Begleitmaterial zum Kurs

Computersicherheit
(nicht nur für Senioren)

Version 24-Dez-2004

Quellen:

Das in diesem Dokument referenzierte Material entstammt der folgenden von Günter Born verfassten Publikationen:

»Sicherheit für Windows XP - leichter Einstieg für Senioren«, ISBN 3-8272-6821-4
»Computer - leichter Einstieg für Senioren«, ISBN 3-8272-6756-0
»Internet - leichter Einstieg für Senioren«, ISBN 3-8272-6757-9
»Windows - leichter Einstieg für Senioren«, ISBN 3-8272-6758-7
»Office - leichter Einstieg für Senioren«, ISBN 3-8272-6251-8

»Easy - Computer - Alles rund um den PC «, ISBN 3-8272-6785-4

Die Publikationen sind erschienen im Markt + Technik Verlag München

Pearson Education Deutschland GmbH
Martin-Kollar-Str. 10-12
81829 München
www.mut.de

Das Begleitmaterial lässt sich in der aktuellen Fassung von der Webseite *www.borncity.de* im Bereich »Senioren« herunterladen.

Inhaltsverzeichnis

Computersicherheit im Überblick

In der letzten Zeit häufen sich die Meldungen in Zeitungen, Radio und Fernsehen über Virenbefall in Computern, über betrügerische Aktionen mit Wählprogrammen (so genannten Dialern) oder über Missbrauch bei Geldgeschäften im Internet. Der größte Teil der Schadensfälle geht dabei auf grob fahrlässiges Verhalten der Benutzer zurück. Manche Benutzer verzichten dann aus Angst vor Viren oder anderen Schädlingen auf Internet oder E-Mail. Aber das muss nicht sein. Nachfolgend möchte ich Ihnen einen Überblick über die Thematik geben und einige Sicherheitsfragen beleuchten.

Die gemeinsten Fallen für Computerbenutzer

Vorweg: Das **größte Risiko** am Computer **ist** letztendlich **der Benutzer**. Unkenntnis, Ignoranz oder Bequemlichkeit erhöhen das Risiko für Schadensfälle ungemein. Also gilt es gefährliche Stellen zu erkennen und möglichst zu meiden bzw. angemessen darauf zu reagieren. Hier einige der gemeinsten Fallen für Computerbenutzer.

- **Viren:** Viren sind Programmteile, die **per E-Mail**, **über Internetseiten** oder auch **über Disketten** oder **andere Datenträger** (CDs, DVDs) verbreitet werden. Der Virus versteckt sich dabei in anderen Dateien und ist für den Benutzer nicht direkt zu erkennen. Gelangt ein solches infiziertes Programm auf einen Computer und wird es ausgeführt oder geladen, kopiert sich der Virus in andere Programmdateien dieses Rechners. Man sagt auch »Die Dateien werden infiziert«. Geben Sie solche infizierten Dateien an Dritte weiter oder kopieren Sie diese auf einen anderen Rechner, verbreitet sich das Virus auch dort. Neuere Viren versuchen sich auch von einem befallenen Rechner per E-Mail über das Internet zu verbreiten (die Adressen holt sich das Virus aus dem Adressbuch des Opfers). Das Schlimme an Viren ist, dass diese Windows, Daten oder Programme unbrauchbar machen können und so zu Schäden führen.

- **Trojaner:** Trojaner verbreiten sich ähnlich wie Viren **per E-Mail**, **über Internetseiten** oder **über Datenträger** (Disketten, CDs, DVDs). Ein Trojaner steckt meist in einem vordergründig sinnvollen Programm. Das Tückische an Trojanern ist, das diese ggf. Tastatureingaben des Benutzers oder Bildschirmausgaben am Rechner und Dateien auf der Festplatte ausspionieren und an den Urheber des Schadprogramms melden. Dadurch lassen sich beispielsweise Kennwörter für Internetbanking, E-Mail, Online-Depots, Bestellseiten etc. ausspionieren.

- **Würmer:** Ein **Wurm** ist ein Programmteil, der sich **über** das **Internet auf viele** Millionen **Rechner verbreitet**. Der Programmcode des Wurms nutzt dabei Schwachstellen des Betriebssystems (wie z.B. Windows) zur Verbreitung aus. Das Schädliche an einem Wurm ist, dass dieser einerseits die Übertragungsleitungen des Internet bei der Verbreitung verstopft. Zudem dienen je-

doch Würmer oft auch als Hintertür (so genannte **Backdoor**) zum Einschleusen anderer Schädlinge.

- **Dialer:** Dialer sind Programme zur Interneteinwahl, eigentlich eine feine Sache, die auch von seriösen Anbietern genutzt wird. Leider gibt es auch 0190er- oder 0900er-Dialer, die sich ungewollt auf dem Computer installieren und die Internetverbindung heimlich auf sehr teuere Einwahlnummern (30 Euro pro Einwahl oder 2 Euro pro Minute) umleiten. Verbreitet werden solche Dialer als Anlage zu E-Mails oder über Webseiten, von denen das Programm installiert wird.

Neben diesen wirklichen Schadprogrammen, die den Computer unbenutzbar machen oder hohe Kosten verursachen, gibt es noch eine Reihe anderer **Tücken** beim Arbeiten mit oder ohne Internet. Dies reicht von Webseiten, die die **Startseite des Browsers kapern** über das **Ausspionieren des Benutzers** beim Surfen bis hin zum Sammeln von Daten über die auf dem Computer installierten Programme. Auch ungefragt zugeschickte **Werbe-E-Mails** (auch als **Spam** bezeichnet) nerven durch ihre schiere Menge ungemein. Mit zunehmender Anzahl an Internetteilnehmern werden zudem betrügerische Angriffe für kriminelle Kreise immer attraktiver. Die gute Nachricht ist aber, dass es wirksame Gegenstrategien gibt, die kaum Aufwand erfordern und wenig bis gar nichts kosten.

FACHWORT

Viren, **Trojaner** und **Würmer** sind Schadprogramme, die Sicherheitslücken und die Unachtsamkeit/Unerfahrenheit des Benutzers ausnutzen, um sich auf dem Computer zu installieren und dort Schaden anzurichten. Der Begriff **Dialer** ist das englische Wort für »Wähler«, ein Programm zur Einwahl ins Internet. Problematisch werden Dialer, wenn sich diese ungefragt auf dem Rechner installieren und dann beim Surfen im Internet teure 0190er- oder 0900er-Nummern für die Internetverbindung benutzen.

Verbessern Sie die Sicherheit!

Hier einige Punkte, um die Sicherheit beim Umgang mit dem Computer zu verbessern:

- **Halten Sie die Software des Computers auf dem aktuellen Stand:** Es ist wie im täglichen Leben. Die von den Herstellern ausgelieferten Programme sind in der Regel nicht fehlerfrei. Meist ist es aber so, dass die Hersteller auf entdeckte Fehler und Sicherheitslücken reagierten und Programmverbesserungen – oft kostenlos – anbieten. Hier ist es wichtig, dass der Anwender diese bereitgestellten Programmverbesserungen, speziell, wenn diese Sicherheitsaspekte betreffen, auch auf den eigenen Computern installieren. Wie dies geht, können Sie in **Kapitel 2** nachlesen.

- **Nutzen Sie die Sicherheitsmöglichkeiten Ihrer Software:** Windows XP (siehe Kapitel 2), der Internet Explorer (siehe Kapitel 4) und Outlook Express (siehe Kapitel 5) bieten eine Reihe von Einstellmöglichkeiten, die das Aus-

breiten von Schadprogrammen verhindern. Zudem stellt das Service Pack 2 für Windows XP (eine Aktualisierung für Windows) ein eigenes Sicherheitscenter bereit, welches die Systemeinstellungen überwacht.

- **Verwenden Sie ein aktuelles Virenschutzprogramm:** Solche Programme erkennen Viren etc. und verhindern deren Ausbreitung auf dem Rechner (siehe Kapitel 3). Ist das Malheur bereits passiert, kann ein Virenschutzprogramm die Infektion erkennen und oft auch beseitigen. Allerdings ist es wichtig, dass Sie das Virenschutzprogramm nach der Installation auf dem aktuellen Stand halten, da andernfalls neue Viren etc. nicht erkannt werden können.

