

Matthias Schüssler

Kummerbox 07

Antworten auf die brennendsten Computerprobleme.

TagesAnzeiger

MIDAS

Matthias Schüssler ist Informatik-Journalist, Web-Autor und Programmierer (www.clickomania.ch). Er schreibt seit April 2000 für den «Tages-Anzeiger», betreut die Kummerbox und zeichnet für den «Tipp der Woche» verantwortlich. Er ist zudem Mitbegründer und Produzent des «Digitalk», einem wöchentlichen Podcast des «Tages-Anzeigers», in dem Experten aus der Computerszene News und Trends diskutieren. Der Podcast kann kostenlos unter www.tagi.ch/digitalk angehört und abonniert werden.

Die Arbeit an den Texten und Abbildungen dieses Buches erfolgte mit grösster Sorgfalt. Trotzdem können Fehler nicht komplett ausgeschlossen werden. Weder der Autor noch der Verlag können für fehlerhafte Angaben und deren Folgen irgendeine Form der Haftung übernehmen; jede Gewährleistung ist ausdrücklich ausgeschlossen. Der Autor empfiehlt, vor Veränderungen an Hard- und Software eine Sicherheitskopie aller Daten zu erstellen.

Alle erwähnten Firmen- und Markennamen sowie Produktbezeichnungen sind Eigentum der jeweiligen Inhaber und unterliegen firmen-, marken-, patent- oder wettbewerbsrechtlichem Schutz.

Alle Rechte vorbehalten, einschliesslich derjenigen des auszugsweisen Abdrucks und der elektronischen Wiedergabe

© 2007 Midas Computer Verlag AG

Lektorat: Elisabeth Schüsslbauer

Umschlag: Thomas Dätwyler

ISBN: 978-3-907020-XX-X

www.midas.ch

Vorwort

Diesen Januar schlug der Puls der Apple-Gemeinde noch einen Tick höher als sonst. In San Francisco war mit der «Macworld» das langersehnte, jährliche Klassentreffen angesagt. Höhepunkt dieser ausgeklügelten Präsentations-Show ist jeweils der Auftritt des Unternehmenschefs Steve Jobs. Im Vorfeld hatte Verkaufstalent Jobs geschickt durch absolute Geheimhaltung die Fantasien erst richtig angekurbelt. Die Internetforen waren voll von Spekulationen. Schliesslich erfüllte er die hohen Erwartungen souverän – mit der Vorstellung des ersten Apple-Handys iPhone, das den Trend der totalen digitalen Vernetzung aller Medien eindrucksvoll verkörpert: Telefon, Musik- und Videoplayer, Digitalkamera, Navigationsgerät, Organizer und Internet-Browser in einem. Im 31. Jahr des Bestehens von Apple strich Jobs die Bezeichnung Computer aus dem Firmennamen und nennt das Unternehmen künftig nur noch Apple Inc. Die Botschaft ist klar: Apple ist viel mehr als ein reiner Computerhersteller, er ist ein Multimediakonzern.

Vieles, was früher Zukunftsmusik war, ist machbar geworden. Die Frage bleibt, ob eine Mehrheit diese neuen Entwicklungen nutzen beziehungsweise sich leisten will. Die Lücke zwischen den Möglichkeiten neuer Technologien und ihrer tatsächlichen Nutzung wird immer grösser. Das liegt etwa daran, dass einem Teil der Kunden das Zusammenwachsen der Geräte gar nicht so wichtig ist. Manche interessiert nur, dass das Teil schick aussieht, dass man damit telefonieren und smsen kann, es leicht zu bedienen und erschwinglich ist. Hinzu kommt, dass es *den* Kunden gar nicht mehr gibt. Zwischen den Fernseh-, Internet- und Handynutzern im Alter von 14 bis 74 Jahren klaffen Welten, ebenso zwischen Männern und Frauen. So zerfällt die Käuferschaft in immer kleinere Grüppchen mit speziellen Interessen, in Onlin gamer und Internetshopper, in Musikdownloader und Hobbyfotografen und in solche, die einfach nur traditionell Fernsehen schauen wollen.

Genauso unterschiedlich wie ihre Bedürfnisse und Anforderungen sind deren tägliche Sorgen und Nöte. Das spiegelt sich auch in den Fragen, welche die Leserinnen und Leser des «Tages-Anzeigers» an Matthias Schüssler stellen. Es werden von Jahr zu Jahr mehr. Das mag daran liegen, dass die digitale Welt für viele fester Bestandteil unseres Lebens geworden ist, es liegt aber auch an den verständlichen und sehr kenntnisreichen Hilfestellungen Schüsslers. Die Rubrik «Kummerbox» ist in den letzten Jahren zu einem festen Markenzeichen des «Tages-Anzeigers» geworden.

