteller
Sygate Personal Firewall	4.2	Sygate
Programmtyp	Software-Firewall	
Preis	Freeware (für private Verwendung) / Kostenlos	

Sygate Private Firewall überwacht als Software-Firewall die TCP/IP Verbindungen in das und aus dem Internet.

Die Firewall-Regeln können sowohl Programm-übergreifend (mit Vorrang) als auch spezifisch für einzelne Programme angegeben werden.

Das Programm ist professionell und effektiv. Die Log-Ausgabemöglichkeiten sind sehr umfangreich.

Das Programm ist für den privaten Gebrauch kostenlos. Das Programm ermahnt einen ständig, sich beim Hersteller zu registrieren. Das Programm ist in englischer Sprache.

Ein empfehlenswertes Programm, der Einsatz ist sinnvoll in Kombination mit einem Virens scanner.

E.11 Tiny Personal Firewall

Name	Version	Hersteller
Tiny Personal Firewall	2.0	Tiny Software
Programmtyp	Software-Firewall	
Preis	Freeware (für private Verwendung) / Kostenlos	

Tiny Personal Firewall überwacht als Software-Firewall die TCP/IP Verbindungen in das und aus dem Internet.

Das Programm ist recht klein und paßt auf eine Diskette.

Das Programm ist effektiv (die Grundeinstellungen sind sicher, es existiert ein Schutz gegen Trojaner die unter gefälschten Programm-Namen auftreten), die Dokumentation sollte umfangreicher (und fehlerfreier) sein.

Leider müssen oft IP-Adressen (statt Hostnamen) angegeben werden.

Das Programm ist für den privaten Gebrauch kostenlos. Das Programm ist in englischer Sprache, eine separate deutsche Anleitung existiert jedoch im Internet.

Ein empfehlenswertes Programm, der Einsatz ist sinnvoll in Kombination mit einem Virens scanner.

E.12 Outpost Firewall

Name	Version	Hersteller
Outpost Firewall	1.0 beta	Agnitum
Programmtyp	Software-Firewall	
Preis	Freeware / Kostenlos	

Outpost Firewall überwacht als Software-Firewall die TCP/IP Verbindungen in das und aus dem Internet.

Der Anwender kann die Programme auf seinem PC angeben, die Verbindungen ins Internet aufbauen dürfen. Im „Lern-Modus“ fragt die Software bei jedem Zugriff eines Programms nach, und erlaubt, eine Zugriffsregel aufzustellen.

Die Firewall Software ist vom Funktionsumfang vergleichbar mit den Firewalls von Tiny Software oder Sygate. Ein kurzer Test ergab keine Sicherheitslücken, das automatische Update funktionierte noch nicht richtig.

Das Programm ist für den privaten Gebrauch kostenlos. Das Programm ist in deutscher Sprache.

Ein empfehlenswertes Programm, der Einsatz ist sinnvoll in Kombination mit einem Virenschanner.

E.13 Norton Internet Security 2003

Name	Version	Hersteller
Norton Internet Security	2003	Symantec
Programmtyp	Firewall + Virenschanner	
Preis	65 € (Straßenpreis) / 77 € (Liste)	

Diese Kombination aus Internet-Firewall und Virenschanner wird in Testberichten und Vergleichstests empfohlen.

Der Firewall ist deutlich leistungsfähiger und feiner konfigurierbar als z.B. die kostenlose Alternative „Zone Alarm“. Für den „Normal-Anwender“ ist die Bedienung gut verständlich, der Experte muß sich zwar etwas umständlich durch einige Menüs bewegen, kann dann aber die Firewallregeln detailliert einstellen. Für den Experten, der sich mit IP-Adressen und Portnummern gut auskennt, gibt es allerdings auch kostenlose Firewall-Alternativen (Sygate Personal Firewall, Tiny Personal Firewall).

Der Virenschanner entspricht von der Funktionalität „Norton AntiVirus 2003“, siehe Kapitel E.7. Allerdings ist die diesbezügliche Beschreibung im Handbuch abgespeckt, das Original-Handbuch zu „Norton AntiVirus 2003“ läßt sich jedoch als PDF-Datei auf der CD-ROM anschauen oder ausdrucken.

Zusätzlich bietet das Programm die Funktion „Privacy Control“, bei der das Versenden von Kreditkarten-Nummer und ähnlichen sensiblen Daten ins Internet abgeblockt wird. Der Nachteil ist natürlich, daß man all diese sensiblen Daten erst einmal per Konfiguration dem Programm bekanntmachen muß. Ob sie dort gut geschützt sind und ob sie möglicherweise durch eine Hintertür des Programms in falsche Hände geraten, ist aus Anwendersicht nicht überprüfbar.

Leider ist das Handbuch nicht so ausführlich wie es zum Verständnis von IP-Adressen, Ports und Protokollen wünschenswert wäre. Auf der halben Seite, auf welcher versucht wird, IP-Adressen und Protokolle zu erklären, sind zudem einige Fehler enthalten.