- **Lassen Sie Ihren gesunden Menschenverstand walten:** Die Tricks der Betrüger werden immer ausgebuffter. Viren, die als angebliche Grußkarte oder Programmverbesserung per E-Mail verschickt werden. Gefälschte Webseiten, die Kreditkartennummern oder Geheimzahlen von Scheckkarten abfischen. Internetangebote, die nur nach Eingabe einer Adresse, Telefonnummer oder E-Mail-Adresse abrufbar sind. Solche Fallen lassen sich viele aufzählen. Mit etwas Wissen, genügend Vorsicht und einem gesunden Menschenverstand lassen sich solche Fallen erkennen und umgehen.

Details zu den obigen Punkten, mit denen sich die Computersicherheit verbessern lässt, lernen Sie in den folgenden Kapiteln kennen. Und das Ganze muss nicht teuer oder aufwändig sein. Mit dem richtigen Wissen ist es sogar recht einfach, sein System sicher zu machen.

HINWEIS

Die Kapitelverweise im obigen Text beziehen sich auf den Titel **Sicherheit für Windows XP - leichter Einstieg für Senioren** (ISBN 3-8272-6821-4). Einige Hinweis, zur Verbesserung der Sicherheit, erhalten Sie auf den folgenden Seiten.

Wie erkenne ich einen Virenbefall?

Viren, Würmer oder Trojaner können den Rechner außer Gefecht setzen und großen Schaden anrichten. Es ist daher wichtig, dass diese Gefahr möglichst schnell erkannt und gebannt wird. Zuerst stellt sich die Frage, wie man den Befall durch Würmer, Viren, Dialer oder Trojaner erkennt? Vorab eine klare Aussage, in den wenigsten Fällen kann ein normaler Anwender einer Programmdatei nicht ansehen, ob diese einen solchen Schädling enthält. Manchmal gibt es aber Indizien, dass etwas faul ist und vielleicht ein Virus im Computer wütet:

- Auf dem Bildschirm erscheinen plötzlich Hinweise auf einen Virus oder Buchstaben bzw. Desktop-Elemente verschwinden plötzlich.

- Auf dem Desktop oder im Windows-Startmenü gibt es plötzlich mysteriöse Einträge, obwohl keine Programme installiert wurden.

- Die Festplatte ist für Minuten in Benutzung, obwohl keine Programme gestartet wurden oder jemand am Rechner arbeitet.

- Auf dem Computer werden Dateien gelöscht, verändert oder überschrieben. Der Computer reagiert bei Tastatureingaben langsamer als gewohnt (z.B. weil gerade ein Trojaner die Tastenanschläge aufzeichnet).
- Im Postausgang des E-Mail-Programms finden sich plötzlich fremde E-Mails, die man nicht erstellt hat. Bekannte melden sich, weil sie E-Mails mit Virenbefall von Ihnen erhalten haben.
- Bei ungewollt installierten Dialern findet sich meist ein neuer Eintrag im Ordnerfenster der Netzwerkumgebung oder die Internetverbindung wird kurz unterbrochen und dann wieder hergestellt. Auf der Telefonrechnung tauchen plötzlich Kosten für die durch den Dialer genutzten Verbindungen auf.

Dies alles kann ein Anhaltspunkt für einen Befall durch einen Schädling sein, es kann aber auch andere Ursachen geben. Sicher erkennen lassen sich Viren, Trojaner oder ähnliches nur durch aktuelle Virenschutzprogramme (siehe Kapitel 3).

Soforthilfe im Schadensfall

Wurde Ihr System von einem Virus, einem Wurm oder einem Dialer heimgesucht? In diesem Fall ist planvolles Handeln angesagt, um das Ganze nicht noch schlimmer zu machen und die Schädlinge wirkungsvoll auszusperren.

Maßnahmen bei Virenbefall

Viren, Würmer oder Trojaner können den Rechner außer Gefecht setzen und großen Schaden anrichten. Falls Sie sicher sind, oder zumindest den Verdacht haben, dass das System befallen ist, gilt es **Ruhe** zu **bewahren** und den Rechner gezielt zu säubern:

- **Trennen Sie den Rechner vom Internet** (Telefonanschlusskabel des Modems bzw. der ISDN-Karte abziehen). Falls der Rechner über Netzwerkkabel mit anderen Computern verbunden ist, sollten Sie auch diese Verbindung trennen.
- **Lassen Sie** eine aktuelle Version eines **Virenschutzprogramms laufen**, um den Befall durch Viren, Würmer, Trojaner oder andere Schädlinge sicher zu überprüfen. Im Idealfall ist das betreffende Programm auf dem Rechner enthalten und kann sogar die Viren oder Schadprogramme beseitigen.

Verfügen Sie über kein aktuelles Virenschutzprogramm oder besitzen Sie noch nicht genügend Kenntnisse im Umgang mit diesem Thema, lassen Sie sich von Experten helfen. In manchen Fällen hilft allerdings nur noch, den Inhalt der Festplatte zu löschen und Windows sowie die gesamten Programme neu zu installieren. Ihre auf dem Medium gespeicherten Daten sind dann natürlich verloren. Da Vorbeugen besser als Heilen ist, sollten Sie den aktuellen Befall zum Anlass nehmen und sich das **Kapitel 3** zum Thema Virenschutz durchlesen.

Wenn ein Dialer zuschlägt

Haben Sie den Verdacht, dass sich ein unerwünschtes Wählprogramm (Dialer) auf Ihrem Computer eingenistet hat? Auch hier hilft planvolles Handeln und verhindert Schlimmeres:

- **Bewahren Sie Ruhe**, trennen Sie den Computer als erstes vom Telefonnetz (Telefonstecker des Modems oder der ISDN-Karte aus der Telefonanschlussdose ziehen). So kann der Dialer keine weiteren Verbindungen aufbauen und zusätzliche Kosten verursachen.

- Hat bereits eine Einwahl stattgefunden bzw. wurden durch den Dialer Kosten verursacht, ist es **wichtig**, dass Sie den Dialer jetzt **nicht** panisch vom System zu **löschen**. Falls Sie sich von dem Anbieter des Dialers getäuscht oder gar betrogen fühlen, müssen Sie **eine Beweissicherung** (durch Gutachter oder mit Zeugen) **durchführen**.

- **Überprüfen Sie den Ordner** *Netzwerkverbindungen* (z.B. indem Sie im Startmenü auf den Befehl *Systemsteuerung* klicken und dann im Fenster der Systemsteuerung das Symbol *Netzwerkverbindungen* wählen). Sind im Ordner **Netzwerkverbindungen** plötzlich unbekannte Einträge für Wählverbindungen hinterlegt, deutet dies auf einen Dialer hin.

Falls Sie sich technisch nicht besonders gut auskennen, sollten Sie auf keinen Fall den Dialer auf eigene Faust entfernen, sondern dies Fachleuten überlassen.

TIPP

Eigentlich sind Dialer eine gute Sache! So handelt es sich bei dem Tarifmanager von WEB.DE, der Ihnen auf Wunsch die Auswahl der günstigsten Internetanbieter ermöglicht, auch um einen Dialer. Manche Firmen nutzen Dialer auch, um Leistungen (z.B. Hotline-Beratung) unbürokratisch abzurechnen. Unerwünscht sind aber Dialer, bei denen der Benutzer die anfallenden Kosten nicht erkennt und die dann ungewollt zu horrenden Telefonrechnungen führen. Gerade Kinder und unerfahrene Surfer werden von den Anbietern mit allerlei Tricks dazu gebracht, den Dialer zu installieren. Da gibt es Hausaufgabenseiten (z.B. *hausaufgaben.de*), Rezeptseiten etc., auf denen dann ein Dialer als »erforderliche Zugangssoftware« angeboten wird. Seit August 2003 müssen solche Dialer jedoch bei der RegTP (dies ist Regulierungsbehörde für Telekommunikation und Post, Tulpenfeld 4, 53113 Bonn, Telefon 02 28/14-0, Fax 02 28/14-88 72, Internet *www.regtp.de*) angemeldet werden. Die RegTP begrenzt die Tarifstruktur solcher Dialer auf max. 30 Euro pro Anwahl oder max. 2 Euro pro Minute – was auch noch recht happig ist, wenn kein Gegenwert hinter dem abgerufenen Angebot steckt. Ab Anfang 2005 schreibt die RegTP den Dialeranbietern jedoch vor, wie die Seiten zum Abrufen des Dialers und zur Installation zu gestalten sind. Leider gibt es auch illegale Anbieter, die Satellitenverbindungen nach Übersee oder ins Ausland über Dialer aufbauen und dann die Gebühren kassieren. Falls Sie auf ungewollte Dialer hereinfallen und Kosten entstanden sind, sollten Sie sich auf der Webseite der

RegTP informieren, ob der Dialer registriert ist. Sie können gegenüber der Telekom Einspruch gegen den vom Dialer verursachten Gebührenanteil einlegen. Zahlen Sie aber auf jeden Fall den auf der Telefonrechnung ausgewiesenen Betrag für reguläre Telefongespräche – Sie riskieren sonst die Sperre des Telefonanschlusses. Auf der Internetseite *www.regtp.de* finden Sie verschiedene Hinweise, was Sie tun können, wenn sich ein Dialer ungewollt installiert hat und zu strittigen Gebührenpositionen auf der Telefonrechnung führte.