Zürich, im Mai 2007

Daniela Decurtins

Stv. Chefredaktorin «Tages-Anzeiger»


Inhalt


Vorwort von Daniela Decurtins	5
Sicherheit.....	9
Wie man Virenresistenz entwickelt	10
Schadenssoftware hat keine Chance!	19
Hardware	21
Den Gerätepark im Griff.....	22
Wie das Netzwerk, der Drucker und der Brenner mitspielen	25
Windows-System	31
Therapien gegen Windows-Ärger.....	32
Nothelferkurs für Windows.....	44
Schneller in die Gänge kommen	52
Wenn der Desktop verrückt spielt	54
Desktop in Top-Verfassung.....	58
Wissenswertes über Windows.....	63
Datenverwaltung.....	65
Schneller finden, was wichtig ist.....	66
Daten und Dokumente, aufgeräumt und ordentlich	68
Mac-System	73
Hilfe naht, wenn der Mac Mucken macht.....	74
Mac-Pannen schnell beseitigen	78
Mobil-Computing.....	81
Unterwegs auf Draht	82
Handreichungen fürs Handy	88
Surfen	89
Am Pannestreifen der Datenautobahn	90
Web-Mysterien klären	93
Im Web auf Entdeckungsreise.....	98

Den Browser-Turbo einlegen.....	104
Flotte Firefox-Finten	108
E-Mail	111
Da geht die elektronische Post ab	112
Das Postfach auf Vordermann bringen.....	115
Subito-Hilfe für Outlook Express.....	121
Mit Thunderbird abheben	127
Office	129
Wie man als Büroarbeiter brilliert	130
Maximale Office-Gestaltungsfreiheit.....	136
Tipps für Office-Harmonie	139
Wo Büro-Missgeschicke lauern.....	142
Word an die Kandare nehmen	144
Planen, aber systematisch.....	152
Schnelle Excel-Einsichten	157
Tricks gegen üble Outlook-Ticks.....	166
Wie Powerpoint die Nerven schont	171
Multimedia	173
Mit seinen Digitalfotos ein tolles Bild abgeben.....	174
Verrutschte Pixel zurechtrücken.....	181
Bei MP3 voll dabei.....	185
Ein Musikgehör für Soundprobleme.....	195
Bewegte Bilder kommen in Fahrt	201
Wilde Video-Wirrnisse	208
Digitales Vergnügen	211
Software, über- und ausserirdisch.....	212
Spielerischer Zeitvertreib	214
Index	221

Die Symbole in diesem Buch

Der Schwierigkeitsgrad und der Anwendungsbereich der Beiträge in diesem Buch sind gekennzeichnet. Folgende Symbole finden Verwendung:


 Die grauen Kästchen mit weisser Schrift bezeichnen das Betriebssystem. Soweit keine Version des Betriebssystems angegeben ist, gilt der Tipp für alle Versionen mit folgender Einschränkung: Wir berücksichtigten die Betriebssysteme ab MacOS 9 und ab Windows 98.


 Bitte haben Sie Verständnis dafür, dass bei allgemeinen Tipps zu mehreren Versionen des Betriebssystems unter Umständen nicht alle erwähnten Möglichkeiten auf jeder Version zur Verfügung stehen.


 Dieses Symbol bezeichnet einen Tipp für Windows XP.


 Dieses Symbol bezeichnet einen Tipp für Windows Vista.


 Dieses Symbol bezeichnet Windows 2000.


 Dieses Symbol bezeichnet Mac OS X.

 Dieses Symbol bezeichnet Mac OS 9.

 Dieses Symbol bezeichnet einen Tipp, in dem eine Software vorgestellt wird, die auch unter Linux eingesetzt werden kann.

 Dieses Symbol bezeichnet bei einem Frage-Antwort-Beitrag einen Tipp, der auch von ungeübten Anwendern gefahrlos umgesetzt werden kann.

 Dieses Symbol bezeichnet einen Tipp, der tiefere Eingriffe ins Betriebssystem nötig macht und nur von Anwendern ausgeführt werden sollte, die sich ihrer Sache sicher sind. Wichtig: Vorher ein Backup machen!

 Dieses Symbol steht für einen Beitrag, der dabei hilft, das Betriebssystem oder eine Software besser zu verstehen und mit mehr Raffinesse am Computer zu arbeiten.