Außerdem schlägt das Programm sowohl bei der Installation als auch bei der Erstellung von Firewall-Regeln regelmäßig Einstellungen vor, welche nur geringe Sicherheit bieten. Die automatisch erstellten Regeln sowie die unkritische Übernahme der vom Programm vorgeschlagenen Regeln bieten keinen besseren Schutz als die kostenlose Alternative „Zone Alarm“. Wenn man jedoch die Regeln sorgfältig manuell erstellt, bzw. die vom Programm vorgeschlagenen Regeln richtig korrigiert, läßt sich ein deutlich besserer und flexiblerer Schutz als mit der Freeware-Alternative Zone Alarm erzielen. Bei ausreichenden Englisch- und TCP/IP-Kenntnissen kann man jedoch auch die privat kostenlos nutzbaren Produkte Sygate Personal Firewall oder Tiny Personal Firewall benutzen.

Ebenfalls ist es schade, daß man die so sorgfältig definierten Regeln des Firewalls weder ausdrucken noch in eine Datei abspeichern kann.

Bei einem Test unter Windows 98 SE wurde der PC nach Installation von „Norton Internet Security 2001“ nur geringfügig langsamer (Booten: 100 sec statt 90 sec; MS Word 97 starten und Dokument öffnen: 4 sec, mit oder ohne Aktivierung von NIS gleich).

Auch der Autor hat aufgrund der positiven Testberichte ebenfalls dieses Programm gekauft und empfiehlt es aufgrund der umfassenden Funktion und leichten Bedienbarkeit weiter. Allerdings wurde innerhalb eines Jahres der Rechner (unter Windows NT) mehrmals durch fehlerhafte Updates von Symantec unbenutzbar, so daß die Verwendung ohne ein sicher funktionierendes Backup nicht ratsam erscheint.

E.14 SuSE Linux

Name	Version	Hersteller
SuSE Linux	8.1	SuSE
Programmtyp	Betriebssystem, Anwendungen, Support	
Preis	50 € (Personal Version) / 80 € (Professional Version)	

Linux empfiehlt sich als Alternative zu MS-Windows, insbesondere wenn man auf Installation und Konfiguration Einfluß nehmen will und nicht darauf vertrauen will, daß „MS-Windows es schon richtig macht“.

SuSE Linux ist die in Deutschland meistverbreitete Linux Distribution und wird als „Personal Version“ (3 CD-ROMs, 3 Handbücher, 50 €) oder als „Professional Version“ (7 CD-ROMs, 4 Handbücher, 80 €) angeboten. Für den Heimanwender ist die preisgünstigere „Personal Version“ (3 CD-ROMs) ausreichend. Das zusätzliche Handbuch der „Professional“ Version ist jedoch fast schon den Mehrpreis wert.

Der Hersteller bietet 60 Tage (Personal) bzw. 90 Tage (Professional) Support bei Fragen und Problemen zur Installation.

Die Programme und Dokumentation sind zum großen Teil in deutscher Sprache.

Die Besonderheit der Linux-Distribution von SuSE ist die sehr gute Unterstützung für ISDN und hierzulande anzutreffende Internet-Provider.

Die Standard-Konfiguration ist (wie bei den meisten anderen Linux-Distributionen auch) in Bezug auf Datensicherheit verbesserungsbedürftig.

SuSE Linux ist eine ausgereifte und gerade für hiesige Verhältnisse empfehlenswerte Linux Distribution. Ohne Computerkenntnisse und Einarbeitung in Linux wird man aber nicht weit kommen.

F Nicht empfehlenswerte Programme

F.1 Einleitung

Nicht jede Software taugt auch, und wird trotzdem für teures Geld verkauft. Andererseits gibt es auch teure und gute Software, die jedoch nicht für den Heim-PC gedacht und geeignet ist. Deshalb sollen hier deshalb auch die nach Ansicht des Autors weniger empfehlenswerten Programme erwähnt werden. Auf diese Weise soll es dem Leser erspart bleiben, unnötig „Lehrgeld“ zu bezahlen!

Um dem Sponsor dieses Readers juristische Scherereien mit den Herstellern der „nicht empfehlenswerten“ Programmen zu ersparen, werden keine Details zu den einzelnen bemängelten Programm-Fehlern angegeben. Bei Interesse an Details wende man sich an den Autor persönlich.

F.2 PTS Boot Manager Pro 2000

Name	Version	Hersteller
Boot Manager Pro	2000	PTS / bhv
Programmtyp	Boot Manager	
Preis	3 € (Wühltisch) / 25 € (Liste)	

Nach Test dieser Software kommt der Autor zum Ergebnis:
Nicht Empfehlenswert (Details zensiert)!