Hilfe, ich habe einen Trojaner

Hat sich auf Ihrem Rechner ein Trojaner eingeschlichen? Die Handlungsweise ist die Gleiche wie beim Virenbefall:

- **Bewahren Sie Ruhe**, trennen Sie den Computer als erstes vom Telefonnetz (Telefonstecker des Modems oder der ISDN-Karte aus der Telefonanschlussdose ziehen). So kann der Trojaner keine weiteren Daten per Internet melden.
- **Benutzen Sie zum Nachweis** des Trojaners und **zum Säubern** des Systems eine aktuelle Version eines **Virenschutzprogramms**.
- Ist das System wieder sauber, sollten Sie die **Kennwörter** Ihrer im Internet geführten **Benutzerkonten** (Internetbanking, eBay, E-Mail-Konto etc.) **ändern**. Dies verhindert, dass Ihre Konten mit den ausspionierten Zugangsdaten missbraucht werden.

Auch hier gilt: Falls Sie sich technisch nicht besonders gut auskennen, sollten Sie den Trojaner von Fachleuten entfernen lassen.

ACHTUNG

Ein Befall durch Viren, Würmer, Trojaner oder Dialer deutet auf einen Sicherheitsmangel hin. Sie sollten daher dringend die Schwachstellen beseitigen(fehlender oder nicht aktueller Virenscanner, fehlende oder abgeschaltete Firewall, nicht aktuelles Windows etc.). Lesen Sie in den betreffenden Kapiteln des Titels **Sicherheit für Windows XP - leichter Einstieg für Senioren** (ISBN 3-8272-6821-4), wie Sie solche Schwachstellen erkennen bzw. beseitigen und sich gegen eine neuen Befall schützen können.

Absicherung des Systems

Um sich gegen die vielfältigen Gefahren zu schützen, sollten Sie ihr Computersystem in geeigneter Weise absichern. Dies ist mit wenig Aufwand und ohne größere Kosten möglich.

Verhaltensmaßregeln zur Erhöhung der Sicherheit

Mit ein paar Verhaltensregeln lässt sich die Gefahr fast auf Null reduzieren:

- Melden Sie sich zum **Arbeiten mit** Windows über **ein normales Benutzerkonto** mit eingeschränkten Rechten an (siehe Kapitel 2). Fangen Sie sich dann trotz der nachfolgenden Vorsichtsmaßnahmen einen Virus oder einen Trojaner ein, bleibt der Schaden auf den Ordner *Eigene Dateien* begrenzt (sofern das Schadprogramm nicht eine Sicherheitslücke ausnutzen kann, um die Benutzerprivilegien für Administratoren zu erhalten).

- **Installieren Sie** ein **Virenschutzprogramm** auf dem Computer **und halten Sie dieses auf dem aktuellen Stand** (siehe die folgenden Seiten). Das Programm schlägt Alarm, sobald ein Virus erkannt wird. Lassen Sie zudem sporadisch eine Virenprüfung durchführen und testen Sie neu auf den Computer übertragene Programme auf Virenbefall.

- **Beziehen Sie Programmdateien nur aus vertrauenswürdigen Quellen** (z.B. Webseiten renommierter Anbieter, CDs aus Büchern oder Zeitschriften) und lassen Sie diese vor dem Öffnen durch ein Virenschutzprogramm prüfen. Wer sich illegale Programme aus obskuren Quellen beschafft und ungeprüft ausprobiert, darf sich über einen eventuellen Virenbefall nicht wundern.

- **E-Mail-Anhänge** sollten Sie zunächst **speichern und** vor dem Öffnen **auf** einen möglichen **Virenbefall testen**. Ist ein Virenschutzprogramm installiert, wird dieses bereits beim Versuch eines Zugriffs auf die betreffende Datei Alarm schlagen.

- **E-Mails von unbekannten Personen** sollten Sie **ungelesen löschen** (es sei denn, Sie erwarten gelegentlich E-Mails von unbekannten Absendern). Das Löschen empfiehlt sich insbesondere, wenn Sie mit dem Betrefftext wenig anfangen können (z.B. englischer Text) oder Sie erhalten plötzlich zehn E-Mails von bekannten Absendern mit gleichlautendem Betreff (dann hat vermutlich ein Virus bei diesen Personen zugeschlagen).

- **Seien Sie auf der Hut**, wenn eine freundliche Mail von Microsoft oder anderen mit einem angeblichen Windows-Update, mit Sicherheitspatches oder einem Virenscanner im Anhang eintrifft. Firmen verschicken so etwas grundsätzlich nicht. Vielmehr muss man sich Updates von den betreffenden Firmenseiten herunterladen. Mit diesem Trick wurden aber bereits einige Viren verbreitet.

- Erhalten Sie eine E-Mail, in deren Text ein Link auf eine Webseite mit einem angeblichen Update enthalten ist? Dann sollten Sie sehr vorsichtig sein. Diese **Links können gefälscht sein**, statt des Updates wird ein Schädling auf Ihren Computer eingeschleust. Tippen Sie die Ihnen bekannten Adressen der Updateseiten von Microsoft oder anderer Programmhersteller immer manuell ein. Nur so lässt sich sicherstellen, dass Sie nicht auf gefälschte Links hereinfallen.

- Auch als E-Mail-Anhänge verschickte **Grußkarten** (*.exe*-Dateien) oder **Bildschirmschoner** (*.scr*-Dateien) **sind** häufig **Virenverstecke**. Selbst in E-Mail-

Anhängen von Bekannten könnte ein Virus enthalten sein (falls deren PC befallen ist oder ein Virus deren System zur Verbreitung benutzt hat). Bearbeiten Sie Ihre E-Mails nach Möglichkeit immer offline (also ohne aktive Internet-Verbindung), um die automatische Verbreitung von Viren zu verhindern (dann lässt sich der Postausgang vor der nächsten Online-Sitzung auf obskure Mails kontrollieren).

- Schalten Sie daher die **Anzeige der Dateinamenerweiterung** für bekannte Dateitypen unter Windows ein. Öffnen Sie hierzu ein Ordnerfenster (z.B. *Arbeitsplatz*) und wählen Sie im Menü *Extras* den Befehl *Ordneroptionen*. Auf der Registerkarte *Ansicht* löschen Sie die Markierung des Kontrollkästchens der Option *Erweiterungen bei bekannten Dateitypen ausblenden* (einfach die Option anklicken, damit das Häkchen verschwindet). Sobald Sie die Registerkarte über die *OK*-Schaltfläche schließen, werden die Erweiterungen sichtbar und Sie können auch bei heruntergeladenen Dateien oder E-Mail-Anhängen den Dateityp erkennen.

- **Verhindern Sie** die **ungewollte Ausführung von Makros** in Microsoft Office-Dokumenten. Starten Sie eine der Microsoft Office-Anwendungen und wählen Sie (z.B. in Word) im Menü *Extras* den Befehl *Makros/Sicherheit*. Im dann angezeigten Dialogfeld markieren Sie das Optionsfeld *Hoch* oder *Mittel* und schließen Sie das Dialogfeld über die *OK*-Schaltfläche.

- Bei StarOffice bzw. OpenOffice.org gilt es ebenfalls die **ungewollte Ausführung von Makros zu verhindern**. Wählen Sie (z.B. im Writer) im Menü *Extras* den Befehl *Optionen*. Im angezeigten Dialogfeld wählen Sie den Zweig *OpenOffice.org* bzw. *StarOffice* und klicken dann auf den Eintrag *Sicherheit*. Markieren Sie die Optionen *Nachfragen bei anderen Dokumentquellen* und *Vor Ausführung immer warnen*. Versucht der Benutzer ein Dokument, welches Makros enthält, zu laden, zeigt das Office-Programm eine Warnung an oder sperrt die Makroausführung (falls in Microsoft Office die Option *Hoch* oder in StarOffice der Wert des Listenfelds *Makro ausführen* auf »Niemals« gesetzt ist).