Internetlinks können sich ändern: Alle Hyperlinks in diesem Buch wurden vor der Drucklegung überprüft; dennoch kann nicht ausgeschlossen werden, dass eine Webadresse nicht mehr funktioniert. Auf der Website **www.kummerbox.ch** werden die Angaben jedoch nachgeführt. Hier finden Sie neben dem Linkverzeichnis auch einen durchsuchbaren Index und die für dieses Buch erstellten Download-Dateien.

SICHERHEIT

Wie man Virenresistenz entwickelt



Garantiert auf der sicheren Seite

Ein guter Vorsatz für Internetausflügler: sich mit wohl dosierten Massnahmen gegen Webgefahren wappnen.

Wer mit einem Windows-PC ins Internet geht, kommt auch 2006 am Thema Sicherheit nicht vorbei. «Das grösste Sicherheitsloch überhaupt» habe sich Ende Dezember 2005 aufgetan, vermehren Medienberichte. Über den «WMF-Exploit» holt man sich nur durch den Aufruf einer böswilligen Website Spyware oder einen Browser-Hijacker (eine «Entführungssoftware») auf den Computer – oder irgendeinen Wurm, eine Werbesoftware (Adware) oder sonst ein Schadensprogramm.

Als Surfer wüsste man Besseres mit seiner Zeit anzufangen, als Schutzprogramme zu installieren und den Computer auf Schwachstellen zu untersuchen. Aber es hilft nichts – wer Herr seines Computers bleiben will, muss vorbeugen.

Das Antivirenprogramm ist unverzichtbar. Nur mit einem aktuellen Virenwächter bleibt der Computer von bösartigen Programmen verschont. Privatanwender ohne markantes Risikoverhalten dürfen sich mit einem Gratisprogramm zufrieden geben. Empfehlenswert sind Avast Home Edition (www.avast.at/avasthome.htm) oder AVG Free Edition (www.grisoft.de). Alle anderen Nutzer kommen nicht um ein kommerzielles Produkt herum.

Womit man Viren wirkungsvoll killt

Bei den kostenpflichtigen Virenjägern gehören laut einem brandaktuellen Test der deutschen Computerzeitschrift «c't» F-Secure Anti-Virus 2006, der Antivirenkit von G-Data und Kaspersky Anti-Virus Personal zur Topliga. Die bekanntesten Produkte schneiden schlecht ab: McAfee setzt für seine Arbeit auf die problematische ActiveX-Technologie des Internet Explorer. Bei Norton lässt die Aktualisierung der Virendefinitionen zu lange auf sich warten.

F-Secure Anti-Virus ist für 59 Franken bei www.res-software.ch erhältlich. G-Data's Produkt gibt es unter www.pcp.ch für 37 Franken. Kaspersky Anti-Virus kostet 42 Franken, erhältlich unter www.kaspersky.com/de/store.

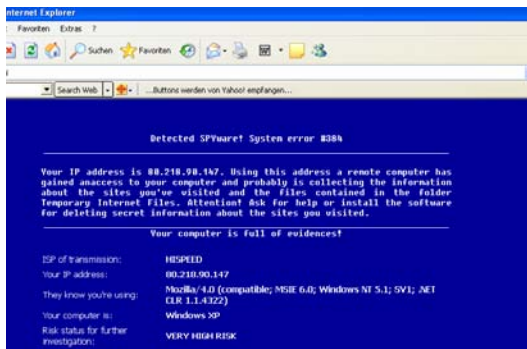
Übrigens: Wenn der Provider für die Mailbox einen Virenschutz anbietet, ist das praktisch, da Virenmails nicht im Posteingang landen. Dieser Schutz ersetzt aber nicht die eigene Antivirensoftware – Viren verbreiten sich zwar sehr oft, aber nicht nur über die elektronische Post.

Spyware und Hijacker sind ein lästiges Problem, das bislang vor allem Anwender des Internet Explorer betrifft. Solche Schadensprogramme ändern die Startseite im Browser oder die Suchfunktion, um die Surfer auf bestimmte Websites zu

locken. Andere Spywareprogramme geben vor, Spyware bekämpfen zu wollen – die klassische Trojaner-Methode. Mit scheinheiligen Warnungen wie der unten abgebildeten versucht beispielsweise Spyaxe, den Leuten Geld aus der Tasche zu ziehen.