F.3 PTS Drive Backup 2000

Name	Version	Hersteller
Drive Backup	2000	PTS / bhv
Programmtyp	Image Backup Software	
Preis	3 € (Wühltisch) / 25 € (Liste)	

Nach Test dieser Software kommt der Autor zum Ergebnis:
Nicht Empfehlenswert (Details zensiert)!

F.4 Norton Ghost

Name	Version	Hersteller
Norton Ghost	2002	Symantec
Programmtyp	Image Backup Software	
Preis	41 € (Straßenpreis) / 46 € (Liste)	

Hinweis: Die Beschreibung beruht auf der dem Autor verfügbaren Vorgängerversion 2001.

Nach Test dieser Software kommt der Autor zum Ergebnis:
Nicht Empfehlenswert (Details zensiert)!

F.5 Drive Star

Name	Version	Hersteller
Drive Star	2.05	Star Tools
Programmtyp	Image-Backup	
Preis	Shareware / 20 €	

Nach Test dieser Software kommt der Autor zum Ergebnis:
Nicht Empfehlenswert (Details zensiert)!

F.6 VirusScan

Name	Version	Hersteller
McAfee VirusScan	6.0	Network Associates
Programmtyp	Virens scanner	
Preis	25 € (Straßenpreis) / 40 € (Liste)	

Nach Test dieser Software kommt der Autor zum Ergebnis:
Nicht Empfehlenswert (Details zensiert)!

F.7 PGP Desktop Suite

Name	Version	Hersteller
PGP Desktop Suite	7.0	Network Associates
Programmtyp	Firewall + PGP (kommerz. Version)	
Preis	45 € (Straßenpreis) / 45 € (Liste)	

Nach Test dieser Software kommt der Autor zum Ergebnis:
Nicht Empfehlenswert (Details zensiert)!

F.8 McAfee Internet Security

Name	Version	Hersteller
McAfee Internet Security	4.01	Network Associates
Programmtyp	Firewall + Virens scanner	
Preis	60 € (Straßenpreis) / 60 € (Liste)	

Nach Test dieser Software kommt der Autor zum Ergebnis:
Nicht Empfehlenswert (Details zensiert)!

F.9 Warum in diesem Kapitel „Details zensiert“ steht

Das deutsche Computermagazin c't berichtete Anfang 2002 über Versuche von Network Associates, unvoreilhaft Besprechungen ihrer Softwareprodukte zu zensieren, sowie erste Gegenwehr gegen solche Eingriffe in Meinungsfreiheit und Verbraucherschutz. Nachfolgend der c't Artikel:

Network Associates wegen Zensur verklagt

Der Justizminister des Bundesstaates New York beschuldigt Network Associates (NAI) der Zensur. In einer Klage gegen den Software-Hersteller und Sicherheits-Spezialisten wirft Eliot Spitzer NAI vor, durch Bestimmungen in Software-Lizenzen das Recht auf freie Meinungsäußerung zu beschränken.

Laut der Klage, die sich vor allem auf Antivirus- und Firewall-Software der NAI-Tochter McAfee bezieht, will NAI verhindern, dass über die Produkte unkontrolliert in der Öffentlichkeit diskutiert wird. Beim Download der Software werde den Nutzern eine Vereinbarung präsentiert, die eine Klausel enthalte, nach der Produktbesprechungen oder Benchmark-Ergebnisse nicht ohne Erlaubnis des Herstellers veröffentlicht werden dürften. Dies erfüllt nach Ansicht von Spitzer den Tatbestand der Zensur und verletzt die in der amerikanischen Verfassung verankerten Rechte zur freien Meinungsäußerung: „Egal, ob es um eine politische Debatte geht oder um eine Diskussion, welche Software man kaufen soll: Wir müssen freie und offene Rede vor Einschüchterung in Schutz nehmen, um das Recht der Öffentlichkeit auf Information zu bewahren.“

Die Klage, die beim obersten Gericht des Bundesstaates New York eingereicht wurde, bezieht sich auf einen Fall, in dem NAI bereits die Vertragsklausel benutzte, um das Magazin Network World zur Rücknahme einer negativen Besprechung von McAfees Firewall-Software zu zwingen. NAI-Sprecher betonten allerdings, die Bestimmung diene lediglich dazu, eine Kontrolle zu ermöglichen, dass in Besprechungen immer die neuesten Software-Versionen benutzt würden. Man sei immer darum bemüht, dass Kunden die besten und vor allem aktuelle Informationen bekommen, wenn sie eine Kaufentscheidung treffen, hieß es bei NAI. Die Bestimmungen seien übrigens inzwischen auch geändert worden, sodass sich dies mehr wie eine Aufforderung als eine bindende Klausel lese. Aber selbst mit der ursprünglichen Fassung sei man im Recht gewesen, verteidigte sich NAI gegen die Klage des New Yorker Justizministers. (jk/c't)