- **Verwenden Sie** auch die im Sicherheitsbuch erwähnten **Sicherheitseinstellungen für Internet Explorer** und **Outlook Express** (siehe z.B. Kapitel 4), um Skriptviren an der Ausführung zu hindern. Bei älteren Outlook- oder Outlook Express-Versionen reichte bereits die Vorschau einer E-Mail, um ein Virus zu aktivieren (ist dem Autor vor vielen Jahren passiert). Aber mit ein paar Einstellungen lässt sich dies verhindern.

- Bei Systemen, die durch Minderjährige genutzt werden, sollten Sie im Internet Explorer das Abrufen von Webseiten mit jugendgefährdenden Inhalten (Sex, Gewalt etc.) sperren. Die betreffende Funktion steht im Internet Explorer über den **Inhaltsratgeber** zur Verfügung. Details zur Konfigurierung des Inhalts-

ratgebers finden Sie beispielsweise im Easy-Titel »Computer - Alles rund um den PC« des Markt+Technik-Verlages.

Es gilt das Sprichwort »Vorsicht ist die Mutter der Porzellankiste «. Einige Viren konnten sich nur verbreiten, weil unvorsichtige Benutzer entsprechende E-Mail-Anhänge sofort per Doppelklick geöffnet haben und kein Virenschutzprogramm installiert war. Speichern Sie niemals wichtige Informationen (z.B. Kennwörter) auf dem Computer und fertigen Sie Sicherheitskopien von wichtigen Dateien an (für den Fall, dass doch mal ein Virus auf den Rechner gelangt und die infizierten Dateien gelöscht werden müssen).

Nutzen Sie ein Virenschutzprogramm

Ist es trotz aller Vorsicht doch passiert und Sie haben sich einen Virus, einen Trojaner, einen Wurm etc. eingefangen, gilt es das System schleunigst von diesem Schädling zu säubern. Hierzu benötigen Sie ein Virenschutzprogramm mit aktueller Virensignaturdatei. In der Virensignaturdatei speichert der Hersteller Informationen für den Virenscanner, damit das Virenschutzprogramm die Viren auch erkennen kann. Sobald neue Viren, Würmer oder Trojaner auftreten, ergänzen die Hersteller die Signaturdatei. Dies erklärt auch, warum es so immens wichtig ist, mit aktuellen Virenscannern bzw. Signaturdateien zu arbeiten.

TIPP

Ein recht leistungsfähiges und für private Nutzung kostenloses Virenschutzprogramm ist AntiVir. Sie können das Programm »AntiVir Personal Edition« kostenlos von der Webseite *www.antivir.de* herunterladen und dann durch einen Doppelklick auf die betreffende Datei installieren. Das Programm richtet sich dann automatisch unter Windows ein und überwacht alle eingehenden Dateien auf einen Virenbefall. Ist die Virensignatur veraltet, meldet Antivir dies und ermöglicht Ihnen eine Aktualisierung der Signaturdatei.

Ist ein aktuelles Virenschutzprogramm auf dem Computer vorhanden, lassen Sie dieses durchlaufen.

1 Öffnen Sie das Startmenü, suchen Sie den Eintrag für AntiVir und starten Sie das Programm über den betreffenden Eintrag.

2 Warten Sie, bis AntiVir den Arbeitsspeicher überprüft hat und markieren Sie dann die Kontrollkästchen der zu überprüfenden Laufwerke.

3 Klicken Sie anschließend auf die in der Symbolleiste des AntiVir-Fensters eingeblendete Schaltfläche *Suchen*.

AntiVir beginnt dann mit dem Scan der markierten Laufwerke. Enthalten diese Viren oder Trojaner, erkennt das Programm in aller Regel den Befall und meldet diesen. Dann gibt es mehrere Möglichkeiten:

- Es ist nur eine Datei durch das Schadprogramm befallen. Wurde die Datei gerade aus dem Internet oder von einem Datenträger übernommen, kann das Virenschutzprogramm diese Datei löschen und alles ist gut.
- Manche erkannten Schädlinge können durch das Virenschutzprogramm auch aus den befallenen Dateien entfernt werden. Dann lassen Sie das Virenschutzprogramm durchlaufen und erlauben diesem das Entfernen des Virencodes.
- Die befallene Datei darf nicht gelöscht werden und das Virus lässt sich auch nicht aus der Datei entfernen. Dann kann der Virenscanner die Datei in den so genannten Quarantänebereich verschieben. Dies eröffnet die Möglichkeit, der infizierten Datei ggf. mit weiteren Werkzeugen zu Leibe zu rücken.

Sie werden in entsprechenden Dialogfeldern über den Befall informiert und können über Optionsfelder wählen, was passieren soll.

4 Markieren Sie ggf. das Optionsfeld *Betroffene Datei löschen* und klicken Sie auf die *OK*-Schaltfläche.

Die betreffende Datei wird dann entfernt. Falls Systemdateien befallen sind, könnte aber die Funktionsfähigkeit von Windows oder von Anwendungsprogrammen beeinträchtigt werden. Sie müssen dann ggf. Windows oder die betroffenen Programme reparieren.

HINWEIS

Eine wesentlich detailliertere Einführung mit Schritt-für-Schritt-Anleitungen zum Umgang mit AntiVir (und Norton Antivirus) finden Sie in den betreffenden Kapiteln des Titels **Sicherheit für Windows XP - leichter Einstieg für Senioren** (ISBN 3-8272-6821-4).

So bleibt Windows aktuell

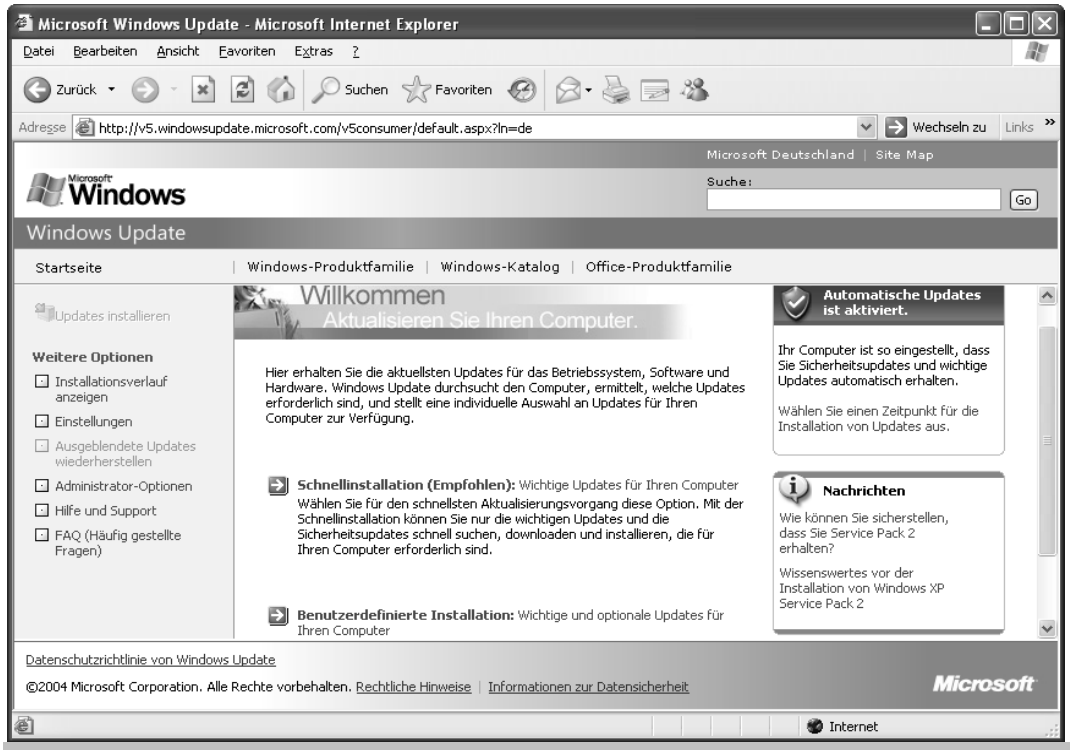
Wer mit Windows XP arbeitet, besitzt zwar ein modernes und komfortables Betriebssystem mit vielen Funktionen. Aber kein Programm ist wirklich fehlerfrei, was auch für Windows XP gilt. Gelegentlich werden Fehler und Sicherheitslücken aufgedeckt, die eine Gefahr für die Computersicherheit darstellen können. Dies gilt übrigens auch für ältere Windows-Versionen. Microsoft stellt kostenlos Programmverbesserungen zur Verfügung, die der Benutzer auf dem Computer einspielen kann. Leider ist es bisher so, dass viele Benutzer solche Verbesserungen an Windows ignorieren und nichts gegen die entdeckten Sicherheitslücken tun. Dies ist einer der Gründe, warum sich manche Viren explosionsartig vermehren können (denn die Urheber dieser Programme erfahren auch von diesen Lücken und nutzen sie gezielt aus).