Welches Kraut gegen Hijacker wächst

Gegen Hijacker und Spyware gibt es bislang kein Universalheilmittel. Selbst die besten Spionjäger entdecken lediglich 80 bis 90 Prozent der Schädlinge. Am besten schneidet bei Tests von Computerzeitschriften HijackThis ab (gratis unter www.merijn.org). Allerdings sind die Befunde dieses Programms nur von versierten Anwendern richtig zu deuten. Sehr auskunftsfreudig ist E-Trust Pest Patrol (63.50 Franken bei www.res-software.ch). Ewido Anti-Malware schlägt sich gerade bei den besonders fiesen Programmen wie Spyaxe und Konsorten gut. Dieses Programm gibt es für 40 Franken, die Basis-Version ist gratis: www.ewido.net/de.



Wolf im Schafspelz: Ein Spywareprogramm warnt vor sich selbst.

Die Firewall pariert Angriffe aus dem Internet und unterbindet ungewollte Datentransfers. Windows XP enthält eine Firewall, die für normale Sicherheitsbedürfnisse völlig ausreicht. Ältere Rechner lässt man von einem Daten-Wachhund beaufsichtigen, der seinen Dienst umsonst verrichtet. Unentgeltlich zu haben sind ZoneAlarm (www.zonelabs.de) oder Sunbelt Kerio Personal Firewall (www.sunbelt-software.com). Die sicherste Sache ist ein Router – diese Hardwarekomponente organisiert das private Heimnetzwerk und kontrolliert den Verkehr mit dem Internet. Beim Kauf eines Routers lohnt es sich, einige Franken mehr in ein Gerät zu investieren, das eine Firewall enthält.

Wer am liebsten gar nichts mit der kompliziert zu konfigurierenden Firewall zu tun haben möchte, lässt sich vom Provider schützen. Bluewin-Kunden erhalten diesen zusätzlichen Schutz mit dem Service-Pack Gold, bei Solnet.ch abonniert man den Firewall-Dienst für 4.20 Franken pro Monat.



Misstrauen ist der beste Schutz

«Phishing» bezeichnet den Versuch, den Nutzern von Telebanking-Plattformen, Auktions-Sites oder Zahlungsdiensten die Zugangsdaten zu stehlen. «Phishing» ist ein Kunstwort aus «Password fishing». Die Passwortfischer verschicken auf gut Glück Massenmails und versuchen unter einem Vorwand, die Kunden einer Bank auf eine gefälschte Website zu locken. Wer dort die Zugangsdaten eingibt, öffnet den Betrügern Tür und Tor für ihre illegalen Beutezüge.

Schützen kann man sich mit technischen Mitteln – etwa einem Programm, das bei verdächtigen E-Mails oder Internetadressen Alarm schlägt. Anwender des Internet Explorer 6 schützen sich mit dem Microsoft Phishing Filter (gratis):

www.microsoft.com/switzerland/athome/de/security/online/phishing_filter.msp.

Bei Internet Explorer 7 und bei Firefox ab Version 2 ist ein Phishing-Filter eingebaut. Auch Thunderbird ab Version 1.5 schützt vor Phishing. Schliesslich gibt es Schutz vor Phishing auch durch kommerzielle Sicherheitsprogramme. Norton Internet Security in der neuen Version 2007 warnt vor potenziell betrügerischen Websites.

Der beste Schutz bleibt indes eine gesunde Portion Misstrauen: Keine Bank fordert Kunden per E-Mail zum Einloggen ins Telebanking-System auf. Mails, die dazu auffordern, sind ohne jeden Zweifel gefälscht.



Auf sicheren Wegen durch das Internet

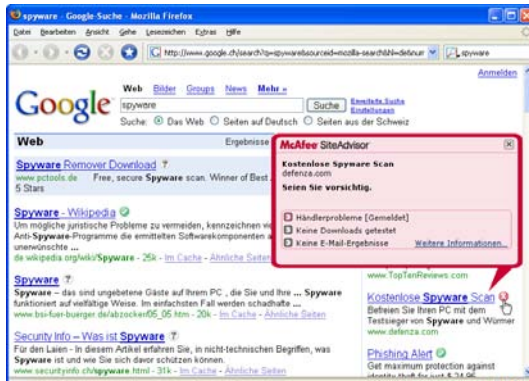
Surfen ohne Risiko: SiteAdvisor markiert harmlose Homepages per grünes Label und schaltet bei dubiosen Sites auf Rot.

Das Internet hat seine Gefahrenzonen. Gefährliche Websites seien für fünf Prozent des Datenaufkommens im Web verantwortlich, schätzt das US-Sicherheitsunternehmen SiteAdvisor. Solche Sites wollen Spyware, Hijacker oder Viren herunterladen, versenden Spam oder sind auf persönliche Daten der Besucher aus.

Die Risikoanalyse basiert auf den Erkenntnissen eines Suchprogramms, das automatisch Internetseiten abklappert und deren Gebaren analysiert. Abgänger des Massachusetts Institute of Technology (MIT) haben den digitalen Kundschafter entwickelt. Ihr Unternehmen, SiteAdvisor stellt auch eine kostenlose Browser-Komponente bereit, die Auskunft über die Vertrauenswürdigkeit von Webseiten gibt. Im April 2006 wurde das Startup-Unternehmen vom Antiviren-Spezialist McAfee gekauft, sodass das Internet-Warnsystem nun den Namen McAfee SiteAdvisor trägt.

Den Sicherheitsberater gibt es für den Internet Explorer und Firefox. Nach der Installation erscheint in der Statusleiste ein Label, das bei unverdächtigen Websites Grün zeigt und bei riskanten Adressen auf Rot umschaltet. Zeigt sich das Label in Grau, gibt es keine Sicherheitsanalyse. Per Klick auf das SiteAdvisor-Logo und den Menübefehl «Site-Details anzeigen» erfährt man Näheres zum Gefahrenpotenzial.

Bei einer Suche per Google bewertet SiteAdvisor die Resultate in der Liste. Bei harmlosen Treffern steht ein grünes Häkchen, bei nicht analysierten Sites ein graues Fragezeichen und bei Online-Fallen ein rotes X. Zeigt man mit der Maus aufs Symbol, erscheint eine Sprechblase mit einer kurzen Analyse. Laut den Sicherheitsprofis von SiteAdvisor stecken unsichere Links fast dreimal häufiger in den Werbeeinseraten (sie sind bei Google am rechten Rand zu finden) als in den normalen Suchergebnissen.



Gut oder böse? Der Browser zeigt die Verlässlichkeit einer Website an.

SiteAdvisor ist eine gute Orientierungshilfe für Leute, die gern kreuz und quer durchs Web surfen und sich bei den Online-Ausflügen eher von der Neugierde als von der Vorsicht leiten lassen. Eine hundertprozentige Sicherheit bietet SiteAdvisor – wie jede technische Sicherheitslösung – nicht. Die gesunde Portion Misstrauen ist somit weiterhin angebracht. Als mündiger Surfer sollte man nicht jeden Link anklicken, gerade wenn man auf abgelegenen Pfaden surft oder heisses Internetpflaster besucht. Da SiteAdvisor jede angesurfte Adresse überprüft, gibt es beim Seitenabruf merkliche Verzögerungen. Diese sind bei einer schnellen Verbindung zu verkraften.

SiteAdvisor erfährt genau, auf welchen Wegen man sich durchs Web bewegt. «Wir speichern nicht, welche Sites ein User aufruft und was er online tut», heisst es in den Datenschutzbestimmungen. Da mit McAfee ein renommiertes Sicherheitsunternehmen hinter dem Dienst steht, darf man der Beteuerung glauben. Die Erweiterungen für Firefox und den Internet Explorer gibt es als Downloads auf www.siteadvisor.com.

Wie kann man sich sonst noch vor Schadenssoftware, so genannter «Malware», schützen? Unnutze oder kontraproduktive Spyware-Jäger enttarnt man mit Hilfe der «Spyware Warrior List of Rogue/Suspect Anti-Spyware Products & Web Sites» – hier sind die schwarzen Schafe unter den Sicherheitsprogrammen aufgeführt. Von diesen lässt man die Finger, selbst wenn sie aggressiv beworben werden: http://spywarewarrior.com/rogue_anti-spyware.htm.

Allianzen gegen «Schlechtware»

Gegen böse Programme wurden in den letzten zwölf Monaten mehrere Allianzen geschmiedet. Die Anti-Spyware Coalition (Antispywarecoalition.org) wird unter anderem von Yahoo, AOL und Microsoft getragen und hat Richtlinien zur Spyware-Klassifizierung veröffentlicht. Google, Lenovo und Sun sponsern Stopbadware.org. Diese Kämpfer gegen «Schlechtware» testen Programme und prangern in den «Badware Reports» Programme an, die durch ungebührliches Verhalten auffallen. Dieser Ansatz ist viel versprechend. Die Liste der Übeltäter beschränkt sich bis jetzt auf «alte Bekannte» wie Winfixer oder Spyaxe. Wer sichere Downloads schätzt, sieht sich auf Qarchive.org oder www.safe-install.com um: Dort sind Viren- und Spyware-freie Programme zu finden.



Ein Vorhängeschloss für den Dateiordner

Wie man mit Windows XP Vertrauliches vor unbefugtem Zugriff schützt.