Sie sollten daher von Zeit zu Zeit kontrollieren, ob sogenannte Updates für Windows bereitstehen. Die nachfolgenden Anweisungen funktionieren für alle Windows-Versionen ab Windows 98.

1 Gehen Sie online und starten Sie den Internet Explorer (z.B. über das Startmenü).

2 Öffnen Sie im Fenster des Internet Explorers das Menü *Extras* und wählen Sie den Befehl *Windows Update* an.

Im Internet Explorer erscheint dann eine Webseite, die ähnlich wie hier gezeigt aussieht.



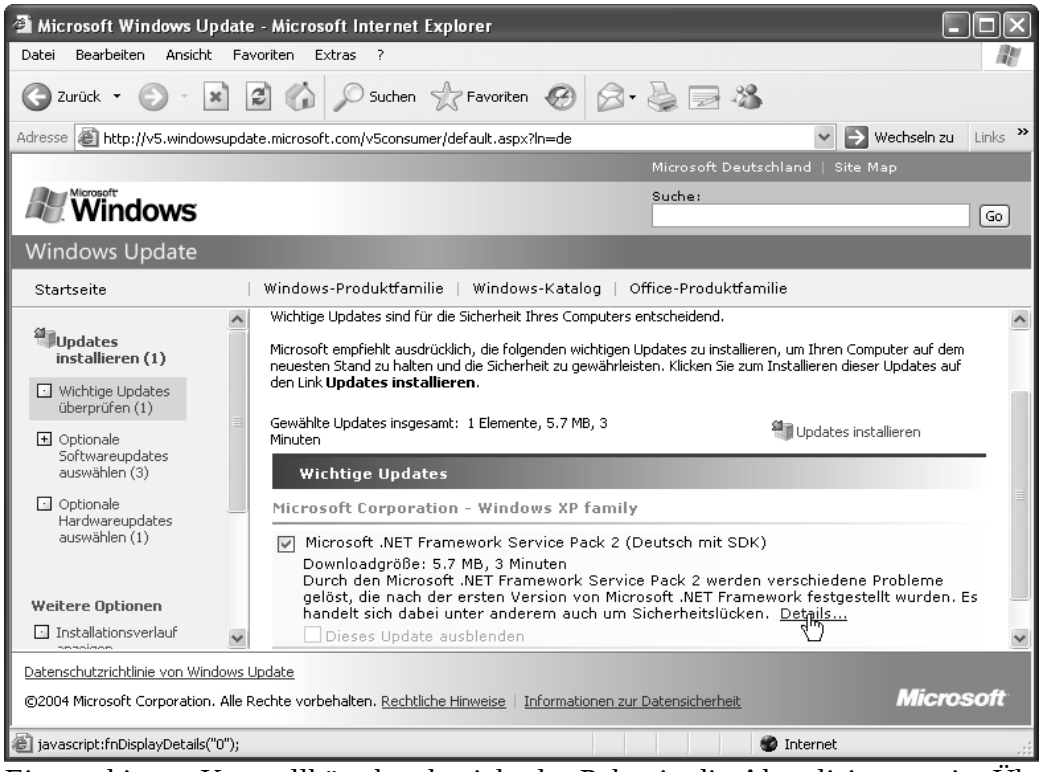
HINWEIS

Beim ersten Aufruf der Update-Seite wird einmalig ein kleines (ActiveX-)Zusatzmodul auf den Computer übertragen, dessen Installation Sie zulassen müssen. Dieses Zusatzmodul vergleicht bei jedem Aufruf der Update-Seite die auf dem lokalen Computer bereits installierten Aktualisierungen mit der Liste der verfügbaren Updates. Beachten Sie aber, dass sich der genaue Aufbau der Update-Seite im Internet mit der Zeit etwas ändern kann. Die grundsätzliche Vorgehensweise zum Abrufen der Aktualisierungen bleibt aber gleich. Denken Sie auch daran, dass Sie zum Installieren eventuell verfügbarer Updates an einem Administratorenkonto angemeldet sein müssen.

Über Hyperlinks können Sie die Funktionen der Webseite abrufen. Die linke Spalte enthält Befehle zum Abrufen verschiedener Informationen. Im rechten Teil können Sie über Hyperlinks nach Updates suchen lassen.

3 Klicken Sie im Fenster des Internet Explorers auf den Hyperlink *Schnellinstallation*, um nach wichtigen Updates und Sicherheitsupdates (Patches) suchen zu lassen. Oder wählen Sie den Hyperlink *Benutzerdefinierte Installation*, um neben Updates und Sicherheitspatches auch nach optionalen Aktualisierungen zu suchen.

Das Update-Modul analysiert dann die verfügbaren Updates und vergleicht diese mit den bereits installierten Paketen. Anschließend werden die noch zu installierenden Updates in der Seite angezeigt.



Ein markiertes Kontrollkästchen bezieht das Paket in die Aktualisierung ein. Über den Hyperlink *Details* im Erklärungstext können Sie ein Fenster mit zusätzlichen Informationen zum jeweiligen Paket anzeigen lassen.

4 Markieren Sie die Kontrollkästchen der zu installierenden Pakete und klicken Sie dann auf den Hyperlink *Updates installieren*.

Die Pakete werden heruntergeladen und automatisch installiert. Der Vorteil dieses Ansatzes besteht u.a. darin, dass Sie den Umfang der Updates bestimmen und über *Details* Zusatzinformationen abrufen können.

HINWEIS

Für Windows XP gibt es sogenannte Service Packs, die unbedingt auf dem Computer installiert werden sollten. Wenn Sie den *Windows Update*-Befehl im Menü *Extras* des Internet Explorer aufrufen und kein Service Pack 2 installiert ist, wird diese Aktualisierung als Express Update auf der Internetseite angeboten. Dieses

Update schlägt »nur« mit 80 bis 100 Megabyte (statt der 260 Megabyte der vollen Update-Version des Service Pack 2) zu Buche. Bei installiertem Service Pack 2 verfügt Windows XP über eine automatische Update-Funktion und stellt zusätzliche Sicherheitseinrichtungen (Sicherheitscenter, Firewall etc.) bereit. Details zu diesen Funktionen finden Sie in dem Titel **Sicherheit für Windows XP - leichter Einstieg für Senioren** (ISBN 3-8272-6821-4).

Sicherheitsrisiko Benutzerkonto

Wenn Sie mit Windows NT, Windows 2000 oder Windows XP arbeiten, stehen Ihnen verschiedene Typen von Benutzerkonten zur Verfügung. Nachfolgende Ausführungen beziehen sich auf Windows XP, sind aber in ähnlicher Form auch unter Windows NT/2000 vorhanden. Zum Arbeiten mit Windows XP muss mindestens ein so genanntes Benutzerkonto vorhanden sein. Windows benutzt dieses Konto, um die Benutzereinstellungen und Berechtigungen zu verwalten. So werden alle vom Benutzer oder von Programmen benutzerspezifisch vorgenommenen Einstellungen pro Benutzerkonto gespeichert. Die Verwendung mehrerer Benutzerkonten verhindert, dass sich verschiedene Benutzer, die einen Computer gemeinsam verwenden, gegenseitig in die Quere kommen. Es ist dann nicht möglich, Dateien, E-Mails oder Einstellungen fremder Benutzer gewollt oder ungewollt zu verändern oder zu löschen. Allerdings unterscheidet Windows XP Home Edition sogenannte Administratorenkonten und eingeschränkte Benutzerkonten.

- **Administratorenkonten** erlauben dem angemeldeten Benutzer Programme und Hardware zu installieren sowie Windows-Einstellungen zu verändern. Dies wird auch durch Viren und andere Schädlinge genutzt.

- **Eingeschänkte Benutzerkonten** erlauben dem Benutzer Programme aufzurufen, im Internet zu surfen und den Computer zu nutzen. Er kann aber keine Programme installieren oder entfernen und darf auch keine allgemeinen Windows-Einstellungen verändern.

Leider legt Windows XP bei der Installation nur Benutzerkonten mit Administratorenrechten an – Viren und anderen Schädlingen werden dann alle Möglichkeiten zur Verbreitung eingeräumt.

1 Melden Sie sich unter einem Administratorenkonto unter Windows XP an und rufen Sie im Startmenü den Befehl *Systemsteuerung* auf.