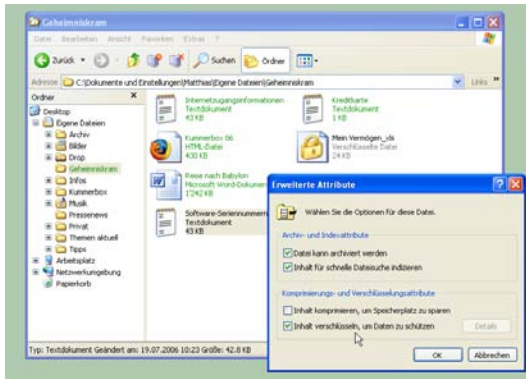
Diskretion im Umgang mit Dateien ist ein Dauerbrenner unter den Kummerbox-Lesern. Wie behält man Privatdaten unter Verschluss, wenn mehrere Leute Zugang zum PC haben? Diese Frage interessiert all jene, die Staatsgeheimnisse zu hüten haben, und natürlich auch User, die Alltagskram vor fremden Augen schützen wollen.

Die Antwort heisst Verschlüsselung: Durch die codierte Speicherung auf der Festplatte bleiben die Vermögensaufstellung in Excel, der Romanentwurf in Word oder die Fotosammlung mit den Privatbildern unter Verschluss. Windows XP in der Professional-Version enthält eine weitherum unbekannte, aber einfach zu nutzende Geheimhaltungsmethode namens verschlüsselndes Dateisystem (englisch «Encrypting File System», EFS).

Um eine Datei oder einen Ordner in die Obhut des EFS zu geben, markiert man das schutzbedürftige Objekt im Windows Explorer, wählt den Befehl «Datei > Eigenschaften» und klickt im Reiter «Allgemein» auf die Schaltfläche «Erweitert». Bei den erweiterten Attributen kreuzt man nun die Option «Inhalt verschlüsseln, um Daten zu schützen» an. Bei Dateien stellt Windows beim Klick auf «OK» die Frage, ob man die einzelne Datei oder den ganzen Ordner verschlüsseln will. Entschieden man sich für den ganzen Ordner, werden alle neuen Dateien codiert abgelegt, ansonsten betrifft die Sicherheitsmassnahme nur die ausgewählte Datei.

Ein Schutz, der kaum auffällt

Verschlüsselte Dateien verhalten sich genau wie unverschlüsselte. Windows (de)chiffriert automatisch, und nur bei grossen Dateien ist eine Verzögerung zu bemerken. Auch Mailablagen, Browser-Lesezeichen oder Startmenü-Einträge lassen sich sichern. Ein Passwort braucht man nicht einzugeben – die Legitimation erlangt man durch die Anmeldung am PC mit Benutzernamen und Kennwort. So versteht es sich von selbst, dass das EFS nur dann etwas bringt, wenn jeder Anwender sein eigenes Windows-Konto hat.



Grüne Dateien sind verschlüsselt und vor fremden Augen sicher.

Versucht man einen illegitimen Zugriff auf eine geschützte Datei, zeigt Windows eine Fehlermeldung wie «Zugriff verweigert» oder «Stellen Sie sicher, dass der Datenträger weder voll noch schreibgeschützt ist» an. Verschlüsselte Dateien sind aber leicht zu erkennen. Sie werden im Explorer mit grüner Schrift angezeigt.

Was beim EFS zu beachten ist:

- Es steht nur auf NTFS-formatierten Laufwerken zur Verfügung.
- Versucht man, eine verschlüsselte Datei auf ein Laufwerk zu kopieren, das nicht mit NTFS formatiert ist, erscheint eine Fehlermeldung.
- Die Verschlüsselung ist nur so sicher wie das Benutzerpasswort – und das lässt sich bei Windows relativ leicht knacken. Fürs Notebook mit Geschäftsdokumenten ist ein kommerzielles Produkt wie DriveCrypt ein Muss (www.securstar.com).
- Zur Verschlüsselung verwendet Windows ein Zertifikat, das man sichern sollte – geht es verloren, sind die verschlüsselten Daten nicht mehr zugänglich. Die Sicherung findet im Internet Explorer über «Extras > Internetoptionen» im Reiter «Inhalte» statt: Klicken Sie auf «Zertifikate», öffnen Sie den Reiter «Eigene Zertifikate», markieren Sie den Eintrag, bei dem als Zweck «verschlüsseln des Dateisystem» aufgeführt ist, und betätigen Sie «Exportieren». Der private

Schlüssel sollte nun ebenfalls exportiert werden, und die «Verstärkte Sicherheit» ist zu aktivieren.

- Vor einer Windows-Neuinstallation sollten alle Dateien entschlüsselt werden.

Als Alternative zu EFS bietet sich das Programm Advanced File Security an – es ist kostenlos (www.osborn-software.de). Der Einsatz ist einfach: Nach der Installation erscheinen die Befehle «Verschlüsseln» und «Entschlüsseln» im Menü «Datei» des Windows Explorers. Wichtig ist ein langes Passwort (16 Zeichen oder mehr), das sich nicht leicht erraten lässt. Als Gedächtnisstütze dient zum Beispiel Goethes «Erkönig». Nehmen Sie von jedem Wort den ersten Buchstaben, dann wird aus «Wer reitet so spät durch Nacht und Wind? Es ist der Vater mit seinem Kind.» das starke Passwort «WrssdNuW?EidVmsK.»



Hilfe holen, wenn Norton streikt

Symantecs Antivirenprogramm ist populär. In Sachen Kundendienst muss sich der Hersteller aber Kritik gefallen lassen.

Norton Antivirus ist der Virenjäger, dem die User vertrauen. Trotz starker Konkurrenz durch F-Secure, G-Data oder Kaspersky greift jeder Zweite zu Symantecs gelber Softwarebox. Oft findet die Zuneigung zu Norton aber ein jähes Ende: Wenn er, statt Viren zu jagen, selbst Ärger macht. Über Symantecs Kundendienst gehen bei der Kummerbox mehr Klagen ein als über jeden anderen Softwarehersteller. Wer Hilfe brauche, so empören sich viele Tagi-Leser, dem stünden nur teure Hotlines offen. Doch wieso für Hilfe zahlen, wenn das Problem bei der Installation oder dem Download eines online gekauften Produktes liegt?

Mit Mut zur Selbsthilfe erspart man sich indes oft die teure Hotline:

Wer sein Problem in zwei oder drei präzise Suchbegriffe fassen kann, findet eine Lösung in der kostenlosen Supportdatenbank:

www.symantec.com/de/de/home_homeoffice/support

Wer 48 Stunden auf eine Antwort warten mag, kann sein Anliegen kostenlos per E-Mail unterbreiten:

http://symantec.teleperformance.gr/symantecsupport/ger_ask_ts.php.

Und bei gängigen Norton-Problemen weiss auch die Kummerbox Rat.



Windows 98 reif fürs Altenteil?

Für Windows 98 und ME gibt es bald keine Sicherheitsupdates mehr. Müssen alte PCs nun aus dem Verkehr gezogen werden?

Rund fünf Prozent der Computer laufen mit Windows 98 und Windows ME. Die beiden Oldie-Betriebssysteme haben somit etwa gleich viel Anwender wie Mac OS X von Apple. Dieser Kundengruppe fühlt sich Microsoft nicht mehr verpflichtet: Ab dem 11. Juli gibt es keine Updates mehr für Windows 98, die «Second Edition» von Windows 98 und Windows Millennium Edition (ME). Sicherheitslöcher bleiben künftig ungestopft, und für die Anwender stellt sich die bange Frage, ob nun notgedrungen ein Update auf Windows XP oder Vista fällig wird. Und weil diese beiden Betriebssysteme auf alter Hardware meist nicht laufen (Vista ganz bestimmt nicht), bleibt nur eine Neuanschaffung.



Vom Aussterben bedroht: Betriebssystem-Dinosaurier wie Win 98.

Die offizielle Begründung Microsofts für den Update-Stopp lautet, es werde zunehmend schwierig, die alten Betriebssysteme vor neuen Gefahren zu schützen. Selbstredend kommt es dem Computergiganten nicht ungelegen, wenn Anwender nun angejahrte Rechenmaschinen austauschen. Wenn die vielen bunten Features von Windows XP oder der 3-D-Flip von Vista die Updateunwilligen nicht locken, dann greift wenigstens das Sicherheitsargument.

Ausreichend für Gelegenheitssurfer

Soll man sich als Anwender dem Fortschritt beugen und seinen digitalen Veteranen ehrenhaft entlassen, selbst wenn er zuverlässig seinen Dienst tut? Soll man aus Angst vor Viren den Abfallberg vergrößern und Geld ausgeben, auch wenn einem nicht danach ist? Wer mit seinem Computer Geld verdient oder liebe und teure Daten auf ihm hortet, kommt um das Update nicht herum – aber an-

spruchsvolle Anwender mit Digitalfotos und einer grossen MP3-Sammlung haben sowieso längst auf XP umgesattelt. Wer mit seinem acht Jahre alten Rechner noch immer glücklich ist, verwendet ihn nicht für Extravagantes. Windows-98-User sind nicht in illegalen Tauschbörsen zu finden, noch laden sie ständig Dateien aus dem Netz. Wer ab und zu eine «harmlose» Website ansurft und E-Mail und die Textverarbeitung nutzt, darf das auch mit einem veralteten Betriebssystem tun. Für den Schutz alter Rechner sollte man Folgendes beachten:

- Viele neue Antivirenprogramme laufen nicht mehr auf Windows 98. Die Virenschutzprogramme von Kaspersky oder NOD32 schützen auch alte PCs.
- Manche Provider (zum Beispiel Bluewin) bieten einen Firewall-Dienst an: Ein solcher sichert auch Oldie-PCs ab, ohne dass Software installiert werden müsste.
- Praktisch für alte Rechner ist auch ein Dienst wie www.cleanmail.ch: Er eliminiert Viren und Spam noch vor dem Herunterladen auf den PC.
- Wer seinen Rechner nicht direkt ans Internet hängt, sondern via Router surft, setzt sich weniger Angriffen aus. Ansonsten ist es wichtig, die Datei- und Druckerfreigabe abzuschalten.
- Der Firefox-Browser und das Thunderbird-Mailprogramm laufen auch auf Windows 98: In diesen Programmen werden Sicherheitslücken weiterhin geschlossen.

Schadenssoftware hat keine Chance!



Achtung, Bierfrösche!

Ich habe von einem Kollegen eine E-Mail bekommen, die vor Viren in den Budweiser Frogs warnt. Ich bin PC-Fan und weiss, dass es ein Hoax sein kann.

Auf Virenwarnungen sollten Sie nur etwas geben, wenn sie aus gesicherter Quelle stammen. Vertrauenswürdig ist zum Beispiel das Antivirenprogramm. Viren- oder irgendwelche Sicherheitswarnungen per E-Mail sind es nicht – die darf man unbeesehen löschen: Seriöse Meldungen zum Thema werden nie per E-Mail verbreitet. Bei den Budweiser Frogs handelt es sich um einen Werbe-Bildschirmschoner von 1997. Sie sind abgestandenes Bier und ein Hoax (Schwindel), aber kein Virus.



Quakt, schadet aber nicht.



Widersinnige Warnung

Mein Antivirenprogramm, Antivir von Avira, gibt ständig Warnungen aus, wonach gewisse Dateien nicht geöffnet werden können. Was muss ich tun?

Im Normalfall nichts: Meist handelt es sich bei den nicht untersuchten Dateien um Komponenten des Betriebssystems. Dateien wie «pagefile.sys», «ntuser.dat» oder «sam.log» sind gesperrt und dürfen beim Virenskan übergegangen werden. Entsprechend sind die Warnungen bei Systemdateien sinnlos und unnötig verunsichernd. Und sie bergen ein Sicherheitsrisiko. Nur versierte Windows-Benutzer erkennen, wenn eine der ausgeklammerten Dateien nicht zu Windows gehört und allenfalls gefährlich ist. Sie verkleinern das Risiko, indem Sie den Scan im abgesicherten Modus durchführen (siehe Beitrag «Fixe Windows-Wiederbelebung», Seite 32) oder ein Antivirenprogramm mit mehr Differenzierungsvermögen einsetzen – solche werden ganz am Anfang dieses Buchs im Beitrag «Garantiert auf der sicheren Seite» (Seite 10) empfohlen.



Sicherheitscenter ausser Betrieb

Wenn ich das Sicherheitscenter öffnen will, heisst es: «Das Sicherheitscenter ist momentan nicht verfügbar, da der Dienst nicht gestartet bzw. beendet wurde.» Was kann man machen?

So rufen Sie das Sicherheitscenter zum Dienstantritt: Klicken Sie im Startmenü auf «Ausführen» und geben Sie «services.msc» ein. Doppelklicken Sie in der Liste der Dienste auf den passenden Eintrag. Geben Sie als «Starttyp» «Automatisch» an und klicken Sie auf «Starten».



Nortons «Aus»-Schalter

Ich verwende seit Kurzem Norton Internet Security 2007. Nun wollte ich den Internet Explorer 7 herunterladen und das Antivirenprogramm deaktivieren, wie man das bei Installationen tun sollte. Aber den «Schalter» dafür finde ich nicht mehr.

Die Norton Internet Security 2007 lässt sich nicht mehr mit einem Klick deaktivieren. Einzelne Komponenten wie die Firewall oder Antivirus lassen sich aber weiterhin abschalten. In Nortons Hauptfenster schalten Sie mit einem Mausklick auf das grüne «Ein» auf «Aus» um.