2 Im Fenster der Systemsteuerung müssen Sie nun das Symbol der *Benutzerverwaltung* aufrufen. Im Fenster der Benutzerverwaltung finden Sie Befehle, um neue Benutzer anzulegen, Kennwörter zu vereinbaren und den Typ der Benutzerkonten anzupassen.

3 Legen Sie für jeden Benutzer ein eingeschränktes Benutzerkonto an und stellen Sie sicher, dass ein Administratorkonto bestehen bleibt. Weisen Sie allen Benutzerkonten ein Anmeldekennwort zu.

Anschließend sollten alle Benutzer die eingeschränkten Konten zum Arbeiten nutzen. Die Benutzer können das Anmeldekennwort für das eigene Konto nach einer Anmeldung über die Benutzerverwaltung ändern. Wurde ein Kennwort vergessen, kann der Administrator dieses Kennwort für das Konto zurücksetzen. Das Administratorenkonto dient dann nur noch zum Installieren von Software oder zur Verwaltung des Systems. Normale Arbeiten führt der Administrator ebenfalls unter einem getrennten eingeschränkten Benutzerkonto aus. Dies verhindert i.d.R., dass sich eingeschleppte Schädlinge auf dem Computer installieren und verbreiten können.

HINWEIS

Leider gibt es schlampig programmierte Anwendungen, die nur unter Administratorenkonten funktionieren. Dann müssen Sie diese unter einem entsprechenden Konto laufen lassen. Wie so etwas funktioniert und weitere Details finden Sie in dem Titel **Sicherheit für Windows XP - leichter Einstieg für Senioren** (ISBN 3-8272-6821-4).

Sicherheits-Checkliste

Hier finden Sie noch eine kleine Checkliste, mit der Sie die Absicherung eines Computers überprüfen können.

Windows und Benutzerkonten

- ► Sind unterschiedliche Benutzerkonten eingerichtet und nutzen die Anwender normale (eingeschränkte) Benutzerkonten (siehe Kapitel 2)?
- ► Sind alle Benutzerkonten mit »guten« Kennwörtern abgesichert (siehe Kapitel 2)?
- ► Sind alle von Microsoft bereitgestellten sicherheitskritischen Updates für Windows XP, den Internet Explorer und Outlook Express installiert (siehe Kapitel 2)?

Schutz gegen Viren, Trojaner, Adware und Dialer

- ► Ist ein Virenschutzprogramm installiert und ist dessen Signaturdatei aktuell (siehe Kapitel 3)?
- ► Führen Sie zyklisch eine Überprüfung des Systems auf Viren durch und prüfen Sie Fremddateien, die Sie per Internet oder über Datenträger erhalten haben, auf Viren (siehe Kapitel 3)?
- ► Verfügen Sie über eine Notfall-CD oder ein Notfall-Set, mit dem sich der Computer ggf. starten und auf Viren überprüfen lässt (siehe Kapitel 3)?
- ► Ist ein aktuelles Adware-Programme installiert und führen Sie zyklisch eine Prüfung auf unerwünschte Spyware-Programme durch (siehe Kapitel 6)?
- ► Ist der Internetzugang abgesichert und existiert ggf. ein Schutz gegen unerwünschte Dialer (siehe Kapitel 6)?
- ► Ist die Windows XP-Firewall (oder eine andere Firewall) vorhanden und aktiviert (siehe Kapitel 6)?
- ► Sind Ihnen die Verhaltensmaßregeln bezüglich E-Mail-Anhängen bekannt und beachten Sie diese (siehe Kapitel 5)?

Internetsicherheit

- ► Sind die Sicherheitseinstellungen des Browsers so gesetzt, dass aktive Komponenten nicht unbemerkt oder ungewollt installiert werden können (siehe Kapitel 4)?
- ► Haben Sie die Sicherheitszonen des Internet Explorers korrekt eingestellt (siehe Kapitel 4)?

- ► Sind die Browsereinstellungen hinsichtlich Cookies, Speicherung von Kennwörtern, Blockieren von Popup-Fenstern etc. gemäß Ihren Anforderungen eingestellt (siehe Kapitel 4)?
- ► Löschen Sie Cookies und Ihre Surfspuren im Browser zyklisch (siehe Kapitel 4)?
- ► Haben Sie sich im Hinblick auf Geldgeschäfte im Internet über Risiken und Maßnahmen zur Erhöhung der Sicherheit informiert (siehe Kapitel 4)?
- ► Achten Sie bei Geldgeschäfte im Internet auf eine gesicherte Verbindung und prüfen Sie die Zertifikate (siehe Kapitel 4)?
- ► Sind die Sicherheitseinstellungen des E-Mail-Programms so gesetzt, dass schädliche Inhalte von Nachrichten automatisch blockiert werden (z.B. keine automatische Vorschau, HTML-Inhalte nicht nachladen, gefährliche Anhänge nicht öffnen, siehe Kapitel 5)?
- ► Haben Sie Filter für Werbe-E-Mails definiert bzw. können Sie unerwünschte Nachrichten blockieren (siehe Kapitel 5)?

Datensicherung

- ► Verfügen Sie über Sicherungskopien der wichtigsten Dokumentdateien und liegen die Installationsdateien benötigter Programme auf CD-ROMs vor?
- ► Haben Sie wichtige Einstellungen für Windows gesichert oder zumindest notiert (Kennwörter für E-Mail, Internetzugang etc. sollten auf Papier notiert sein und an einem sicheren Ort aufbewahrt werden).

Die Kapitelverweise beziehen sich (sofern nicht angegeben) auf den Titel **Sicherheit für Windows XP - leichter Einstieg für Senioren** (ISBN 3-8272-6821-4). An dieser Stelle möchte ich das Tutorial schließen. Sie haben einen groben Überblick über Sicherheitsmassnahmen erhalten und gelernt, wie Sie sich vor Viren und Schädlingen schützen können. Es gibt aber eine Menge weitere Punkte, die beim Arbeiten mit dem Computer zu beachten sind (z.B. Absicherung der Internetverbindung, Absicherung von E-Mails gegen Spam, Sicherheit bei Geldgeschäften im Internet, Schutz gegen Phishing etc.). Diese Themen werden im oben erwähnten Titel ausführlich besprochen.

Notizen

Anhang: Kindersicherung

Sicherheitsmaßnahme: Wenn Kinder im Internet surfen

Sofern der Computer von Minderjährigen zum Surfen im Internet benutzt wird, sollten die nachfolgenden Punkte beachten.

- **Unerwünschte Inhalte sperren:** Aktivieren Sie die Kindersicherung des Browsers. Beim Internet Explorer heißt diese Sicherung »Inhaltsratgeber« und lässt sich über den Befehl *Internetoptionen* im Menü *Extras* aufrufen (Details zu den Einstellungen finden sich z.B. im Easy-Titel »Computer - Alles rund um den PC« von Markt+Technik).

- **Regeln festlegen:** Sprechen Sie mit den Kindern ab, welche Angebote diese im Internet abrufen dürfen (z.B. Webseiten, Chats etc.). Legen Sie Regeln für den Umgang mit dem Internet fest (wann gesurft werden darf, welche Seiten die Kinder aufrufen dürfen, ob jemand dabei sein muss, ob Chats besucht werden dürfen und welche Chaträume zugelassen sind etc.). Bei Angeboten, die eine Registrierung erfordern, sollten die Kinder explizit Ihre Zustimmung einholen. Führen Sie die Registrierung gemeinsam mit dem Kind durch und lesen Sie sich das »Kleingedruckte« vorher durch.

- **Kontrolle:** Kontrollieren Sie, welche Seiten von den Kindern aufgerufen wurden (z.B. im Internet Explorer über die Liste der Favoriten – es gibt eine entsprechende Schaltfläche dafür, überprüfen Sie ggf. über den Befehl *Internetoptionen* im Menü *Extras* die hinterlegten Cookies etc.).

Auf diese Weise können Sie zumindest kontrollieren, welche Internetangebote die Kinder wahrnehmen und bei Zugriffen auf jugendgefährdende Inhalte eingreifen. Natürlich sollten Sie den Computer wie oben beschrieben konfigurieren (eingeschränkte Benutzerkonten, Webinhaltszonen etc.) und darauf achten, dass ein aktueller Virenschutz auf dem Computer vorhanden ist.

Notizen

Borns kleines PC-Lexikon

A

Account (Zugang)

Berechtigung, sich an einen Computer per Datenleitung anzumelden und z.B. im WWW zu surfen.

ActiveX

Technologie von Microsoft, mit der Zusatzfunktionen in Webseiten eingebracht werden. Dabei wird ein Programm auf den lokalen Computer installiert, welches die Funktionen bereitstellt. Wegen der damit verbundenen Missbrauchsmöglichkeiten stellen ActiveX-Module ein Problem dar.

Address Spoofing

Sieh *Spoofing*

Anonymisierer

Programme oder Webdienste, die das anonyme Surfen im Internet ermöglichen.

B

Backdoor

Englischer Name für Hintertür, eine Schwachstelle im Computer, über die sich Sicherheitsmechanismen umgehen lassen.

Backup

Bezeichnung für die Datensicherung (Dateien werden auf Diskette/Band gesichert).

Banner

In Webseiten eingeblendete Werbung (z.B. über Popup-Fenster).

Betriebssystem

Dies ist das Betriebsprogramm (z.B. Windows Me, Windows 2000), das sich nach dem Einschalten des Computers meldet.

Bit

Dies ist die kleinste Informationseinheit in einem Computer (kann die Werte 0 oder 1 annehmen). 8 Bit werden zu einem Byte zusammengefasst.

Booten

Starten des Computers.

Browser

Dies ist das Programm, mit dem der Computer die Seiten im World Wide Web anzeigt.

Bug

Englische Bezeichnung für einen Softwarefehler in einem Programm.

Byte

Ein Byte ist die Informationseinheit, die aus 8 Bit besteht. Mit einem Byte lassen sich Zahlen von 0 bis 255 darstellen.

C

Chat

Englischer Ausdruck für »schwatzen« oder »plaudern«. Bezeichnet einen Internetdienst, bei dem sich Teilnehmer in so genannten Chaträumen unterhalten können.

Client

Rechner oder Programm, die mit einem Server Kontakt aufnehmen und Daten austauschen.

Cracker
Leute, die Kopierschutzmassnahmen von Programmen illegal umgehen.

D

DFÜ
Abkürzung für Datenfernübertragung.

Dialogfeld
Fenster in Windows, in dem Eingaben abgefragt werden.

Download
Herunterladen von Daten per Modem z.B. aus dem Internet auf Ihren Rechner.

E

Editor
Programm zum Erstellen und Bearbeiten einfacher Textdateien.

Electronic Mail (E-Mail)
Nachrichten, die auf elektronischem Wege verschickt werden.

Error
Englische Bezeichnung für einen Programmfehler.

Ethernet
Technik zur Übertragung von Daten in Netzwerken.

Exploit
Veröffentlichte Sicherheitslücke in einem Programm.

F

FAT
Abkürzung für File Allocation Table. Besagt, wie Windows Dateien auf der Diskette oder Festplatte ablegt.

Floppy-Disk
Dies ist ein andere Name für eine Diskette.

Freeware
Software, die kostenlos benutzt und nur kostenlos weitergegeben werden darf.

FTP
FTP steht für File Transfer Protocol. Dies ist eine Funktion im Internet, mit der sich Dateien zwischen Computern übertragen lassen.

G

Gbyte
Abkürzung für Gigabyte (entspricht 1.024 Megabyte).

GIF
Grafikformat, das für Grafiken in Webseiten benutzt wird.

H

Hacker
Person, die unerlaubt in fremde Computer eindringt.

Hardware
Als Hardware werden alle Teile eines Computers bezeichnet, die sich anfassen lassen (das Gegenteil ist Software).

Homepage
Startseite einer Person/Firma im World Wide Web. Von der Startseite führen Hyperlinks zu weiteren Webseiten.

HTML
Steht für Hypertext Markup Language, dem Dokumentformat im World

Wide Web.

HTTP

Abkürzung für Hypertext Transfer Protocol, ein Standard zum Abrufen von Webseiten.

Hyperlink

Verweis in einem HTML-Dokument zu einer anderen Webseite.

I

IMAP

Standard (wie POP3) zur Verwaltung von E-Mail-Konten.

Internet

Weltweiter Verbund von Rechnern in einem Netzwerk.

J

Joystick

Ein Joystick ist eine Art Steuerknüppel zur Bedienung von Spielprogrammen.

JPEG

Grafikformat, das für Grafiken in Webseiten benutzt wird.

Junk-Mail

Unerwünschte E-Mail, die meist Müll enthält.

K

Kbyte

Abkürzung für Kilobyte (entspricht 1.024 Byte).

L

LAN

Abkürzung für Local Area Network; bezeichnet ein Netzwerk innerhalb einer Firma.

Linux

Unix-Betriebssystem, welches von einer internationalen Gemeinde weiterentwickelt wird und frei verfügbar ist. Konkurrenz bzw. Alternative zu Microsoft Windows.

M

Mailbox

Englischer Name für einen elektronischen Briefkasten.

Mbyte

Abkürzung für Megabyte (1 Million Byte).

Modem

Zusatzgerät, mit dem ein PC Daten über eine Telefonleitung übertragen kann. Wird z.B. zum Zugriff aufs Internet benötigt.

MP3

Standard zur Komprimierung und Speicherung von Musik in Dateien.

Multimedia

Techniken, bei denen auf dem Computer Texte, Bilder, Video und Sound integriert werden.

N

Netzwerk

Verbindung zwischen Rechnern, um untereinander Daten austauschen zu können.

Newsgroups

Diskussionsgruppen zu bestimmten Themen im Internet.

O

Onlinedienst

Dienste zum Zugang zum Internet wie T-Online, AOL oder CompuServe.

Outlook Express

Windows-Programm zum Erstellen, Versenden, Lesen und Empfangen von E-Mails.

P

Public Domain

Public Domain ist Software, die öffentlich zugänglich ist und mit Erlaubnis des Autors frei kopiert oder weitergeben werden darf (siehe auch Freeware).

Phishing

Kunstwort aus Password + Fishing, eine Technik, mit der versucht wird, Kennwörter auszuspähen. Phishing-E-Mails suggerieren beispielsweise, dass sich jemand zur Überprüfung an seinem Internet(Bank-)Konto anmelden soll. Der in der Mail angegebene Hyperlink führt aber zu einer gefälschten Webseite, auf der dann Benutzername und Kennwort zu den Betrübern weitergeleitet wird.

Q

QWERTY-Tastatur

Dieser Name bezeichnet die englische Tastatur (die ersten sechs Tasten der zweiten Reihe ergeben das Wort QWERTY).

R

Router

Gerät, welches verschiedene Netzwerke miteinander verbindet. Wird häufig benutzt, um mehrere Computer mit dem Internet zu verbinden.

S

Scanner

Ein Zusatzgerät, mit dem sich Bilder oder Schriftstücke in den Computer einlesen lassen. Bei Viren ein Programmteil zum Aufspüren des Virencodes.

Scriptviren

Virus, welches als Scriptprogramm realisiert wurde. Manchmal auch als Makrovirus in einem Makroprogramm realisiert (Makros dienen in Office-Programmen bzw. -Dokumenten zur Automatisierung von Aufgaben).

Spoofing

Technik, um gefälschte Webseiten unter einer anderen Webadresse einzuschmuggeln.

Server

Hauptrechner in einem Netzwerk.

Shareware

Software, die kostenlos weitergegeben und zum Prüfen ausprobiert werden darf. Bei einer weiteren Benutzung muss die Software beim Programmautor gegen eine meist geringe Gebühr registriert werden. Damit hat der Benutzer die Möglichkeit, die Software vorher ausgiebig zu testen. Der Autor kann auf aufwändige Vertriebswege verzichten und daher die Software meist preiswert anbieten.

Spyware
Spyware ist ein Name für Programme, die intern Spionagefunktionen enthalten.

T

Trial
Anderer Name für Probesoftware. Die Funktion läuft nach einem Testzeitraum aus, d.h. das Trial-Programm ist nicht mehr nutzbar.

Trojaner
Programme zum Ausspionieren eines Rechners. Gaukeln im Vordergrund dem Benutzer eine Funktion vor und übertragen im Hintergrund Kennwörter an eine Internetadresse.

U

Unix
Unix ist ein Betriebssystem, das insbesondere für Großrechner (Mainframes) eingesetzt wird.

URL
Abkürzung für Uniform Resource Locator (Adresse einer Web-Seite).

USB
Universal Serial Bus, Technik zum Anschließen von Geräten (Maus, Modem etc.) über eine serielle Leitung.

V

VGA
Grafikstandard (16 Farben und 640 x 480 Bildpunkte). Heute wird Super-VGA mit mehr Farben und Bildpunkten benutzt.

Viren
Programme, die sich selbst verbreiten und in andere Programme kopieren, wobei häufig Schäden an anderen Programmen, an Daten oder an der Hardware auftreten. Meist werden Viren durch ein bestimmtes Ereignis ausgelöst (z.B. an einem bestimmten Tag).

W

Webseite
Dokument im HTML-Format.

Webbug
Kleines Bild in HTML-E-Mails. Der Absender der E-Mail erkennt beim Öffnen, dass seine Mail gelesen wurde.

WWW
World Wide Web, Teil des Internet, über den sich Texte und Bilder mit einem Browser sehr leicht abrufen lassen.

X

XML
Abkürzung für Extended Markup Language, eine Spezifikation zur Speicherung von Daten in Webseiten.

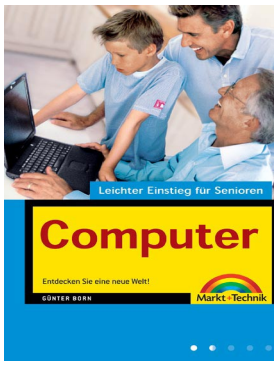
Z

Zertifikat
Dient im Web zur Echtheitsbestätigung eines Dokuments.

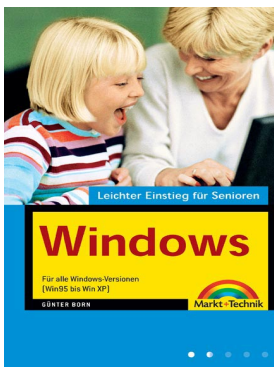
Literatur

Diese Titel wurden von mir speziell für die Zielgruppe der über 50jährigen entwickelt.

Günter Born: Sicherheit für Windows XP - leichter Einstieg für Senioren,
ISBN 3-8272-6821-4, Markt + Technik Verlag
Das Sicherheitsbuch für Einsteiger mit leichtverständlichen, bildreichen Workshops. Damit Ihr Windows-PC endlich sicher wird und Sie ohne Angst im Internet surfen oder E-mailen können. In sechs Kapiteln erfahren Sie, wie Sie den Computer richtig absichern und wie Sie sich vor den Gefahren des Internet (z.B. bei E-Mail, beim Internetbanking, beim Surfen etc.) schützen können.



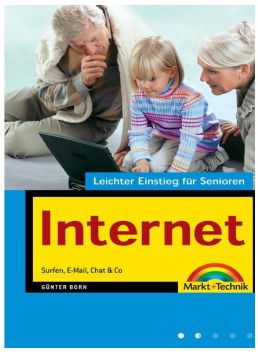
Günter Born: Computer – leichter Einstieg für Senioren,
ISBN 3-8272-6756-0, Markt + Technik Verlag
Das erste Mal am Computer? Oder noch vor der Kaufentscheidung? Dieses Buch ist genau richtig für Sie. In sechs Kapiteln erfahren Sie, was es zum Computer alles zu wissen gibt. Leicht verständliche Erläuterungen und bebilderte Arbeitsschritte zeigen wie es geht und was man mit dem Computer machen kann. Fachbegriffe werden getrennt erklärt. Entdecken Sie die Möglichkeiten, die der Computer bietet. Mit diesem Buch verlieren Sie nicht die Nerven und Erfolgserlebnisse stellen sich sofort ein.



Günter Born: Windows – leichter Einstieg für Senioren,
ISBN 3-8272-6758-7, Markt + Technik Verlag

Sie besitzen einen Computer und möchten wissen, was man alles damit machen kann? Dieses Buch bietet Ihnen einen angenehmen Einstieg und zeigt Ihnen, wie man mit dem Computer bzw. Microsoft Windows umgeht. Fachbegriffe werden getrennt erläutert und bebilderte Arbeitsschritte zeigen wie etwas geht. Schnell haben Sie den Umgang mit der Maus und mit Fenstern gelernt.

Wie wäre es mit einer Partie Solitär zur Entspannung? Oder möchten Sie Ihre Briefe und Einladungen nicht schon längst per Computer gestalten. Dies ist alles kein Problem. Entdecken auch Sie die vielfältigen Möglichkeiten, die der Computer bietet. Ein Anhang gibt kleine Hilfen bei Pannen und ein kleines PC-Lexikon erlaubt unbekannte Begriffe nachzuschlagen.



Günter Born: Internet – leichter Einstieg für Senioren,
ISBN 3-8272-6757-9, Markt + Technik Verlag

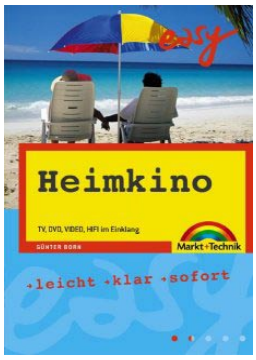
Dieses Buch wendet sich an Menschen ab der Lebensmitte, die das Internet für sich entdecken und nutzen möchten. Das Buch beginnt ganz von vorn und führt den Leser/die Leserin mit einer einfachen, verständlichen Sprache an die Thematik sowie an die entsprechenden Begriffe heran. Schritt-für-Schritt-Anleitungen, viele großformatige Abbildungen sowie eine bestens lesbare Schrift erlauben auch dem Neuling, schnell seine erste Webseite zu besuchen und seine erste E-Mail zu verschicken.

In fortgeschrittenen Kapiteln finden sich eine Auswahl an interessanten Themen wie Chatten, Sicherheit im Internet oder Tipps zum Versenden von FAX- oder SMS-Nachrichten. Ein Anhang vermittelt die nötigsten Windows-Grundlagen und gibt kleine Hilfen bei Pannen. Ein PC-Lexikon erlaubt Begriffe nachzuschlagen.

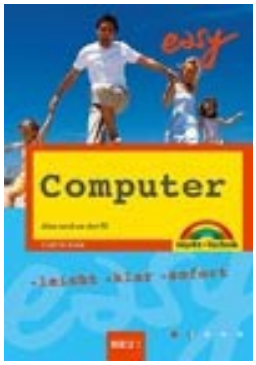
Günter Born: Office – leichter Einstieg für Senioren,
ISBN 3-8272-6251-8, Markt + Technik Verlag

Dieses Buch bietet Ihnen einen leichten Einstieg in die Welt der Büroprogramme Word, Excel und Works von Microsoft. Sie lernen den Umgang mit dem Schreibprogramm Word, gestalten Einladungen, persönliche Briefbogen, Serienbriefe und mehr. Mit Excel kriegen Sie Ihre Finanzverwaltung in den Griff. Weiterhin lernen Sie, wie diese Funktionen in Microsoft Works (das Programm ist auf vielen Computern vorhanden) genutzt werden.

Günter Born: Digitale Fotografie – leichter Einstieg für Senioren
ISBN 3-8272-6784-6, Markt + Technik Verlag
Möchten Sie sich eine Digitalkamera zulegen oder benötigen Sie einen Überblick wie die Bilder auf den Computer oder auf Papierabzüge kommen? Möchten Sie wissen, wie man scannt und Fotos am Computer bearbeitet? Sollen die Fotos als Diashow am Computer angezeigt werden. In diesem Buch finden Sie alle zu Digitalkameras, Aufnahmetechniken, Scannen und Bildbearbeitung.



Günter Born: Heimkino – Easy 50 Plus
ISBN 3-8272-6872-9, Markt + Technik Verlag
Stehen Sie hilflos vor den vielen Fachbegriffen, wenn es um DVD-Player, DVD-Recorder oder andere TV-Geräte geht? Möchten Sie wissen, was Geräte wie DVD-Recorder, Beamer oder LCD-Fernseher eigentlich können und worauf beim Kauf zu achten ist? Möchten Sie sich zu Hause eine eigene Heimkinoanlage leicht und schnell einrichten? Oder stehen Sie vor der Frage, wie sich eigene Videos auf CD bzw. DVD brennen lassen. In diesem Buch finden Sie Informationen zu diesen Themen.



Günter Born: Easy Computer – Alles rund um den PC
ISBN 3-8272-6785-4, Markt + Technik Verlag
Möchten Sie den Computer für sich entdecken? Dieses Buch ist für Jung und Alt gedacht und bietet das ganze Wissen rund um den PC: Grundlagen, Internet, E-Mail, Website, Homebanking, Sicherheit, Grundschritte in Word, Excel, PowerPoint etc., Spielen, digitale Fotografie, Scannen, Bildbearbeitung, Video, CDs/DVDs brennen, Systempflege, Handy und PC, Heim-Netzwerk uvm. Die ganze Familie wird darin fündig, egal von welcher Interessenslage man ausgeht.

Index